Conjunto de geradores dum subgrupo de índice finito em $\mathcal{U}(\mathbb{Z}G)$ de cardinalidade $\log |G|$.

de

Roberto Paulo Ribeiro Neto

UFRJ

2016

Conjunto de geradores dum subgrupo de índice finito em $\mathcal{U}(\mathbb{Z}G)$ de cardinalidade $\log|G|$.

de

Roberto Paulo Ribeiro Neto

Orientador: Guilherme Augusto de La Rocque Leal

Tese de doutorado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro — UFRJ, como parte dos requisitos necessários à obtenção do título de Doutor em Matemática.

Aprovada por:

Presidente, Prof. Guilherme Augusto de La Rocque Leal, IM-UFRJ

Prof. Ilir Snopce, IM-UFRJ

Prof. Said Sidki, DM-UNB

Prof. Jairo Zacarias Gonçalves, IME-USP

Prof. Osnel Boche Cristo, DCE-UFLA

Suplente, Prof. Severino Collier Coutinho, IM/UFRJ

Rio de Janeiro, 19/10/2016

Resumo

Não se pode determinar com facilidade a estrutura do grupo de unidades $\mathcal{U}(\mathbb{Z}G)$ do anel $\mathbb{Z}G$ dum grupo G não abeliano. Na maioria dos casos, tenta-se construir um subgrupo $H < \mathcal{U}(\mathbb{Z}G)$ que tenha índice finito. Nalguns trabalhos o grupo assim gerado é tão abstrato que não pode ser trabalhado; noutros, é, por assim dizer, tão complexo que seus geradores crescem, em quantidade, numa função geométrica do número de elementos do grupo G. Como quer que seja, pouca atenção se presta aos geradores do próprio grupo G. Nesta tese, considero o grupo E_n, o produto central de n cópias de D_4, e aproveito sua estrutura simplificada, para gerar, com $\log|E_n|$ geradores, um subgrupo de índice finito em $\mathcal{U}(\mathbb{Z}E_n)$.

Abstract

One cannot hope to easily determine the structure of the group of units $\mathcal{U}(\mathbb{Z}G)$ of the group ring $\mathbb{Z}G$ of a nonabelian group G. In most cases, one tries to construct a subgroup $H < \mathcal{U}(\mathbb{Z}G)$ of finite index. In some works, the group obtained in this manner is so abstract that it cannot be manipulated; in other works, it is, so to say, so complex that its generators grow, in number, as a geometric function of the number of elements of G. However it may be, very little attention is paid to the generators of the group G itself. In this thesis, I shall consider the group E_n, the central product of n copies of D_4, and take advantage of its simplified structure, in order to generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}E_n)$ with $\log|E_n|$ generators.

Sumário

Capítulo 1

Introdução.

1.1 Grupos, álgebras e representações.

Ao longo destas linhas, indico por G um grupo finito; por K, um corpo de números; por $\mathcal{O}_K$, seu anel de inteiros; e por KG, a K-álgebra do grupo G. A estrutura algébrica de KG pode ser conhecida pelo seguinte teorema.

Teorema 1.1.1 (Decomposição em soma direta)**.** *Seja G um grupo finito; K, um corpo de números. Então, há $D_1, ..., D_r$ anéis de divisão cujo centro é K; e anéis de matrizes $M_{n_1}(D_1), ..., M_{n_r}(D_r)$ que decompõem, de maneira única, a álgebra KG em soma direta de parcelas irredutíveis.*

$$\begin{aligned} KG &= M_{n_1}(D_1) \oplus ... \oplus M_{n_r}(D_r) \\ \therefore |G| &= \dim_K KG \\ &= \sum n_i^2 [D_i : K] \end{aligned} \tag{1.1}$$

Demonstração. *Veja-se [2] 3.4.10.*

Seja definido como se segue o homomorfismo $i : G \longrightarrow KG$:

$$\begin{aligned} i : G &\longrightarrow KG \\ g &\longmapsto 1g \end{aligned} \tag{1.2}$$

Não é difícil ver que por ele o grupo G é imerso, isomorficamente, na álgebra KG. Como se deduz de 1.1.1, deve haver r homomorfismos $\mathfrak{X}_1, ..., \mathfrak{X}_r$ que satisfaçam as relações:

$$\begin{aligned} \mathfrak{X}_i : G &\longrightarrow M_{n_i}(D_i) \\ i(g) &= \mathfrak{X}_1 \oplus ... \oplus \mathfrak{X}_r \end{aligned} \tag{1.3}$$

Em geral, se R for um anel comutativo dotado de unidade, dá-se o nome de R-representação linear a qualquer homomorfismo $\mathfrak{X} : G \longrightarrow GL_n(V)$, V, R-módulo livre e finitamente gerado.

Definição 1.1.2. *Seja G um grupo finito; R, um anel comutativo dotado de unidade. Seja, ainda, V um R-módulo livre e finitamente gerado de posto n. O homomorfismo $\mathfrak{X} : G \longrightarrow GL_n(V)$ chama-se R-representação linear de grau n. Caso a representação linear $\mathfrak{X}$ não possa ser decomposta em soma direta doutras representações lineares, como na equação 1.3, ou equivalentemente, caso o módulo V seja irredutível, $\mathfrak{X}$ recebe o nome de representação linear irredutível.*

1.2 Relações entre grupos e álgebras.

Em virtude da identificação 1.2 e da definição 1.1.2, é possível estudar o grupo G pelas suas álgebras ou pelas representações lineares. É o caso, por exemplo, do teorema abaixo, que relaciona a ordem do grupo derivado com o número de parcelas lineares da decomposição em soma direta da álgebra $\mathbb{C}G$.

Teorema 1.2.1. *Seja G um grupo finito e denote-se por G' o seu grupo derivado. Considere-se a álgebra $\mathbb{C}G$: então, o número de parcelas*[1] *M_{n_i} de dimensão $\dim_{\mathbb{C}} M_{n_i} = 1$ coincide com o valor do índice $\left[G : G'\right]$.*

Demonstração. *Cf. [7] 2.23 b.*

[1] Doravante chamadas *parcelas lineares*.

Por outro lado, a álgebra de grupo, — dado que é um anel, portanto, é uma estrutura interessante por si mesma —, pode ser investigada através das propriedades do grupo G. O próprio teorema 1.1.1 pode ser refinado, a fim de determinar a quantidade de parcelas da decomposição em soma direta.

Teorema 1.2.2. *Seja G um grupo finito; s, o número de suas classes de conjugação. Então,*

$$\mathbb{C}G = M_{n_1}(\mathbb{C}) \oplus ... \oplus M_{n_s}(\mathbb{C}). \tag{1.4}$$

Demonstração. *Cf. [7] 2.4 e 2.5.*

1.3 Unidades do anel de grupo.

Ao matemático sempre lhe parece interessante estudar o grupo dos elementos invertíveis dum anel. Se com isso ninguém se preocupasse, não haveria, por exemplo, o teorema das unidades de Dirichlet.

