UNIDADES EM ANÉIS DE GRUPO
SOBRE OS INTEIROS

Nair Alexandre Fernandes

TESE APRESENTADA AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA OBTENÇÃO DO GRAU DE DOUTOR EM MATEMÁTICA

ORIENTADOR: PROF. DR. FRANCISCO CESAR POLCINO MILIES

SÃO PAULO, DEZEMBRO DE 1987.

Durante a execução deste trabalho, a autora recebeu apoio financeiro da CAPES.

ERRATA

ERRATA

PÁGINA	LINHA	ONDE SE LÊ	LEIA-SE	PÁGINA	LINHA	ONDE SE LÊ	LEIA-SE
iii	-2	$u = \gamma^{-1} g \gamma$	$u = \gamma \gamma^{-1} g \gamma$	57	2,3	γ é uma unidade e, portanto,	γ é uma unidade.
vi	6	$u = \gamma^{-1} g \gamma$	$u = \gamma \gamma^{-1} g \gamma$				Analogamente, se
x	1	subgrupo	grupo			$\rho: U_1(ZD_{2n}) \rightarrow T$ é um epimorfismo. Δ	$M \in T_2$, então $M = \rho(\theta)$, com $\theta = \theta(M) \in U_1(ZD_{2n})$.
14	-7	$k-l+5, k+l-3$	$k-l+5, \dots, k+l-3$				Portanto,
17	-1	$m_{2n+1} =$	$m_{2n+1,1} =$	61	5	$-1-s_1-s_4-t_1-t_4$	$\rho: U_1(ZD_{2n}) \rightarrow T$ é um epimorfismo. Δ
19	8	$m_{2k+1,2n-k+2} = 1 +$	$m_{k+1,2n-k+2} = -1 +$	68	-5	$y(a-1)$	$1-s_1-s_4-t_1-t_4$
21	-4	$+ m_{k-n-1, k+n+3} +$	$+ m_{k-n-1, k+n+4} +$	69	1	$U(I+I_k)$	$y(h-1)$
28	-5	$t_{oo} = t_{oo} \equiv 0 \pmod{2n+1}$	$t_{oo} = t_{oo}(M) \equiv 0 \pmod{2n+1}$	69	2	$I+I_k$	$U(1+I_k)$
29	-6	$u_{11} = \sum_{i=1}^n x_{2i} \equiv D$;	$u_{11} = \sum_{i=1}^n x_{2i} \equiv D \pmod{2n+1}$;	69	10	$M_3(Z)$	$1+I_k$
31	3	monorfismo	monomorfismo	70	11	$(a-1), ab-1,$	$M_3(Z)$
33	5	$U_2(Z(\frac{2n}{2})) = \frac{D_{2n}}{\langle b^2 \rangle}$	$U_1(Z(\frac{2n}{2})) = \frac{D_{2n}}{\langle b^2 \rangle}$	74	2	$\rho(U(1+\Delta(D_4)\Delta(\langle b^2 \rangle))) \subseteq P$	$(a-1), (ab-1),$
39	1	$\sum_{i=1}^n m_{2i,1} = \sum_{i=1}^n m_{2i-1,1}$	$\sum_{i=1}^n m_{2i,1} = \sum_{i=1}^n m_{2i-1,2}$	75	-5	$t_{oo} = 4 + t_{oo}(F)$	$\rho(U(1+\Delta(D_4)\Delta(\langle b^2 \rangle))) \subseteq P$
40	-6	$\sum_{i=0}^{n-1}$	$\sum_{i=1}^{n-1}$	78	-1	$x_5 3 \ 1 \ 0 \ -1 \ 1$	$t_{oo} = 4 + 4t_{oo}(F)$
40	-5	$\sum_{i=0}^{n-1}$	$\sum_{i=1}^{n-1}$	84	-8	$\rho_3(k) = \{I_2\}$	$x_5 3 \ 1 \ 0 \ -1 \ -1$
44	6	condição (iii)	condição (ii)				$\rho_3(K) = \{I_2\}$
46	-3	condição (iii)	condição (ii)				
49	4	$k-l+5, k+l-3$	$k-l+5, \dots, k+l-3$				
50	10	$+ t_{o, 2n-2k-2n}$	$+ t_{o, 2n-2k-2}$				
53	1	$T_2(\text{resp.}, T_2)$	$T_1(\text{resp.}, T_2)$				

À minha mãe

ABSTRACT

Let G be a finite group, $\mathbb{Z}G$ the integral group ring of G , and $U(\mathbb{Z}G)$ the group of units in $\mathbb{Z}G$. In this work we investigate $U(\mathbb{Z}G)$ for special groups.

Chapters I and II are concerned with the problem of determining $U(\mathbb{Z}G)$. We give a characterization of $U(\mathbb{Z}G)$, for $G = \langle a \rangle * \langle b \rangle$, an arbitrary split metacyclic group, and for $G = D_m$, the dihedral group of order $2m$, $m \geq 3$. In the first case we describe the image of $U(\mathbb{Z}G)$ by the regular representation of G , and in the second, working also with a permutation representation of G , we characterize $U(\mathbb{Z}G)$ as a group in $GL_m(\mathbb{Z})$.

In Chapter III we specialize the characterization of $U(\mathbb{Z}D_m)$, for $m=3$ and $m=4$, and calculate in both cases the image of certain torsion free normal complements of D_m in $U(\mathbb{Z}D_m)$.

Finally, the last chapter is devoted to solve a conjecture of Zassenhaus on torsion units of $\mathbb{Z}G$, for the particular case where $G = S_4$, the symmetric group on four letters. This conjecture says that for any torsion unit u in $U(\mathbb{Z}G)$ there exists a group element g in G and a unit γ in the rational group algebra $\mathbb{Q}G$ such that $u = \gamma^{-1}g\gamma$. We observe that S_4 is the only non metabelian group for which the conjecture is proved so far.

P R E F Á C I O

Sejam G um grupo finito, $\mathbb{Z}G$ o anel de grupo de G sobre o anel $\mathbb{Z}$ dos inteiros, e $U(\mathbb{Z}G)$ o grupo das unidades em $\mathbb{Z}G$.

Resolver um problema em $U(\mathbb{Z}G)$ pode ser bastante difícil, desde que já existe a dificuldade em se determinar o próprio grupo, isto é, em se decidir quais os elementos em $\mathbb{Z}G$ que são, de fato, unidades.

O que se tem feito é considerar uma representação de G num grupo de matrizes; em seguida, estendê-la linearmente a $\mathbb{Z}G$ e, finalmente, olhar o problema na imagem de $U(\mathbb{Z}G)$.

Quando a extensão, restrita ao grupo das unidades, for um isomorfismo, o problema da determinação de $U(\mathbb{Z}G)$ é resolvido pela sua caracterização por um grupo de matrizes.

Desse modo, alguns autores caracterizaram $U(\mathbb{Z}G)$, para grupos particulares, como um grupo de matrizes sobre os inteiros. Citamos I. Hughes e K.R. Pearson [5], C. Polcino Milies [11], e P.J. Allen e C.Hobby [1], que caracterizaram $U(\mathbb{Z}S_3)$, $U(\mathbb{Z}D_4)$, e $U(\mathbb{Z}A_4)$, respectivamente. Ainda, P.J. Allen e C. Hobby, recentemente, deram em [3] uma outra caracterização de $U(\mathbb{Z}S_3)$ e em [2] uma caracterização de $U(\mathbb{Z}G)$, para um determinado grupo metacíclico.

No Capítulo I, trabalhando com a representação regular, caracterizamos $U(\mathbb{Z}G)$, para um grupo que é o produto semidireto de subgrupos cíclicos, e no Capítulo II, também trabalhando com uma determinada representação de permutação, caracterizamos $U(\mathbb{Z}D_m)$, onde D_m é o grupo diedral de ordem $2m$, $m \geq 2$; assim, em ambos os ca-

sos, a caracterização obtida é dada como um grupo de matrizes sobre os inteiros.

Outras formas de caracterizações do grupo das unidades podem ser encontradas nos trabalhos de D.S. Passman e P.F. Smith [10], E. Kleinert [7], e S.A. Park [9] que caracterizam $U(\mathbb{Z}D_m)$, para m um primo ímpar, m ímpar livre de quadrados, e $m \geq 3$, respectivamente, e ainda no trabalho de J. Ritter e S.K. Sehgal [14] que caracteriza $U(\mathbb{Z}G)$, para um grupo não abeliano de ordem p^3 , p um primo ímpar.

O problema da determinação de um complemento normal livre de torção para G em $U(\mathbb{Z}G)$ foi considerado em alguns trabalhos, entre os quais [1], [3], e [10] já citados. Os resultados mais gerais referem-se a grupos metabelianos e foram obtidos por G.H. Cliff, S.K. Sehgal e A.R. Weiss em [4], onde, em particular, determinaram uma família de complementos normais livres de torção, para o caso em que G contém um subgrupo normal abeliano H tal que $\frac{G}{H}$ é abeliano cujo expoente é um divisor de 4 ou 6.

Essa família é formada por conjuntos construídos a partir de certos ideais denotados em [4] por I_k , $k \in \mathbb{Z}$; entretanto, a descrição destes conjuntos implica em se decidir quando um elemento em $1+I_k$ é uma unidade, e pode ser mais fácil responder esta questão quando se tem uma caracterização do grupo das unidades como um grupo de matrizes. Então, no Capítulo III, especializamos a caracterização obtida de $U(\mathbb{Z}D_m)$, para $m=3$ e $m=4$, e calculamos, nestes casos, a imagem de um dos complementos determinados em [4]; em particular, para $m=3$, os resultados são os mesmos que P.J. Allen e C. Hobby obtiveram em [3].

Outro problema relacionado ao grupo das unidades trata-se de uma conjectura de H.J. Zassenhaus que afirma ser toda unidade de torção racionalmente conjugada a uma unidade trivial; mais precisamente, se u é uma unidade de torção em $\mathbb{Z}G$, então existem um elemento g em G e uma unidade γ na álgebra de grupo $\mathbb{Q}G$ sobre o corpo $\mathbb{Q}$ dos racionais, satisfazendo $u = \gamma^{-1}g\gamma$. Esta conjectura foi confirmada para grupos nilpotentes de classe 2 por J. Ritter e S.K. Sehgal em [15], grupos metacíclicos $\langle a \rangle \rtimes \langle x \rangle$, com $(o(a), o(x))=1$, por C. Polcino Milies, J. Ritter e S.K. Sehgal em [13], e outros grupos metabelianos por Z. Marciniak, J. Ritter, S.K. Sehgal e A.R. Weiss em [8], e S.K. Sehgal e A.R. Weiss em [17]. A maioria destes trabalhos comprova a eficácia do uso das representações irreduzíveis do grupo em questão.

No contexto dos grupos simétricos, a conjectura para S_3 segue de [13]. Então, no Capítulo IV, consideramos S_4 e, através de uma técnica que usa fortemente a tábua de caracteres deste grupo, provamos que a conjectura também é verdadeira neste caso. Observamos que S_4 é o único grupo não metabeliano para o qual a conjectura está confirmada até agora.

É com alegria e profundo reconhecimento pela colaboração obtida que expressamos os seguintes agradecimentos:

aos Professores Elza Furtado Gomide, Edson Farah, Alfredo R. Jones e Hector A. Merklen, cujos ensinamentos constituem parte importante de nossa formação matemática;

à Professora Sonia P. Coelho, por ter acompanhado com interesse e sugestões valiosas a fase inicial de nossas pesquisas;

ao Professor Sudarshan K. Sehgal, por ter sugerido e orientado este trabalho no período em que a seu convite estagiamos na Universidade de Alberta, Canadá;

ao Professor Francisco Cesar Polcino Milies, por ter orientado nossos estudos desde quando escolhemos a Álgebra como área de especialização, em particular, por ter orientado e incentivado nossas pesquisas sobre as unidades em anéis de grupo e, ainda, por sugestões que contribuíram para que vários pontos deste trabalho fossem apresentados de uma forma mais clara;

à equipe da Biblioteca, que sempre auxiliou nossas pesquisas;

à Senhorita Elen Del Sole, pelo paciente trabalho de datilografia;

e, finalmente, ao pessoal do Xerox e da Gráfica, pelo cuidado com a impressão e encadernação.

São Paulo, dezembro de 1987.

Nair Alexandre Fernandes

ÍNDICE

CONCEITOS BÁSICOS	ix
I. UNIDADES EM ANÉIS DE GRUPO DE GRUPOS METACÍCLICOS SOBRE OS INTEIROS	1
1. A representação regular de $\langle a \rangle \ltimes \langle b \rangle$	1
2. As unidades em $\mathbb{Z}(\langle a \rangle \ltimes \langle b \rangle)$	2
II. UMA CARACTERIZAÇÃO DAS UNIDADES EM $\mathbb{ZD}_m$	8
3. As unidades em $\mathbb{ZD}_{2n+1}$	12
4. As unidades em $\mathbb{ZD}_{2n}$	31
III. AS UNIDADES EM $\mathbb{ZD}_3$ E $\mathbb{ZD}_4$	58
5. Caracterizações de $U_1(\mathbb{ZD}_3)$ e $U_1(\mathbb{ZD}_4)$	58
6. Caracterizações de complementos para D_3 em $U_1(\mathbb{ZD}_3)$ e D_4 em $U_1(\mathbb{ZD}_4)$	68
IV. UNIDADES DE TORÇÃO EM $\mathbb{ZS}_4$	78
7. Alguns resultados sobre S_4	78
8. A conjectura de Zassenhaus para S_4	80
REFERÊNCIAS BIBLIOGRÁFICAS	89

CONCEITOS BÁSICOS

Este trabalho trata essencialmente de unidades em anéis de grupo no caso particular em que o grupo é finito e o anel dos coeficientes é o anel dos inteiros; assim, vamos introduzir certos conceitos básicos da Teoria de Anéis de Grupo apenas neste caso específico.

Sejam G um grupo finito, H um subgrupo normal de G e $f: \mathbb{Z}G \rightarrow \mathbb{Z}(\frac{G}{H})$ o homomorfismo natural, isto é, para cada $g \in G$, se gH é a classe lateral de H em G determinada por g , então $f(g) = gH$.

O núcleo de f , que denotaremos por $\Delta(G, H)$, é um $\mathbb{Z}$ -módulo livre; de fato, por [12, Proposições (7.1) e (7.4)], se Y é um conjunto completo de representantes das classes laterais de H em G , então o conjunto $\{y(h-1): y \in Y, h \in H, h \neq 1\}$ é uma base de $\Delta(G, H)$ sobre $\mathbb{Z}$.

Em particular, se $H=G$, então $\frac{G}{H} = \{1\}$ e $gH=1$, para todo $g \in G$. Neste caso, f denomina-se a *função de aumento* de $\mathbb{Z}G$ e diremos que um elemento $\alpha \in \mathbb{Z}G$ tem aumento 1 se $f(\alpha)=1$.

O núcleo da função de aumento é denominado o *ideal de aumento* de $\mathbb{Z}G$ e o denotaremos por $\Delta(G)$. Então, o conjunto $\{g-1: g \in G, g \neq 1\}$ é uma base de $\Delta(G)$ sobre $\mathbb{Z}$ e um elemento $\alpha \in \mathbb{Z}G$ tem aumento 1 se, e somente se, $\alpha \in 1 + \Delta(G)$.

Denotaremos o conjunto $U(\mathbb{Z}G) \cap (1 + \Delta(G))$ das unidades de aumento 1 em $\mathbb{Z}G$ por $U_1(\mathbb{Z}G)$. Então, $U_1(\mathbb{Z}G)$ é um grupo multiplicativo e $U(\mathbb{Z}G) = \{\pm 1\} \times U_1(\mathbb{Z}G)$.

Assim, nossa caracterização de $U(\mathbb{Z}G)$, para $G = \langle a \rangle * \langle b \rangle$ no Capítulo I e $G = D_m$ no Capítulo II, será dada através de uma carac-

terização de $U_1(\mathbb{Z}G)$ como um subgrupo de matrizes sobre os inteiros tais que a soma de suas entradas em toda linha ou coluna é igual a 1; a estas matrizes chamaremos *duplamente estocásticas*.

Os complementos normais livres de torção de D_m em $U_1(\mathbb{Z}D_m)$, que vamos considerar no Capítulo III, para $m=3$ e $m=4$, serão da forma $U(\mathbb{Z}D_m) \cap (1 + \Delta(D_m)\Delta(H_m))$, onde H_m é um subgrupo de D_m .

Finalmente, com as definições que introduzimos, a conjectura de H.J. Zassenhaus, a qual irá se referir o Capítulo IV, pode ser enunciada na seguinte forma: se u é uma unidade de torção em $U_1(\mathbb{Z}G)$, então existem um elemento $g \in G$ e uma unidade $\gamma \in \mathbb{Q}G$ tais que $u = \gamma^{-1}g\gamma$. É nesta forma que provaremos a conjectura para $G=S_4$.

CAPÍTULO I

UNIDADES EM ANÉIS DE GRUPO DE GRUPOS METACÍCLICOS SOBRE OS INTEIROS

Em [2, Lema 2], P.J. Allen e C. Hobby deram uma caracterização das unidades em anéis de grupo de grupos cíclicos sobre os inteiros.

Neste capítulo, obtemos uma extensão desse resultado para um grupo $G = \langle a \rangle * \langle b \rangle$, o produto semidireto dos subgrupos cíclicos $\langle a \rangle$ e $\langle b \rangle$, isto é,

$$G = \langle a, b : a^r = 1 = b^s, a^{-1} b a = b^t \rangle$$

com r, s e t inteiros positivos; assim, r e s são as ordens de a e b , respectivamente, e $n = rs$ é a ordem de G .

Essencialmente, o que fazemos é descrever a imagem de $U_1(\mathbb{Z}G)$ pela representação regular de G ; entretanto, introduzimos técnicas que serão úteis no Capítulo II.

1. A REPRESENTAÇÃO REGULAR DE $\langle a \rangle * \langle b \rangle$.

Definiremos a representação regular de $G = \langle a \rangle * \langle b \rangle$ como um homomorfismo de G no grupo $\text{Aut}(\mathbb{Q}G)$ das transformações lineares do espaço vetorial $\mathbb{Q}G$ sobre o corpo $\mathbb{Q}$ dos racionais.

Consideremos $G = \{g_1, g_2, \dots, g_n\}$. Seja S_n o grupo das permutações de n elementos e seja $\pi: G \rightarrow S_n$ o homomorfismo definido

da seguinte forma: dado $g \in G$, temos que, para cada j , $1 \leq j \leq n$, existe um único i , $1 \leq i \leq n$, que satisfaz $gg_j = g_i$ e, então, definimos

$$\pi(g)j = i.$$

Com isto, a representação regular de G é o homomorfismo $\xi: G \rightarrow \text{Aut}(\mathbb{Q}G)$ tal que, para todo $g \in G$ e todo j , $1 \leq j \leq n$,

$$\xi(g)g_j = g_{\pi(g)j} = g g_j$$

ou, equivalentemente, como o homomorfismo $\rho: G \rightarrow GL_n(\mathbb{Q})$ tal que, para todo $g \in G$, $\rho(g)$ é a matriz de $\xi(g)$ em relação à base G .

Denotaremos ainda por ρ a extensão linear de ρ a $\mathbb{Z}G$.

2. AS UNIDADES EM $\mathbb{Z}(\langle a \rangle \rtimes \langle b \rangle)$.

Sejam $A = \rho(a)$ e $B = \rho(b)$. Pela definição da representação regular, é imediato o seguinte

LEMA (2.1). (i) Para quaisquer i e j , $0 \leq i \leq r-1$, $0 \leq j \leq s-1$, as entradas em cada linha ou coluna da matriz $A^i B^j$ são iguais a 0, exceto em uma única posição cuja entrada é igual a 1.

(ii) Se $A^i B^j$, $0 \leq i \leq r-1$, $0 \leq j \leq s-1$, tem 1 na posição (p, q) , então, para quaisquer k e ℓ , $0 \leq k \leq r-1$, $0 \leq \ell \leq s-1$, com $k \neq i$ ou $\ell \neq j$, $A^k B^\ell$ tem 0 na posição (p, q) .

O próximo resultado sugere a descrição que daremos de $\rho(U_1(\mathbb{Z}G))$.

LEMA (2.2). Seja $\alpha = \sum_{i,j} \alpha_{i,j} a^i b^j \in \mathbb{Z}G$.

(i) Para quaisquer k e ℓ , $0 \leq k \leq r-1$, $0 \leq \ell \leq s-1$, todas as entradas na diagonal principal de $A^k \rho(\alpha) B^\ell$ são iguais entre si.

(ii) Se α tem aumento 1, então $\rho(\alpha)$ é duplamente estocástica.

Demonstração. (i) Seja $N = A^{-k} \rho(\alpha) B^{-\ell}$, $0 \leq k \leq r-1$, $0 \leq \ell \leq s-1$. Então,

$$N = A^{-k} (\sum \alpha_{ij} A^i B^j) B^{-\ell} = \sum \alpha_{ij} A^{i-k} B^{j-\ell}.$$

Como $A^0 B^0$ é a matriz identidade e, portanto, tem entradas iguais a 1 na diagonal principal, segue do Lema (2.1), parte (ii), que as outras parcelas da soma tem entradas iguais a 0 nestas posições; logo, as entradas na diagonal principal de N são iguais a $\alpha_{k\ell}$.

(ii) Seja $M = \rho(\alpha)$. Então, $M = \sum \alpha_{ij} A^i B^j$; logo, pelo Lema (2.1), a soma das entradas em cada linha ou coluna de M é igual a $\sum \alpha_{ij}$. Agora, desde que α tem aumento 1, segue $\sum \alpha_{ij} = 1$. Δ

Seja R o conjunto das matrizes $M \in GL_n(\mathbb{Z})$ tais que

(i) M é duplamente estocástica;

(ii) para quaisquer k e ℓ , $0 \leq k \leq r-1$, $0 \leq \ell \leq s-1$, todas as entradas na diagonal principal de $A^k M B^\ell$ são iguais entre si.

Já vimos que $\rho(U_1(\mathbb{Z}G)) \subseteq R$; mais ainda, nossa caracterização de $U_1(\mathbb{Z}G)$ consistirá em mostrar que $U_1(\mathbb{Z}G) \cong R$, onde o isomorfismo é dado pela restrição de ρ .

Para isso, precisaremos de alguns resultados e definições que introduzimos a seguir.

Dada uma matriz $X = (x_{ij}) \in M_n(\mathbb{Z})$, indicaremos por $d(X)$ a entrada de M na posição (1,1), isto é, $d(X) = x_{11}$.

DEFINIÇÃO. Seja $M \in R$. Então, definimos os números

$$\delta_{ij} = \delta_{ij}(M) = d(A^{-i}MB^{-j}), \quad \forall i, j, 0 \leq i \leq r-1, 0 \leq j \leq s-1,$$

e o elemento em $\mathbb{Z}G$.

$$\delta(M) = \sum \delta_{ij} a^i b^j.$$

O próximo passo será mostrar que $\delta = \delta(M)$ é um elemento de aumento 1 tal que $\rho(\delta) = M$; mas antes precisamos do seguinte

LEMA (2.3). Sejam $X, Y \in M_n(\mathbb{Z})$. Se X e Y satisfazem a condição (ii) do conjunto R e $d(A^i X B^j) = d(A^i Y B^j)$, para quaisquer $i \in j, 0 \leq i \leq r-1, 0 \leq j \leq s-1$, então $X=Y$.

Demonstração. Se $X = (x_{ij})$ e $Y = (y_{ij})$, provaremos que, para quaisquer p e $q, 1 \leq p, q \leq n$, existem k e $\ell, 0 \leq k \leq r-1, 0 \leq \ell \leq s-1$, tais que $x_{pq} = d(A^{-k} X B^{-\ell})$. Com isto, teremos

$$x_{pq} = d(A^{-k} X B^{-\ell}) = d(A^{-k} Y B^{-\ell}) = y_{pq}, \quad \forall p, q, 1 \leq p, q \leq n,$$

o que implica $X=Y$.

É fácil ver que

$$A^{-k} X B^{-\ell} = (x_{\pi(a^k)_i, \pi(b^{-\ell})_j}), \quad \forall k, \ell, 0 \leq k \leq r-1, 0 \leq \ell \leq s-1.$$

Fixando p e $q, 1 \leq p, q \leq n$, desde que a ordem do conjunto

$$\{\pi(a^k)_i \pi(b^\ell)_q : 0 \leq k \leq r-1, 0 \leq \ell \leq s-1\}$$

é $rs = n$, existem k e $\ell, 0 \leq k \leq r-1, 0 \leq \ell \leq s-1$, tais que $\pi(a^k)_i \pi(b^\ell)_q = p$; logo, $\pi(a^{-k})_p = \pi(b^\ell)_q = i$, com $1 \leq i \leq n$, o que implica $p = \pi(a^k)_i$,

$$q = \pi(b^{-k})_i \text{ e, portanto, } d(A^{-k} X B^{-k}) = x_{\pi(a^k)_i, \pi(b^{-k})_i} = x_{pq}. \Delta$$

LEMA (2.4). Sejam $M \in R$ e $\delta = \delta(M)$. Então,

- (i) $\rho(\delta) = M$;
- (ii) δ tem aumento 1.

Demonstração. (i) Seja $N = \rho(\delta)$. Como $\delta = \sum \delta_{ij} a^i b^j \in \mathbb{Z}G$, segue do Lema (2.2), parte (i), que N satisfaz a condição (ii) do conjunto R . Além disto, temos que

$$d(A^{-i} N B^{-j}) = \delta_{ij}(M) = d(A^{-i} M B^{-j}), \forall i, j, 0 \leq i \leq r-1, 0 \leq j \leq s-1$$

logo, pelo Lema (2.3), $N=M$.