Teorema 1.3.1 (de Dirichlet)**.** *Proposto um corpo de números K, seja $\mathcal{O}_K$ o seu anel de inteiros. Seja, ainda, U o grupo das raízes da unidade que estejam contidas em K. Então, se houver r imersões reais e $2c$ complexas; os elementos invertíveis de $\mathcal{O}_K$ caracterizam-se pelo isomorfismo*

$$\mathcal{O}_K^* \cong U \times \mathbb{Z}^{r+c-1}. \tag{1.5}$$

À luz do teorema 1.1.1 e da identificação 1.2, é muito fácil caracterizar a estrutura dos elementos invertíveis duma álgebra de grupos, — de $\mathbb{Q}G$, por exemplo:

$$\mathcal{U}(\mathbb{Q}G) = GL_{n_1}(D_1) \oplus ... \oplus GL_{n_r}(D_r). \tag{1.6}$$

Contudo, quando se trata dos anéis de grupo, aparecem dificuldades formidáveis. A igualdade análoga à 1.6, por exemplo, não é válida:

$$\mathcal{U}(\mathbb{Z}G) \neq GL_{n_1}(\mathcal{O}(D_1)) \oplus ... \oplus GL_{n_r}(\mathcal{O}(D_r)). \tag{1.7}$$

Exemplo 1.3.2. *Seja a apresentação* $D_4 = \{a, b : a^2 = b^4 = 1, ab = b^3a\}$. *Seja* δ_{ij} *matriz elementar; então:*

$$1 + \frac{1}{4}b - \frac{1}{4}b^3 - \frac{1}{4}a + \frac{1}{4}ab^3 = 1 + \delta_{12} \notin \mathbb{Z}D_4. \tag{1.8}$$

Em geral, os teoremas que caracterizam completamente a estrutura de $\mathcal{U}(\mathbb{Z}G)$ dizem respeito a grupos abelianos, como o teorema de Higman, que fixa uma fórmula deveras semelhante à do teorema de Dirichlet 1.3.1.

Teorema 1.3.3 (de Higman)**.** *Seja* A *um grupo abeliano. Suponho que* A *contém* c *grupos cíclicos e* i *elementos de ordem* 2. *Nessa notação, pode-se dizer que vale:*

$$\mathcal{U}(\mathbb{Z}A) = \pm A \times \mathbb{Z}^{\frac{1}{2}(|A|+i-2c+1)}. \tag{1.9}$$

Demonstração. *Cf. [5] ou [14] 3.1.*

Quanto aos anéis de grupos não comutativos, no mais das vezes se consegue um subgrupo $H < \mathcal{U}(\mathbb{Z}G)$, de índice finito. Abaixo seguem-se dois exemplos.

Teorema 1.3.4 (de Ritter e Sehgal)**.** *Seja* K *um corpo de números;* $\mathcal{O}_K$*, o seu anel de inteiros;* G*, um grupo finito;* $KG = M_{n_1}(D_1) \oplus ... \oplus M_{n_k}(D_k)$*, a sua decomposição em soma direta de parcelas irredutíveis, à qual decomposição se impõem as seguintes restrições:*

1. *de que as parcelas da forma* $M_{1\times 1}(D_x) = D_x$ *sejam corpos de números ou anéis de quatérnios;*

2. *de que cada parcela da forma* $M_{2\times 2}(D_x)$ *tenha centro* $Z(M_{2\times 2}(D_x)) = Z(D_x)$ *que seja corpo algébrico e cuja dimensão racional seja maior do que* 2.

Nessas condições, o subgrupo gerado pelo centro de $\mathcal{U}(\mathcal{O}_K G)$ *e pelas unidades da forma* $1+\alpha,\ \alpha^2=0$, *terá índice finito em* $\mathcal{U}(\mathcal{O}_K G)$.

Demonstração. *Cf. [10]*

Teorema 1.3.5 (de Ritter e Sehgal)**.** *Seja* G *um grupo finito; seja, também,* $\mathbb{Q}G = M_{n_1}(D_1) \oplus ... \oplus M_{n_k}(D_k)$, *a sua decomposição em soma direta de parcelas irredutíveis, à qual decomposição se impõem as seguintes exceções:*

1. *de que não haja parcela da forma* $M_{2\times 2}(D_x)$ *cujo centro* $Z(M_{2\times 2}(D_x)) = Z(D_x)$ *seja racional ou corpo quadrático complexo;*

2. *de que não haja parcelas da forma* $M_{2^k\times 2^k}(\mathbb{H}_k)$, *cujas entradas sejam elementos de* $\mathbb{H}_k$, *quatérnios hamiltonianos de centro* $\mathbb{Q}\left(\zeta_{2^{k-1}} + \zeta_{2^{k-1}}^{-1}\right)$, ζ, *raiz primitiva da unidade.*

Sejam a *e* b *elementos de* G; *seja* $o(a)$ *a ordem de* a; $\phi(n)$, *a função de Euler;* $j \in \mathbb{Z},\ mdc(j, o(a)) = 1,\ 1 \leq j \leq o(a)$. *Em função de cada par* (j,a) *e de cada par* (a,b), *definem-se as unidades* $u(j,a)$ *e* $\mu(a,b)$, *do seguinte modo:*

1. $u(j,a) = (1+a+a^2+...+a^{j-1})^{\phi(|G|)} + \frac{1-j^{\phi(|G|)}}{o(a)}\left(1+a+...+a^{o(a)-1}\right)$;

2. $\mu(a,b) = 1 + (a-1)\, b\left(1+a+...+a^{o(a)-1}\right)$.

Se as condições acima impostas forem observadas, o subgrupo B *de* $\mathcal{U}(\mathbb{Z}G)$, *gerado pelas unidades* $u(j,a)$ *e* $\mu(a,b)$, *terá índice finito.*

Demonstração. *[11]*

1.4 Problema de tese.

O problema desta tese, o qual é motivado por esses dois resultados, é o de gerar explicitamente em $\mathcal{U}(\mathbb{Z}G)$ um subgrupo de índice finito. O grupo G, antes, a família de grupos que vou estudar neste trabalho não terá decerto o caráter abrangente de 1.3.4, nem de 1.3.5; ao contrário, vou considerar, somente, a família dos 2-grupos extra-especiais do grupo diedral[2] de oito elementos, que pode ser apresentada como se segue.

Definição 1.4.1. *Defina-se, em função de cada n, o grupo E_n pela seguinte apresentação:*

1. $E_n = \langle a_1, ..., \ a_n, \ b_1, ..., \ b_n \rangle$,

2. $a_i^2 = b_i^4 = 1, \ \forall \ i, \ 1 \leq i \leq n$,

3. $a_i b_i = b_i^3 a_i, \ \forall \ i, \ 1 \leq i \leq n$,

4. $a_i b_j = b_j a_i, \forall \ i, \ j, \ i \neq j$,

5. $a_i a_j = a_j a_i, \forall \ i, \ j, \ i \neq j$,

6. $b_i b_j = b_j b_i, \forall \ i, \ j, \ i \neq j$,

[2]Os 2-grupos extra-especiais são produtos centrais de cópias de D_4 ou de K_8. No próximo capítulo, explico mais detidamente este ponto.

7. $b_i^2 = b_j^2, \forall\ i,\ j,\ i \neq j.$

O efeito da limitação imposta ao grupo G será simplificar a estrutura do grupo de índice finito que pretendo construir. Eis o enunciado da tese:

Teorema 1.4.2. *Seja* E_n *como na definição 1.4.1. Definam-se, em função dos geradores de* E_n*, os* $n+1$ *elementos* h_n *e* $h_{n,i}$*:*

$$h_n = (1 - a_1) \dots (1 - a_n) \left(1 - b_n^2\right); \tag{1.10}$$

$$h_{n,i} = 1 - h_n b_i. \tag{1.11}$$

Então, o subgrupo $\langle b_1, ..., b_n,\ h_{n,1}, ..., h_{n,n} \rangle < \mathcal{U}(\mathbb{Z}E_n)$ *tem índice finito.*

Não o disse no enunciado acima, mas decerto demonstrarei mais à frente, que a ordem dos grupos E_n pode ser estimada em 2^{2n+1}. Se aplicasse o teorema 1.3.5 ao presente caso, precisaria construir cerca de 2^{4n+2} elementos — matriciais. Contudo, mesmo que levasse em conta alguns resultados básicos da teoria de representação de grupos, essa estimativa, que eu poderia limitar — por baixo — pelo valor $|G|^2$, continuaria a crescer, em função de n, em progressão exponencial. Ao mesmo tempo, como se observa na sua definição, as unidades $\mu(a, b)$ são definidas em função de pares dos elementos do grupo; e não em função dos seus geradores.

Se, porém, empregasse o teorema 1.3.4; teria de lidar com todas as unidades da forma $1 + \alpha,\ \alpha^2 = 0$, que existem em número infinito e não podem ser expressas, com facilidade, em função dos geradores de E_n.

Em contrapartida, o teorema desta tese, embora não tenha de fato o alcance desses dois, fixa um subgrupo de $\mathcal{U}(\mathbb{Z}E_n)$ cujo conjunto de geradores angaria, na passagem de E_n para E_{n+1}, tão-somente dois novos elementos, — um subgrupo, diga-se, cuja lei de formação depende, apenas, dos geradores de E_n.

Capítulo 2

Grupos extra-especiais.

Os objetos que figuram no enunciado do problema desta tese são os 2-grupos extra-especiais E_n e a álgebra $\mathbb{Z}E_n$. Convém falar nesses objetos antes de proceder à prova do teorema 1.4.2. Neste capítulo apresento as características mais notáveis dos grupos extra-especiais, e no próximo dedico algumas linhas à álgebra racional $\mathbb{Q}E_n$, sem cujo conhecimento nada se pode dizer do anel de inteiros $\mathbb{Z}E_n$.

Em primeiro lugar vou explicar o significado do prefixo 2 da expressão 2-*grupos extra-especiais* — esse 2 poderia ser qualquer número primo, pois que os grupos extra-especiais nada mais são do que um subgênero dos p-grupos. Em seguida introduzo a definição de grupo extra-especial e, depois de comentar brevemente algumas de suas qualidades que me serão úteis na solução do problema de tese, passo a focar a exposição nos próprios grupos E_n: para além de demonstrar que são de fato extra-especiais, vou propor uma definição recursiva, que me facilite, mais à frente, o trabalho de manipular os geradores da álgebra $\mathbb{Q}E_n$. Enfim a exposição não ficaria firme, se não caracterizasse os 2-grupos extra-especiais.

2.1 P-grupos e grupos extra-especiais.

Definição 2.1.1. *Seja G um grupo; p, um número inteiro e primo. Se a ordem de cada elemento $g \in G$ for uma potência de p; G recebe a classificação de p-grupo. Se porventura todos os elementos de G tiverem ordem p, diz-se que G é p-elementar.*

Exemplo 2.1.2. *D_n, o grupo diedral de $2n$ elementos; K_8, o grupo dos quatérnios; $\mathbb{Z}_{2^n}$ o grupo cíclico de ordem 2^n — todos esses são exemplos de 2-grupos.*

Observação 2.1.3. *Talvez não seja ocioso mencionar estes dois resultados básicos da teoria de grupos:*

1 — Se $\dfrac{G}{Z(G)}$ for cíclico, então, G será abeliano.

2 — Se G for p-grupo não trivial, então, seu centro não será trivial.

Ao abrir este capítulo mencionei que os grupos extra-especias são subgênero dos p-grupos. Mais do que isso: os grupos extra-especiais são p-grupos cujo centro goza de qualidades especiais.

Definição 2.1.4. *Seja G p-grupo não abeliano. Se seu centro $Z(G)$ for cíclico de ordem p, e se $\frac{G}{Z(G)}$ for abeliano e p-elementar, o grupo G chama-se extra-especial*[1]*.*

Teorema 2.1.5. *Seja G p-grupo extra-especial. Então:*

$$G' = Z(G).$$

Demonstração. *1 — Como G é não abeliano, G' não pode ser trivial.*

2 — Por definição o grupo derivado é o menor subgrupo de G que forma quociente

[1]Em geral, define-se grupo extra-especial pela igualdade $\Phi(G)) = Z(G) = G'$. Como, porém, o grupo de Frattini não terá nenhuma utilidade neste trabalho proponho uma definição que lhe é equivalente.

abeliano.

3 — Pela definição 2.1.4, $\frac{G}{Z(G)}$ *é abeliano.*

4 — Por 3 e por 2, $G' < Z(G)$.

5 — Novamente pela definição 2.1.4, $Z(G)$ *é cíclico de ordem prima, portanto, não pode conter subgrupos não triviais.*

6 — Por 5 e por 4, $G' = Z(G)$ $\square$

Teorema 2.1.6. *Seja G p-grupo extra-especial. Então, o número de classes de conjugação de G é dado pela equação:*

$$\sharp \text{ de classes de conjugação} = \left[G \ : \ G'\right] + p - 1 \tag{2.1}$$

Ademais, se $g \in G$ *não for central, sua classe de conjugação terá a forma:*

$$Cl(g) = gZ(G) \tag{2.2}$$

Demonstração. *1 — Por hipótese G é extra-especial. Segundo a definição 2.1.4, o quociente* $\frac{G}{Z(G)}$ *deve ser abeliano e p-elementar.*

2 — Porque é abeliano, claramente o número de classes de conjugação de $\frac{G}{Z(G)}$ *é igual ao índice* $[G \ : \ Z(G)]$.

3 — Em geral, se $A \triangleleft B$ *forem grupos, o número de classes de conjugação de* $\frac{B}{A}$ *é limitado superiormente pelo número de classes de conjugação de B:*

a — Seja $b \in B$*; então, sua classe de conjugação em B deve ter a forma* $(cbc^{-1}1)_{c\in B}$.

b — Seja, agora, $\phi : B \longrightarrow \dfrac{B}{A}$ *a projeção canônica — sobrejetiva — de B em* $\dfrac{B}{A}$.

c — Nessa notação, a imagem de $(cbc^{-1})_{c\in B}$ *por* ϕ *deverá ser* $\left(\phi(c)\,\phi(b)\,\phi(c)^{-1}\right)_{\phi(c)\in\frac{B}{A}}$.

d — *Como* $\phi(c)$ *percorre todos os elementos de* $\frac{B}{A}$, *segue-se que* $\left(\phi(c)\,\phi(b)\,\phi(c)^{-1}\right)_{\phi(c)\in\frac{B}{A}}$ *é a classe de conjugação de* $\phi(b)$ *em* $\frac{B}{A}$.

4 — *Por 3 e por 2, o número de classes de conjugação de* G *deve ser pelo menos* $[G\ :\ Z(G)]$.

5 — *Excluo, momentaneamente, da contagem realizada em 4, a classe de conjugação da unidade. Sem ela, faço uma nova estimativa do número de classes de conjugação:* $[G\ :\ Z(G)]-1$.