(ii) Por (i), $M = \rho(\delta) = \sum \delta_{ij} A^i B^j$. Então, pelo Lema (2.1), $\sum \delta_{ij}$ é a soma das entradas em cada linha ou coluna de M ; logo, como M é duplamente estocástica, temos $\sum \delta_{ij} = 1$, donde δ tem aumento 1. Δ

Os Lemas (2.5) e (2.6), que seguem, conduzirão à prova de que $\delta = \delta(M)$ é ainda uma unidade em $\mathbb{Z}G$.

LEMA (2.5). Seja $X \in GL_n(\mathbb{Z})$. Se X é duplamente estocástica, então X^{-1} também é duplamente estocástica.

Demonstração. Se $X = (x_{ij})$ é duplamente estocástica, então

$$(1) \quad \sum_{j=1}^n x_{kj} = 1 = \sum_{i=1}^n x_{i\ell}, \forall k, \ell, 1 \leq k, \ell \leq n.$$

Seja D o determinante de X e, para quaisquer i e j , $1 \leq i, j \leq n$, seja D_{ij} o cofator de x_{ij} . Então, $X^{-1} = (y_{ij})$, onde

$$y_{ij} = \frac{D_{ji}}{D}, \quad \forall i, j, 1 \leq i, j \leq n.$$

Com isto e de (1), temos que, para todo $k, 1 \leq k \leq n$,

$$\begin{aligned} \sum_{j=1}^n y_{kj} &= \frac{1}{D} \sum_{j=1}^n D_{jk} = \frac{1}{D} \sum_{j=1}^n \sum_{i=1}^n x_{ji} D_{jk} = \\ &= \frac{1}{D} \sum_{j=1}^n x_{jk} D_{jk} = 1 \end{aligned}$$

e, para todo $\ell, 1 \leq \ell \leq n$,

$$\begin{aligned} \sum_{i=1}^n y_{i\ell} &= \frac{1}{D} \sum_{i=1}^n D_{\ell i} = \frac{1}{D} \sum_{i=1}^n \sum_{j=1}^n x_{ji} D_{\ell i} = \\ &= \frac{1}{D} \sum_{i=1}^n x_{\ell i} D_{\ell i} = 1; \end{aligned}$$

logo, X^{-1} é duplamente estocástica. Δ

LEMA (2.6). Se $M \in R$, então $M^{-1} \in R$.

Demonstração. Pelo Lema (2.5), M^{-1} é duplamente estocástica e, conseqüentemente, satisfaz a condição (i) do conjunto R .

Seja $\chi \in \mathbb{Z}[X]$ o polinômio característico de M . Então, como $M \in GL_n(\mathbb{Z})$, podemos escrever $\chi = X^n + \sum_{i=0}^{n-1} x_i X^i$, com $x_i \in \mathbb{Z}$, $0 \leq i \leq n-1$, e $x_0 = (-1)^n D$, onde $D = \pm 1$ é o determinante de M ; logo,

$$(-1)^{n+1} D = M^n + \sum_{i=1}^{n-1} x_i M^i = M(M^{n-1} + \sum_{i=1}^{n-1} x_i M^{i-1}),$$

donde

$$M^{-1} = (-1)^{n+1} D (M^{n-1} + \sum_{i=1}^{n-1} x_i M^{i-1}).$$

Agora, pelo Lema (2.4), parte (i), para cada $i, 1 \leq i \leq n-1$, $M^i = \rho(\delta^i)$, com $\delta = \delta(M) \in \mathbb{Z}G$; logo, pelo Lema (2.2), parte (i), M^i

satisfaz a condição (ii) do conjunto R.

Portanto, M^{-1} também satisfaz a condição (ii) do conjunto R. Δ

O resultado principal desta seção é, agora, dado pelo

TEOREMA (2.7). A restrição $\rho: U_1(\mathbb{Z}G) \rightarrow R$ é um isomorfismo.

Demonstração. Seja I a matriz identidade $n \times n$ e seja $\alpha = \sum \alpha_{ij} a^i b^j \in \mathbb{Z}G$ tal que $\rho(\alpha) = \sum \alpha_{ij} A^i B^j = I$. Então, do Lema (2.1), é imediato que $\alpha = 1$ e, portanto, $\rho: U_1(\mathbb{Z}G) \rightarrow R$ é um monomorfismo.

Seja, agora, $M \in R$. Então, pelo Lema (2.4), $M = \rho(\delta)$, onde $\delta = \delta(M)$ tem aumento 1.

Além disso, pelo Lema (2.6), $M^{-1} \in R$ e, então, pelo Lema (2.4), parte (i), $M^{-1} = \rho(1)$, onde $1 = \delta(M^{-1})$.

Assim, $I = MM^{-1} = \rho(\delta 1)$, donde $\delta 1 = 1$; logo, δ é uma unidade e, portanto, $\rho: U_1(\mathbb{Z}G) \rightarrow R$ é um epimorfismo. Δ

CAPÍTULO II

UMA CARACTERIZAÇÃO DAS UNIDADES EM $\mathbb{Z}D_m$

Caracterizações de $U_1(\mathbb{Z}S_3)$ como um grupo de matrizes sobre $\mathbb{Z}$ já foram obtidas. Em [5], I. Hughes e K.R. Pearson mostraram que $U_1(\mathbb{Z}S_3)$ é isomorfo ao subgrupo de $GL_2(\mathbb{Z})$ constituído pelas matrizes cujas somas das entradas nas colunas são iguais a 1 módulo 3. A técnica usada foi construir uma matriz 6×6 a partir de um conjunto completo de representantes das classes de equivalência das representações irredutíveis de S_3 , inveter a matriz e, então, resolver um sistema de 6 congruências lineares módulo 6. Em [3], P.J. Allen e C.Hobby usaram um método diferente para obter uma nova descrição de $U_1(\mathbb{Z}S_3)$ como o subgrupo das matrizes duplamente estocásticas de $GL_3(\mathbb{Z})$. Trabalhando em $GL_3(\mathbb{Z})$, em lugar de $GL_2(\mathbb{Z})$, puderam explorar o fato de que uma combinação convexa de matrizes de permutação é sempre duplamente estocástica e não foi necessário inverter uma matriz 6×6 ou resolver um sistema de congruências lineares.

Trabalhando com P.J. Allen e C. Hobby caracterizamos $U_1(\mathbb{Z}D_m)$, para $m \geq 3$, como um subgrupo de matrizes duplamente estocásticas de $GL_m(\mathbb{Z})$.

Vamos considerar, separadamente, $m = 2n+1 \geq 3$ e $m = 2n \geq 4$. Em ambos os casos, representaremos

$$D_m = \langle a, b: a^2 = 1 = b^m, a b a = b^{-1} \rangle$$

por $\rho: D_m \rightarrow GL_m(\mathbb{Z})$ tal que

$$\rho(a) = A = (c_1 c_m c_{m-1} \dots c_4 c_3 c_2) \quad e$$

$$\rho(b) = B = (c_2 c_3 c_4 \dots c_{m-1} c_m c_1),$$

onde c_i , $1 \leq i \leq m$, é uma coluna com 1 na linha i e 0 nas outras linhas, isto é,

$$\rho(a) = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \end{bmatrix} \quad e \quad \rho(b) = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}$$

Denotaremos ainda por ρ a extensão linear de ρ a $\mathbb{Z}D_m$ e seja $\alpha = \sum \alpha_{ij} a^i b^j \in \mathbb{Z}D_m$. Então, mostraremos que a matriz $\rho(\alpha) = \sum \alpha_{ij} A^i B^j$ é da forma $\rho(\alpha) = (x_{k\ell})$, com

$$x_{k\ell} = \alpha_{0, k-\ell} + \alpha_{1, m-k-\ell+2}, \quad \forall k, \ell, \quad 1 \leq k, \ell \leq m,$$

onde $k-\ell$ e $m-k-\ell+2$ são considerados módulo m .

Seja S_m o grupo das permutações de m elementos e seja $\pi: D_m \rightarrow S_m$ o homomorfismo tal que

$$\pi(a) = (2 \ m)(3 \ m-1)(4 \ m-2)\dots \quad e \quad \pi(b) = (1 \ 2 \ 3 \ m-2 \ m-1 \ m).$$

Então,

$$\pi(a)k = m-k+2 \quad e \quad \pi(b)k = k+1, \quad \forall k, \quad 1 \leq k \leq m,$$

onde $m-k+2$ e $k+1$ são considerados módulo m .

É fácil ver que ρ é a representação de permutação determinada por π ; logo,

$$B^k = (c_{\pi(b^k)_1} \quad c_{\pi(b^k)_2} \quad \dots \quad c_{\pi(b^k)_m}) \quad e$$

$$AB^k = (c_{\pi(a)\pi(b^k)_1} \quad c_{\pi(a)\pi(b^k)_2} \quad \dots \quad c_{\pi(a)\pi(b^k)_m}), \quad \forall k, \quad 1 \leq k \leq m.$$

Assim, para quaisquer k e ℓ , $1 \leq k, \ell \leq m$, $x_{k\ell} = \alpha_{0u} + \alpha_{1v}$, com $0 \leq u, v \leq m-1$, $\pi(b^u)_\ell = k$ e $\pi(a)\pi(b^v)_\ell = k$; logo, deve ocorrer $u = k-\ell$ e $v = m-k-\ell+2$, onde $k-\ell$ e $m-k-\ell+2$ são considerados módulo m .

Será importante, para nossa caracterização de $U_1(\mathbb{Z}D_m)$, observar que podemos escrever $x_{k\ell}$, para quaisquer k e ℓ , $1 \leq k \leq m$, $3 \leq \ell \leq m$, em função de $x_{k\ell}$, com $1 \leq k \leq m$ e $\ell = 1, 2$; mais precisamente, mostraremos que

$$x_{k\ell} = -x_{k-\ell+3,1} - x_{k-\ell+5,1} - \dots - x_{k+\ell-3,1} +$$

$$+ x_{k-\ell+2,2} + x_{k-\ell+4,2} + \dots + x_{k+\ell-2,2}, \quad \forall k, \ell, \quad 1 \leq k \leq m,$$

$$3 \leq \ell \leq m,$$

onde $k-\ell+3, k-\ell+5, \dots, k+\ell-3, k-\ell+2, k-\ell+4, \dots, k+\ell-2$ são considerados módulo m .

Para isso, começaremos mostrando que relações análogas valem para B^h e AB^h , $0 \leq h \leq m-1$, isto é, que se $B^h = (u_{k\ell})$ e $AB^h = (v_{k\ell})$, $0 \leq h \leq m-1$, então, temos

$$u_{k\ell} = -u_{k-\ell+3,1} - u_{k-\ell+5,1} - \dots - u_{k+\ell-3,1} +$$

$$+ u_{k-\ell+2,2} + u_{k-\ell+4,2} + \dots + u_{k+\ell-2,2}$$

e

$$v_{k\ell} = -v_{k-\ell+3,1} - v_{k-\ell+5,1} - \dots - v_{k+\ell-3,1} + \\ + v_{k-\ell+2,2} + v_{k-\ell+4,2} + \dots + v_{k+\ell-2,2}, \quad \forall k, \quad 1 \leq k \leq m, \quad 3 \leq \ell \leq m.$$

$$\text{Para cada } h, \quad 0 \leq h \leq m-1, \quad B^h = (c_{\pi(b^h)_1} \quad c_{\pi(b^h)_2} \quad \dots \quad c_{\pi(b^h)_m}).$$

Então,

$$\forall k, \ell, \quad 1 \leq k, \ell \leq m, \quad u_{k\ell} = \begin{cases} 1, & \text{se } k = \pi(b^h)_\ell \equiv h+\ell \pmod{m}, \\ 0, & \text{caso contrário.} \end{cases}$$

Por outro lado, se $k-\ell+i \equiv h+1 \pmod{m}$, para algum i , $3 \leq i \leq 2\ell-3$, então, $k-\ell+j \equiv h+2 \pmod{m}$, para algum j , $4 \leq j \leq 2\ell-2$; logo, para quaisquer k e ℓ , $1 \leq k \leq m$, $3 \leq \ell \leq m$, temos

$$-u_{k-\ell+3,1} - u_{k-\ell+5,1} - \dots - u_{k+\ell-3,1} + \\ + u_{k-\ell+2,2} + u_{k-\ell+4,2} + \dots + u_{k+\ell-2,2} = u_{k-\ell+2,2}.$$

Como,

$$\forall k, \ell, \quad 1 \leq k, \ell \leq m, \quad u_{k-\ell+2,2} = \begin{cases} 1, & \text{se } k-\ell+2 \equiv h+2 \pmod{m} \\ 0, & \text{caso contrário,} \end{cases}$$

temos a primeira relação. Da mesma forma, podemos provar a outra.

Assim, desde que a matriz $\rho(\alpha) = (x_{k\ell})$ é uma combinação linear de matrizes da forma $A^i B^j$, $i = 0, 1$, $0 \leq j \leq m-1$, é imediato que suas entradas verificam a relação dada.

3. AS UNIDADES EM $\mathbb{Z}D_{2n+1}$

Começaremos introduzindo uma notação que será útil no que segue.

Dada uma matriz $X = (x_{ij}) \in M_m(\mathbb{Z})$, denotaremos por $t_{ij}(X)$, $i=0,1$, $0 \leq j \leq m-1$, a soma das entradas de X que ocorrem nas posições onde a matriz de permutação $A^i B^j$ tem 1. Então,

$$t_{0k}(X) = \sum_{i=1}^m x_{\pi(b^k)i,i} \quad \text{e} \quad t_{1k}(X) = \sum_{i=1}^m x_{\pi(a)\pi(b^k)i,i},$$

$$\forall k, 0 \leq k \leq m-1.$$

Definimos as *diagonais* de X como

Diagonal $(0,0)$: $x_{11} \ x_{22} \ \dots \ x_{mm}$,

Diagonal $(0,1)$: $x_{21} \ x_{32} \ \dots \ x_{m,m-1} \ x_{1m}$,

Diagonal $(0,2)$: $x_{31} \ x_{42} \ \dots \ x_{m,m-2} \ x_{1,m-1} \ x_{2m}$,

.....

Diagonal $(0,m-1)$: $x_{m1} \ x_{12} \ x_{23} \ \dots \ x_{m-2,m-1} \ x_{m-1,m}$,

Diagonal $(1,0)$: $x_{11} \ x_{m2} \ x_{m-1,3} \ \dots \ x_{2m}$,

Diagonal $(1,1)$: $x_{m1} \ x_{m-1,2} \ \dots \ x_{1m}$,

Diagonal $(1,2)$: $x_{m-1,1} \ x_{m-2,2} \ \dots \ x_{1,m-1} \ x_{mm}$,

.....

Diagonal $(1,m-1)$: $x_{21} \ x_{12} \ x_{m3} \ x_{m-1,4} \ \dots \ x_{4,m-1} \ x_{3m}$,

isto é, pode-se ilustrar as diagonais de X pelo seguinte diagrama:

$$\begin{array}{c}
 \text{diag}(0,0) \quad \text{diag}(1,0) \\
 \text{diag}(0,1) \quad \text{diag}(0,2) \\
 \text{diag}(1,3) \quad \text{diag}(1,2) \\
 \text{diag}(1,1) \quad \text{diag}(1,0)
 \end{array}
 \begin{bmatrix}
 x_{11} & x_{12} & x_{13} & \cdot & \cdot & \cdot & x_{1,m-2} & x_{1,m-1} & x_{1m} \\
 x_{21} & x_{22} & x_{23} & \cdot & \cdot & \cdot & x_{2,m-2} & x_{2,m-1} & x_{2m} \\
 x_{31} & x_{32} & x_{33} & \cdot & \cdot & \cdot & x_{3,m-2} & x_{3,m-1} & x_{3m} \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 x_{m-2,1} & x_{m-2,2} & x_{m-2,3} & \cdot & \cdot & \cdot & x_{m-2,m-2} & x_{m-2,m-1} & x_{m-2,m} \\
 x_{m-1,1} & x_{m-1,2} & x_{m-1,3} & \cdot & \cdot & \cdot & x_{m-1,m-2} & x_{m-1,m-1} & x_{m-1,m} \\
 x_{m1} & x_{m2} & x_{m3} & \cdot & \cdot & \cdot & x_{m,m-2} & x_{m,m-1} & x_{mm}
 \end{bmatrix}
 \begin{array}{c}
 \text{diag}(0,1) \\
 \text{diag}(0,2) \\
 \text{diag}(1,3) \\
 \text{diag}(1,2)
 \end{array}$$

Note que, com esta definição, $t_{ij}(X)$, $i=0,1$, $0 \leq j \leq m-1$, é a soma das entradas de X na diagonal (i,j) .

Seja, agora, $\alpha = \sum \alpha_{ij} a^i b^j \in U_1(\mathbb{ZD}_{2n+1})$. Então, $\rho(\alpha) = \sum \alpha_{ij} A^i B^j$ é uma matriz em $GL_{2n+1}(\mathbb{Z})$ da forma $\rho(\alpha) = (m_{k\ell})$, com

$$(1) \quad m_{k\ell} = \alpha_{0,k-\ell} + \alpha_{1,2n-k-\ell+3}, \quad \forall k, \ell, \quad 1 \leq k, \ell \leq 2n+1,$$

onde $k-\ell$ e $2n-k-\ell+3$ são considerados módulo $2n+1$, isto é, $\rho(\alpha) =$

$$= \begin{bmatrix} \begin{matrix} (1) & (2) & (3) & & (n) & (n+1) & (n+2) & (n+3) & & (2n) & (2n+1) \end{matrix} \\ \begin{matrix} a_{00}^{+a} a_{10} & a_{0,2n}^{+a} a_{1,2n} & a_{0,2n-1}^{+a} a_{1,2n-1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} a_{01}^{+a} a_{1,2n} & a_{00}^{+a} a_{1,2n-1} & a_{0,2n}^{+a} a_{1,2n-2} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} a_{02}^{+a} a_{1,2n-1} & a_{01}^{+a} a_{1,2n-2} & a_{00}^{+a} a_{1,2n-3} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} a_{03}^{+a} a_{1,2n-2} & a_{02}^{+a} a_{1,2n-3} & a_{01}^{+a} a_{1,2n-4} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \dots \\ \begin{matrix} a_{0i}^{+a} a_{1,2n-i+1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} \dots & a_{0i}^{+a} a_{1,2n-i-1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} \dots & \dots & a_{0i}^{+a} a_{1,2n-i-3} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \dots \\ \begin{matrix} \dots & \dots & \dots & \dots & a_{00}^{+a} a_{13} & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} \dots & \dots & \dots & \dots & \dots & a_{00}^{+a} a_{11} & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} \dots & \dots & \dots & \dots & \dots & \dots & a_{00}^{+a} a_{1,2n} & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} \dots & \dots & \dots & \dots & \dots & \dots & \dots & a_{00}^{+a} a_{1,2n-2} & \dots & \dots & \dots \end{matrix} \\ \dots \\ \begin{matrix} a_{0,2n-3}^{+a} a_{14} & a_{0,2n-4}^{+a} a_{13} & a_{0,2n-5}^{+a} a_{12} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} a_{0,2n-2}^{+a} a_{13} & a_{0,2n-3}^{+a} a_{12} & a_{0,2n-4}^{+a} a_{11} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{matrix} \\ \begin{matrix} a_{0,2n-1}^{+a} a_{12} & a_{0,2n-2}^{+a} a_{11} & a_{0,2n-3}^{+a} a_{10} & \dots & \dots & \dots & \dots & \dots & \dots & a_{00}^{+a} a_{14} & \dots \end{matrix} \\ \begin{matrix} a_{0,2n}^{+a} a_{11} & a_{0,2n-1}^{+a} a_{10} & a_{0,2n-2}^{+a} a_{1,2n} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & a_{00}^{+a} a_{12} \end{matrix} \end{bmatrix} ;$$

ainda mais,

$$(2) \quad m_{k\ell} = -m_{k-\ell+3,1} - m_{k-\ell+5,1} - \dots - m_{k+\ell-3,1} + \\ + m_{k-\ell+2,2} + m_{k-\ell+4,2} + \dots + m_{k+\ell-2,2}, \quad \forall k, \ell, \quad 1 \leq k \leq 2n+1, \\ 3 \leq \ell \leq 2n+1,$$

onde $k-\ell+3$, $k-\ell+5$, $k+\ell-3$, $k-\ell+2$, $k-\ell+4$, $\dots$, $k+\ell-2$ são considerados módulo $2n+1$.

Como α tem aumento 1, segue de (1) que $\rho(\alpha)$ é duplamente estocástica.

Seja $\langle b \rangle$ o subgrupo de D_{2n+1} gerado por b . É claro que $\langle b \rangle$ é um subgrupo normal de D_{2n+1} e, como

$$\frac{D_{2n+1}}{\langle b \rangle} = \{ \langle b \rangle, a \langle b \rangle \},$$

temos que $\frac{D_{2n+1}}{\langle b \rangle}$ é um grupo cíclico de ordem 2; logo, de [16, Teorema II.4.1], as unidades em $\mathbb{Z}(\frac{D_{2n+1}}{\langle b \rangle})$ são triviais, isto é, $U_1(\mathbb{Z}(\frac{D_{2n+1}}{\langle b \rangle})) = \frac{D_{2n+1}}{\langle b \rangle}$.

Seja $f: \mathbb{Z}D_{2n+1} \rightarrow \mathbb{Z}(\frac{D_{2n+1}}{\langle b \rangle})$ o homomorfismo natural. Então,

$$\bar{\alpha} = f(\alpha) = \sum_{i=0}^{2n} \alpha_{oi} \langle b \rangle + \sum_{i=0}^{2n} \alpha_{1i} a \langle b \rangle \in \frac{D_{2n+1}}{\langle b \rangle};$$

logo, um dos números $\sum_{i=0}^{2n} \alpha_{oi}$, $\sum_{i=0}^{2n} \alpha_{1i}$ é igual a 1 e o outro a 0.

O próximo resultado sugere a descrição que daremos de $U_1(\mathbb{Z}D_{2n+1})$.

LEMA (3.1). Seja $\alpha = \sum \alpha_{ij} a^i b^j \in \mathbb{Z}D_{2n+1}$ tal que

$$\bar{\alpha} = f(\alpha) = \sum_{i=0}^{2n} \alpha_{oi} \langle b \rangle + \sum_{i=0}^{2n} \alpha_{1i} a \langle b \rangle \in \frac{D_{2n+1}}{\langle b \rangle}$$

e seja $M = \rho(\alpha)$.

- (i) Se $\bar{\alpha} = \langle b \rangle$, então $t_{oo}(M) \equiv 0 \pmod{2n+1}$
e $t_{11}(M) \equiv 1 \pmod{2n+1}$.
- (ii) Se $\bar{\alpha} = a \langle b \rangle$, então $t_{oo}(M) \equiv 1 \pmod{2n+1}$
e $t_{11}(M) \equiv 0 \pmod{2n+1}$.

Demonstração. Como $M = \rho(\alpha) = \sum \alpha_{ij} A^i B^j$, temos $M = (m_{k\ell})$,
com

$$m_{k\ell} = \alpha_{0, k-\ell} + \alpha_{1, 2n-k-\ell+3}, \quad \forall k, \ell, \quad 1 \leq k, \ell \leq 2n+1,$$

onde $k-\ell$ e $2n-k-\ell+3$ são considerados módulo $2n+1$; logo,

$$t_{00}(M) = \sum_{i=1}^{2n+1} m_{ii} = \sum_{i=1}^{2n+1} (\alpha_{00} + \alpha_{1,2n-2i+3}) = (2n+1)\alpha_{00} + \sum_{i=0}^{2n} \alpha_{1i}$$

e

$$\begin{aligned} t_{11}(M) &= \sum_{i=1}^{2n+1} m_{\pi(a)\pi(b)i,i} = \sum_{i=1}^{2n+1} m_{2n-i+2,i} = \sum_{i=1}^{2n+1} (\alpha_{0,2n-2i+2} + \alpha_{11}) = \\ &= \sum_{i=0}^{2n} \alpha_{0i} + (2n+1)\alpha_{11}. \end{aligned}$$

Se $\bar{\alpha} = \langle b \rangle$, então $\sum_{i=0}^{2n} \alpha_{0i} = 1$ e $\sum_{i=0}^{2n} \alpha_{1i} = 0$; logo, $t_{00}(M) = (2n+1)\alpha_{00} \equiv 0 \pmod{2n+1}$ e $t_{11}(M) = 1 + (2n+1)\alpha_{11} \equiv 1 \pmod{2n+1}$, o que prova (i).

De forma análoga, podemos demonstrar (ii). Δ

Seja V o conjunto das matrizes $M = (m_{k\ell}) \in GL_{2n+1}(\mathbb{Z})$ tais que

- (i) M é duplamente estocástica;
- (ii) $m_{k\ell}$ satisfaz a relação (2);
- (iii) $t_{00}(M) \equiv 0 \pmod{2n+1}$ ou $t_{00}(M) \equiv 1 \pmod{2n+1}$.

Já vimos que $\rho(U_1(\mathbb{ZD}_{2n+1})) \subseteq V$; mais ainda, nossa caracterização de $U_1(\mathbb{ZD}_{2n+1})$ consistirá em mostrar que $U_1(\mathbb{ZD}_{2n+1}) \cong V$, onde o isomorfismo é dado pela restrição de ρ .