6 — *Visto que na construção do quociente* $\frac{G}{Z(G)}$ *excluí os elementos do centro, e que cada elemento do centro constitui, por si mesmo, uma classe de conjugação; a estimativa que propus em 5 posso corrigi-la da seguinte maneira:*

$$\sharp \text{ de classes de conjugação de } G \geq [G\ :\ Z(G)]-1+p.$$

7 — *Seja, agora,* $g \notin Z(G)$. *Valendo-me da proposição 2.1.5, justifico os seguintes cálculos:*

$$\begin{aligned} y \in Cl(g) &\iff \exists\ x,\ x\in G,\ xgx^{-1}=y \\ &\iff \exists\ x,\ x\in G,\ xgx^{-1}g^{-1}g=y \\ &\iff \exists\ x,\ x\in G,\ [x,\ g]\,g=y \\ &\iff \exists\ z,\ z\in Z(G),\ zg=y \\ &\therefore\ gZ(G)=Cl(g). \end{aligned}$$

8 — *Assim o segundo item do teorema fica demonstrado. Para demonstrar o primeiro, basta empregar o próprio item 7: uma vez que a aplicação* $g \longmapsto zg$ *é*

injetiva, deduzo que

$$|Cl\,(g)| = |gZ\,(G)|$$

$$= p.$$

9 — Como, por 5, o número de classes de conjugação que não contêm elemento central é $[G\ :\ Z\,(G)] - 1$*, e como, por 8, o número de elementos contidos em cada uma dessas classes é* p*; posso contar, ao todo,* $p\,([G\ :\ Z\,(G)] - 1)$ *elementos contidos nessas classes.*

10 — Reinserindo de volta na contagem os elementos do centro que, desde o parágrafo 7, excluíra da estimativa, encontro $p\,([G\ :\ Z\,(G)] - 1) + p$ *elementos de* G*. Simplificando essa expressão, obtenho isto:*

$$\begin{aligned} p\,([G\ :\ Z\,(G)] - 1) + p &= p\,[G\ :\ Z\,(G)] - p + p \\ &= p\,[G\ :\ Z\,(G)] \\ &= |G| \quad \textit{cf. teorema de Lagrange e 2.1.4} \end{aligned}$$

11 — Por 10 descubro que cada elemento do grupo G *se encontra numa das* $[G\ :\ Z\,(G)] - 1 + p$ *classes de conjugação, que propus nos §§4-6.*

12 — Novamente pelo teorema 2.1.5, $Z\,(G) = G'$*, por isso afirmo a validade do primeiro item do enunciado:*

$$\sharp \textit{ de classes de conjugação} = \left[G\ :\ G^{'}\right] + p - 1 \quad \square$$

2.2 Os objetos de trabalho — os grupos da forma E_n

Proposição 2.2.1. *Os grupos da forma* E_n*, definidos em 1.4.1, são extra-especiais.*

Demonstração. *1 — Fixado* $i,\ 1 \leq i \leq n$*, seja* D_i *o subgrupo de* E_n*, gerado pelos elementos* a_i *e* b_i*.*

2 — Segundo as leis de formação 1.4.1.2 e 1.4.1.3; D_i *é isomórfico ao grupo diedral de 8 elementos.*

3 — Como D_i *é 2-grupo, seu centro não pode ser trivial — cf 2.1.3.2.*

4 — Considero, agora, o quociente $\dfrac{D_i}{Z(D_i)}$*: segundo o teorema de Lagrange, sua ordem deve ser um destes quatro valores: 1, 2, 4, 8.*

5 — Por 3, o primeiro e o último valor não devem ser levados em conta.

6 — Se o quociente $\dfrac{D_i}{Z(D_i)}$ *fosse cíclico, o grupo* D_i *seria abeliano — cf 2.1.3. É-me lícito deduzir que a ordem de* $\frac{D_i}{Z(D_i)}$ *é 4 e que esse grupo é 2-elementar e abeliano*[2]*.*

7 — Da regra 1.4.1.3, infiro o centro: $\langle b_i^2 \rangle = Z(D_i)$

$$a_i b_i = b_i^3 a_i \Longrightarrow a_i b_i^2 = b_i^2 a_i$$

$$\Longrightarrow b_i^2 \in Z(D_i)$$

8 — Segundo as regras 1.4.1.4-6, se i *for diferente de* j*;* D_i *estará contido no centralizador de* D_j*.*

9 — Por essa razão, $Z(E_n) = \bigcap Z(D_i)$

10 — Pela lei de formação 1.4.1.7, percebe-se que $Z(E_n) = \langle b_i^2 \rangle$ *é cíclico de ordem 2.*

11 — Segundo o §6 e o teorema 2.1.5, D_i *é extra-especial e seu centro é idêntico ao grupo derivado* D_i'*.*

12 — Segundo o §8, o subgrupo derivado de E_n *deve estar contido no centro* $Z(E_n)$*.*

13 — Em virtude da regra 1.4.1.3, E_n *não é abeliano, portanto,* E_n' *não pode ser*

[2] Afinal, há somente dois grupos de ordem 4, ambos abelianos, um cíclico, outro 2-elementar.

trivial.

14 — Por 10 e por 13, $E_n' = Z(E_n)$

15 — Por 14, $\dfrac{E_n}{Z(E_n)}$ *é abeliano.*

16 — Ademais, a regra 1.4.1.2, converte-se, em relação ao quociente $\frac{E_n}{Z(E_n)}$*, na fórmula:*

$$a_i^2 = b_i^4 = 1,\ \forall\ i,\ 1 \leq i \leq n \underbrace{\longrightarrow}_{\text{pela passagem ao quociente}} a_i^2 = b_i^2 = 1,\ \forall\ i,\ 1 \leq i \leq n$$

17 — Por 16 e por 15, $\dfrac{E_n}{Z(E_n)}$ *é 2-elementar e abeliano; por 10,* $Z(E_n)$*, cíclico de ordem prima: segundo a definição 2.1.4,* E_n *é extra-especial.* □

2.3 Produto central de grupos e a caracterização dos grupos extra-especiais.

Trabalhar com o grupo E_n, diretamente pela apresentação 1.4.1, seria sobremodo penoso e infrutífero, para o propósito deste trabalho: para demonstrar o problema de tese, precisarei empregar uma construção recursiva, definida em função dos geradores do grupo. Com as considerações abaixo viso a conferir à família de grupos E_n a estrutura recursiva que me é mais conveniente.

Definição 2.3.1. *Sejam* G *e* H *grupos finitos;* $Z(G)$ *e* $Z(H)$*, seus centros, sendo* $Z(G) \cong Z(H)$*. Seja* $\phi : Z(G) \longrightarrow Z(H)$ *um isomorfismo de grupos. Denote-se por* $diag(Z(G),\ \phi(Z(G)))$ *o subgrupo normal de* $G \times H$ *formado pelos pares* $(g, \phi(g))_{g \in G}$*. Chama-se produto central entre* G *e* H *— doravante indicado por* $G \times^{\circ} H$ *— o grupo:*

$$G \times^{\circ} H = \frac{G \times H}{diag(Z(G),\ \phi(Z(G)))}$$

Observação 2.3.2. *$diag(Z(G),\ \phi(Z(G))) < Z(G) \times Z(H)$ é normal em $G \times H$ por ser central. O grupo $G \times^{\circ} H$ fica, portanto, bem definido.*

A seguinte definição mostra uma maneira de, conhecido um grupo extra-especial, construir novos, pelo produto central.

Definição 2.3.3. *Denote-se por P_1 um p-grupo extra-especial. Seja P_n definido pela relação de recursão que se segue:*

$$P_n = P_{n-1} \times^{\circ} P_1 \tag{2.3}$$

Proposição 2.3.4. *A família dos grupos da definição recursiva 2.3.3 é família de grupos extra-especiais.*

Demonstração. *1 — Convém verificar que P_n está, de fato, bem definido.*

2 — No caso de P_2, isso é trivial:

$$Z(P_1) = Z(P_1) \Longrightarrow \exists P_2 = P_1 \times^{\circ} P_1$$

3 — Veja-se, no entanto, o que vem a ser $Z(P_2)$

$$\begin{aligned} Z(P_2) &= Z(P_1 \times^{\circ} P_1) \\ &= Z\left(\frac{P_1 \times P_1}{diag(Z(P_1), Z(P_1))}\right) \\ &= \frac{Z(P_1) \times Z(P_1)}{diag(Z(P_1), Z(P_1))} \\ \therefore |Z(P_2)| &= \frac{|Z(P_1)|\,|Z(P_1)|}{|diag(Z(P_1), Z(P_1))|} \\ &= \frac{p^2}{p} \\ &= p \end{aligned}$$

4 — Como os grupos de ordem p, p primo, são, sempre, isomórficos, segue-se que:

$$Z(P_2) \cong Z(P_1)$$

$$\therefore\ \exists P_3$$

5 — Se, por indução, eu supuser que $|Z(P_k)| = p \implies Z(P_k) \cong Z(P_1),\ \forall\, k,\ 1 \leq k \leq n$, *então,* P_{n+1} *fica bem definido e:*

$$\begin{aligned} Z(P_{n+1}) &= Z(P_n \times^{\circ} P_1) \\ &= Z\left(\frac{P_n \times P_1}{diag(Z(P_n), Z(P_1))}\right) \\ &= \frac{Z(P_n) \times Z(P_1)}{diag(Z(P_n), Z(P_1))} \\ \therefore |Z(P_n)| &= \frac{|Z(P_n)|\,|Z(P_1)|}{|diag(Z(P_n), Z(P_1))|} \\ &= \frac{p^2}{p} \\ &= p \end{aligned}$$

$$\therefore Z(P_{n+1}) \cong Z(P_1)$$

$$\implies \exists P_{n+2}$$

6 — Segundo o parágrafo 5 e a definição 2.1.4, metade do trabalho está pronta: $|Z(P_n)| = p, \forall n \in \mathbb{N}$.

7 — Agora, faço a seguinte observação:

$$\begin{aligned} \forall n,\ \frac{P_n}{Z(P_n)} &= \frac{P_{n-1} \times^{\circ} P_1}{Z(P_{n-1} \times^{\circ} P_1)} \\ &= \frac{\dfrac{P_n \times P_1}{diag(Z(P_n), Z(P_1))}}{\dfrac{Z(P_n) \times Z(P_1)}{diag(Z(P_n), Z(P_1))}} \\ &= \frac{P_n \times P_1}{Z(P_n) \times Z(P_1)} \text{ pelo primeiro teorema dos isomorfismos} \\ &= \frac{P_n}{Z(P_n)} \times \frac{P_1}{Z(P_1)}. \end{aligned}$$

8 — Em particular, se n for igual a 2:

$$\frac{P_2}{Z(P_2)} = \frac{P_1}{Z(P_1)} \times \frac{P_1}{Z(P_1)}$$

9 — $\dfrac{P_2}{Z(P_2)}$ *será, portanto, produto cartesiano entre dois grupos abelianos p-*

elementares, segue-se que $\frac{P_2}{Z(P_2)}$ *é abeliano e p-elementar.*

10 — Se, por indução, eu supuser que $\frac{P_k}{Z(P_k)}$ *é abeliano e p-elementar,* $\forall k, 1 \leq k \leq n$*, poderei inferir de 7 que* $\frac{P_{n+1}}{Z(P_{n+1})}$ *é abeliano e p-elementar.*

11 — Segundo a definição 2.1.4, P_n *é extra-especial.* □

Corolário 2.3.5. *No caso particular em que* $P_1 = D_4$ *é o grupo diedral de oito elementos, a ordem de cada termo da recursão 2.3.3 pode estimar-se com facilidade, do seguinte modo:*

$$\begin{aligned} |P_n| &= |P_{n-1} \times^{\circ} P_1| \\ &= \frac{|P_{n-1}|\,|P_1|}{2} \\ &= |P_{n-1}|\,2^2 \end{aligned}$$

Sucessivas aplicações retro-ativas da fórmula acima resultam na igualdade:

$$|P_{n+1}| = 2^{2(n+1)+1}. \quad \square \tag{2.4}$$

Para arrematar este capítulo, menciono o teorema de caracterização dos 2-grupos extra-especiais, segundo o qual os grupos P_n da definição recursiva 2.3.3, quando $P_1 = E_1$, coincidem, por isomorfismo, com os da apresentação 1.4.1.

Teorema 2.3.6 (de Caracterização)**.** *Se G for 2-grupo extra-especial, então, a ordem de G terá a forma* 2^{2n+1}*, e G poderá ser enquadrado numa das duas classes de isomorfismo abaixo arroladas:*

1. *O produto central de n cópias de* D_4*;*

2. *O produto central de n-1 cópias de* D_4 *e uma cópia dos quatérnios* K_8*.*

Demonstração. *Cf. [1] 13.8*

Capítulo 3

A álgebra racional dos grupos extra-especiais.

O primeiro termo da seqüência infinita de grupos E_n é o D_4. Para construir o segundo termo da série, é preciso realizar dois passos: determinar o produto direto $D_4 \times D_4$, em seguida, o quociente $\frac{D_4 \times D_4}{\langle (b^2, b^2) \rangle}$. Diga-se o mesmo dos demais elementos da lista: construído o produto $E_n \times D_4$, pode-se formar o quociente $E_{n+1} = \frac{E_n \times D_4}{\langle (b_n^2, b^2) \rangle}$.

Semelhantes passos se manifestam na passagem de $\mathbb{Q}E_n$ para $\mathbb{Q}E_{n+1}$: em geral, propostos dois grupos G e H, a álgebra $\mathbb{Q}(G \times H)$ do produto direto $G \times H$ é o produto tensorial[1] $\mathbb{Q}G \otimes_{\mathbb{Q}} \mathbb{Q}H$. Quanto aos quocientes, por exemplo, $\frac{G}{N}$, $N \triangleleft G$, a álgebra do grupo $\mathbb{Q}\frac{G}{N}$ se recupera, por assim dizer, através da multiplicação da álgebra inteira por um elemento idempotente central, convenientemente escolhido, e: $\mathbb{Q}\frac{G}{N} \cong \mathbb{Q}Ge$.

De posse desses resultados, será possível mostrar que a álgebra racional $\mathbb{Q}E_n$

[1] sc., o produto tensorial de Kronecker. Com o símbolo $\otimes$ pretendo indicar o produto tensorial de Kronecker construído sobre os racionais, ou seja, $\otimes_{\mathbb{Q}}$. Na seção 3.1 arrolo algumas características interessantes desse produto tensorial.

goza duma estrutura simplicíssima:

$$\mathbb{Q}E_n \cong \oplus^{2^{2n}}\mathbb{Q} \oplus M_{2^n}(\mathbb{Q})$$

Em parte o objetivo deste capítulo é demonstrar o isomorfismo da equação acima proposta; em parte, ele conterá os resultados necessários à obtenção e manipulação das representações da forma $\mathfrak{X} : E_n \longrightarrow \mathbb{Q}E_n$.

O primeiro dos objetivos alcanço-o com recurso à apresentação 1.4.1; o segundo, com o auxílio da construção recursiva 2.3.3 — mas sobre este último tema, falo no próximo capítulo, por enquanto, centro-me nos resultados sobre álgebras de grupos.

3.1 A álgebra do produto direto de grupos.

Teorema 3.1.1. *Sejam G e H grupos; e K, corpo. Sejam, ainda, V e W K-espaços lineares. Então:*

1. $K(G \times H) \cong KG \otimes KH$;
2. *Sejam $\mathfrak{X} : G \longrightarrow GL_n(V)$ e $\mathfrak{Y} : H \longrightarrow GL_m(W)$ representações lineares. Então, $\mathfrak{X} \otimes \mathfrak{Y}$ é representação linear de G por $GL_{nm}(V \otimes W)$;*
3. *Ademais, $\mathfrak{X} \otimes \mathfrak{Y}$ será irredutível se, e somente se, $\mathfrak{X}$ e $\mathfrak{Y}$ forem irredutíveis.*

Corolário 3.1.2. *Sejam G e H grupos. Caso $\mathbb{Q}G$ e $\mathbb{Q}H$ sejam dados por estas relações:*

$$\mathbb{Q}G = M_{n_1}(\mathbb{Q}) \oplus ... \oplus M_{n_r}(\mathbb{Q})$$

$$\mathbb{Q}H = M_{n_1}(\mathbb{Q}) \oplus ... \oplus M_{n_s}(\mathbb{Q})$$

Então,

$$\mathbb{Q}(G \times H) = \bigoplus_{i,j} M_{n_i n_j}(\mathbb{Q})$$

3.2 Algumas propriedades do produto tensorial de Kronecker.

Neste trabalho vou realizar cálculos explícitos com matrizes. Convém, portanto, deixar claro que pelo símbolo $\otimes$, quando aparecer junto a representações lineares, como na equação $\mathfrak{X} \otimes \mathfrak{Y}$, indico o produto tensorial de Kronecker. Talvez não seja ocioso arrolar as propriedades desse produto que me serão mais úteis.