Para isso, precisaremos de alguns resultados e definições que introduzimos a seguir.

Antes, porém, observamos que a caracterização para $U_1(\mathbb{ZD}_3)$ será a mesma obtida por P.J. Allen e C. Hobby em [3]. De fato, no Capítulo III, veremos que, para $n = 1$, o conjunto V é, simplesmente, o conjunto das matrizes duplamente estocásticas em $GL_3(\mathbb{Z})$; mais ainda, veremos que isto não ocorre para $n=2$.

Definição. Seja $M \in V$. Então, definimos

$$\lambda = \lambda(M) = \begin{cases} 1, & \text{se } t_{00}(M) \equiv 1 \pmod{2n+1}, \\ 0, & \text{caso contrário} \end{cases}$$

Ainda, definimos os números

$$\beta_{ok} = \beta_{ok}(M) = \frac{t_{ok}(M) - \lambda}{2n+1}, \quad \beta_{1k} = \beta_{1k}(M) = \frac{t_{1k}(M) + \lambda - 1}{2n+1}, \quad \forall k, \quad 0 \leq k \leq 2n$$

e, finalmente, o elemento em $\mathbb{QD}_{2n+1}$

$$\beta(M) = \sum \beta_{ij} a^i b^j.$$

O próximo passo será mostrar que, de fato, $\beta = \beta(M)$ é um elemento de aumento 1 em $\mathbb{ZD}_{2n+1}$ tal que $\rho(\beta) = M$; mas antes precisamos do seguinte

LEMA (3.2). Sejam $M \in V$ e $t_{ij} = t_{ij}(M)$, $i=0,1$, $0 \leq j \leq 2n$. Então,

- (i) para todo k , $0 \leq k \leq 2n$, $t_{00} + t_{1k} \equiv 1 \pmod{2n+1}$ e $t_{0k} + t_{11} \equiv 1 \pmod{2n+1}$;
- (ii) $\sum_{i=0}^{2n} t_{0i} = 2n+1 = \sum_{i=0}^{2n} t_{1i}$.

Demonstração. Se $M = (m_{k\ell}) \in V$, então $m_{k\ell}$ satisfaz (2); ainda mais, M é duplamente estocástica e, portanto, em particular, temos

$$(3) \quad m_{2n+1} = 1 - \sum_{i=1}^{2n} m_{i1} \quad \text{e} \quad m_{2n+1,2} = 1 - \sum_{i=1}^{2n} m_{i2}.$$

A seguir, com as relações (2) e (3), vamos calcular $t_{ij} = t_{ij}(M)$, $i=0,1$, $0 \leq j \leq 2n$, em função de $m_{k\ell}$, $1 \leq k \leq 2n$, $\ell=1,2$.

Para $0 \leq k \leq n-1$, e considerando os índices módulo $2n+1$, temos $t_{0,2k} = m_{2k+1,1} + m_{2k+2,2} + m_{2k+3,3} + m_{2k+4,4} + \dots +$
 $+ m_{2k+(n-k+1),n-k+1} + m_{n+k+2,n-k+2} + m_{n+k+3,n-k+3} + m_{n+k+4,n-k+4} + \dots +$
 $+ m_{k,2n-k+1} + m_{k+1,2n-k+2} + m_{k+2,2n-k+3} + m_{k+3,2n-k+4} + \dots +$
 $+ m_{2n+2k,2n} + m_{2k,2n+1}.$

Agora, de (2) e (3), vem

$$m_{2k+3,3} = -m_{2k+3,1} + m_{2k+2,2} + m_{2k+4,2},$$

$$m_{2k+4,4} = -m_{2k+3,1} - m_{2k+5,1} + m_{2k+2,2} + m_{2k+4,2} + m_{2k+6,2},$$

.....

$$m_{2k+(n-k+1),n-k+1} = -m_{2k+3,1} - m_{2k+5,1} - \dots - m_{2n-1,1} +$$

$$+ m_{2k+2,2} + m_{2k+4,2} + \dots + m_{2n,2}$$

$$m_{n+k+2,n-k+2} = -m_{2k+3,1} - m_{2k+5,1} - \dots - m_{2n+1,1} +$$

$$+ m_{2k+2,2} + m_{2k+4,2} + \dots + m_{2n,2} + m_{12} =$$

$$= -m_{2k+3,1} - m_{2k+5,1} - \dots - (1 - \sum_{i=1}^{2n} m_{i1}) +$$

$$+ m_{2k+2,2} + m_{2k+4,2} + \dots + m_{2n,2} + m_{12} =$$

$$= -1 + m_{21} + m_{41} + \dots + m_{2n,1} + m_{11} + m_{31} + \dots + m_{2k+1,1} +$$

$$+ m_{2k+2,2} + m_{2k+4,2} + \dots + m_{2n,2} + m_{12},$$

$$m_{n+k+3,n-k+3} = -1+m_{41}+m_{61}+\dots+m_{2n,1}+m_{11}+m_{31}+\dots+m_{2k+1,1}+ \\ +m_{2k+2,2}+m_{2k+4,2}+\dots+m_{2n,2}+m_{12}+m_{32},$$

$$m_{n+k+4,n-k+4} = -1+m_{61}+m_{81}+\dots+m_{2n,1}+m_{11}+m_{31}+\dots+m_{2k+1,1}+ \\ +m_{2k+2,2}+m_{2k+4,2}+\dots+m_{2n,2}+m_{12}+m_{32}+m_{52},$$

.....

$$m_{k,2n-k+1} = -1+m_{2n,1}+m_{11}+m_{31}+\dots+m_{2k+1,1}+ \\ +m_{2k+2,2}+m_{2k+4,2}+\dots+m_{2n,2}+m_{12}+m_{32}+\dots+m_{2n-1,2},$$

$$m_{2k+1,2n-k+2} = 1+m_{11}+m_{31}+\dots+m_{2k+1,1}+ \\ +m_{2k+2,2}+m_{2k+4,2}+\dots+m_{2n,2}+m_{12}+m_{32}+\dots+m_{2n+1,2}= \\ = -1+m_{11}+m_{31}+\dots+m_{2k+1,1}+ \\ +m_{2k+2,2}+m_{2k+4,2}+\dots+m_{2n,2}+m_{12}+m_{32}+\dots+(1-\sum_{i=1}^{2n} m_{i2}) = \\ = m_{11}+m_{31}+\dots+m_{2k+1,1}-m_{22}-m_{42}-\dots-m_{2k,2},$$

$$m_{k+2,2n-k+3} = m_{31}+m_{51}+\dots+m_{2k+1,1}-m_{42}-m_{62}-\dots-m_{2k,2},$$

$$m_{k+3,2n-k+4} = m_{51}+m_{71}+\dots+m_{2k+1,1}-m_{62}-m_{82}-\dots-m_{2k,2},$$

.....

$$m_{2n+2k,2n} = m_{2k-3,1}+m_{2k-1,1}+m_{2k+1,1}-m_{2k-2,2}-m_{2k,2},$$

$$m_{2k,2n+1} = m_{2k-1,1}+m_{2k+1,1}-m_{2k,2};$$

logo,

$$\begin{aligned}
 t_{o,2k} = & -n+(n+1)m_{11}+(n+2)m_{31}+\dots+(n+k+1)m_{2k+1,1}-(n-k-1)m_{2k+3,1}-\dots-m_{2n-1,1}+ \\
 & + m_{21}+2m_{41}+\dots+km_{2k,1}+\dots+nm_{2n,1}+ \\
 & +nm_{12}+(n-1)m_{32}+\dots+(n-k+1)m_{2k-1,2}+\dots+m_{2n-1,2}- \\
 & -m_{22}-2m_{42}-\dots-km_{2k,2}+(2n-k)m_{2k+2,2}+\dots+(n+1)m_{2n,2}.
 \end{aligned}$$

Da mesma forma, podemos calcular

$$\begin{aligned}
 t_{o,2n} = & m_{2n+1,1} + m_{12} + m_{23} + m_{34} + \dots + \\
 & + m_{(n+1)-1,n+1} + m_{n+1,n+2} + m_{n+2,n+3} + m_{n+3,n+4} + \dots + \\
 & + m_{2n-1,2n} + m_{2n,2n+1} = \\
 = & (n+1) - nm_{11} - (n-1)m_{31} - \dots - (n-i+1)m_{2i-1,1} - \dots - m_{2n-1,1} - \\
 & - 2nm_{21} - (2n-1)m_{41} - \dots - (2n-i+1)m_{2i,1} - \dots - (n+1)m_{2n,1} + \\
 & + nm_{12} + (n-1)m_{32} + \dots + (n-i+1)m_{2i-1,2} + \dots + m_{2n-1,2} - \\
 & - m_{22} - 2m_{42} - \dots - im_{2i,2} - \dots - nm_{2n,2},
 \end{aligned}$$

para $1 \leq k \leq n$,

$$\begin{aligned}
 t_{o,2k-1} = & m_{2k,1} + m_{2k+1,2} + m_{2k+2,3} + m_{2k+3,4} + \dots + \\
 & + m_{2k+(n-k+1)-1,n-k+1} + m_{n-k+1,n-k+2} + m_{n-k+2,n-k+3} + m_{n-k+3,n-k+4} + \dots + \\
 & + m_{2n-k+1,2n-k+2} + m_{k+1,2n-k+3} + m_{k+2,2n-k+4} + m_{k+3,2n-k+5} + \dots + \\
 & + m_{2k-2,2n} + m_{2k-1,2n+1} =
 \end{aligned}$$

$$\begin{aligned}
&= (n+1)-nm_{11}-(n-1)m_{31}-\dots-(n-k+1)m_{2k-1,1}-\dots-m_{2n-1,1}^+ \\
&+m_{21}+2m_{41}+\dots+km_{2k,1}-(2n-k)m_{2k+2,1}-\dots-(n+1)m_{2n,1}^- \\
&-(n+1)m_{12}-(n+2)m_{32}-\dots-(n+k)m_{2k-1,2}^+(n-k)m_{2k+1,2}^++\dots+m_{2n-1,2}^- \\
&-m_{22}-2m_{42}-\dots-km_{2k,2}-\dots-nm_{2n,2},
\end{aligned}$$

$$\begin{aligned}
t_{10} &= m_{11} + m_{2n+1,2}^+ m_{2n,3} + m_{2n-1,4} + \dots + \\
&+ m_{2n-(n+1)+3,n+1} + m_{n+1,n+2} + m_{n,n+3} + m_{n-1,n+4} + \dots + \\
&+ m_{3,2n} + m_{2,2n+1} = \\
&= (n+1)+nm_{11}+(n-1)m_{31}+\dots+(n-i+1)m_{2i-1,1}+\dots+m_{2n-1,1}^- \\
&-m_{21} - 2m_{41} - \dots - im_{2i,1} - \dots - nm_{2n,1}^- \\
&-nm_{12} - (n-1)m_{32} - \dots - (n-i+1)m_{2i-1,2} - \dots - m_{2n-1,2}^- \\
&-2nm_{22} - (2n-1)m_{42} - \dots - (2n-i+1)m_{2i,2} - \dots - (n+1)m_{2n,2},
\end{aligned}$$

para $0 \leq k \leq n-1$,

$$\begin{aligned}
t_{1,2n-2k} &= m_{2k+2,1} + m_{2k+1,2} + m_{2k,3} + m_{2k-1,4} + \dots + \\
&+ m_{2k-(k+2)+3,k+2} + m_{k,k+3} + m_{k-1,k+4} + m_{k-2,k+5} + \dots + \\
&+ m_{k-n+1,n+k+2} + m_{k-n,k+n+3} + m_{k-n-1,k+n+3} + m_{k-n-2,k+n+5} + \dots + \\
&+ m_{2k+4,2n} + m_{2k+3,2n+1} = \\
&= -n+nm_{11}+(n-1)m_{31} + \dots + (n-k+1)m_{2k-1,1} + \dots + m_{2n-1,1}^- \\
&-m_{21} - 2m_{41} - \dots - km_{2k,1} + (2n-k)m_{2k+2,1}+\dots+(n+1)m_{2n,1}^+
\end{aligned}$$

$$\begin{aligned}
& +(n+1)m_{12} + (n+2)m_{32} + \dots + (n+k+1)m_{2k+1,2} - (n-k-1)m_{2k+3,2} - \dots - m_{2n-1,2} + \\
& + m_{22} + 2m_{42} + \dots + km_{2k,2} + \dots + nm_{2n,2},
\end{aligned}$$

para $0 \leq k \leq n-1$,

$$\begin{aligned}
t_{1,2n-2k-1} &= m_{2k+3,1} + m_{2k+2,2} + m_{2k+1,3} + m_{2k,4} + \dots + \\
& + m_{2k-(k+2)+4,k+2} + m_{k+1,k+3} + m_{k,k+4} + m_{k-1,k+5} + \dots + \\
& + m_{k-n+2,k+n+2} + m_{k-n+1,k+n+3} + m_{k-n,k+n+4} + m_{k-n-1,k+n+5} + \dots + \\
& + m_{2k+5,2n} + m_{2k+4,2n+1} = \\
& = (n+1) - (n+1)m_{11} - (n+2)m_{31} - \dots - (n+k+1)m_{2k+1,1} + (n-k-1)m_{2k+3,1} + \dots + m_{2n-1,1} - \\
& - m_{21} - 2m_{41} - \dots - km_{2k,1} - \dots - nm_{2n,1} - \\
& - nm_{12} - (n-1)m_{32} - \dots - (n-k+1)m_{2k-1,2} - \dots - m_{2n-1,2} + \\
& + m_{22} + 2m_{42} + \dots + (k+1)m_{2k+2,2} - (2n-k-1)m_{2k+4,2} - \dots - (n+1)m_{2n,2}.
\end{aligned}$$

Agora, é fácil ver que valem as relações de (i).

A seguir, vamos calcular $\sum_{i=0}^{2n} t_{oi}$, o que levará à primeira igualdade de (ii).

Para cada k , $2 \leq k \leq n$, os coeficientes de $m_{2k-1,1}$ em t_{01} , $t_{03}, \dots, t_{0,2n-1}, t_{00}, t_{02}, \dots, t_{0,2k-4}, t_{0,2n}$ são iguais a $-(n-k+1)$, e em $t_{0,2k-2}, t_{0,2k}, \dots, t_{0,2n-2}$ são iguais a $(n+k)$; logo, o coeficiente de $m_{2k-1,1}$ em $\sum_{i=0}^{2n} t_{oi}$ é

$$-(n-k+1)(n+k) + (n+k)(n-k+1) = 0.$$

Para cada k , $2 \leq k \leq n$, os coeficientes de $m_{2k,1}$ em $t_{00}, t_{02}, \dots, t_{0,2n-2}, t_{0,2k-1}, t_{0,2k+1}, \dots, t_{0,2n-1}$ são iguais a k , e em $t_{0,2n}, t_{01}, t_{03}, \dots, t_{0,2k-3}$ são iguais a $-(2n-k+1)$; logo, o coeficiente de $m_{2k,1}$ em

$$\sum_{i=0}^{2n} t_{oi} \text{ é}$$

$$k(2n-k+1) - (2n-k+1)k = 0.$$

Para cada k , $2 \leq k \leq n$, os coeficientes de $m_{2k-1,2}$ em $t_{00}, t_{02}, \dots, t_{0,2n}, t_{01}, t_{03}, \dots, t_{0,2k-3}$ são iguais a $(n-k+1)$, e em $t_{0,2k-1}, t_{0,2k+1}, \dots, t_{0,2n-1}$ são iguais a $-(n+k)$, donde o coeficiente de

$$m_{2k-1,2} \text{ em } \sum_{i=0}^{2n} t_{oi} \text{ é}$$

$$(n-k+1)(n+k) - (n+k)(n-k+1) = 0.$$

Para cada k , $1 \leq k \leq n$, os coeficientes de $m_{2k,2}$ em $t_{01}, t_{03}, \dots, t_{0,2n-1}, t_{0,2k}, t_{0,2k+2}, \dots, t_{0,2n}$ são iguais a $-k$, e em $t_{00}, t_{02}, \dots, t_{0,2k-2}$ são iguais a $(2n-k+1)$, donde o coeficiente de $m_{2k,2}$ em $\sum_{i=0}^{2n} t_{oi}$ é

$$-k(2n-k+1) + (2n-k+1)k = 0.$$

Finalmente, é fácil ver que os coeficientes de m_{11}, m_{21} e m_{12} em $\sum_{i=0}^{2n} t_{oi}$ são também iguais a 0. Portanto,

$$\sum_{i=0}^{2n} t_{oi} = (-n)n + (n+1)(n+1) = 2n+1.$$

Da mesma forma, podemos verificar a segunda igualdade de

(ii). Δ

LEMA (3.3). Seja $M \in V$. Então,

$$(i) \quad \beta = \beta(M) = \sum_{i,j} \beta_{ij} a^i b^j \in \mathbb{Z}D_{2n+1};$$

(ii) Um dos números $\sum_{i=0}^{2n} \beta_{0i}$, $\sum_{i=0}^{2n} \beta_{1i}$ é igual a 1 e o outro a 0;

$$(iii) \quad \rho(\beta) = M.$$

Demonstração. (i) Por definição, $\beta = \sum_{i,j} \beta_{ij} a^i b^j$, com

$$\beta_{0k} = \frac{t_{0k}(M) - \lambda}{2n+1} \quad \text{e} \quad \beta_{1k} = \frac{t_{1k}(M) + \lambda - 1}{2n+1}, \quad \forall k, \quad 0 \leq k \leq 2n,$$

onde $\lambda = 0$ ou $\lambda = 1$ conforme $t_{00}(M) \equiv 0 \pmod{2n+1}$ ou $t_{00}(M) \equiv 1 \pmod{2n+1}$, respectivamente. Então, pelo Lema (3.2), parte (i), é fácil ver que $\beta_{ij} \in \mathbb{Z}$, para quaisquer i e j , $i=0,1$, $0 \leq j \leq 2n$; logo, $\beta \in \mathbb{Z}D_{2n+1}$.

(ii) Pelo Lema (3.2), parte (ii), temos

$$\sum_{i=0}^{2n} t_{0i}(M) = 2n+1 = \sum_{i=0}^{2n} t_{1i}(M).$$

Com isto,

$$\sum_{i=0}^{2n} \beta_{0i} = \frac{1}{2n+1} \left(\sum_{i=0}^{2n} t_{0i}(M) - (2n+1)\lambda \right) = 1-\lambda$$

e

$$\sum_{i=0}^{2n} \beta_{1i} = \frac{1}{2n+1} \left(\sum_{i=0}^{2n} t_{1i}(M) + (2n+1)(\lambda-1) \right) = \lambda,$$

onde $\lambda = 0$ ou $\lambda = 1$; logo, é claro que um dos números $\sum_{i=0}^{2n} \beta_{0i}$, $\sum_{i=0}^{2n} \beta_{1i}$ é igual a 1 e o outro a 0.

(iii) Se $M = (m_{k\ell}) \in V$, então suas entradas satisfazem (2) e (3).

Por outro lado, de (i) e (ii), temos que $\beta = \beta(M) = \sum \beta_{ij} a^i b^j$ é um elemento de aumento 1 em $\mathbb{Z}D_{2n+1}$. Então, as entradas da matriz $\rho(\beta) = \sum \beta_{ij} A^i B^j$ satisfazem relações análogas às de (1), (2) e (3); isto é, $\rho(\beta) = (r_{k\ell})$, com

$$r_{k\ell} = \beta_{0,k-\ell} + \beta_{1,2n-k-\ell+3}, \quad \forall k, \ell, 1 \leq k, \ell \leq 2n+1,$$

onde $k-\ell$ e $2n-k-\ell+3$ são considerados módulo $2n+1$,

$$r_{k\ell} = -r_{k-\ell+3,1} - r_{k-\ell+5,1} - \dots - r_{k+\ell-3,1} + \\ + r_{k-\ell+2,2} + r_{k-\ell+4,2} + \dots + r_{k+\ell-2,2}, \quad \forall k, \ell, 1 \leq k \leq 2n+1, 3 \leq \ell \leq 2n+1,$$

onde $k-\ell+3, k-\ell+5, \dots, k+\ell-3, k-\ell+2, k-\ell+4, \dots, k+\ell-2$ são considerados módulo $2n+1$ e, finalmente,

$$r_{2n+1,1} = 1 - \sum_{i=1}^{2n} r_{i1} \quad \text{e} \quad r_{2n+1,2} = 1 - \sum_{i=1}^{2n} r_{i2}.$$

Assim, é suficiente verificarmos que $\rho(\beta)$ e M têm entradas iguais nas posições (k, ℓ) , $1 \leq k \leq 2n$, $\ell = 1, 2$, o que é equivalente a mostrar que

$$\begin{array}{ll} \beta_{00} + \beta_{10} = m_{11}, & \beta_{0,2n} + \beta_{1,2n} = m_{12}, \\ \beta_{01} + \beta_{1,2n} = m_{21}, & \beta_{00} + \beta_{1,2n-1} = m_{22}, \\ \dots\dots\dots & \dots\dots\dots \\ \beta_{0i} + \beta_{1,2n-i+1} = m_{i+1,1}, & \beta_{0i} + \beta_{1,2n-i-1} = m_{i+2,2}, \\ \dots\dots\dots & \dots\dots\dots \\ \beta_{0,2n-1} + \beta_{12} = m_{2n,1}, & \beta_{0,2n-2} + \beta_{11} = m_{2n,2}. \end{array}$$

Para isso, usaremos os cálculos de $t_{ij} = t_{ij}(M)$, $i=0,1$, $0 \leq j \leq 2n$, efetuados no Lema (3.2).

Se i é par, $2 \leq i \leq 2n-2$, podemos escrever $i=2k$, com $1 \leq k \leq n-1$; logo,

$$\begin{aligned}
 \beta_{oi} + \beta_{1,2n-i+1} &= \beta_{o,2k} + \beta_{1,2n-2k+1} = \\
 &= \frac{1}{2n+1} (t_{o,2k} + t_{1,2n-2k+1} - 1) = \\
 &= \frac{1}{2n+1} (-n+(n+1)m_{11}+(n+2)m_{31}+\dots+(n+k+1)m_{2k+1,1}-(n-k-1)m_{2k+3,1}-\dots-m_{2n-1,1}+ \\
 &\quad + m_{21} + 2m_{41} + \dots + km_{2k,1} + \dots + nm_{2n,1} + \\
 &\quad + nm_{12} + (n-1)m_{32} + \dots + (n-k+1)m_{2k-1,2} + \dots + m_{2n-1,2} - \\
 &\quad - m_{22}-2m_{42}-\dots-km_{2k,2}+(2n-k)m_{2k+2,2}+\dots+(n+1)m_{2n,2}+ \\
 &\quad +(n+1)-(n+1)m_{11}-(n+2)m_{31}-\dots-(n+k)m_{2k-1,1}+(n-k)m_{2k+1,1}+\dots+m_{2n-1,1}- \\
 &\quad - m_{21} - 2m_{41} - \dots - km_{2k,1} - \dots - nm_{2n,1} - \\
 &\quad - nm_{12} - (n-1)m_{32} - \dots - (n-k+1)m_{2k-1,2} - \dots - m_{2n-1,2} + \\
 &\quad + m_{22}+2m_{42}+\dots+km_{2k,2}-(2n-k)m_{2k+2,2}-\dots-(n+1)m_{2n,2}-1) = \\
 &= \frac{1}{2n+1} (1+(2n+1)m_{2k+1,1}-1) = m_{2k+1,1} = m_{i+1,1},
 \end{aligned}$$

e

$$\begin{aligned}
 \beta_{oi} + \beta_{1,2n-i-1} &= \beta_{o,2k} + \beta_{1,2n-2k-1} = \\
 &= \frac{1}{2n+1} (t_{o,2k} + t_{1,2n-2k-1} - 1) =
 \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2n+1} (-n+(n+1)m_{11}+(n+2)m_{31}+\dots+(n+k+1)m_{2k+1,1}-(n-k-1)m_{2k+3,1}-m_{2n-1,1}+ \\
&\quad + m_{21} + 2m_{41} + \dots + km_{2k,1} + \dots + nm_{2n,1} + \\
&\quad + nm_{12} + (n-1)m_{32} + \dots + (n-k+1)m_{2k-1,2} + \dots + m_{2n-1,2} - \\
&\quad - m_{22} - 2m_{42} - \dots - km_{2k,2} + (2n-k)m_{2k+2,2} + \dots + (n+1)m_{2n,2} + \\
&\quad + (n+1)-(n+1)m_{11}-(n+2)m_{31}-\dots-(n+k+1)m_{2k+1,1}+(n-k-1)m_{2k+3,1}+\dots+m_{2n-1,1}- \\
&\quad - m_{21} - 2m_{41} - \dots - km_{2k,1} - \dots - nm_{2n,1} - \\
&\quad - nm_{12} - (n-1)m_{32} - \dots - (n-k+1)m_{2k-1,2} - \dots - m_{2n-1,2} + \\
&\quad + m_{22}+2m_{42}+\dots+(k+1)m_{2k+2,2}-(2n-k-1)m_{2k+4,2}-\dots-(n+1)m_{2n,2}^{-1}) = \\
&= \frac{1}{2n+1} (1 + (2n+1)m_{2k+2,2} - 1) = m_{2k+2,2} = m_{i+2,2}.
\end{aligned}$$

Da mesma forma, se i é ímpar, $1 \leq i \leq 2n-3$, podemos escrever $i=2k-1$, com $1 \leq k \leq n-1$, e calcular

$$\beta_{0i} + \beta_{1,2n-i+1} = \beta_{0,2k-1} + \beta_{1,2n-2k+2} = m_{2k,1} = m_{i+1,1}$$

e

$$\beta_{0i} + \beta_{1,2n-i-1} = \beta_{0,2k-1} + \beta_{1,2n-2k} = m_{2k+1,2} = m_{i+2,2}.$$

Finalmente, também da mesma forma, podemos calcular

$$\beta_{00} + \beta_{10} = m_{11}, \quad \beta_{00} + \beta_{1,2n-1} = m_{22},$$

$$\beta_{0,2n-1} + \beta_{12} = m_{2n,1} \quad e \quad \beta_{0,2n} + \beta_{1,2n} = m_{12}. \quad \Delta$$

O próximo resultado conduzirá à prova de que $\beta = \beta(M)$ é ainda uma unidade em $\mathbb{ZD}_{2n+1}$.