Teorema 3.2.1 (cf. [3])**.** *Sejam A, B, C, D matrizes quaisquer.*

1. *O produto tensorial é bilinear;*
2. *O produto tensorial é associativo: $A \otimes (B \otimes C) = (A \otimes B) \otimes C$;*
3. *Se os produtos AC e BD estiverem definidos, i.e., se o número de colunas de A for idêntico ao número de linhas de C, e se o número de colunas de B for idêntico ao número de linhas de D, então, vale:*

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$

3.3 A álgebra do quociente de grupos.

Para terminar o breve arrolo de resultados, eis o modo como se determina a álgebra dum quociente de grupos:

Teorema 3.3.1. *Seja R um anel comutativo dotado de unidade. Seja $H \triangleleft G$ um subgrupo normal dum grupo finito G. Definam-se como se segue $\hat{H} \in RG$ e $e_H \in RG$:*

$$\hat{H} = \sum_{h \in H} h$$

$$e_H = \frac{\hat{H}}{|H|}$$

Se $|H|$ for invertível em R, então:

1. *e_H é idempotente central;*
2. *$RG \cong RGe_H \oplus RG(1 - e_H)$*
3. *$RGe_H \cong R\frac{G}{H}$.*

Observação 3.3.2. *1. Em geral, dado que e_H é central, sua matriz de representação deve ser diagonal.*

$$\therefore \exists \lambda_1, ..., \lambda_n \in R,\ e_H = diag(\lambda_1, ..., \lambda_n).$$

2. E, porque é idempotente, essa matriz deve satisfazer:

$$\begin{aligned} diag(\lambda_1, ..., \lambda_n) &= e_H \\ &= e_H^2 \\ &= diag\left(\lambda_1^2, ..., \lambda_n^2\right) \\ \therefore \lambda_i^2 &= \lambda_i,\ \forall i. \end{aligned}$$

3. Desde que o anel R do enunciado 3.3.1 seja domínio de integridade, os λ_i devem satisfazer:

$$\lambda_i = 0,\ 1.$$

3.4 A decomposição da álgebra $\mathbb{Q}E_n$.

Teorema 3.4.1. $\mathbb{Q}D_4 = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q})$.

Demonstração. *1 — Segundo o teorema 1.1.1, deve haver r anéis de divisão $\mathbb{D}_i$ e anéis de matrizes $M_{n_i}(\mathbb{D}_i)$ que decomponham, de maneira única, a álgebra $\mathbb{Q}D_4$*

em soma direta de parcelas irredutíveis:

$$\mathbb{Q}D_4 = M_{n_1}(\mathbb{D}_1) \oplus ... \oplus M_{n_r}(\mathbb{D}_r).$$

2 — Segundo 2.1.6, o número de classes de conjugação de D_4 é 5.

3 — Segundo o teorema 1.2.2, o número de parcelas da decomposição em soma direta da álgebra $\mathbb{C}D_4$ deve ser idêntico ao número de classes de conjugação, i.e., 5.

4 — Por outro lado, a quantidade de parcelas lineares de $\mathbb{C}D_4$ é fixada pelo índice do grupo derivado, a saber, 4.

5 — Conforme ensina o teorema 1.2.1, que aqui se presta à finalidade inversa para a qual o mencionei na introdução, 4 devem ser as parcelas lineares da soma direta da decomposição de $\mathbb{C}D_4$.

6 — Novamente segundo 1.1.1, a dimensão da parcela restante – indicada por V –, a não linear, deve satisfazer as relações abaixo.

$$\begin{aligned} |D_4| &= 8 \\ &= 1+1+1+1+\dim_{\mathbb{C}} V \\ \therefore \dim_{\mathbb{C}} V &= 4 \end{aligned} \tag{3.1}$$

7 — Assim sendo, $\mathbb{C}D_4$ deve decompor-se desta maneira:

$$\mathbb{C}D_4 = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus M_{2x2}(\mathbb{C}). \tag{3.2}$$

8 — Em geral, quando se trata dum grupo G finito, qualquer homomorfismo $\mathfrak{X} : G \longrightarrow \mathbb{C}$ deve ter imagem algébrica, porquanto, se g pertencer a G, haverá n, $g^n = 1$.

$$\begin{aligned} \therefore g^n = 1 &\Longrightarrow \mathfrak{X}^n(g) = 1 \\ &\Longleftrightarrow \mathfrak{X}^n(g) - 1 = 0 \end{aligned}$$

9 — Em princípio, na restrição dos escalares complexos de $\mathbb{C}D_4$ aos racionais de $\mathbb{Q}D_4$, as parcelas lineares complexas poderiam tornar-se corpos de números K. Por conseguinte, se fosse esse o caso, as parcelas lineares complexas cindir-se-iam em uma, duas, três, enfim, tantas parcelas, quanto valesse o índice $[K : \mathbb{Q}]$.

10 — No presente caso, a apresentação 1.3.2 enseja a verificação de que os homomorfismos lineares complexos são, em verdade, racionais:

$$\begin{aligned} \mathfrak{X}(a)\,\mathfrak{X}(b) &= \mathfrak{X}(b)^3\,\mathfrak{X}(a) \\ \mathfrak{X}(a)^2 &= \mathfrak{X}(b)^4 \\ &= 1 \end{aligned} \tag{3.3}$$

11 — Da primeira equação de compatibilidade proposta em 10, deduz-se que

$$\begin{aligned} \mathfrak{X}(a) &= \pm 1 \\ \mathfrak{X}(b) &= \pm 1,\ \pm i \end{aligned} \tag{3.4}$$

12 — Já a primeira equação de 11 limita os resultados possíveis da última equação de 11:

$$\begin{aligned} \mathfrak{X}(a)\,\mathfrak{X}(b) = \mathfrak{X}(b)^3\,\mathfrak{X}(a) &\Longrightarrow \mathfrak{X}(b) = \mathfrak{X}(b)^3 \\ &\Longrightarrow 1 = \mathfrak{X}(b)^2 \\ \therefore \mathfrak{X}(b) &= \pm 1. \end{aligned}$$

13 — De volta ao teorema 1.1.1: a contagem das dimensões racionais das parcelas irredutíveis de $\mathbb{Q}D_4$ até agora exibidas sugere que deve haver mais uma parcela irredutível, de dimensão racional 4.

14 — Seja $M_{n_5}(D_5)$ a parcela de dimensão racional 4. Então:

$$\begin{aligned} \dim_{\mathbb{Q}} M_{n_5}(D_5) &= n_5^2\,[D_5 : \mathbb{Q}] \\ &= 4 \end{aligned}$$

14 — Portanto, das duas uma:

$$n_5^2 = 4,\ [D_5 : \mathbb{Q}] = 1 \Longrightarrow M_{n_5}(\mathbb{Q})$$

$$n_5^2 = 1,\ [D_5 : \mathbb{Q}] = 4 \Longrightarrow \mathbb{H},\ \textit{quatérnios hamiltonianos.}$$

15 — Para decidir qual das duas possibilidades descobertas acima é a verdadeira convém exibir explicitamente a representação matricial irredutível $\mathfrak{X} : D_4 \longrightarrow M_2(\mathbb{Q})$.

16 — Por sua natureza geométrica, D_4 *pode ser representado isomorficamente por matrizes ortogonais:*

$$\mathfrak{X}(a) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{3.5}$$

$$\mathfrak{X}(b) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \tag{3.6}$$

17 — Como $\mathfrak{X}(b)$ *não admite, para além da origem, nenhum ponto fixo, deve ser irredutível.*

18 — Segue-se, portanto, que

$$\mathbb{Q}D_4 = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}). \quad \square$$

Enfim, a estrutura de $\mathbb{Q}E_n$:

Teorema 3.4.2. *Seja* E_k, $\forall k \in \mathbb{N}$, *como na definição 1.4.1; e* $E_1 = D_4$. *Então, a decomposição em soma direta da sua álgebra é:*

$$\mathbb{Q}E_k \cong \oplus^{2^{2k}}\mathbb{Q} \oplus M_{2^k}(\mathbb{Q}) \tag{3.7}$$

Demonstração. *1 — Segundo 2.3.6 e 2.3.4, o grupo* E_k *pode ser construído por recursão, conforme a lei 2.3.3.*

2 — Segundo 3.1.1 e 3.3.1, a álgebra $\mathbb{Q}E_k$ pode ser construída por recursão:

$$\begin{aligned}\mathbb{Q}E_1 &= \mathbb{Q}D_4 \\ &= \mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}\oplus M_2(\mathbb{Q}) \quad \textit{por 3.4.1.}\\ \mathbb{Q}E_k &= (\mathbb{Q}E_{k-1}\otimes\mathbb{Q}D_4)\left(\frac{1+b_i^2b^2}{2}\right)\end{aligned}$$

3 — Segundo o corolário 3.1.2, a álgebra $\mathbb{Q}E_k$ deve decompor-se na forma:

$$\mathbb{Q}\oplus ...\oplus\mathbb{Q}\oplus M_{n_1}(\mathbb{Q})\oplus ...\oplus M_{n_r}(\mathbb{Q})$$

4 — Considere-se $\mathbb{C}E_k$: segundo 1.2.2, 2.1.6 e 2.3.5, o número de componentes da decomposição de $\mathbb{C}E_k$ em soma direta deve ser:

$$\frac{2^{2k+1}}{2}+2-1=2^{2k}+1.$$

5 — Segundo 1.2.1, o número de parcelas lineares deve ser idêntico ao índice do grupo derivado: 2^{2k}

6 — De acordo com 1.1.1, a dimensão δ da parcela restante deve obedecer à esta relação:

$$\begin{aligned}2^{2k+1} &= |E_k| \\ &= 2^{2k}+n. \\ \therefore n &= 2^{2k+1}-2^{2k} \\ &= 2^{2k}\end{aligned}$$

7 — De 4-6 deduzo

$$\mathbb{C}E_k=\oplus^{2^{2k}}\mathbb{C}\oplus M_{2^k}(\mathbb{C})$$

8 — Por 3 e por 7 concluo que:

$$\mathbb{Q}E_k=\oplus^{2^{2k}}\mathbb{Q}\oplus M_{2^k}(\mathbb{Q}) \quad \square$$

Capítulo 4

$\mathbb{Z}E_n$

No teorema 1.3.4, que serviu de inspiração a esta tese, requer-se, para gerar um subgrupo de índice finito em $\mathcal{U}(\mathbb{Z}G)$, o centro de $\mathcal{U}(\mathbb{Z}G)$, para além de todas as unidades da forma $1+\alpha,\ \alpha^2=0$. Nas próximas linhas vou demonstrar por que o centro é necessário à construção de subgrupos de índice finito em $\mathcal{U}(\mathbb{Z}G)$; por que o centro não precisa ser levado em conta no caso de $\mathbb{Z}E_n$; e por que nem todas as unidades da forma $1+\alpha,\ \alpha^2=0$ são necessárias para resolver o problema de tese. Enfim, explicados esses pontos, convém dizer qual será o método de prova do teorema central da tese.

4.1 A relação entre o índice e o centro.

Em geral, a presença do centro dum grupo infinito é condição necessária à produção dum subgrupo de índice finito.

Proposição 4.1.1. *Sejam $H<G$ grupos infinitos. Se $Z(G)$ tiver ordem infinita, e $Z(G)\cap H=1$, então, $[G:H]=\infty$.*

Demonstração. *1 — Tem-se $Z(G)\triangleleft G$, portanto, $HZ(G)<G$.*

2 — Aplico o segundo teorema dos isomorfismos, levando em conta a hipótese

$Z(G) \cap H = 1$*:*

$$\begin{aligned} Z(G) &\cong \frac{Z(G)}{Z(G) \cap H} \\ &\cong \frac{HZ(G)}{H} \\ &\leq \frac{G}{H} \end{aligned}$$

3 — Por conseguinte, posso deduzir a seguinte relação entre as ordens:

$$\begin{aligned} +\infty = |Z(G)| \\ \leq [G : H] \quad \square \end{aligned}$$

4.2 A caracterização das unidades centrais do anel de grupo.

Para caracterizar as unidades centrais de ordem finita dum anel de grupo é preciso introduzir o seguinte termo:

Definição 4.2.1. *Seja R anel comutativo dotado de unidade. As unidades da forma $y = rg,\ r \in R^*,\ g \in G$, chamam-se unidades triviais.*

Teorema 4.2.2. *Seja G grupo finito. Então, as unidades centrais de ordem finita de $\mathbb{Z}G$ são triviais.*

Demonstração. *Cf. [2] 7.3*

Assim sendo, o número de unidade triviais é $2|G|$. Portanto, o foco das atenções devem sê-lo as unidades de ordem infinita. Felizmente, há o seguinte teorema de caracterização que pode ser empregado com proveito no estudo dos E_n.

Teorema 4.2.3. *Seja G grupo finito. Sejam, também, $x \in G$ e $j \in \mathbb{N}$, $(j, |G|) = 1$. Então, todas as unidades centrais de $\mathbb{Z}G$ serão triviais se, e somente se, x^j for conjugado de x ou x^{-1}.*

Demonstração. *Cf. [13]*

Corolário 4.2.4. *Seja G 2-grupo extra-especial. Então, todas as unidades centrais de $\mathbb{Z}G$ são triviais.*

Demonstração. *1 — Seja $x \in G$. Segundo 2.1.6, a classe de conjugação de x deve ter a forma $xZ(G)$.*

2 — Então, para cada g in G deve haver $z_g \in Z(G)$ que satisfaça:

$$\begin{aligned} x^g &= xz_g \\ \implies (x^g)^2 &= x^2 z_g^2 \quad z_g \text{ é central} \\ &= x^2 \quad \text{o centro é, por hipótese, cíclico de ordem } 2. \\ \therefore (x^g)^2 &= x^2 \ \forall \ g \in G. \end{aligned}$$

3 — Por 2, x^2 deve ser elemento central. Se $x^2 = 1$, x é conjugado consigo mesmo e x^1 é a única potência possível de construir.

4 — Se, porém, $x^2 = z$, sendo z o único elemento não trivial do centro, então, $x^4 = 1$, portanto, $x^3 = x^{-1}$.

5 — A classe de conjugação de x será, à luz de 2.1.6, x, x^3.

6 — Por 3, 4, 5 e pelo teorema 4.2.3, todas as unidades centrais de G são triviais.