LEMA (3.4). Se $M \in V$, então $M^{-1} \in V$.

Demonstração. Do Lema (2.5), segue que M^{-1} é duplamente estocástica. A seguir, mostraremos que M^{-1} também satisfaz as condições (ii) e (iii) do conjunto V .

Seja $\chi \in \mathbb{Z}[X]$ o polinômio característico de M . Então, como $M \in GL_{2n+1}(\mathbb{Z})$, podemos escrever $\chi = X^{2n+1} + \sum_{i=0}^{2n} x_i X^i$, com $x_i \in \mathbb{Z}$, $0 \leq i \leq 2n$, e $x_0 = -D$, onde $D = \pm 1$ é o determinante de M ; logo,

$$D = M^{2n+1} + \sum_{i=1}^{2n} x_i M^i = M(M^{2n} + \sum_{i=1}^{2n} x_i M^{i-1}),$$

donde

$$M^{-1} = D(M^{2n} + \sum_{i=1}^{2n} x_i M^{i-1}).$$

Pelo Lema (3.3), partes (i) e (iii), temos que, para cada i , $1 \leq i \leq 2n+1$, $M^i = \rho(\beta^i)$, onde $\beta = \beta(M) = \sum \beta_{ij} a^i b^j \in \mathbb{ZD}_{2n+1}$; logo, $M^{-1} \in \rho(\mathbb{ZD}_{2n+1})$ e, portanto, M^{-1} satisfaz a condição (ii) do conjunto V .

Seja $s_{00} = t_{00}(M^{-1})$ e $s_{11} = t_{11}(M^{-1})$ e, para cada k , $2 \leq k \leq 2n+1$, sejam $t_{00}^{(k)} = t_{00}(M^k)$ e $t_{11}^{(k)} = t_{11}(M^k)$.

Da demonstração do Lema (3.3), parte (ii), temos

$$\sum_{i=0}^{2n} \beta_{0i} = 1 - \lambda \quad \text{e} \quad \sum_{i=0}^{2n} \beta_{1i} = \lambda,$$

onde $\lambda=0$ ou $\lambda=1$ conforme $t_{00} = t_{00} \equiv 0 \pmod{2n+1}$ ou $t_{00} = t_{00}(M) \equiv 1 \pmod{2n+1}$, respectivamente.

Se $t_{00} \equiv 0 \pmod{2n+1}$, então $\bar{\beta} = f(\beta) = \langle b \rangle$; logo, para cada k , $2 \leq k \leq 2n+1$, $\bar{\beta}^k = \langle b \rangle$ e, portanto, pelo Lema (3.1), parte (i), temos

$$t_{oo}^{(k)} = t_{oo}(M^k) = t_{oo}(\rho(\beta^k)) \equiv 0 \pmod{2n+1}.$$

Conseqüentemente, $s_{oo} \equiv 0 \pmod{2n+1}$.

Se $t_{oo} \equiv 1 \pmod{2n+1}$, então $\bar{\beta} = a\langle b \rangle$; logo, se k é ímpar, $3 \leq k \leq 2n+1$, $\bar{\beta}^k = a\langle b \rangle$ e, portanto, pelo Lema (3.1), parte (ii), temos

$$t_{oo}^{(k)} \equiv 1 \pmod{2n+1} \quad \text{e} \quad t_{11}^{(k)} \equiv 0 \pmod{2n+1},$$

e, se k é par, $2 \leq k \leq 2n$, $\bar{\beta}^k = \langle b \rangle$ e, portanto, pelo Lema (3.1), parte (i), temos

$$t_{oo}^{(k)} \equiv 0 \pmod{2n+1} \quad \text{e} \quad t_{11}^{(k)} \equiv 1 \pmod{2n+1}.$$

Conseqüentemente,

$$s_{oo} \equiv D \sum_{i=1}^n x_{2i} \pmod{2n+1}$$

Por outro lado, se $N = M^{2n+1} + \sum_{i=1}^{2n} x_i M^i = D$ e $u_{11} = t_{11}(N)$, então

$$u_{11} \equiv \sum_{i=1}^n x_{2i} \equiv D;$$

logo,

$$s_{oo} \equiv D \sum_{i=1}^{2n} x_{2i} \equiv D^2 \equiv 1 \pmod{2n+1}.$$

Portanto, $s_{oo} \equiv 0 \pmod{2n+1}$ ou $s_{oo} \equiv 1 \pmod{2n+1}$, donde M^{-1} também satisfaz a condição (iii) do conjunto V. Δ

O resultado principal desta seção é, agora, dado pelo

TEOREMA (3.5). A restrição $\rho: U_1(\mathbb{Z}D_{2n+1}) \rightarrow V$ é um isomorfismo.

Demonstração. Seja

$$U = \{\alpha \in \mathbb{Z}D_{2n+1} : \bar{\alpha} = f(\alpha) \in \frac{D_{2n+1}}{\langle b \rangle}\}.$$

Seja I a matriz identidade $(2n+1) \times (2n+1)$ e seja $\alpha = \sum \alpha_{ij} a^i b^j \in U$ tal que $\rho(\alpha) = I$. Mostraremos, nestas condições, que $\alpha = 1$.

Como $\alpha \in U$, um dos números $\sum_{i=0}^{2n} \alpha_{oi}$, $\sum_{i=0}^{2n} \alpha_{1i}$ é igual a 1 e o outro a 0. Por outro lado, a matriz $\rho(\alpha) = \sum \alpha_{ij} A^i B^j$ é da forma $\rho(\alpha) = (m_{kl})$, com

$$m_{kl} = \alpha_{o, k-l} + \alpha_{1, 2n-k-l+3}, \quad \forall k, l, \quad 1 \leq k, l \leq 2n+1,$$

onde $k-l$ e $2n-k-l+3$ são considerados módulo $2n+1$. Assim, como $\rho(\alpha) = (m_{kl}) = I$, temos

$$t_{oo}(\rho(\alpha)) = (2n+1)\alpha_{oo} + \sum_{i=0}^{2n} \alpha_{1i} = 2n+1 \geq 3;$$

$$\text{logo, } \sum_{i=0}^{2n} \alpha_{1i} = 0 \text{ e } \alpha_{oo} = 1.$$

Agora, as entradas na diagonal principal de $\rho(\alpha)$ são iguais a $m_{kk} = \alpha_{oo} + \alpha_{1, 2n-2k+3}$, $1 \leq k \leq 2n+1$; logo, para todo k , $0 \leq k \leq 2n$, $\alpha_{oo} + \alpha_{1k} = 1$, donde $\alpha_{1k} = 0$.

Além disso, as entradas na primeira coluna de $\rho(\alpha)$, a menos da posição $(1,1)$, são iguais a $m_{k1} = \alpha_{o, k-1} + \alpha_{1, 2n-k+2}$, $2 \leq k \leq 2n+1$; logo, para todo k , $1 \leq k \leq 2n$, $\alpha_{ok} + \alpha_{1, 2n-k+1} = 0$, donde

$$\alpha_{ok} = 0.$$

Assim, $\alpha = 1$ e, como $U_1(\mathbb{Z}D_{2n+1}) \subseteq U$, temos que $\rho: U_1(\mathbb{Z}D_{2n+1}) \rightarrow V$ é um monorfismo.

Seja, agora, $M \in V$. Então, pelo Lema (3.3), $M = \rho(\beta)$, onde $\beta = \beta(M) \in U$.

Além disso, pelo Lema (3.4), $M^{-1} \in V$ e, então, pelo Lema (3.3), $M^{-1} = \rho(\beta_1)$, onde $\beta_1 = \beta(M^{-1}) \in U$.

Assim, $I = MM^{-1} = \rho(\beta_1)$, com $\beta_1 \in U$, donde $\beta_1 = 1$; logo, β é uma unidade e, portanto, $\rho: U_1(\mathbb{Z}G) \rightarrow V$ é um epimorfismo. Δ

4. AS UNIDADES EM $\mathbb{Z}D_{2n}$.

Esta seção é bastante semelhante à anterior. Achamos, neste caso, que a diferença está no ponto em que consideramos $\frac{D_{2n}}{\langle b^2 \rangle}$ em lugar de $\frac{D_{2n}}{\langle b \rangle}$.

Isto nos levará à uma caracterização de $U_1(\mathbb{Z}D_{2n})$ como um grupo de matrizes ainda duplamente estocásticas, mas da forma particular pela qual definiremos os conjuntos S_1 e S_2 adiante.

Seja, agora, $\alpha = \sum \alpha_{ij} a^i b^j \in U_1(\mathbb{Z}D_{2n})$. Então, $\rho(\alpha) = \sum \alpha_{ij} A^i B^j$ é uma matriz em $GL_{2n}(\mathbb{Z})$ da forma $\rho(\alpha) = (m_{kl})$, com

$$(4) \quad m_{kl} = \alpha_{0, k-l} + \alpha_{1, 2n-k-l+2}, \quad \forall k, l, \quad 1 \leq k, l \leq 2n,$$

onde $k-l$ e $2n-k-l+2$ são considerados módulo $2n$, isto é, $\rho(\alpha) =$

$$\begin{array}{c}
= \\
\begin{array}{c} (n+1) \\ (n+2) \end{array}
\end{array}
\left[\begin{array}{cccccc}
(1) & (2) & & (n+1) & (n+2) & \\
\alpha_{00}^{+a} \alpha_{10} & \alpha_{0,2n-1}^{+a} \alpha_{1,2n-1} & \dots & \alpha_{0n}^{+a} \alpha_{1,n} & \alpha_{0,n-1}^{+a} \alpha_{1,n-1} & \dots \\
\alpha_{01}^{+a} \alpha_{1,2n-1} & \alpha_{00}^{+a} \alpha_{1,2n-2} & \dots & \alpha_{0,n+1}^{+a} \alpha_{1,n-1} & \alpha_{0,n}^{+a} \alpha_{1,n-2} & \dots \\
\alpha_{02}^{+a} \alpha_{1,2n-2} & \alpha_{01}^{+a} \alpha_{1,2n-3} & \dots & \alpha_{0,n+2}^{+a} \alpha_{1,n-2} & \alpha_{0,n+1}^{+a} \alpha_{1,n-3} & \dots \\
\alpha_{03}^{+a} \alpha_{1,2n-3} & \alpha_{02}^{+a} \alpha_{1,2n-4} & \dots & \alpha_{0,n+3}^{+a} \alpha_{1,n-3} & \alpha_{0,n+2}^{+a} \alpha_{1,n-4} & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\alpha_{01}^{+a} \alpha_{1,2n-1} & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \alpha_{01}^{+a} \alpha_{1,2n-1-2} & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\alpha_{0n}^{+a} \alpha_{1n} & \vdots & \vdots & \alpha_{00}^{+a} \alpha_{10} & \alpha_{0,2n-1}^{+a} \alpha_{1,2n-1} & \vdots \\
\vdots & \alpha_{0n}^{+a} \alpha_{1,2n-2} & \vdots & \alpha_{01}^{+a} \alpha_{1,2n-1} & \alpha_{00}^{+a} \alpha_{1,2n-2} & \vdots \\
\vdots & \vdots & \vdots & \alpha_{02}^{+a} \alpha_{1,2n-2} & \alpha_{01}^{+a} \alpha_{1,2n-3} & \vdots \\
\vdots & \vdots & \vdots & \alpha_{03}^{+a} \alpha_{1,2n-3} & \alpha_{02}^{+a} \alpha_{1,2n-4} & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\alpha_{02,2n-4}^{+a} \alpha_{14} & \alpha_{0,2n-5}^{+a} \alpha_{13} & \vdots & \alpha_{0,n-4}^{+a} \alpha_{1,n+4} & \alpha_{0,n-5}^{+a} \alpha_{1,n+3} & \vdots \\
\alpha_{0,2n-3}^{+a} \alpha_{13} & \alpha_{0,2n-4}^{+a} \alpha_{12} & \vdots & \alpha_{0,n-3}^{+a} \alpha_{1,n+3} & \alpha_{0,n-4}^{+a} \alpha_{1,n+2} & \vdots \\
\alpha_{0,2n-2}^{+a} \alpha_{12} & \alpha_{0,2n-3}^{+a} \alpha_{11} & \vdots & \alpha_{0,n-2}^{+a} \alpha_{1,n+2} & \alpha_{0,n-3}^{+a} \alpha_{1,n+1} & \vdots \\
\alpha_{0,2n-1}^{+a} \alpha_{11} & \alpha_{0,2n-2}^{+a} \alpha_{10} & \vdots & \alpha_{0,n-1}^{+a} \alpha_{1,n+1} & \alpha_{0,n-2}^{+a} \alpha_{1n} & \vdots
\end{array} \right] ;$$

ainda mais,

$$(5) \quad m_{kl} = -m_{k-l+3,1} - m_{k-l+5,1} - \dots - m_{k+l-3,1} + m_{k-l+2,2} + m_{k-l+4,2} + \dots + m_{k+l-2,2},$$

$$\forall k, l, \quad 1 \leq k \leq 2n, \quad 3 \leq l \leq 2n,$$

onde $k-l+3, k-l+5, \dots, k+l-3, k-l+2, k-l+4, \dots, k+l-2$ são considerados módulo $2n$.

Como α tem aumento 1, segue de (4) que $\rho(\alpha)$ é duplamente estocástica. Além disso, também de (4), segue que

$$(6) \quad m_{kl} = m_{k+n, l+n}, \quad \forall k, l, \quad 1 \leq k, l \leq 2n,$$

onde $k+n$ e $l+n$ são considerados módulo $2n$.

Seja $\langle b^2 \rangle$ o subgrupo de D_{2n} gerado por b^2 . Então, $\langle b^2 \rangle$

é um subgrupo normal de D_{2n} e, como

$$\frac{D_{2n}}{\langle b^2 \rangle} = \{ \langle b^2 \rangle, b\langle b^2 \rangle, a\langle b^2 \rangle, ab\langle b^2 \rangle \},$$

temos que $\frac{D_{2n}}{\langle b^2 \rangle}$ é um grupo abeliano de expoente 2; logo, de [16, Teorema II.4.1], as unidades em $\mathbb{Z}(\frac{D_{2n}}{\langle b^2 \rangle})$ são triviais, isto é, $U_2(\mathbb{Z}(\frac{D_{2n}}{\langle b^2 \rangle})) = \frac{D_{2n}}{\langle b^2 \rangle}$.

Seja $g: \mathbb{Z}D_{2n} \rightarrow \mathbb{Z}(\frac{D_{2n}}{\langle b^2 \rangle})$ o homomorfismo natural. Então,

$$\bar{\alpha} = g(\alpha) = \sum_{i=0}^{n-1} \alpha_{0,2i} \langle b^2 \rangle + \sum_{i=0}^{n-1} \alpha_{0,2i+1} b\langle b^2 \rangle + \sum_{i=0}^{n-1} \alpha_{1,2i} a\langle b^2 \rangle + \sum_{i=0}^{n-1} \alpha_{1,2i+1} ab\langle b^2 \rangle \in \frac{D_{2n}}{\langle b^2 \rangle};$$

logo, um dos números $\sum_{i=0}^{n-1} \alpha_{0,2i}$, $\sum_{i=0}^{n-1} \alpha_{0,2i+1}$, $\sum_{i=0}^{n-1} \alpha_{1,2i}$, $\sum_{i=0}^{n-1} \alpha_{1,2i+1}$ é igual a 1 e os outros são iguais a 0.

O próximo resultado sugere a descrição que daremos de $U_1(\mathbb{Z}D_{2n})$.

LEMA (4.1). Seja $\alpha = \sum_{i,j} \alpha_{ij} a^i b^j \in \mathbb{Z}D_{2n}$ tal que

$$\bar{\alpha} = g(\alpha) = \sum_{i=0}^{n-1} \alpha_{0,2i} \langle b^2 \rangle + \sum_{i=0}^{n-1} \alpha_{0,2i+1} b\langle b^2 \rangle + \sum_{i=0}^{n-1} \alpha_{1,2i} a\langle b^2 \rangle + \sum_{i=0}^{n-1} \alpha_{1,2i+1} ab\langle b^2 \rangle \in \frac{D_{2n}}{\langle b^2 \rangle}$$

e seja $M = \rho(\alpha)$.

(i) Se $\bar{\alpha} = \langle b^2 \rangle$ ou $\bar{\alpha} = a\langle b^2 \rangle$, então M é uma matriz duplamente estocástica da forma $M = (m_{k\ell})$ tal que

$$\sum_{j=1}^n m_{2k-1,2j-1} = 1, \quad \sum_{j=1}^n m_{2k,2j-1} = 0, \quad \forall k, 1 \leq k \leq n,$$

e

$$\sum_{i=1}^n m_{2i-1, 2\ell-1} = 1, \quad \sum_{i=1}^n m_{2i-1, 2\ell} = 0, \quad \forall \ell, \quad 1 \leq \ell \leq n,$$

isto é, M é uma matriz duplamente estocástica tal que em toda linha (resp., coluna) ímpar, a soma de suas entradas que ocupam colunas (resp., linhas) ímpares é igual a 1, e em toda linha (resp., coluna) par, a soma de suas entradas que ocupam colunas (resp., linhas) ímpares é igual a 0. Ainda mais,

$$t_{11}(M) \equiv 0 \pmod{2n} \quad \text{e} \quad t_{00}(M) \equiv \begin{cases} 0 \pmod{2n}, & \text{se } \bar{\alpha} = \langle b^2 \rangle, \\ 2 \pmod{2n}, & \text{se } \bar{\alpha} = a \langle b^2 \rangle. \end{cases}$$

(ii) Se $\bar{\alpha} = b \langle b^2 \rangle$ ou $\bar{\alpha} = ab \langle b^2 \rangle$, então M é uma matriz duplamente estocástica da forma $M = (m_{k\ell})$ tal que

$$\sum_{j=1}^n m_{2k-1, 2j-1} = 0, \quad \sum_{j=1}^n m_{2k, 2j-1} = 1, \quad \forall k, \quad 1 \leq k \leq n,$$

e

$$\sum_{i=1}^n m_{2i-1, 2\ell-1} = 0, \quad \sum_{i=1}^n m_{2i-1, 2\ell} = 1, \quad \forall \ell, \quad 1 \leq \ell \leq n,$$

isto é, M é uma matriz duplamente estocástica tal que em toda linha (resp., coluna) ímpar, a soma de suas entradas que ocupam colunas (resp., linhas) ímpares é igual a 0, e em toda linha (resp., coluna) par, a soma de suas entradas que ocupam colunas (resp., linhas) ímpares é igual a 1. Ainda mais,

$$t_{00}(M) \equiv 0 \pmod{2n} \quad \text{e} \quad t_{11}(M) \equiv \begin{cases} 2 \pmod{2n}, & \text{se } \bar{\alpha} = b \langle b^2 \rangle, \\ 0 \pmod{2n}, & \text{se } \bar{\alpha} = ab \langle b^2 \rangle. \end{cases}$$

Demonstração. Como $\bar{\alpha} \in \frac{D_{2n}}{\langle b^2 \rangle}$, é imediato que α tem aumento

1 e, como $M = \rho(\alpha) = \sum_{i,j} \alpha_{ij} A^i B^j$, temos $M = (m_{k\ell})$, com

$$m_{k\ell} = \alpha_{0,k-\ell} + \alpha_{1,2n-k-\ell+2}, \quad \forall k, \ell, \quad 1 \leq k, \ell \leq 2n,$$

onde $k-\ell$ e $2n-k-\ell+2$ são considerados módulo $2n$. Então, $M = (m_{k\ell})$ é uma matriz duplamente estocástica tal que, para todo k , $1 \leq k \leq n$,

$$\sum_{j=1}^n m_{2k-1, 2j-1} = \sum_{j=1}^n \alpha_{0, 2k-2j} + \sum_{j=1}^n \alpha_{1, 2n-2k-2j+4} = \sum_{j=0}^{n-1} \alpha_{0, 2j} + \sum_{j=0}^{n-1} \alpha_{1, 2j},$$

$$\sum_{j=1}^n m_{2k, 2j-1} = \sum_{j=1}^n \alpha_{0, 2k-2j+1} + \sum_{j=1}^n \alpha_{1, 2n-2k-2j+3} = \sum_{j=0}^{n-1} \alpha_{0, 2j+1} + \sum_{j=0}^{n-1} \alpha_{1, 2j+1}$$

e, para todo ℓ , $1 \leq \ell \leq n$,

$$\sum_{i=1}^n m_{2i-1, 2\ell-1} = \sum_{i=1}^n \alpha_{0, 2i-2\ell} + \sum_{i=1}^n \alpha_{1, 2n-2i-2\ell+4} = \sum_{i=0}^{n-1} \alpha_{0, 2i} + \sum_{i=0}^{n-1} \alpha_{1, 2i},$$

$$\sum_{i=1}^n m_{2i-1, 2\ell} = \sum_{i=1}^n \alpha_{0, 2i-2\ell-1} + \sum_{i=1}^n \alpha_{1, 2n-2i-2\ell+3} = \sum_{i=0}^{n-1} \alpha_{0, 2i+1} + \sum_{i=0}^{n-1} \alpha_{1, 2i+1},$$

ainda mais,

$$t_{00}(M) = \sum_{i=1}^{2n} m_{ii} = \sum_{i=1}^{2n} (\alpha_{00} + \alpha_{1, 2n-2i+2}) = 2n \alpha_{00} + 2 \sum_{i=0}^{n-1} \alpha_{1, 2i}$$

e

$$t_{11}(M) = \sum_{i=1}^{2n} m_{\pi(a)\pi(b)i, i} = \sum_{i=1}^{2n} m_{2n-i+1, i} = \sum_{i=1}^{2n} (\alpha_{0, 2n-2i+1} + \alpha_{11}) = 2 \sum_{i=0}^{n-1} \alpha_{0, 2i+1} + 2n \alpha_{11}.$$

Se $\bar{\alpha} = \langle b^2 \rangle$, então

$$\sum_{i=0}^{n-1} \alpha_{0,2i} = 1, \quad \sum_{i=0}^{n-1} \alpha_{1,2i} = \sum_{i=0}^{n-1} \alpha_{0,2i+1} = \sum_{i=0}^{n-1} \alpha_{1,2i+1} = 0$$

e, se $\bar{\alpha} = \alpha \langle b^2 \rangle$, então

$$\sum_{i=0}^{n-1} \alpha_{1,2i} = 1, \quad \sum_{i=0}^{n-1} \alpha_{0,2i} = \sum_{i=0}^{n-1} \alpha_{0,2i+1} = \sum_{i=0}^{n-1} \alpha_{1,2i+1} = 0;$$

logo, pelos cálculos acima valem as relações de (i).

De forma análoga, podemos demonstrar (ii). Δ

Seja S_1 (resp., S_2) o conjunto das matrizes $X \in GL_{2n}(\mathbb{Z})$ que são duplamente estocásticas da forma $X = (x_{k\ell})$ tal que, para todo k , $1 \leq k \leq n$,

$$\sum_{j=1}^n x_{2k-1,2j-1} = 1, \quad \sum_{j=1}^n x_{2k,2j-1} = 0 \quad (\text{resp.}, \quad \sum_{j=1}^n x_{2k-1,2j} = 0, \quad \sum_{j=1}^n x_{2k,2j} = 1)$$

e, para todo ℓ , $1 \leq \ell \leq n$,

$$\sum_{i=1}^n x_{2i-1,2\ell-1} = 1, \quad \sum_{i=1}^n x_{2i-1,2\ell} = 0 \quad (\text{resp.}, \quad \sum_{i=1}^n x_{2i,2\ell-1} = 0, \quad \sum_{i=1}^n x_{2i,2\ell} = 1).$$

Seja, ainda, T_1 (resp., T_2) o subconjunto de S_1 (resp., S_2) constituído pelas matrizes $M = (m_{k\ell})$ tais que

(i) $m_{k\ell}$ satisfaz a relação (5);

(ii) $t_{11}(M) \equiv 0 \pmod{2n}$ (resp., $t_{00}(M) \equiv 0 \pmod{2n}$);

(iii) $t_{00}(M) \equiv 0 \pmod{2n}$ ou $t_{00}(M) \equiv 2 \pmod{2n}$ (resp., $t_{11}(M) \equiv 0 \pmod{2n}$ ou $t_{11}(M) \equiv 2 \pmod{2n}$).

Seja, finalmente, $T = T_1 \cup T_2$. Já vimos que $\rho(U_1(\mathbb{ZD}_{2n})) \subseteq T$; mais ainda, nossa caracterização de $U_1(\mathbb{ZD}_{2n})$ consistirá em mostrar que $U_1(\mathbb{ZD}_{2n}) \cong T$, onde o isomorfismo é dado pela restrição de ρ .

Para isso, precisaremos de alguns resultados e definições que introduzimos a seguir.

DEFINIÇÃO. Seja $M \in T$. Se $M \in T_1$, definimos

$$\mu = \mu(M) = \begin{cases} 1, & \text{se } t_{00}(M) \equiv 2 \pmod{2n} \\ 0, & \text{se } t_{00}(M) \equiv 0 \pmod{2n}. \end{cases}$$

Ainda, definimos os números

$$\gamma_{0,2k} = \gamma_{0,2k}(M) = \frac{t_{0,2k}(M) - 2\mu}{2n}, \quad \gamma_{0,2k+1} = \gamma_{0,2k+1}(M) = \frac{t_{0,2k+1}(M)}{2n},$$

$$\gamma_{1,2k} = \gamma_{1,2k}(M) = \frac{t_{1,2k}(M) + 2(\mu - 1)}{2n},$$

$$\gamma_{1,2k+1} = \gamma_{1,2k+1}(M) = \frac{t_{1,2k+1}(M)}{2n}, \quad \forall k, 0 \leq k \leq n-1,$$

e, finalmente, o elemento em $\mathbb{QD}_{2n}$

$$\gamma(M) = \sum \gamma_{ij} a^i b^j.$$

Analogamente, se $M \in T_2$, definimos

$$v = v(M) = \begin{cases} 1, & \text{se } t_{11}(M) \equiv 2 \pmod{2n}, \\ 0, & \text{se } t_{11}(M) \equiv 0 \pmod{2n}, \end{cases}$$

os números

$$\theta_{0,2k} = \theta_{0,2k}^{(M)} = \frac{t_{0,2k}^{(M)}}{2n}, \quad \theta_{0,2k+1} = \theta_{0,2k+1}^{(M)} = \frac{t_{0,2k+1}^{(M)} + 2(v-1)}{2n},$$

$$\theta_{1,2k} = \theta_{1,2k}^{(M)} = \frac{t_{1,2k}^{(M)}}{2n}, \quad \theta_{1,2k+1} = \theta_{1,2k+1}^{(M)} = \frac{t_{1,2k+1}^{(M)} - 2v}{2n},$$

$$\forall k, 0 \leq k \leq n-1,$$

e o elemento

$$\theta(M) = \sum \theta_{ij} a^i b^j.$$

O próximo passo será mostrar que, de fato, $\gamma = \gamma(M)$ (resp., $\theta = \theta(M)$) é um elemento de aumento 1 em $\mathbb{ZD}_{2n}$ tal que $\rho(\gamma) = M$ (resp., $\rho(\theta) = M$); mas antes precisamos dos Lemas (4.2) e (4.3), a seguir.

LEMA (4.2). Seja M uma matriz em S_1 ou S_2 . Se as entradas de M satisfazem a relação (5), então também satisfazem a relação (6).

Demonstração. Se as entradas de $M = (m_{k\ell})$ satisfazem (5), então

$$m_{k\ell} = -m_{k-\ell+3,1} - m_{k-\ell+5,1} - \dots - m_{k+\ell-3,1} + \\ + m_{k-\ell+2,2} + m_{k-\ell+4,2} + \dots + m_{k+\ell-2,2}, \quad \forall k, \ell, 1 \leq k \leq 2n, 3 \leq \ell \leq 2n,$$

onde $k-\ell+3, k-\ell+5, \dots, k+\ell-3, k-\ell+2, k-\ell+4, \dots, k+\ell-2$ são considerados módulo $2n$.

Por outro lado, se $M = (m_{k\ell}) \in S_1 \cup S_2$, então é imediato que

$$(7) \quad \sum_{i=1}^n m_{2i-1,1} = \sum_{i=1}^n m_{2i,2} \quad \text{e} \quad \sum_{i=1}^n m_{2i,1} = \sum_{i=1}^n m_{2i-1,1}.$$

A seguir, consideremos todos os índices módulo $2n$ e fixemos, inicialmente, k e ℓ , com $1 \leq k \leq 2n$ e $3 \leq \ell \leq 2n$. Então, de (5), temos

$$\begin{aligned} m_{k+n, \ell+n} &= m_{k-\ell+3,1}^{-} m_{k-\ell+5,1}^{-} \cdots m_{k+\ell-3,1}^{-} m_{k+\ell-1,1}^{-} m_{k+\ell+1,1}^{-} \cdots m_{k+\ell+2n-3,1}^{+} \\ &\quad + m_{k-\ell+2,2}^{+} m_{k-\ell+4,2}^{+} \cdots m_{k+\ell-2,2}^{+} m_{k+\ell,2}^{+} m_{k+\ell+2,2}^{+} \cdots m_{k+\ell+2n-2,2}^{+} = \\ &= m_{k-\ell+3,1}^{-} m_{k-\ell+5,1}^{-} \cdots m_{k+\ell-3,1}^{-} m_{k+\ell+2i-1,1}^{+} \sum_{i=0}^{n-1} \\ &\quad + m_{k-\ell+2,2}^{+} + m_{k-\ell+4,2}^{+} + \cdots + m_{k+\ell-2,2}^{+} + m_{k+\ell+2i,2}^{+} \sum_{i=0}^{n-1}; \end{aligned}$$

logo, de (5) e (7), segue

$$m_{k+n, \ell+n} = m_{k, \ell}, \quad \forall k, \ell, \quad 1 \leq k \leq 2n, \quad 3 \leq \ell \leq 2n.$$

Fixemos, agora, k , com $1 \leq k \leq 2n$, e $\ell=1$. Então, de (5), temos

$$\begin{aligned} m_{k+n, 1+n} &= m_{k+2,1}^{-} m_{k+4,1}^{-} \cdots m_{k+2n-2,1}^{-} m_{k+1,2}^{+} m_{k+3,2}^{+} \cdots m_{k+2n-1,2}^{+} = \\ &= - \sum_{i=1}^n m_{k+2i,1}^{-} + m_{k,1} + \sum_{i=1}^n m_{k+2i-1,2}^{+}; \end{aligned}$$

logo, de (7), segue

$$m_{k+n, 1+n} = m_{k,1}, \quad \forall k, \quad 1 \leq k \leq n.$$

Finalmente, de forma análoga à anterior, podemos provar que

$$m_{k+n, 2+n} = m_{k,2}, \quad \forall k, \quad 1 \leq k \leq n. \quad \Delta$$

LEMA (4.3). Sejam $M \in T$ e $t_{ij} = t_{ij}(M)$, $i=0,1$, $0 \leq j \leq 2n-1$.

Se $M \in T_1$, então,

(i) para todo $k, 0 \leq k \leq n-1$, $t_{0,2k+1} \equiv 0 \equiv t_{1,2k+1} \pmod{2n}$,

$t_{0,2k} \equiv t_{00} \pmod{2n}$ e $t_{00} + t_{1,2k} \equiv 2 \pmod{2n}$;

(ii) $\sum_{i=0}^{n-1} t_{0,2i} = 2n = \sum_{i=0}^{n-1} t_{1,2i}$ e $\sum_{i=0}^{n-1} t_{0,2i+1} = 0 = \sum_{i=0}^{n-1} t_{1,2i+1}$.

Se $M \in T_2$, então,

(iii) para todo $k, 0 \leq k \leq n-1$, $t_{0,2k} \equiv 0 \equiv t_{1,2k} \pmod{2n}$,

$t_{1,2k+1} \equiv t_{11} \pmod{2n}$ e $t_{0,2k+1} + t_{11} \equiv 2 \pmod{2n}$;

(iv) $\sum_{i=0}^{n-1} t_{0,2i} = 0 = \sum_{i=0}^{n-1} t_{1,2i}$ e $\sum_{i=0}^{n-1} t_{0,2i+1} = 2n = \sum_{i=0}^{n-1} t_{1,2i+1}$.

Demonstração. Se $M = (m_{kl}) \in T_1$, então m_{kl} satisfaz (5) e, pelo Lema (4.2), também satisfaz (6); ainda mais, $M \in S_1$ e, portanto, em particular, temos

$$(8) \quad \begin{aligned} m_{2n-1,1} &= 1 - \sum_{i=0}^{n-1} m_{2i-1,1}, & m_{2n,1} &= - \sum_{i=0}^{n-1} m_{2i,1}, \\ m_{2n-1,2} &= - \sum_{i=0}^{n-1} m_{2i-1,2} & \text{e} & \quad m_{2n,2} = 1 - \sum_{i=0}^{n-1} m_{2i,2}. \end{aligned}$$

A seguir, com as relações (5), (6) e (8), vamos calcular $t_{ij} = t_{ij}(M)$, $i = 0,1$, $0 \leq j \leq 2n-1$, em função de m_{kl} , $1 \leq k \leq 2n-2$, $l=1,2$.

Para $0 \leq k \leq n-2$, e considerando os índices módulo $2n$, temos

$$m_{n+2k-1,n-1} = m_{2k-3,1} + m_{2k-1,1} + m_{2k+1,1} - m_{2k-2,2} - m_{2k,2},$$

$$m_{n+2k,n} = m_{2k-1,1} + m_{2k+1,1} - m_{2k,2};$$

logo,

$$t_{0,2k} = 2(m_{11} + 2m_{31} + \dots + (k+1)m_{2k+1,1} - (n-k-2)m_{2k+3,1} - \dots - m_{2n-3,1} - \\ - m_{22} - 2m_{42} - \dots - km_{2k,2} + (n-k-1)m_{2k+2,2} + \dots + m_{2n-2,2}).$$

Da mesma forma, podemos calcular

$$t_{0,2n-2} = 2(m_{2n-1,1} + m_{2n,2} + m_{13} + m_{24} + \dots + m_{n-3,n-1} + m_{n-2,n}) = \\ = 2(n - (n-1)m_{11} - (n-2)m_{31} - \dots - (n-i)m_{2i-1,1} - \dots - m_{2n-3,1} - \\ - m_{22} - 2m_{42} - \dots - im_{2i,2} - \dots - (n-1)m_{2n-2,2}),$$

$$t_{10} = 2(m_{11} + m_{2n,2} + m_{2n-1,3} + m_{2n-2,4} + \dots + m_{n+3,n-1} + m_{n+2,n}) = \\ = 2(1 + (n-1)m_{11} + (n-2)m_{31} + \dots + (n-i)m_{2i-1,1} + \dots + m_{2n-3,1} - \\ - (n-1)m_{22} - (n-2)m_{42} - \dots - (n-i)m_{2i,2} - \dots - m_{2n-2,2}),$$

para $0 \leq k \leq n-2$,

$$t_{1,2n-2k-2} = 2(m_{2k+3,1} + m_{2k+2,2} + m_{2k+1,3} + m_{2k,4} + \dots + \\ + m_{2k-(k+2)+4,k+2} + m_{k+1,k+3} + m_{k,k+4} + m_{k-1,k+5} + \dots + \\ + m_{n+2k+5,n-1} + m_{n+2k+4,n}) = \\ = 2(1 - m_{11} - 2m_{31} - \dots - (k+1)m_{2k+1,1} + (n-k-2)m_{2k+3,1} + \dots + m_{2n-3,1} + \\ + m_{22} + 2m_{42} + \dots + (k+1)m_{2k+2,2} - (n-k-2)m_{2k+4,2} - \dots - m_{2n-2,2}),$$

para $1 \leq k \leq n-1$,

$$\begin{aligned}
 t_{0,2k-1} &= 2(m_{2k,1} + m_{2k+1,2} + m_{2k+2,3} + m_{2k+3,4} + \dots + \\
 &\quad + m_{2k+(n-k)-1,n-k} + m_{n+k,n-k+1} + m_{n+k+1,n-k+2} + m_{n+k+2,n-k+3} + \dots + \\
 &\quad + m_{n+2k-2,n-1} + m_{n+2k-1,n}) = \\
 &= 2(m_{21} + 2m_{41} + \dots + km_{2k,1} - (n-k-1)m_{2k+2,1} - \dots - m_{2n-2,1} - \\
 &\quad - m_{12} - 2m_{32} - \dots - km_{2k-1,2} + (n-k-1)m_{2k+1,2} + \dots + m_{2n-3,2}),
 \end{aligned}$$

$$\begin{aligned}
 t_{0,2n-1} &= 2(m_{2n,1} + m_{12} + m_{23} + m_{34} + \dots + m_{n-2,n-1} + m_{n-1,n}) = \\
 &= 2(-(n-1)m_{21} - (n-2)m_{41} - \dots - (n-i)m_{2i,1} - \dots - m_{2n-2,1} + \\
 &\quad + (n-1)m_{12} + (n-2)m_{32} + \dots + (n-i)m_{2i-1,2} + \dots + m_{2n-3,2}),
 \end{aligned}$$

$$\begin{aligned}
 t_{11} &= 2(m_{2n,1} + m_{2n-1,2} + m_{2n-2,3} + m_{2n-3,4} + \dots + m_{n+2,n-1} + m_{n+1,n}) = \\
 &= 2(-m_{21} - 2m_{41} - \dots - im_{2i,1} - \dots - (n-1)m_{2n-2,1} - \\
 &\quad - (n-1)m_{12} - (n-2)m_{32} - \dots - (n-i)m_{2i-1,2} - \dots - m_{2n-3,2}),
 \end{aligned}$$

para $0 \leq k \leq n-2$

$$\begin{aligned}
 t_{1,2n-2k-1} &= 2(m_{2k+2,1} + m_{2k+1,2} + m_{2k,3} + m_{2k-1,4} + \dots + \\
 &\quad + m_{2k-(k+2)+3,k+2} + m_{k,k+3} + m_{k-1,k+3} + m_{k-2,k+5} + \dots + \\
 &\quad + m_{n+2k+4,n-1} + m_{n+2k+3,n}) = \\
 &= 2(-m_{21} - 2m_{41} - \dots - km_{2k,1} + (n-k-1)m_{2k+2,1} + \dots + m_{2n-2,1} + \\
 &\quad + m_{12} + 2m_{32} + \dots + (k+1)m_{2k+1,2} - (n-k-2)m_{2k+3,2} - \dots - m_{2n-3,2}).
 \end{aligned}$$

Agora, é fácil ver que, para todo k , $0 \leq k \leq n-1$,

$$t_{0,2k} \equiv t_{00} \pmod{2n}, \quad t_{1,2k} \equiv t_{10} \pmod{2n},$$

$$t_{0,2k+1} \equiv t_{01} \pmod{2n}, \quad t_{1,2k+1} \equiv t_{11} \pmod{2n},$$

e ainda que

$$t_{00} + t_{10} = 2 + 2nm_{11}, \quad t_{0,2n-1} + t_{11} = -2n \sum_{i=1}^{n-1} m_{2i,1}.$$

Por outro lado, da condição (iii) do conjunto T_1 , temos $t_{11} \equiv 0 \pmod{2n}$.

Com isso, as relações de (i) são então imediatas.

A seguir, vamos calcular $\sum_{i=0}^{n-1} t_{0,2i}$, o que levará à primeira igualdade de (ii).

Para cada k , $2 \leq k \leq n-1$, os coeficientes de $m_{2k-1,1}$ em t_{00} , $t_{02}, \dots, t_{0,2k-4}, t_{0,2n-2}$ são iguais a $-(n-k)$, e em $t_{0,2k-2}, t_{0,2k}, \dots, t_{0,2n-4}$ são iguais a k ; logo, o coeficiente de $m_{2k-1,1}$ em $\sum_{i=0}^{n-1} t_{0,2i}$ é

$$-(n-k)k + k(n-k) = 0.$$

Para cada k , $1 \leq k \leq n-1$, os coeficientes de $m_{2k,2}$ em $t_{00}, t_{02}, \dots, t_{0,2k-2}$ são iguais a $(n-k)$, e em $t_{0,2k}, t_{0,2k+2}, \dots, t_{0,2n-2}$ são iguais a $-k$; logo, o coeficiente de $m_{2k,2}$ em $\sum_{i=0}^{n-1} t_{0,2i}$ é

$$(n-k)k - k(n-k) = 0.$$

Finalmente, é fácil ver que o coeficiente de m_{11} em $\sum_{i=0}^{n-1} t_{0,2i}$ é também igual a 0.

Com isso, é então imediato que $\sum_{i=0}^{n-1} t_{0,2i} = 2n$.

Da mesma forma, podemos obter as outras relações de (ii).

Suponhamos, agora, que $M = (m_{kl}) \in T_2$. Então, como antes, as entradas de M satisfazem (5) e (6); ainda mais, aqui $M \in S_2$ e, portanto, temos

$$(9) \quad \begin{aligned} m_{2n-1,1} &= - \sum_{i=1}^{n-1} m_{2i-1,1}, & m_{2n,1} &= 1 - \sum_{i=1}^{n-1} m_{2i,1}, \\ m_{2n-1,2} &= 1 - \sum_{i=1}^{n-1} m_{2i-1,2} & \text{e} & \quad m_{2n,2} = - \sum_{i=1}^{n-1} m_{2i,2}. \end{aligned}$$

Com isso, procedendo como no caso anterior, aqui usando as relações (5), (6) e (9), podemos calcular:

para $0 \leq k \leq n-2$,

$$\begin{aligned} t_{0,2k} &= 2(m_{11} + 2m_{31} + \dots + (k+1)m_{2k+1,1} - (n-k-2)m_{2k+3,1} - \dots - m_{2n-3,1} - \\ &\quad - m_{22} - 2m_{42} - \dots - km_{2k,2} + (n-k-1)m_{2k+2,2} + \dots + m_{2n-2,2}), \end{aligned}$$

$$\begin{aligned} t_{0,2n-2} &= 2(-(n-1)m_{11} - (n-2)m_{31} - \dots - (n-i)m_{2i-1,1} - \dots - m_{2n-3,1} - \\ &\quad - m_{22} - 2m_{42} - \dots - im_{2i,2} - \dots - (n-1)m_{2n-2,2}), \end{aligned}$$

$$\begin{aligned} t_{10} &= 2((n-1)m_{11} + (n-2)m_{31} + \dots + (n-i)m_{2i-1,1} + \dots + m_{2n-3,1} - \\ &\quad - (n-1)m_{22} - (n-2)m_{42} - \dots - (n-i)m_{2i,2} - \dots - m_{2n-2,2}), \end{aligned}$$

para $0 \leq k \leq n-2$,

$$\begin{aligned} t_{1,2n-2k-2} &= 2(-m_{11} - 2m_{31} - \dots - (k+1)m_{2k+1,1} + (n-k-2)m_{2k+3,1} + \dots + m_{2n-3,1} + \\ &\quad + m_{22} + 2m_{42} + \dots + (k+1)m_{2k+2,2} - (n-k-2)m_{2k+4,2} - \dots - m_{2n-2,2}), \end{aligned}$$

para $1 \leq k \leq n-1$,

$$t_{0,2k-1} = 2(1 + m_{21} + 2m_{41} + \dots + km_{2k,1} - (n-k-1)m_{2k+2,1} - \dots - m_{2n-2,1} - \\ - m_{12} - 2m_{32} - \dots - km_{2k-1,2} + (n-k-1)m_{2k+1,2} + \dots + m_{2n-3,2}),$$

$$t_{0,2n-1} = 2(1 - (n-1)m_{21} - (n-2)m_{41} - \dots - (n-i)m_{2i,1} - \dots - m_{2n-2,1} + \\ + (n-1)m_{12} + (n-2)m_{32} + \dots + (n-i)m_{2i-1,2} + \dots + m_{2n-3,2}),$$

$$t_{11} = 2(n - m_{21} - 2m_{41} - \dots - im_{2i,1} - \dots - (n-1)m_{2n-2,1} - \\ - (n-1)m_{12} - (n-2)m_{32} - \dots - (n-i)m_{2i-1,2} - \dots - m_{2n-3,2}),$$

para $0 \leq k \leq n-2$,

$$t_{1,2n-2k-1} = 2(-m_{21} - 2m_{41} - \dots - km_{2k,1} + (n-k-1)m_{2k+2,1} + \dots + m_{2n-2,1} + \\ + m_{12} + 2m_{32} + \dots + (k+1)m_{2k+1,2} - (n-k-2)m_{2k+3,2} - \dots - m_{2n-3,2}).$$

Agora, também neste caso é fácil ver que, para todo k ,

$0 \leq k \leq n-1$,

$$t_{0,2k} \equiv t_{00} \pmod{2n}, \quad t_{1,2k} \equiv t_{10} \pmod{2n},$$

$$t_{0,2k+1} \equiv t_{01} \pmod{2n}, \quad t_{1,2k+1} \equiv t_{11} \pmod{2n},$$

e ainda que

$$t_{00} + t_{10} = 2nm_{11}, \quad t_{0,2n-1} + t_{11} = 2 + 2n(1 - \sum_{i=1}^{n-1} m_{2i,1}).$$

Por outro lado, da condição (iii) do conjunto T_2 , temos $t_{00} \equiv 0 \pmod{2n}$.

Com isso, as relações de (iii) são então imediatas.

Finalmente, mais uma vez procedendo como no caso anterior, podemos verificar as relações de (iv). Δ

LEMA (4.4). Seja $M \in T$. Se $M \in T_1$, então

$$(i) \quad \gamma = \gamma(M) = \sum \gamma_{ij} a^i b^j \in \mathbb{Z}D_{2n};$$

$$(ii) \quad \text{um dos números } \sum_{i=0}^{n-1} \gamma_{0,2i}, \quad \sum_{i=0}^{n-1} \gamma_{0,2i+1}, \quad \sum_{i=0}^{n-1} \gamma_{1,2i},$$

$$\sum_{i=0}^{n-1} \gamma_{1,2i+1} \text{ é igual a 1 e os outros são iguais a 0;}$$

$$(iii) \quad \rho(\gamma) = M.$$

Se $M \in T_2$, então

$$(iv) \quad \theta = \theta(M) = \sum \theta_{ij} a^i b^j \in \mathbb{Z}D_{2n};$$

$$(v) \quad \text{um dos números } \sum_{i=0}^{n-1} \theta_{0,2i}, \quad \sum_{i=0}^{n-1} \theta_{0,2i+1}, \quad \sum_{i=0}^{n-1} \theta_{1,2i},$$

$$\sum_{i=0}^{n-1} \theta_{1,2i+1} \text{ é igual a 1 e os outros são iguais a 0;}$$

$$(vi) \quad \rho(\theta) = M.$$

Demonstração. (i) Por definição $\gamma = \sum \gamma_{ij} a^i b^j$, com

$$\gamma_{0,2k} = \frac{t_{0,2k}(M) - 2\mu}{2n}, \quad \gamma_{0,2k+1} = \frac{t_{0,2k+1}(M)}{2n},$$

$$\gamma_{1,2k} = \frac{t_{1,2k}(M) + 2(\mu-1)}{2n}, \quad \gamma_{1,2k+1} = \frac{t_{1,2k+1}(M)}{2n},$$

$$\forall k, 0 \leq k \leq n-1,$$

onde $\mu=0$ ou $\mu=1$ conforme $t_{00}(M) \equiv 0 \pmod{2n}$ ou $t_{00}(M) \equiv 2 \pmod{2n}$, respectivamente. Então, pelo Lema (4.3), parte (i), é fácil ver que $\gamma_{ij} \in \mathbb{Z}$, para quaisquer $i, j, i=0, 1, 0 \leq j \leq 2n-1$; logo, $\gamma \in \mathbb{Z}D_{2n}$.

(ii) Pelo Lema (4.3), parte (ii), temos

$$\sum_{i=0}^{n-1} t_{0,2i}(M) = 2n = \sum_{i=0}^{n-1} t_{1,2i}(M) \text{ e } \sum_{i=0}^{n-1} t_{0,2i+1}(M) = 0 = \sum_{i=0}^{n-1} t_{1,2i+1}(M).$$

Com isto,

$$\sum_{i=0}^{n-1} \gamma_{0,2i} = \frac{1}{2n} \left(\sum_{i=0}^{n-1} t_{0,2i}(M) - 2n\mu \right) = 1 - \mu,$$

$$\sum_{i=0}^{n-1} \gamma_{0,2i+1} = \frac{1}{2n} \sum_{i=0}^{n-1} t_{0,2i+1}(M) = 0,$$

$$\sum_{i=0}^{n-1} \gamma_{1,2i} = \frac{1}{2n} \left(\sum_{j=0}^{n-1} t_{1,2i}(M) + 2n(\mu-1) \right) = \mu$$

e

$$\sum_{i=0}^{n-1} \gamma_{1,2i+1} = \frac{1}{2n} \sum_{i=0}^{n-1} t_{1,2i+1}(M) = 0,$$

onde $\mu = 0$ ou $\mu = 1$; logo, é claro que um dos núemros $\sum_{i=0}^{n-1} \gamma_{0,2i}$, $\sum_{i=0}^{n-1} \gamma_{0,2i+1}$, $\sum_{i=0}^{n-1} \gamma_{1,2i}$, $\sum_{i=0}^{n-1} \gamma_{1,2i+1}$ é igual a 1 e os outros são iguais a 0.

(iii) Se $M = (m_{kl}) \in T_1$, então suas entradas satisfazem (5) e (8).

Por outro lado, de (i) e da demonstração de (ii), temos que $\gamma = \gamma(M) = \sum_{i,j} \gamma_{ij} a^i b^j$ é um elemento de aumento 1 em $\mathbb{Z}D_{2n}$ com $\sum_{i=0}^{n-1} \gamma_{0,2i+1} = 0 = \sum_{i=0}^{n-1} \gamma_{1,2i+1}$. Então, as entradas da matriz $\rho(\gamma) = \sum_{i,j} \gamma_{ij} A^i B^j$ satisfazem relações análogas às de (4), (5) e (8); isto é, $\rho(\gamma) = (s_{kl})$, com

$$s_{kl} = \gamma_{0,k-l} + \gamma_{1,2n-k-l+2}, \quad \forall k, l, 1 \leq k, l \leq 2n,$$

onde $k-l$ e $2n-k-l+2$ são considerados módulo $2n$,

$$s_{k,l} = -s_{k-l+3,1} - s_{k-l+5,1} - \dots - s_{k+l-3,1} + s_{k-l+2,2} + s_{k-l+4,2} + \dots + s_{k+l-2,2},$$

$$\forall k, l, 1 \leq k \leq 2n, 3 \leq l \leq 2n,$$

onde $k-l+3, k-l+5, k+l-3, k-l+2, k-l+4, \dots, k+l-2$ são considerados módulo $2n$ e, finalmente,

$$s_{2n-1,1} = 1 - \sum_{i=1}^{n-1} s_{2i-1,1}, \quad s_{2n,1} = - \sum_{i=1}^{n-1} s_{2i,1},$$

$$s_{2n-1,2} = - \sum_{i=1}^{n-1} s_{2i-1,2} \quad \text{e} \quad s_{2n,2} = 1 - \sum_{i=1}^{n-1} s_{2i,2}.$$

Assim, é suficiente verificarmos que $\rho(\gamma)$ e M têm entradas iguais nas posições (k, l) , $1 \leq k \leq 2n-2$, $l=1,2$, o que é equivalente a mostrar que

$$\begin{aligned} \gamma_{00} + \gamma_{10} &= m_{11}, & \gamma_{0,2n-1} + \gamma_{1,2n-1} &= m_{12}, \\ \gamma_{01} + \gamma_{1,2n-1} &= m_{21}, & \gamma_{00} + \gamma_{1,2n-2} &= m_{22}, \\ \dots & & \dots & \\ \gamma_{0i} + \gamma_{1,2n-i} &= m_{i+1,1}, & \gamma_{0i} + \gamma_{1,2n-i-2} &= m_{i+2,2}, \\ \dots & & \dots & \\ \gamma_{0,2n-3} + \gamma_{13} &= m_{2n-2,1}, & \gamma_{0,2n-4} + \gamma_{12} &= m_{2n-2,2}. \end{aligned}$$

Para isso, usaremos os cálculos de $t_{ij} = t_{ij}(M)$, $i=0,1$, $0 \leq j \leq 2n-1$, efetuados no Lema (4.3).

Se i é par, $2 \leq i \leq 2n-4$, podemos escrever $i=2k$, com $1 \leq k \leq n-2$; logo,

$$\gamma_{0i} + \gamma_{1,2n-i} = \gamma_{0,2k} + \gamma_{1,2n-2k} =$$

$$= \frac{1}{2n} (t_{0,2k} + t_{1,2n-2k} - 2) =$$

$$\begin{aligned} &= \frac{2}{2n} (m_{11} + 2m_{31} + \dots + km_{2k-1,1} + (k+1)m_{2k+1,1} - (n-k-2)m_{2k+3,1} - \dots - m_{2n-3,1} - \\ &\quad - m_{22} - 2m_{42} - \dots - km_{2k,2} + (n-k-1)m_{2k+2,2} + \dots + m_{2n-2,2} + \\ &\quad + 1 - m_{11} - 2m_{31} - \dots - km_{2k-1,1} + (n-k-1)m_{2k+1,1} + (n-k-2)m_{2k+3,1} + \dots + m_{2n-3,1} + \\ &\quad + m_{22} + 2m_{42} + \dots + km_{2k,2} - (n-k-1)m_{2k+2,2} - \dots - m_{2n-2,2} - 1) = \\ &= \frac{1}{n} (nm_{2k+1,1}) = m_{2k+1,1} = m_{i+1,1}, \end{aligned}$$

e

$$\gamma_{0i} + \gamma_{1,2n-i-2} = \gamma_{0,2k} + \gamma_{0,2n-2k-2} =$$

$$= \frac{1}{2n} (t_{0,2k} + t_{0,2n-2k-2} - 2) =$$

$$\begin{aligned} &= \frac{2}{2n} (m_{11} + 2m_{31} + \dots + (k+1)m_{2k+1,1} - (n-k-2)m_{2k+3,1} - \dots - m_{2n-3,1} - \\ &\quad - m_{22} - 2m_{42} - \dots - km_{2k,2} + (n-k-1)m_{2k+2,2} + (n-k-2)m_{2k+4,2} + \dots + m_{2n-2,2} + \\ &\quad + 1 - m_{11} - 2m_{31} - \dots - (k+1)m_{2k+1,1} + (n-k-2)m_{2k+3,1} + \dots + m_{2n-3,1} + \\ &\quad + m_{22} + 2m_{42} + \dots + km_{2k,2} + (k+1)m_{2k+2,2} - (n-k-2)m_{2k+4,2} - \dots - m_{2n-2,2} - 1) = \\ &= \frac{1}{n} (nm_{2k+2,2}) = m_{2k+2,2} = m_{i+2,2}. \end{aligned}$$

Da mesma forma, se i é ímpar, $1 \leq i \leq 2n-5$, podemos escrever $i=2k-1$, com $1 \leq k \leq n-1$, e calcular

$$\gamma_{0i} + \gamma_{1,2n-i} = \gamma_{0,2k-1} + \gamma_{1,2n-2k+1} = m_{2k,1} = m_{i+1,1}$$

e

$$\gamma_{0i} + \gamma_{1,2n-i-2} = \gamma_{0,2k-1} + \gamma_{1,2n-2k-1} = m_{2k+1,2} = m_{i+2,2}.$$

Finalmente, também da mesma forma, podemos calcular

$$\gamma_{00} + \gamma_{10} = m_{11}, \quad \gamma_{00} + \gamma_{1,2n-2} = m_{22},$$

$$\gamma_{0,2n-3} + \gamma_{13} = m_{2n-2,1} \quad \text{e} \quad \gamma_{0,2n-1} + \gamma_{1,2n-1} = m_{12}.$$

Agora, é claro que as demonstrações de (iv), (v) e (vi) são análogas às de (i), (ii) e (iii), respectivamente. Δ

Os Lemas (4.5) e (4.6), que seguem, conduzirão à prova de que $\gamma = \gamma(M)$ e $\theta = \theta(M)$ são ainda unidades em $\mathbb{Z}D_{2n}$.

LEMA (4.5). Se X é uma matriz em S_1 (resp., S_2), então X^{-1} também é uma matriz em S_1 (resp., S_2).

Demonstração. Se $X \in S_1$, então X é uma matriz duplamente estocástica da forma $X = (x_{k\ell})$ tal que

$$(10) \quad \sum_{j=1}^n x_{2k-1,2j-1} = 1, \quad \sum_{j=1}^n x_{2k,2j-1} = 0, \quad \forall k, \quad 1 \leq k \leq n, \text{ e}$$

$$(11) \quad \sum_{i=1}^n x_{2i-1,2\ell-1} = 1, \quad \sum_{i=1}^n x_{2i-1,2\ell} = 0, \quad \forall \ell, \quad 1 \leq \ell \leq n.$$

Do Lema (2.5), já sabemos que X^{-1} é duplamente estocástica.

Por outro lado, se D é o determinante de X e, para quais-

quer i e j , $1 \leq i \leq 2n$, D_{ij} é o cofator de x_{ij} , então $X^{-1} = (y_{ij})$, onde

$$y_{ij} = \frac{D_{ji}}{D}, \quad \forall i, j, \quad 1 \leq i, j \leq 2n.$$

Com isto e de (10), temos que, para todo k , $1 \leq k \leq n$,

$$\begin{aligned} \sum_{j=1}^n y_{2k-1, 2j-1} &= \frac{1}{D} \sum_{j=1}^n D_{2j-1, 2k-1} = \\ &= \frac{1}{D} \sum_{j=1}^n \sum_{i=1}^n x_{2j-1, 2i-1} D_{2j-1, 2k-1} + \frac{1}{D} \sum_{j=1}^n \sum_{i=1}^n x_{2j, 2i-1} D_{2j, 2k-1} = \\ &= \frac{1}{D} \sum_{j=1}^{2n} \sum_{i=1}^n x_{j, 2i-1} D_{j, 2k-1} = \frac{1}{D} \sum_{j=1}^{2n} x_{j, 2k-1} D_{j, 2k-1} = 1, \end{aligned}$$

e

$$\begin{aligned} \sum_{j=1}^n y_{2k, 2j-1} &= \frac{1}{D} \sum_{j=1}^n D_{2j-1, 2k} = \\ &= \frac{1}{D} \sum_{j=1}^n \sum_{i=1}^n x_{2j-1, 2i-1} D_{2j-1, 2k} + \frac{1}{D} \sum_{j=1}^n \sum_{i=1}^n x_{2j, 2i-1} D_{2j, 2k} = \\ &= \frac{1}{D} \sum_{j=1}^{2n} \sum_{i=1}^n x_{j, 2i-1} D_{j, 2k} = 0. \end{aligned}$$

Analogamente, de (11), podemos provar que, para todo ℓ , $1 \leq \ell \leq n$,

$$\sum_{i=1}^n y_{2i-1, 2\ell-1} = 1 \quad \text{e} \quad \sum_{i=1}^n y_{2i-1, 2\ell} = 0.$$

Assim, $X^{-1} \in S_1$ e, é claro, que se $X \in S_2$, então podemos repetir o mesmo argumento e provar que $X^{-1} \in S_2$. Δ

LEMA (4.6). Se M é uma matriz em T_2 (resp., T_2), então X^{-1} também é uma matriz em T_1 (resp., T_2).

Demonstração. Seja $M \in T_1$. Então, do lema anterior, já sabemos que $M^{-1} \in S_1$ e, a seguir, provaremos que M^{-1} satisfaz as outras condições do conjunto T_1 .

Seja χ o polinômio característico de M . Então, como $M \in GL_{2n}(\mathbb{Z})$, podemos escrever $\chi = X^{2n} + \sum_{i=0}^{2n-1} x_i X^i$, com $x_i \in \mathbb{Z}$, $0 \leq i \leq 2n-1$, e $x_0 = D$, onde $D = \pm 1$ é o determinante de M ; logo,

$$-D = M^{2n} + \sum_{i=1}^{2n-1} x_i M^i = M(M^{2n-1} + \sum_{i=1}^{2n-1} x_i M^{i-1}),$$

donde

$$M^{-1} = -D(M^{2n-1} + \sum_{i=1}^{2n-1} x_i M^{i-1}).$$

Pelo Lema (4.4), partes (i) e (iii), temos que para cada i , $1 \leq i \leq 2n$, $M^i = \rho(\gamma^i)$, onde $\gamma = \gamma(M) = \sum \gamma_{ij} a^i b^j \in \mathbb{ZD}_{2n}$; logo, $M^{-1} \in \rho(\mathbb{ZD}_{2n})$ e, portanto, M^{-1} satisfaz a condição (i) do conjunto T_1 .

Sejam $s_{00} = t_{00}(M^{-1})$ e $s_{11} = t_{11}(M^{-1})$ e, para cada k , $2 \leq k \leq 2n$, sejam $t_{00}^{(k)} = t_{00}(M^k)$ e $t_{11}^{(k)} = t_{11}(M^k)$.

Da demonstração do Lema (4.4), parte (ii), temos

$$\sum_{i=0}^{n-1} \gamma_{0,2i} = 1 - \mu, \quad \sum_{i=0}^{n-1} \gamma_{0,2i+1} = 0, \quad \sum_{i=0}^{n-1} \gamma_{1,2i} = \mu \quad \text{e} \quad \sum_{i=0}^{n-1} \gamma_{1,2i+1} = 0,$$

onde $\mu = 0$ ou $\mu = 1$ conforme $t_{00} = t_{00}(M) \equiv 0 \pmod{2n}$ ou $t_{00} = t_{00}(M) \equiv 2 \pmod{2n}$, respectivamente.

Se $t_{00} \equiv 0 \pmod{2n}$, então $\bar{\gamma} = g(\gamma) = \langle b^2 \rangle$; logo, para cada k , $2 \leq k \leq 2n$, $\bar{\gamma}^k = \langle b^2 \rangle$ e, portanto, pelo Lema (4.1), parte (i), temos

$$t_{00}^{(k)} = t_{00}(M^k) = t_{00}(\rho(\gamma^k)) \equiv 0 \pmod{2n}$$

e

$$t_{11}^{(k)} = t_{11}(M^k) = t_{11}(\rho(\gamma^k)) \equiv 0 \pmod{2n}.$$

Conseqüentemente, $s_{00} \equiv 0 \equiv s_{11} \pmod{2n}$, donde M^{-1} satisfaz as condições (ii) e (iii) do conjunto T_1 .

Agora, se $t_{00} \equiv 2 \pmod{2n}$, então $\bar{\gamma} = a\langle b^2 \rangle$; logo, se k é ímpar, $3 \leq k \leq 2n-1$, $\bar{\gamma}^k = a\langle b^2 \rangle$ e, portanto, pelo Lema (4.1), parte (i), temos

$$t_{00}^{(k)} \equiv 2 \pmod{2n} \quad \text{e} \quad t_{11}^{(k)} \equiv 0 \pmod{2n},$$

e, se k é par, $2 \leq k \leq 2n$, $\bar{\gamma}^k = \langle b^2 \rangle$ e, portanto, pelo Lema (4.1), parte (i), temos

$$t_{00}^{(k)} \equiv 0 \equiv t_{11}^{(k)} \pmod{2n}.$$

Conseqüentemente, $s_{11} \equiv 0 \pmod{2n}$, donde M^{-1} satisfaz a condição (ii) do conjunto T_1 , e

$$s_{00} \equiv -D(2 + 2 \sum_{i=1}^{n-1} x_{2i}) \pmod{2n}.$$

Por outro lado, se $N = M^{2n} + \sum_{i=1}^{2n-1} x_i M^i = -D$, $u_{00} = t_{00}(N)$ e x é a soma das entradas de N que ocorrem nas linhas ímpares da primeira coluna, então, pelo Lema (4.1), parte (i),

$$u_{00} \equiv 2 \sum_{i=1}^n x_{2i-1} \equiv -2nD \equiv 0 \pmod{2n} \text{ e } x = 1 + \sum_{i=1}^{2n-1} x_i = -D;$$

logo,

$$s_{00} \equiv -D(2 + 2 \sum_{i=1}^{n-1} x_{2i}) \equiv -D(2 + 2 \sum_{i=1}^{2n-1} x_i) \equiv 2D^2 \equiv 2 \pmod{2n}$$

e, portanto, M^{-1} satisfaz a condição (iii) do conjunto T_1 .

Assim, $M^{-1} \in T_1$ e é claro que com o mesmo argumento podemos provar que se $M \in T_2$, então $M^{-1} \in T_2$. Δ

O resultado principal desta seção é, agora, dado pelo

TEOREMA (4.7). A restrição $\rho: U_1(\mathbb{ZD}_{2n}) \rightarrow T$ é um isomorfismo.

Demonstração. Seja

$$W = \{\alpha \in \mathbb{ZD}_{2n} : \bar{\alpha} = g(\alpha) \in \frac{D_{2n}}{\langle b^2 \rangle}\}.$$

Seja I a matriz identidade $2n \times 2n$ e seja $\alpha = \sum_{i,j} \alpha_{ij} a^i b^j \in W$ tal que $\rho(\alpha) = I$. Mostraremos, nestas condições, que $\alpha = 1$.

$$\text{Como } \alpha \in W, \text{ um dos números } \sum_{i=0}^{n-1} \alpha_{0,2i}, \sum_{i=0}^{n-1} \alpha_{0,2i+1}, \sum_{i=0}^{n-1} \alpha_{1,2i},$$

$\sum_{i=0}^{n-1} \alpha_{1,2i+1}$ é igual a 1 e os outros são iguais a 0. Por outro lado, a matriz $\rho(\alpha) = \sum_{i,j} \alpha_{ij} A^i B^j$ é da forma $\rho(\alpha) = (m_{k\ell})$, com

$$m_{k\ell} = \alpha_{0,k-\ell} + \alpha_{1,2n-k-\ell+2}, \quad \forall k, \ell, \quad 1 \leq k, \ell \leq 2n,$$

onde $k-\ell$ e $2n-k-\ell+2$ são considerados módulo $2n$. Assim, como $\rho(\alpha) = (m_{k\ell}) = I$, temos

$$t_{00}(\rho(\alpha)) = 2n\alpha_{00} + 2 \sum_{i=0}^{n-1} \alpha_{1,2i} = 2n \geq 4;$$

$$\text{logo, } \sum_{i=0}^{n-1} \alpha_{1,2i} = 0 \text{ e } \alpha_{00} = 1.$$

Agora, as entradas na diagonal principal de $\rho(\alpha)$ são iguais a $m_{kk} = \alpha_{00} + \alpha_{1,2n-2k+2}$, $1 \leq k \leq 2n$; logo, para todo k , $0 \leq k \leq n-1$, $\alpha_{00} + \alpha_{1,2k} = 1$, donde $\alpha_{1,2k} = 0$.

Além disso, as entradas na primeira coluna de $\rho(\alpha)$, que ocorrem nas linhas ímpares, a menos da posição $(1,1)$, são iguais a $m_{2k-1,1} = \alpha_{0,2k-2} + \alpha_{1,2n-2k+2}$, $2 \leq k \leq n$; logo, para todo k , $1 \leq k \leq n-1$, $\alpha_{0,2k} + \alpha_{1,2n-2k} = 0$, donde $\alpha_{0,2k} = 0$.

Assim, $\sum_{i=0}^{n-1} \alpha_{0,2i} = 1$ e, portanto, deve ocorrer $\sum_{i=0}^{n-1} \alpha_{1,2i+1} = 0$. Por outro lado, para todo k , $0 \leq k \leq n-1$,

$$t_{0,2k+1}(\rho(\alpha)) = 2n\alpha_{0,2k+1} + 2 \sum_{i=0}^{n-1} \alpha_{1,2i+1} = t_{0,2k+1}(I) = 0;$$

logo, para todo k , $0 \leq k \leq n-1$, $\alpha_{0,2k+1} = 0$.

Finalmente, as entradas na primeira coluna de $\rho(\alpha)$, que ocorrem nas linhas pares, são iguais a $m_{2k,1} = \alpha_{0,2k-1} + \alpha_{1,2n-2k+1}$, $1 \leq k \leq n$; logo, para todo k , $0 \leq k \leq n-1$, $\alpha_{0,2k+1} + \alpha_{1,2n-2k-1} = 0$, donde $\alpha_{1,2k+1} = 0$.

Portanto, $\alpha=1$ e, como $U_1(\mathbb{ZD}_{2n}) \subseteq W$, temos que $\rho: U_1(\mathbb{ZD}_{2n}) \rightarrow T$ é um monomorfismo.

Seja, agora, $M \in T$. Se $M \in T_1$, então, pelo Lema (4.4), partes (i), (ii) e (iii), $M = \rho(\gamma)$, onde $\gamma = \gamma(M) \in W$.

Além disso, pelo Lema (4.6), $M^{-1} \in T_1$ e, então, pelo Lema (4.4), partes (i), (ii) e (iii), $M^{-1} = \rho(l)$, onde $l = \gamma(M^{-1}) \in W$.

Assim, $I = MM^{-1} = \rho(\gamma_1)$, com $\gamma_1 \in W$, donde $\gamma_1 = 1$; logo, γ é uma unidade e, portanto, $\rho: U_1(\mathbb{Z}D_{2n}) \rightarrow T$ é um epimorfismo. Δ

CAPÍTULO III

AS UNIDADES EM $\mathbb{ZD}_3$ E $\mathbb{ZD}_4$

Usaremos aqui a mesma notação introduzida no capítulo anterior.

Assim, vamos especializar a caracterização de $U_1(\mathbb{ZD}_m)$, para $m=3$ e $m=4$; ainda mais, daremos exemplos, para valores pequenos de m , que mostram a independência de algumas das condições que definem os conjuntos V , T_1 e T_2 e, finalmente, vamos calcular, nas caracterizações obtidas, a imagem dos conjuntos

$$U(\mathbb{ZD}_3) \cap (1 + \Delta(D_3)\Delta(\langle b \rangle)) \text{ e } U(\mathbb{ZD}_4) \cap (1 + \Delta(D_4)\Delta(\langle b^2 \rangle)).$$

Tais conjuntos são complementos normais livres de torção para D_3 e D_4 em $U_1(\mathbb{ZD}_3)$ e $U_1(\mathbb{ZD}_4)$, respectivamente, e foram determinados por G.H. Cliff, S.K. Sehgal e A.R. Weiss em [4], onde trabalharam num contexto mais geral de grupos metabelianos.

Observamos que para o caso $m=3$ os resultados serão os mesmos de P.J. Allen e C. Hobby em [3].

5. CARACTERIZAÇÕES DE $U_1(\mathbb{ZD}_3)$ E $U_1(\mathbb{ZD}_4)$.

Seja $M \in GL_3(\mathbb{Z})$ uma matriz duplamente estocástica. Mostraremos que M satisfaz também as condições (ii) e (iii) do conjunto V considerado para $n=1$.

Para isso, vamos proceder como em [3, Lema 2].

Inicialmente, escrevemos M na forma

$$M = \begin{bmatrix} s & u & 1-s-u \\ t & v & 1-t-v \\ 1-s-t & 1-u-v & -1+s+t+u+v \end{bmatrix},$$

com $s, t, u, v \in \mathbb{Z}$.

Assim, denotando por $m_{k\ell}$ a entrada de M na posição (k, ℓ) , $1 \leq k, \ell \leq 3$, é fácil ver que

$$m_{13} = -m_{11} + m_{32} + m_{22},$$

$$m_{23} = -m_{21} + m_{12} + m_{32},$$

e

$$m_{33} = -m_{31} + m_{22} + m_{12};$$

logo, M satisfaz a condição (ii) do conjunto V .

Agora, calculamos o determinante de M , módulo 3, da seguinte maneira: somamos as duas primeiras linhas à terceira linha, obtendo

$$|M| = \begin{vmatrix} s & u & 1-s-u \\ t & v & 1-t-v \\ 1 & 1 & 1 \end{vmatrix};$$

em seguida, somamos as duas primeiras colunas à terceira coluna, obtendo

$$|M| = \begin{vmatrix} s & u & 1 \\ t & v & 1 \\ 1 & 1 & 3 \end{vmatrix}$$

e, finalmente, subtraímos a segunda coluna da primeira coluna, obtendo

$$|M| \equiv \begin{vmatrix} s-u & u & 1 \\ t-v & v & 1 \\ 0 & 1 & 0 \end{vmatrix} \pmod{3}$$

Assim, desde que $M \in GL_3(\mathbb{Z})$, e desenvolvendo o determinante acima pela terceira linha, temos

$$\pm 1 \equiv -s + u + t - v \pmod{3}.$$

Por outro lado,

$$t_{00}(M) = -1 + 2s + t + u + 2v \equiv -1 - s + t + u - v \pmod{3}.$$

Com isso,

$$\pm 1 \equiv 1 + t_{00}(M) \pmod{3};$$

logo, $t_{00}(M) \equiv 0 \pmod{3}$ ou $t_{00}(M) \equiv 1 \pmod{3}$ e, portanto, M satisfaz também a condição (iii) do conjunto V .

Dessa forma, fica provado o seguinte

TEOREMA (5.1) [3, Teorema 1]. O grupo $U_1(\mathbb{Z}D_3)$ é isomorfo ao subgrupo das matrizes duplamente estocásticas de $GL_3(\mathbb{Z})$.

Consideramos importante observar que para matrizes em $GL_5(\mathbb{Z})$ a condição (iii) do conjunto V , aqui considerado para $n=2$, não é consequência das demais condições que definem este conjunto. De fato, a matriz

$$M = \begin{bmatrix} s_1 & t_1 & 1-s_1-t_1-t_3-t_4 & -1+s_1+s_3+s_4+t_1+t_3+t_4 & 1-s_1-s_3-s_4-t_1 \\ s_2 & t_2 & -s_2+t_1+t_3 & 1-s_1-s_3-t_1-t_3 & s_1+s_3-t_2 \\ s_3 & t_3 & -s_3+t_2+t_4 & 1-s_2-s_4-t_2-t_4 & s_2+s_4-t_3 \\ s_4 & t_4 & 1-s_4-t_1-t_2-t_4 & -1+s_1+s_2+s_4+t_1+t_2+t_4 & 1-s_1-s_2-s_4-t_4 \\ 1-\sum_{i=1}^4 s_i & 1-\sum_{i=1}^4 t_i & -1+\sum_{i=1}^4 s_i+t_1+t_4 & -1-s_1-s_4-t_1-t_4 & -1+s_1+s_4+\sum_{i=1}^4 t_i \end{bmatrix}$$

satisfaz as condições (i) e (ii) do conjunto V, com

$$t_{oo}(M) = -2+3s_1+s_2-s_3+2s_4+2t_1+4t_2+t_3+3t_4.$$

Agora, fazendo $s_2=1$ e $s_1=0=s_3=s_4=t_1=t_2=t_3=t_4$, obtemos

$$t_{oo}(M) = -1,$$

e calculando o determinante de M, obtemos

$$|M| = \begin{vmatrix} 0 & 0 & 1 & -1 & 1 \\ 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & -1 \end{vmatrix} = -1;$$

logo, M satisfaz todas as condições do conjunto V, exceto a condição (iii).

Passamos, agora, à caracterização de $U_1(\mathbb{ZD}_4)$.

Seja $M \in GL_4(\mathbb{Z})$ uma matriz no conjunto $S = S_1 \cup S_2$, onde S_1 e S_2 são considerados para $n=2$. Ainda mais, suponhamos que se $M \in S_1$, então $t_{11}(M) \equiv 0 \pmod{4}$ e se $M \in S_2$, então $t_{00}(M) \equiv 0 \pmod{4}$. Mostremos que, nestas condições, M é uma matriz no conjunto $T = T_1 \cup T_2$, onde T_1 e T_2 são considerados para $n=2$.

Se $M \in S_1$, então M é da forma

$$M = \begin{bmatrix} s & u & 1-s & -u \\ t & v & -t & 1-v \\ 1-s & -u & s & u \\ -t & 1-v & t & v \end{bmatrix},$$

com $s, t, u, v \in \mathbb{Z}$ e $t_{11}(M) = -2(t+u) \equiv 0 \pmod{4}$.

Com isso, é fácil ver que M satisfaz as condições (i) e (ii) do conjunto T_1 . Além disso, como $t_{00}(M) = 2(s+v)$, é imediato que $t_{00}(M) \equiv 0 \pmod{4}$ ou $t_{00}(M) \equiv 2 \pmod{4}$; logo, M satisfaz também a condição (iii) do conjunto T_1 e, portanto, $M \in T_1$.

Da mesma forma, se $M \in S_2$, então podemos provar que $M \in T_2$.

Assim, fica demonstrado o seguinte

TEOREMA (5.2). O grupo $U_1(\mathbb{ZD}_4)$ é isomorfo ao grupo das matrizes $M \in GL_4(\mathbb{Z})$ que satisfazem uma das condições:

- (i) $M \in S_1$ e $t_{11}(M) \equiv 0 \pmod{4}$;
- (ii) $M \in S_2$ e $t_{00}(M) \equiv 0 \pmod{4}$.

Observamos que a condição $t_{11}(M) \equiv 0 \pmod{4}$ não é consequência do fato de M ser uma matriz em S_1 . Com efeito, a matriz

$$X = \begin{bmatrix} 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 1 \\ 1 & -1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \in S_1,$$

mas $t_{11}(X) \equiv 2 \pmod{4}$.

Analogamente, a condição $t_{00}(M) \equiv 0 \pmod{4}$ não é consequência do fato de M ser uma matriz em S_2 . Com efeito, a matriz

$$X = \begin{bmatrix} 1 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 \\ -1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \in S_2,$$

mas $t_{00}(X) \equiv 2 \pmod{4}$.

Terminaremos esta seção mostrando que para matrizes em $GL_6(\mathbb{Z})$ a condição (iii) do conjunto T_1 (resp., T_2) é consequência das demais condições que definem este conjunto, mas que o mesmo não ocorre para matrizes em $GL_8(\mathbb{Z})$.

Seja $M \in GL_6(\mathbb{Z})$ uma matriz no conjunto S_1 . Ainda mais, suponhamos que M satisfaça as condições (i) e (ii) do conjunto T_1 . Mostraremos que, nestas condições, $t_{00} = t_{00}(M) \equiv 0 \pmod{6}$ ou $t_{00} = t_{00}(M) \equiv 2 \pmod{6}$.

Inicialmente, escrevemos M na forma

$$M = \begin{bmatrix} s & w & 1-s-z & v & z & -v-w \\ t & x & -t+w+y & 1-s-u & -w-y & s+u-x \\ u & y & -u+x+z & -t-v & 1-x-z & t+v-y \\ v & z & -v-w & s & w & 1-s-z \\ 1-s-u & -w-y & s+u-x & t & x & -t+w+y \\ -t-v & 1-x-z & t+v-y & u & y & -u+x+z \end{bmatrix}$$

com $t_{11} = t_{11}(M) = 2(-t-2v-2w-y) \equiv 0 \pmod{6}$.

Como $t_{00} = 2(s-u+2x+z)$, temos que $t_{00} \equiv 0 \pmod{2}$; logo, é suficiente mostrarmos que $t_{00} \equiv 0 \pmod{3}$ ou $t_{00} \equiv 2 \pmod{3}$.

Para isso, calculamos o determinante de M , módulo 3, da seguinte maneira: somamos a primeira e a terceira linhas à quinta linha, e somamos a segunda e a quarta linhas à sexta linha, obtendo

$$|M| = \begin{vmatrix} s & w & 1-s-z & v & z & -v-w \\ t & x & -t+w+y & 1-s-u & -w-y & s+u-x \\ u & y & -u+x+z & -t-v & 1-x-z & t+v-y \\ v & z & -v-w & s & w & 1-s-z \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{vmatrix};$$

em seguida, somamos a primeira e a terceira colunas à quinta coluna, e somamos a segunda e a quarta colunas à sexta coluna, obtendo

$$|M| \equiv \begin{vmatrix} s & w & 1-s-z & v & 1 & 0 \\ t & x & -t+w+y & 1-s-u & 0 & 1 \\ u & y & -u+x+z & -t-v & 1 & 0 \\ v & z & -v-w & s & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{vmatrix} \pmod{3};$$

agora, subtraímos a primeira linha da terceira linha, e subtraímos a segunda linha da quarta linha, obtendo

$$|M| \equiv \begin{vmatrix} s & w & 1-s-z & v & 1 & 0 \\ t & x & -t+w+y & 1-s-u & 0 & 1 \\ u-s & y-w & -1-u+x+2z+s & -t-2v & 0 & 0 \\ v-t & z-x & -v-2w+t-y & -1+2s+u & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{vmatrix} \pmod{3}$$

e, finalmente, subtraímos a primeira coluna da terceira coluna e subtraímos a segunda coluna da quarta coluna, obtendo

$$|M| \equiv \begin{vmatrix} s & w & 1-2s-z & v-w & 1 & 0 \\ t & x & -2t+w+y & 1-s-u-x & 0 & 1 \\ u-s & y-w & 1-2u+x+2z+2s & -t-2v-y+w & 0 & 0 \\ v-t & z-x & -2v-2w+2t-y & -1+2s+u-z+x & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{vmatrix} \pmod{3}.$$

Assim, desde que $M \in GL_6(\mathbb{Z})$, e desenvolvendo o determinante acima, primeiro, pela sexta linha e, em seguida, sucessivamente, pela quinta linha, quarta coluna e terceira coluna, obtemos

$$\pm 1 \equiv (-1-s+u+x-z)^2 - (-t+v+w-y)^2 \pmod{3}$$

Por outro lado,

$$t_{11} \equiv t-v-w+y \pmod{3} \quad \text{e} \quad t_{00} \equiv -s+u+x-z \pmod{3}.$$

Portanto,

$$\pm 1 \equiv (-1+t_{00})^2 - t_{11}^2 \equiv 1 + t_{00} + t_{00}^2 \pmod{3},$$

donde

$$t_{00}^2 + t_{00} \equiv 0 \pmod{3} \quad \text{ou} \quad t_{00}^2 + t_{00} \equiv 1 \pmod{3}.$$

Da primeira equação, segue $t_{00} \equiv 0 \pmod{3}$ ou $t_{00} \equiv 2 \pmod{3}$, e a segunda equação não pode ocorrer; conseqüentemente, M satisfaz também a condição (iii) do conjunto T_1 .

Da mesma forma, se $M \in GL_6(\mathbb{Z})$ é uma matriz em S_2 que satisfaz as condições (i) e (ii) do conjunto T_2 , então podemos provar que $t_{11}(M) \equiv 0 \pmod{6}$ ou $t_{11}(M) \equiv 2 \pmod{6}$.

Com isso, fica provado que $U_1(\mathbb{ZD}_6)$ admite uma caracterização análoga à de $U_1(\mathbb{ZD}_4)$ dada no Teorema (5.2).

Finalmente, seja $M \in GL_8(\mathbb{Z})$ uma matriz em S_1 que satisfaz as condições (i) e (ii) do conjunto T_1 . Então, M deve ser da forma

$$= \begin{bmatrix} s_1 & u_1 & 1-s_1-v_2-v_3 & t_2+t_3-u_3 & s_3 & u_3 & -s_3+v_2+v_3 & -t_2-t_3-u_1 \\ t_1 & v_1 & -t_1+u_1+u_2 & 1-s_1-s_2-v_3 & t_3 & v_3 & -t_3-u_1-u_2 & s_1+s_2-v_1 \\ s_2 & u_2 & -s_2+v_1+v_2 & -t_1-t_2+\sum_{i=1}^3 u_i & 1-\sum_{i=1}^3 s_i & -\sum_{i=1}^3 u_i & \sum_{i=1}^3 s_i-v_1-v_2 & t_1+t_2-u_2 \\ t_2 & v_2 & -t_2+u_2+u_3 & -s_2-s_3+\sum_{i=1}^3 v_i & -\sum_{i=1}^3 t_i & 1-\sum_{i=1}^3 v_i & \sum_{i=1}^3 t_i-u_2-u_3 & s_2+s_3-v_2 \\ s_3 & u_3 & -s_3+v_2+v_3 & -t_2-t_3-u_1 & s_1 & u_1 & 1-s_1-v_2-v_3 & t_2+t_3-u_3 \\ t_3 & v_3 & -t_3-u_1-u_2 & s_1+s_2-v_1 & t_1 & v_1 & -t_1+u_1+u_2 & 1-s_1-s_2-v_3 \\ 1-\sum_{i=1}^3 s_i & -\sum_{i=1}^3 u_i & \sum_{i=1}^3 s_i-v_1-v_2 & t_1+t_2-u_2 & s_2 & u_2 & -s_2+v_1+v_2 & -t_1-t_2+\sum_{i=1}^3 u_i \\ -\sum_{i=1}^3 t_i & 1-\sum_{i=1}^3 v_i & \sum_{i=1}^3 t_i-u_2-u_3 & s_2+s_3-v_2 & t_2 & v_2 & -t_2+u_2+u_3 & -s_2-s_3+\sum_{i=1}^3 v_i \end{bmatrix};$$

com $t_{11}(M) = 2(-t_1-2t_2-3t_3-3u_1-2u_2-u_3) \equiv 0 \pmod{8}$.

Com isso, $t_{00}(M) = 2(s_1-2s_2-s_3+3v_1+2v_2+v_3)$; assim, fazendo $s_2=1$ e $s_1=0=s_3=t_1=t_2=t_3=u_1=u_2=u_3=v_1=v_2=v_3$, temos que a condição $t_{11}(M) \equiv 0 \pmod{8}$ é verificada, $t_{00}(M) = -4$ e ainda, calculando o determinante de M , obtemos

$$|M| = \begin{vmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & -1 \end{vmatrix} = 1$$

Portanto, M satisfaz todas as condições do conjunto T_1 , exceto a condição (iii).

Da mesma forma, a matriz

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

satisfaz todas as condições do conjunto T_2 , exceto a condição (iii).

6. CARACTERIZAÇÕES DE COMPLEMENTOS PARA D_3 EM $U_1(\mathbb{Z}D_3)$ E D_4 EM $U_1(\mathbb{Z}D_4)$

Seja G um grupo finito com um subgrupo normal abeliano H tal que $\frac{G}{H}$ é abeliano cujo expoente é um divisor de 4 ou 6. Seja Y um conjunto completo de representantes das classes laterais de H em G e, finalmente, seja $f: \mathbb{Z}G \rightarrow \mathbb{Z}(\frac{G}{H})$ o homomorfismo natural. Então, observando que o conjunto $\{y(a-1): y \in Y, h \in H, h \neq 1\}$ é uma base sobre $\mathbb{Z}$ do núcleo $\Delta(G, H)$ de f , G.H. Cliff, S.K. Sehgal e A.R. Weiss definiram em [4], para cada $k \in \mathbb{Z}$, o homomorfismo de grupos abelianos $\phi_k: \Delta(G, H) \rightarrow H$ tal que, para todo $y \in Y$ e todo $h \in H, h \neq 1$,

$$\phi_k(y(h-1)) = h^{y^k}$$

e, denotando por I_k o núcleo de ϕ_k , mostraram que o conjunto $U(I+I_k)$ das unidades em $I+I_k$ é um complemento normal livre de torção para G em $U_1(\mathbb{Z}G)$; em particular, mostraram que $I_0 = \Delta(G)\Delta(H)$.

Considerando os casos $G = D_3$, $H = \langle b \rangle$ e $G = D_4$, $H = \langle b^2 \rangle$, vamos calcular a imagem $\rho(U(1+\Delta(G)\Delta(H)))$; obtendo, assim, uma caracterização de $U(1+\Delta(G)\Delta(H))$ como um grupo de matrizes duplamente estocásticas.

Seja N o conjunto das matrizes $M \in GL_3(\mathbb{Z})$ tais que $M \in V$ e $M \equiv I + DJ \pmod{3}$ onde I é a matriz identidade 3×3 , D é uma matriz diagonal em $M_3(\mathbb{Z})$, com traço igual a 0, e J é a matriz 3×3 cujas entradas são todas iguais a 1. Então, em [3, Teorema 3], P.J. Allen e C. Hobby provaram que N é um complemento normal livre de torção para $\rho(D_3)$ em V .

Aqui provaremos que, de fato, temos o seguinte

TEOREMA (6.1). O conjunto N é a imagem $\rho(U(1+\Delta(D_3)\Delta(\langle b \rangle)))$.

Demonstração. Inicialmente, mostraremos que se $M \in V$ e satisfaz

$$(1) \quad M \equiv I + \begin{bmatrix} s & s & s \\ t & t & t \\ u & u & u \end{bmatrix} \pmod{3},$$

com $s, t, u \in \mathbb{Z}$, então $M \in N$.

Para isso, vamos proceder como em [3, Teorema 3].

Desde que M é duplamente estocástica, a soma das entradas em qualquer coluna da matriz $M-I$ é igual a 0; logo, por (1),

$$s+t+u \equiv 0 \pmod{3}.$$

Assim, fazendo $v = s+t+u$, obtemos

$$M \equiv I + \begin{bmatrix} s & s & s \\ t & t & t \\ u-v & u-v & u-v \end{bmatrix} \equiv I + \begin{bmatrix} s & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & u-v \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \pmod{3},$$

donde $M \in N$.

Agora, todo elemento $\alpha \in U(1+\Delta(D_3)\Delta(\langle b \rangle))$ tem aumento 1; logo, $\rho(\alpha)$ é uma matriz duplamente estocástica em $GL_3(\mathbb{Z})$ e, portanto, $\rho(\alpha) \in V$.

Além disso, os conjuntos

$$B_1 = \{(b-1), (b^2-1), (a-1), ab-1, (ab^2-1)\} \quad \text{e} \quad B_2 = \{(b-1), (b^2-1)\}$$

são bases sobre $\mathbb{Z}$ de $\Delta(D_3)$ e $\Delta(\langle b \rangle)$, respectivamente.

Assim, para obtermos a inclusão $\rho(U(1+\Delta(D_3)\Delta(\langle b \rangle))) \subseteq N$ é suficiente verificarmos que, para todo $x \in B_1$ e todo $y \in B_2$, a matriz $\rho(xy)$ é da forma

$$\rho(xy) \equiv \begin{bmatrix} s & s & s \\ t & t & t \\ u & u & u \end{bmatrix} \pmod{3},$$

com $s, t, u \in \mathbb{Z}$.

Fazemos isso, diretamente, observando que, para quaisquer i, j e k , com $i=0,1$, $j=0,1,2$ e $k=1,2$, temos

$$\rho((a^i b^j - 1)(b^k - 1)) \equiv \begin{bmatrix} s & s & s \\ t & t & t \\ u & u & u \end{bmatrix} \pmod{3},$$

com $s, t, u \in \mathbb{Z}$.

A inclusão contrária é, agora, uma consequência imediata do fato de que ambos os conjuntos $\rho(U(1+\Delta(D_3)\Delta(\langle b \rangle)))$ e N são complementos normais livres de torção para $\rho(D_3)$ em V ; entretanto, daremos uma prova independente deste fato.

Para isso, vamos considerar uma matriz $M \in N$; em seguida, calcular $\beta = \beta(M)$ e, finalmente, provar que β^{-1} é um elemento em $\Delta(D_3, \langle b \rangle)$ tal que $\phi_0(\beta^{-1}) = 1$.

Com isso, desde que $\rho(\beta) = M$ e $\Delta(D_3)\Delta(\langle b \rangle)$ é o núcleo de ϕ_0 , teremos provado que $\rho^{-1}(N) \subseteq U(1+\Delta(D_3)\Delta(\langle b \rangle))$, donde $N \subseteq \rho(U(1+\Delta(D_3)\Delta(\langle b \rangle)))$.

Inicialmente, escrevemos M na forma

$$M = \begin{bmatrix} 1+s & s & s \\ t & 1+t & t \\ -s-t & -s-t & 1-s-t \end{bmatrix} + 3X,$$

com $s, t \in \mathbb{Z}$ e $X = (x_{ij}) \in M_3(\mathbb{Z})$; ainda mais, como M é duplamente estocástica, a soma de suas entradas em toda coluna é igual a 1 e, portanto,

$$(2) \quad \sum_{i=1}^3 x_{ik} = 0, \quad \forall k, 1 \leq k \leq 3.$$

Denotando $t_{ij} = t_{ij}(M)$, para $i=0,1$ e $j=0,1,2$, temos

$$\begin{aligned} t_{00} &= 3 + 3t_{00}(X) & t_{10} &= 1 + 3t_{10}(X) \\ t_{01} &= 3t_{01}(X) & t_{11} &= 1 + 3t_{11}(X) \\ t_{02} &= 3t_{02}(X) & t_{12} &= 1 + 3t_{12}(X) \end{aligned}$$

Como $t_{00} \equiv 0 \pmod{3}$, temos $\beta = \sum \beta_{ij} a^i b^j$, com

$$\beta_{00} = \frac{t_{00}}{3} = 1 + t_{00}(X) \qquad \beta_{10} = \frac{t_{01}-1}{3} = t_{01}(X)$$

$$\beta_{01} = \frac{t_{01}}{3} = t_{01}(X) \qquad \beta_{11} = \frac{t_{11}-1}{3} = t_{11}(X)$$

$$\beta_{02} = \frac{t_{02}}{3} = t_{02}(X) \qquad \beta_{12} = \frac{t_{12}-1}{3} = t_{12}(X)$$

Por outro lado, de (2), temos

$$\sum_{i=0}^2 t_{0i}(X) = 0 = \sum_{i=0}^2 t_{1i}(X).$$

Assim, $\sum_{i=0}^2 \beta_{0i} = 1$ e $\sum_{i=0}^2 \beta_{1i} = 0$, donde $\beta - 1 \in \Delta(D_3, \langle b \rangle)$.

Finalmente, como $\{1, a\}$ é um conjunto completo de representantes das classes laterais de $\langle b \rangle$ em D_3 , temos que $\{(b-1), (b^2-1), a(b-1), a(b^2-1)\}$ é uma base de $\Delta(D_3, \langle b \rangle)$ sobre $\mathbb{Z}$; assim, escrevendo $\beta - 1$ como uma combinação linear dos elementos desta base, obtemos

$$\beta - 1 = \beta_{01}(b-1) + \beta_{02}(b^2-1) + \beta_{11}a(b-1) + \beta_{12}a(b^2-1)$$

e, conseqüentemente,

$$\phi_0(\beta - 1) = b^{\beta_{01} + 2\beta_{02} + \beta_{11} + 2\beta_{12}}.$$

Agora,

$$\begin{aligned}
\beta_{01} + 2\beta_{02} + \beta_{11} + 2\beta_{12} &= t_{01}(X) + 2t_{02}(X) + t_{11}(X) + 2t_{12}(X) = \\
&= x_{21} + x_{32} + x_{13} + 2(x_{31} + x_{12} + x_{23}) + x_{31} + x_{22} + x_{13} + 2(x_{21} + x_{12} + x_{33}) = \\
&= 3(x_{21} + x_{31} + x_{12}) + 2(x_{13} + x_{23} + x_{33}) + x_{12} + x_{22} + x_{32};
\end{aligned}$$

logo, por (2), $\beta_{01} + 2\beta_{02} + \beta_{11} + 2\beta_{12} \equiv 0 \pmod{3}$ e, portanto,
 $\phi_0(\beta-1)=1. \Delta$

Passamos, agora, à caracterização de $U(1+\Delta(D_4)_\Delta(\langle b^2 \rangle))$.

Seja P o conjunto das matrizes $M \in GL_4(\mathbf{Z})$ tais que $M \in S_1$,
 $t_{00}(M) \equiv 0 \equiv t_{11}(M) \pmod{4}$ e

$$X \equiv I + \begin{bmatrix} s & u & -s & -u \\ t & v & -t & -v \\ -s & -u & s & u \\ -t & -v & t & v \end{bmatrix} \pmod{4},$$

onde I é a matriz identidade 4×4 , $s, t, u, v \in \mathbf{Z}$ e $2(s+t) \equiv 0 \pmod{4}$.
Então, nossa caracterização de $U(1+\Delta(D_4)_\Delta(\langle b^2 \rangle))$ é dada pelo

TEOREMA (6.2). O conjunto P é a imagem $\rho(U(1+\Delta(D_4)_\Delta(\langle b^2 \rangle)))$.

Demonstração. Se $\alpha \in U(1+\Delta(D_4)_\Delta(\langle b^2 \rangle))$, então é claro que
 $\alpha \in 1+\Delta(D_4, \langle b^2 \rangle)$; logo, pelo Lema (4.1), parte (i), temos que $\rho(\alpha) \in S_1$
e $t_{00}(\rho(\alpha)) \equiv 0 \equiv t_{11}(\rho(\alpha)) \pmod{4}$.

Por outro lado, os conjuntos

$$B_1 = \{(b-1), (b^2-1), (b^3-1), (a-1), (ab-1), (ab^2-1), (ab^3-1)\}$$

$$\text{e } B_2 = \{(b^2-1)\}$$

são bases sobre $\mathbb{Z}$ de $\Delta(D_4)$ e $\Delta(\langle b^2 \rangle)$, respectivamente.

Assim, para obtermos a inclusão $\rho(U(1+\Delta(D_4)\Delta(\langle b^2 \rangle))) \subseteq P$, é suficiente mostrarmos que, para todo $x \in B_1$ e todo $y \in B_2$, a matriz $\rho(xy)$ é da forma

$$\rho(xy) \equiv \begin{bmatrix} s & u & -s & -u \\ t & v & -t & -v \\ -s & -u & s & u \\ -t & -v & t & v \end{bmatrix} \pmod{4},$$

com $s, t, u, v \in \mathbb{Z}$ e $2(s+t) \equiv 0 \pmod{4}$.

Fazemos isso, diretamente, observando que, para quaisquer i e j , com $i=0,1$ e $j=0,1,2,3$, temos

$$\rho((a^i b^{j-1})(b^2-1)) \equiv \begin{bmatrix} s & u & -s & -u \\ t & v & -t & -v \\ -s & -u & s & u \\ -t & -v & t & v \end{bmatrix} \pmod{4},$$

com $s, t, u, v \in \mathbb{Z}$ e $2(s+t) \equiv 0 \pmod{4}$.

Para a inclusão contrária, vamos considerar uma matriz $M \in P$; em seguida, calcular $\gamma = \gamma(M)$ e, finalmente, provar que γ^{-1} é um elemento em $\Delta(D_4, \langle b^2 \rangle)$ tal que $\phi_0(\gamma^{-1})=1$.

Com isso, desde que $\rho(\gamma) = M$ e $\Delta(D_4)\Delta(\langle b^2 \rangle)$ é o núcleo de ϕ_0 , teremos provado que $\rho^{-1}(P) \subseteq U(1+\Delta(D_4)\Delta(\langle b^2 \rangle))$, donde $P \subseteq \rho(U(1+\Delta(D_4)\Delta(\langle b^2 \rangle)))$.

Inicialmente, escrevemos M na forma

$$M = \begin{bmatrix} 1+s & u & -s & -u \\ t & 1+v & -t & -v \\ -s & -u & 1+s & u \\ -t & -v & t & 1+v \end{bmatrix} + 4E,$$

onde $s, t, u, v \in \mathbb{Z}$, $2(s+v) \equiv 0 \equiv 2(t+u) \equiv 2(s+t) \pmod{4}$ e $E = (e_{ij}) \in M_4(\mathbb{Z})$.

Agora, fazendo $p = 2(s+v)$ e $q = 2(u-t)$, é claro que $p \equiv 0 \equiv q \pmod{4}$ e, então, podemos escrever

$$M = \begin{bmatrix} 1+s & u & -s & -u+q \\ t & 1+v & -t & -v+p \\ -s & -u & 1+s & u-q \\ -t & -v & t & 1+v-p \end{bmatrix} + 4F,$$

onde $F = (f_{ij}) \in M_4(\mathbb{Z})$; ainda mais, como $M \in S_1$, deve ocorrer

$$(3) \quad \sum_{i=1}^2 f_{2i-1,k} = 0 = \sum_{i=1}^2 f_{2i,k}, \quad \forall k, \quad 1 \leq k \leq 4.$$

Denotando $t_{ij} = t_{ij}(M)$, para $i=0,1$ e $j=0,1,2,3$, temos

$$\begin{aligned} t_{00} &= 4 + t_{00}(F) & t_{10} &= 2 + 4s + 4t_{10}(F) \\ t_{01} &= 4t_{01}(F) & t_{11} &= -4t + 4t_{11}(F) \\ t_{02} &= 4t_{02}(F) & t_{12} &= 2 - 4s + 4t_{12}(F) \\ t_{03} &= 4t_{03}(F) & t_{13} &= 4t + 4t_{13}(F) \end{aligned}$$

Como $t_{00} \equiv 0 \pmod{4}$, temos $\gamma = \sum \gamma_{ij} a^i b^j$, com

$$\gamma_{00} = \frac{t_{00}}{4} = 1 + t_{00}(F)$$

$$\gamma_{10} = \frac{t_{10}^{-2}}{4} = s + t_{10}(F)$$

$$\gamma_{01} = \frac{t_{01}}{4} = t_{01}(F)$$

$$\gamma_{11} = \frac{t_{11}}{4} = -t + t_{11}(F)$$

$$\gamma_{02} = \frac{t_{02}}{4} = t_{02}(F)$$

$$\gamma_{12} = \frac{t_{12}^{-2}}{4} = -s + t_{12}(F)$$

$$\gamma_{03} = \frac{t_{03}}{4} = t_{03}(F)$$

$$\gamma_{13} = \frac{t_{13}}{4} = t + t_{13}(F)$$

Por outro lado, de (3), temos

$$t_{00}(F) + t_{02}(F) = 0 = t_{01}(F) + t_{03}(F) = t_{10}(F) + t_{12}(F) = t_{11}(F) + t_{13}(F)$$

Assim,

$$\gamma_{00} + \gamma_{02} = 1 \quad \text{e} \quad \gamma_{01} + \gamma_{03} = 0 = \gamma_{10} + \gamma_{12} = \gamma_{11} + \gamma_{13},$$

donde $\gamma^{-1} \in \Delta(D_4, \langle b^2 \rangle)$.

Finalmente, como $\{1, b, a, ab\}$ é um conjunto completo de representantes das classes laterais de $\langle b^2 \rangle$ em D_4 , temos que $\{(b^2-1), b(b^2-1), a(b^2-1), ab(b^2-1)\}$ é uma base de $\Delta(D_4, \langle b^2 \rangle)$ sobre $\mathbb{Z}$; assim, escrevendo γ^{-1} como uma combinação linear dos elementos desta base, obtemos

$$\gamma^{-1} = \gamma_{02}(b^2-1) + \gamma_{03}b(b^2-1) + \gamma_{12}a(b^2-1) + \gamma_{13}ab(b^2-1)$$

e, conseqüentemente,

$$\phi_0(\gamma^{-1}) = b^{2(\gamma_{02} + \gamma_{03} + \gamma_{12} + \gamma_{13})}$$

Agora,

$$\gamma_{02} + \gamma_{03} + \gamma_{12} + \gamma_{13} = t_{02}(F) + t_{03}(F) - s + t_{12}(F) + t + t_{13}(F) =$$

$$\begin{aligned}
&= -s+t+f_{31}+f_{42}+f_{13}+f_{24}+f_{41}+f_{12}+f_{23}+f_{34}+f_{31}+f_{22}+f_{13}+f_{44} + \\
&+f_{21}+f_{12}+f_{43}+f_{34} = -s+t+2(f_{31}+f_{12}+f_{13}+f_{34})+f_{21}+f_{41}+f_{22}+f_{42}+ \\
&+f_{23}+f_{43}+f_{24}+f_{44};
\end{aligned}$$

logo, por (3) e desde que $2(s+t) \equiv 0 \pmod{4}$, temos

$$\gamma_{02} + \gamma_{03} + \gamma_{12} + \gamma_{13} \equiv 0 \pmod{2}$$

e, portanto, $\phi_0(\gamma-1)=1$. Δ

CAPÍTULO IV

UNIDADES DE TORÇÃO EM $\mathbb{Z}S_4$

Neste capítulo provaremos que toda unidade de torção de ordem 2, 3 ou 4 em $U_1(\mathbb{Z}S_4)$ é racionalmente conjugada a um elemento de S_4 e, então, provaremos que nenhuma outra possibilidade pode ocorrer.

É claro que destes resultados segue que S_4 satisfaz a conjectura de Zassenhaus, enunciada na página x.

7. ALGUNS RESULTADOS SOBRE S_4

Seja $u = \sum u(g)g \neq 1$ uma unidade de torção em $U_1(\mathbb{Z}S_4)$ e, para cada elemento $g \in S_4$, seja $\tilde{u}(g) = \sum_{h \sim g} u(h)$ a soma dos coeficientes de u que correspondem a elementos da classe de conjugação de g em S_4 .

Pelo Teorema de Berman [12, Proposição (11.2)], se $u(1) \neq 0$, então $u=1$, o que é uma contradição; logo, deve ocorrer $u(1) = 0$.

Agora, considerando a tabela de caracteres de S_4 , que está calculada, por exemplo, em [6, pág. 277],

	(1)	(12)	(123)	(12)(34)	(1234)
x_1	1	1	1	1	1
x_2	1	-1	1	1	-1
x_3	2	0	-1	2	0
x_4	3	-1	0	-1	1
x_5	3	1	0	-1	1

e denotando ainda por x_i , $1 \leq i \leq 5$, a extensão linear de x_i a $\mathbb{Z}S_4$, obtemos o seguinte sistema linear em $\tilde{u}(g)$, $g \in S_4$:

$$\begin{aligned}
 x_1(u) &= \tilde{u}(12) + \tilde{u}(123) + \tilde{u}((12)(34)) + \tilde{u}(1234) \\
 x_2(u) &= -\tilde{u}(12) + \tilde{u}(123) + \tilde{u}((12)(34)) - \tilde{u}(1234) \\
 (1) \quad x_3(u) &= -\tilde{u}(123) + 2\tilde{u}((12)(34)) \\
 x_4(u) &= -\tilde{u}(12) - \tilde{u}((12)(34)) + \tilde{u}(1234) \\
 x_5(u) &= \tilde{u}(12) - \tilde{u}((12)(34)) - \tilde{u}(1234).
 \end{aligned}$$

Então, como $x_1(u)$ é o valor da função de aumento de $\mathbb{Z}S_4$ em u e $x_2(u)$ é uma unidade em $\mathbb{Z}$, deve ocorrer

$$(2) \quad x_1(u) = 1 \quad \text{e} \quad x_2(u) = \pm 1.$$

Seja H o subgrupo de S_4 que fixa o elemento 4 e seja $K = \{1, (12)(34), (13)(24), (14)(23)\}$. Então, H é isomorfo a S_3 e K é um subgrupo normal de S_4 tal que $S_4 = H \rtimes K$; assim, H é um conjunto completo de representantes das classes laterais de K em S_4 .

Seja $f: \mathbb{Z}S_4 \rightarrow \mathbb{Z}(\frac{S_4}{K})$ o homomorfismo natural e seja $w: \mathbb{Z}(\frac{S_4}{K}) \rightarrow \mathbb{Z}H$ o isomorfismo tal que, para todo $h \in H$, $w(hK) = h$. Então, desde que H satisfaz a conjectura de Zassenhaus, existem um elemento $h \in H$ e uma unidade $\gamma \in \mathbb{Q}H$ tais que

$$(w \circ f)(u) = \gamma^{-1} h \gamma = (w \circ f)(\gamma^{-1} h \gamma);$$

logo,

$$(3) \quad o(h) | o(u) \quad \text{e} \quad u - \gamma^{-1} h \gamma \in \Delta(S_4, K).$$

Para cada i , $1 \leq i \leq 5$, seja ρ_i uma representação irredutível de S_4 cujo carácter é x_i e denotemos ainda por ρ_i a extensão linear

de ρ_i a $\mathbb{Z}S_4$.

Observando a tábua de caracteres de S_4 , vemos que $\chi_1(K) = \{1\} = \chi_2(K)$ e $\chi_3(K) = \{2\}$, em particular, os graus de ρ_1 e ρ_2 são iguais a 1 e o grau de ρ_3 é igual a 2; logo, $\rho_1(K) = \{1\} = \rho_2(K)$ e $\rho_3(K) = \{I_2\}$, onde I_2 é a matriz identidade 2×2 .

Assim, desde que o conjunto $\{h(k-1) : h \in H, k \in K, k \neq 1\}$ é uma base de $\Delta(S_4, K)$ sobre $\mathbb{Z}$, temos $\rho_i(\Delta(S_4, K)) = \{0\}$, para $i=1, 2$, e $\rho_3(\Delta(S_4, K)) = \{0\}$, onde 0 é a matriz nula 2×2 ; logo, $\chi_i(\Delta(S_4, K)) = \{0\}$, para $i=1, 2, 3$.

8. A CONJECTURA DE ZASSENHAUS PARA S_4 .

Utilizaremos os dois resultados seguintes, os quais estão provados em [8, Teorema 2.5 e 2.7].

TEOREMA (8.1). Sejam G um grupo finito e U um subgrupo de unidades de torção em $U_1(\mathbb{Z}G)$. Então, as seguintes afirmações são equivalentes:

- (i) Para cada $u \in U$, existe $g_0 \in G$ tal que u é racionalmente conjugada a g_0 ;
- (ii) Para cada $u \in U$, existe $g_0 \in G$, único a menos de conjugação, tal que $\tilde{u}(g_0) \neq 0$.

Conforme a prova deste resultado, a afirmação (i) implica que $\tilde{u}(g_0)=1$ e a afirmação (ii), que u é racionalmente conjugada a g_0 .

TEOREMA (8.2). Sejam G um grupo finito, u uma unidade de torção em $U_1(\mathbb{Z}G)$ e g um elemento em G . Se existe um primo p tal que $p \mid o(g)$ e $p \nmid o(u)$, então $\tilde{u}(g) = 0$.

Precisaremos, ainda, do seguinte resultado, que pode ser encontrado em [16, Lemas I.1.4, I.1.5 e III.6.5].

TEOREMA (8.3). Seja G um grupo e seja $\Lambda = [\mathbb{Z}G, \mathbb{Z}G]$, o subgrupo aditivo de $\mathbb{Z}G$ gerado por todos os produtos de Lie $[\alpha, \beta] = \alpha\beta - \beta\alpha$, $\alpha, \beta \in \mathbb{Z}G$. Então,

- (i) $\Lambda = \{\alpha = \sum \alpha(g)g \in \mathbb{Z}G : \tilde{\alpha}(g) = 0, \text{ para todo } g \in G\}$;
- (ii) para todo primo p e todo elemento $\alpha = \sum \alpha(g)g \in \mathbb{Z}G$, $(\sum \alpha(g)g)^p \equiv \sum \alpha(g)^p g^p \pmod{\Lambda + p\mathbb{Z}G}$;
- (iii) para todo primo p , $\Lambda^p \subseteq \Lambda + p\mathbb{Z}G$.

Agora, estamos em condições de demonstrar os resultados anunciados.

TEOREMA (8.4). Seja $u = \sum u(g)g \neq 1$ uma unidade de torção em $U_1(\mathbb{Z}S_4)$.

- (a) Se $o(u)=2$, então u é racionalmente conjugada a (12) ou a (12)(34).
- (b) Se $o(u)=3$, então u é racionalmente conjugada a (123).
- (c) Se $o(u)=4$, então u é racionalmente conjugada a (1234).

Demonstração. (a) Pelo Teorema (8.2), $\tilde{u}(123)=0$ e, pelo Teorema (8.3), parte (i),

$$u - (\tilde{u}(12))(12) - (\tilde{u}(123))(123) - (\tilde{u}((12)(34)))(12)(34) - \\ - (\tilde{u}(1234))(1234) \equiv 0 \pmod{\Lambda}.$$

Então, pelo Teorema (8.3), partes (ii) e (iii),

$$1 + \tilde{u}(12)^2 + \tilde{u}((12)(34))^2 + (\tilde{u}(1234))^2(13)(24) \pmod{(\Lambda + 2\mathbb{Z}S_4)},$$

donde $2 \mid \tilde{u}(1234)$.

Agora, por (2), temos um dos seguintes casos:

$$(a_1) \quad x_2(u) = 1 \quad \text{ou} \quad (a_2) \quad x_2(u) = -1.$$

Além disso, como $o(u) = 2$, temos que a matriz $\rho_i(u)$, $i = 4, 5$, é semelhante a uma das matrizes:

$$I_3, -I_3 \quad \text{ou} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \pm 1 \end{bmatrix}$$

onde I_3 é matriz identidade 3×3 . Então, $x_i(u)$, $i = 4, 5$, pode assumir somente um dos valores: $3, -3, 1$ ou -1 .

Consideremos o caso (a_1) . Então, de (1) e (2), segue

$$2 = x_1(u) + x_2(u) = 2\tilde{u}((12)(34))$$

$$1 = x_1(u) = \tilde{u}(12) + \tilde{u}((12)(34)) + \tilde{u}(1234)$$

$$x_4(u) = -\tilde{u}(12) - \tilde{u}((12)(34)) + \tilde{u}(1234),$$

donde

$$1 = \tilde{u}((12)(34))$$

$$0 = \tilde{u}(12) + \tilde{u}(1234)$$

$$1 + x_4(u) = 2\tilde{u}(1234).$$

Assim, podemos construir a seguinte tabela, com as diversas possibilidades calculadas a partir dos valores possíveis para $x_4(u)$:

	$x_4(u)$	$\tilde{u}(12)$	$\tilde{u}(123)$	$\tilde{u}((12)(34))$	$\tilde{u}(1234)$
(a_{11})	3	-2	0	1	2
(a_{12})	-3	1	0	1	-1
(a_{13})	1	-1	0	1	1
(a_{14})	-1	0	0	1	0

Por (1), $x_5(u) = \tilde{u}(12) - \tilde{u}((12)(34)) - \tilde{u}(1234)$. Então, a possibilidade (a_{11}) leva à contradição $x_5(u) = -5$.

As possibilidades (a_{12}) e (a_{13}) também não podem ocorrer, desde que $2 \mid \tilde{u}(1234)$.

Agora, se temos (a_{14}) e consideramos, no Teorema (8.1), U como o subgrupo gerado por u , então podemos concluir que u é racionalmente conjugada a $(12)(34)$.

Considerando o caso (a_2) , procedemos da mesma forma e obtemos

$$0 = \tilde{u}((12)(34))$$

$$1 = \tilde{u}(12) + \tilde{u}(1234)$$

$$1 + x_4(u) = 2\tilde{u}(1234).$$

Assim, neste caso, podemos construir a seguinte tabela:

	$\chi_4(u)$	$\tilde{u}(12)$	$\tilde{u}(123)$	$\tilde{u}((12)(34))$	$\tilde{u}(1234)$
(a_{21})	3	-1	0	0	2
(a_{22})	-3	2	0	0	-1
(a_{23})	1	0	0	0	1
(a_{24})	-1	1	0	0	0

Para analisarmos a possibilidade (a_{21}) , vamos considerar a fórmula de inversão de Fourier [18, Proposição 11], segundo a qual, para todo $g \in S_4$,

$$u(g) = \frac{1}{24} (\chi_1(g^{-1}u) + \chi_2(g^{-1}u) + 2\chi_3(g^{-1}u) + 3\chi_4(g^{-1}u) + 3\chi_5(g^{-1}u)).$$

Por outro lado, nesta possibilidade, $\chi_1(u)=1$, $\chi_2(u)=-1$, $\chi_4(u)=3$ e $\chi_5(u)=-3$, donde $\rho_1(u)=1$, $\rho_2(u)=-1$, $\rho_4(u)=I_3$ e $\rho_5(u)=-I_3$.

Assim, para todo $g \in S_4$,

$$u(g) = \frac{1}{24} (1 - \chi_2(g^{-1}) + 2\chi_3(g^{-1}u) + 3\chi_4(g^{-1}) - 3\chi_4(g^{-1})).$$

Agora, como observamos na seção 7, $\rho_3(k) = \{I_2\}$; logo, desde que $(12)(1423) \in K$, temos $\rho_3(12) = \rho_3(1423)$.

Portanto,

$$u(12) = \frac{1}{24} (1 + 1 + 2\chi_3((12)u) - 3 - 3) = \frac{1}{12} (\chi_3((12)u) - 2)$$

e

$$u(1234) = \frac{1}{24} (1 + 1 + 2\chi_3((12)u) + 3 + 3) = \frac{1}{12} (\chi_3((12)u) + 4),$$

donde

$$\chi_3((12)u) - 2 \equiv 0 \pmod{12} \quad \text{e} \quad \chi_3((12)u) + 4 \equiv 0 \pmod{12},$$

o que é uma contradição.

De novo, como $2 \mid \tilde{u}(1234)$, as possibilidades (a_{22}) e (a_{23}) não podem ocorrer e, pelo Teorema (8.1), a possibilidade (a_{24}) implica que u é racionalmente conjugada a (12) .

(b) Do Teorema (8.2), temos que $\tilde{u}(g)$ e $\tilde{u}^{-1}(g)$ são diferentes de zero somente se g é conjugado a (123) . Então, pelo Teorema (8.1), podemos concluir que u é racionalmente conjugada a (123) .

(c) Por (3), existem um elemento $h \in H$ e uma unidade $\gamma \in QH$ tais que $o(h) \mid o(u)$ e $u^{-1}h\gamma \in \Delta(S_4, K)$. Então,

$$u^{-1} \in \Delta(S_4, K) \quad \text{ou} \quad u^{-1}(12)\gamma \in \Delta(S_4, K).$$

Agora, K é um grupo de expoente 2. Então, desde que, para todo $k \in K$,

$$1 = (1 + (k-1))^2 = 1 + 2(k-1) + (k-1)^2,$$

é fácil ver que $2\Delta(S_4, K) \subseteq \Delta(S_4, K)^2$. Além disto, como K é abeliano, segue, de [4, Lema 3.3], que o grupo das unidades em $1 + \Delta(S_4, K)^2$ é livre de torção.

Portanto, se $u^{-1} \in \Delta(S_4, K)$, podemos escrever $u = 1 + \delta$, com $\delta \in \Delta(S_4, K)$, e então obter que

$$u^2 = 1 + 2\delta + \delta^2 \in 1 + \Delta(S_4, K)^2,$$

donde segue a contradição $u^2 = 1$.

Assim, devemos ter que $u^{-1}(12)\gamma \in \Delta(S_4, K)$.

Por outro lado, vimos na seção 7 que $\chi_2(\Delta(S_4, K)) = \{0\}$; lo-

go, podemos concluir que $\chi_2(u) = -1$.

Agora, pelo Teorema 8.2, $\tilde{u}(123) = 0$. Então, por (1) e (2),

$$0 = \chi_1(u) + \chi_2(u) = 2\tilde{u}((12)(34))$$

$$1 = \chi_1(u) = \tilde{u}(12) + \tilde{u}((12)(34)) + \tilde{u}(1234)$$

$$\chi_4(u) = -\tilde{u}(12) - \tilde{u}((12)(34)) + \tilde{u}(1234);$$

logo,

$$0 = \tilde{u}((12)(34))$$

$$1 = \tilde{u}(12) + \tilde{u}(1234)$$

$$1 + \chi_4(u) = 2\tilde{u}(1234).$$

Além disso, como $o(u) = 4$ e $\chi_4(u) \in \mathbb{Z}$, temos que a matriz $\rho_4(u)$ é semelhante a uma das matrizes:

$$I_3, -I_3, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \pm 1 \end{bmatrix} \quad \text{ou} \quad \begin{bmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & \pm 1 \end{bmatrix}.$$

Então, $\chi_4(u)$ pode assumir somente um dos valores: 3, -3, 1 ou -1.

Assim, podemos construir a mesma tabela obtida no caso (a_2) . É claro que, aqui, devemos considerar as possibilidades (a_{21}) , (a_{22}) , (a_{23}) e (a_{24}) para $o(u) = 4$.

Em qualquer caso, pelo Teorema (8.3), temos

$$u^2 + \tilde{u}(12)^2 + (\tilde{u}(1234))^2(13)(24) \equiv 0 \pmod{(\Lambda + 2\mathbb{Z}S_4)}.$$

Por outro lado, u^2 é racionalmente conjugada a $(12)(34)$, desde que $o(u^2) = 2$ e $\rho_2(u^2) = \rho_2(u)^2 = 1$.

Portanto, pelo Teorema (8.1), temos que $2 \mid (1 + \tilde{u}(1234))$, donde as possibilidades (a_{21}) e (a_{24}) não podem ocorrer.

Se temos (a_{22}) , então $\rho_4(u) = -I_3$; logo, $\rho_4(u^2) = I_3$, o que leva à contradição $3 = \chi_4(u^2) = \chi_4((12)(34))$.

Finalmente, se vale (a_{23}) , então, pelo Teorema (8.1), podemos concluir que u é racionalmente conjugada a (1234) . Δ

TEOREMA (8.5). S_4 satisfaz a conjectura de Zassenhaus.

Demonstração. Seja u uma unidade de torção em $U_1(\mathbb{Z}S_4)$. Por [16, Teorema VI.2.1], se $p^n \mid o(u)$, p um primo, então existe $g \in S_4$ tal que $o(g) = p^n$; logo, $o(u)$ pode assumir somente um dos valores: 2, 3, 4, 6 ou 12.

Provaremos que se $u^6 = 1$, então $u^2 = 1$ ou $u^3 = 1$. Claramente, disto e do Teorema (8.4), segue que a conjectura é verdadeira para S_4 .

Por (3), podemos supor que $u^{-1} \in \Delta(S_4, K)$ ou que, então, existe uma unidade $\gamma \in \mathbb{Q}H$ tal que $u - \gamma^{-1}(12)\gamma \in \Delta(S_4, K)$ ou $u - \gamma^{-1}(123)\gamma \in \Delta(S_4, K)$.

Se $u^{-1} \in \Delta(S_4, K)$, então, como na prova do Teorema (8.4), parte (c), podemos concluir que $u^2 = 1$.

Se $u - \gamma^{-1}(12)\gamma \in \Delta(S_4, K)$, podemos escrever $u = \gamma^{-1}(12)\gamma + \delta$, com $\delta \in \Delta(S_4, K)$, e então obter que

$$u^2 = 1 + \gamma^{-1}(12)\gamma\delta + \delta\gamma^{-1}(12)\gamma + \delta^2 \in 1 + \Delta(S_4, K),$$

donde $u^2 - 1 \in \Delta(S_4, K)$; logo, como antes, $u^4 = 1$ e, portanto, $u^2 = u^6(u^4)^{-1} = 1$.

Suponhamos, agora, que $u = \gamma^{-1}(123)\gamma \in \Delta(S_4, K)$ e seja $v = (w.f)(u)$, onde f e w são os homomorfismos considerados na seção 7.

É claro que $v = \gamma^{-1}(123)\gamma$ e não é difícil ver que $\tilde{v}(123) = \tilde{u}(123)$. Então, pelo Teorema (8.1), $1 = \tilde{v}(123) = \tilde{u}(123)$ e, portanto, pelo Teorema (8.3),

$$u^3 - (\tilde{u}(12))^3(12) - 1 - (\tilde{u}((12)(34)))^3(12)(34) - \\ - (\tilde{u}(1234))^3(1432) \equiv 0 \pmod{(\Lambda + 3\mathbb{Z}S_4)}.$$

Assim, deve ocorrer $u^3 = 1$, desde que ao contrário, pelo Teorema de Berman [12, Proposição (11.2)], teríamos $u^3(1) = 0$, o que levaria à contradição $1 \equiv 0 \pmod{3}$. Δ

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] P.J. Allen, C. Hobby, "A characterization of units in $\mathbb{Z}A_4$ ", J. Algebra 66, 1980, 534-543.
- [2] P.J. Allen, C. Hobby, "Units in integral group rings of some metacyclic groups", Canad. Math. Bull. (a aparecer).
- [3] P.J. Allen, C. Hobby, "A note on the unit group of $\mathbb{Z}S_3$ ", Proc. Amer. Math. Soc. (a aparecer).
- [4] G. H. Cliff, S.K. Sehgal, A.R. Weiss, "Units of integral group rings of metabelian groups", J. Algebra 73, 1981, 167-185.
- [5] I. Hughes, K.R. Pearson, "The group of units of the integral group ring $\mathbb{Z}S_3$ ", Canad. Math. Bull. 15, 1972, 529-534.
- [6] N. Jacobson, "Basic Algebra II", W.H. Freeman and Company, San Francisco, 1980.
- [7] E. Kleinert, "Einheiten in $\mathbb{Z}[D_{2m}]$ ", J. Number Theory 13, 1981, 541-561.
- [8] Z. Marciniak, J. Ritter, S.K. Sehgal, A.R. Weiss, "Torsion units in integral group rings of some metabelian groups II", J. Number Theory (a aparecer).
- [9] S.A. Park, "The unit group of the integral group ring $\mathbb{Z}D_n$ ", J. Korean Math. Soc. 20, 1983, 75-82.

- [10] D.S. Passman, P.F. Smith, "Units in integral group rings",
J. Algebra 68, 1981, 213-239.
- [11] C. Polcino Milies, "The units of the integral group ring
 $\mathbb{Z}D_4$ ", Bol. Soc. Brasil. Mat. 4, 1972, 85-92.
- [12] C. Polcino Milies, "Anéis de Grupos", IV Escola de Álgebra,
São Paulo, 1976.
- [13] C. Polcino Milies, J. Ritter, S.K. Sehgal, "On a conjecture
of Zassenhaus on torsion units in integral group rings II",
Proc. Amer. Math. Soc. (a aparecer).
- [14] J. Ritter, S.K. Sehgal, "Integral group rings of some p-
groups", Can. J. Math. 34, 1982, 233-246.
- [15] J. Ritter, S.K. Sehgal, "On a conjecture of Zassenhaus on
torsion units in integral group rings", Math. Ann. 264,
1983, 257-270.
- [16] S.K. Sehgal, "Topics in Group Rings", Marcel Dekker, New
York, 1978.
- [17] S.K. Sehgal, A.R. Weiss, "Torsion units in integral group
rings of some metabelian groups", J. Algebra (a aparecer).
- [18] J.-P. Serre, "Linear Representations of Finite Groups",
Springer-Verlag, Heidelberg, 1977.