□

4.3 Unidades e elementos nilpotentes.

O centro, porém, não é o único elemento requerido no teorema 1.3.4: importa comentar as unidades da forma $1+\alpha,\ \alpha^2=0$.

Definição 4.3.1. *Seja π_i, definido para cada $i,\ 1\leq i\leq 2^{2n}+1$, a projeção na i-ésima parcela da decomposição em soma direta*

$$\mathbb{Q}E_n \cong \oplus^{2^{2n}}\mathbb{Q}\oplus M_{2^n}(\mathbb{Q})$$

Observação 4.3.2. *Portanto, $\pi_{2^{2n}+1}$ é a projeção na parcela $M_{2^n}(\mathbb{Q})$.*

Proposição 4.3.3. *Seja $x\in\mathbb{Q}E_n,\ x\neq 0,\ x^2=0$. Então,*

$$\pi_i(x)=0,\ \forall\ i,\ 1\leq i\leq 2^{2n}$$

$$\pi_{2^{2n}+1}(x)\neq 0$$

Demonstração. *1 — Conforme ficou dito em 3.4.2, a decomposição em soma direta de $\mathbb{Q}E_n$ é*

$$\mathbb{Q}E_n = \oplus^{2^{2n}}\mathbb{Q}\oplus M_{2^n}(\mathbb{Q})$$

2 — Por conseguinte, cada $x\in\mathbb{Q}E_n$ admite decomposição em soma direta, de maneira unívoca, na forma abaixo indicada:

$$\begin{aligned} x &= \pi_1(x)+\ldots+\pi_{2^{2n}}(x)+\pi_{2^{2n}+1}(x)\\ \pi_i(x)&\in\mathbb{Q},\ \forall\ i,\ 1\leq i\leq 2^{2n}\\ \pi_{2^{2n}+1}(x)&\in M_{2^n}(\mathbb{Q})\\ \pi_i(x)\,\pi_j(x)&=\pi_j(x)\,\pi_i(x)\\ &=0,\ \forall\ i,j,\ i\neq j. \end{aligned} \tag{4.1}$$

3 — Por hipótese, vale $x^2 = 0$*, então,*

$$\begin{aligned} 0 &= x^2 \\ &= \left(\pi_1(x) + ... + \pi_{2^{2n}}(x) + \pi_{2^{2n}+1}(x)\right)^2 \\ &= \pi_1(x)^2 + ... + \pi_{2^{2n}}(x)^2 + \pi_{2^{2n}+1}(x)^2 \\ \implies \pi_i(x)^2 &= 0,\ \forall\ i,\ 1 \leq i \leq 2^{2n} \\ \therefore \pi_i(x) &= 0 \quad \textit{porque } \mathbb{Q} \textit{ é corpo} \quad \square \end{aligned}$$

Como essa relação vale para todo elemento da álgebra $x \in \mathbb{Q}E_n$, em particular, deve valer para $x \in \mathbb{Z}E_n$. Ou seja, se x satisfizer $x^2 = 0$, então, x admitirá projeção não trivial somente na componente $M_{2^n}(\mathbb{Q})$. Os próximos resultados contêm em si as ferramentas adequadas para lidar com essa componente.

Proposição 4.3.4. *Na representação proposta na seção 3.4, vale a relação:*

$$\mathcal{U}(\mathbb{Z}E_n) \subsetneq \oplus^{2^{2n}} \{\pm 1\} \oplus SL_{2^n}(\mathbb{Z}).$$

Demonstração. *1 — Segundo os parágrafos 11 e 12 da demonstração de 3.4.1, toda representação* $\mathfrak{X} : D_4 \longrightarrow \mathbb{Q}$ *assume valores em* $\mathbb{Z}$*, mais precisamente,* $\{\pm 1\}$*.*

2 — Segundo 3.1.1 e 3.3.1, toda representação $\mathfrak{X} : E_n \longrightarrow \mathbb{Q}$ *deve ser o produto tensorial de Kronecker de representações lineares de* D_4*.*

3 — Como o produto tensorial de números racionais coincide com a multiplicação racional, toda representação $\mathfrak{X} : D_4 \longrightarrow \mathbb{Q}$ *assume valores em* $\{\pm 1\}$*.*

4 — Por outro lado, no parágrafo 16 da demonstração do mesmo 3.4.1, ficou dito que a representação — naquele parágrafo proposta — de grau 2 irredutível de D_4 *tem imagem contida em* $SL_2(\mathbb{Z})$*.*

5 — À semelhança de 2 e 3, é possível concluir que essa representação de grau 2^n *de* E_n *deve ter por contradomínio* $SL_{2^n}(\mathbb{Z})$*.*

6 — Convém lembrar que o anel de grupo $\mathbb{Z}E_n$ é o conjunto das somas formais:

$$\sum a_g g,\ a_g \in \mathbb{Z},\ g \in E_n$$

7 — Pelo que ficou dito em 3 e 5, cada $g \in E_n$ é representável por matrizes de entradas inteiras.

$$\therefore \mathbb{Z}E_n \subsetneq \oplus^{2^{2n}} \mathbb{Z} \oplus M_{2^n}(\mathbb{Z}).$$

8 — Seja o elemento invertível $x \in \mathbb{Z}E_n$ e indique-se por y o seu inverso em $\mathbb{Z}E_n$. Por 3.4.2, esses elementos admitem decomposição em soma direta, como a que indico a seguir:

$$\begin{aligned}
x &= x_1 + ... + x_{2^{2n}} + x_{2^{2n}+1} \\
y &= y_1 + ... + y_{2^{2n}} + y_{2^{2n}+1} \\
x_i, y_i &\in \mathbb{Z},\ \forall\ i,\ 1 \leq i \leq 2^{2n} \\
x_{2^{2n}+1}, y_{2^{2n}+1} &\in M_{2^n}(\mathbb{Z}) \\
x_i x_j &= x_j x_i \\
&= 0,\ \forall\ i, j,\ i \neq j. \\
xy &= 1 \\
\Longrightarrow 1 &= x_1 y_1 + ... + x_{2^{2n}} y_{2^{2n}} + x_{2^{2n}+1} y_{2^{2n}+1} \\
\Longrightarrow x_i y_i &= 1 \in \mathbb{Z},\ \forall\ i,\ 1 \leq i \leq 2^{2n} \\
x_{2^{2n}+1} y_{2^{2n}+1} &= 1 \in M_{2^n}(\mathbb{Z}) \\
\Longrightarrow x_i, y_i &\in \{\pm 1\},\ \forall\ i,\ 1 \leq i \leq 2^{2n} \\
x_{2^{2n}+1}, y_{2^{2n}+1} &\in SL_{2^n}(\mathbb{Z})
\end{aligned} \tag{4.2}$$

9 — É lícito concluir de 8, que:

$$\mathcal{U}(\mathbb{Z}E_n) \subsetneq \oplus^{2^{2n}} \{\pm 1\} \oplus SL_{2^n}(\mathbb{Z}). \quad \square$$

4.4 Índice de grupos e unidades elementares — o problema do subgrupo de congruência.

Convém notar, antes de tudo, que, se $\delta_{i,j}, i \neq j$, for uma matriz elementar contida em $M_{2^n}(\mathbb{Z})$, então, $\delta_{i,j}^2 = 0$.

Definição 4.4.1. *Seja $I \subset \mathbb{Z}$ ideal de números inteiros; $\delta_{r,s}, r \neq s, 1 \leq r, s \leq k$, matrizes elementares contidas em $M_k(\mathbb{Z})$. Indica-se por $F_k(I)$ o subgrupo multiplicativo de $SL_k(\mathbb{Z})$ gerado pelas unidades elementares da forma*

$$1 + i\delta_{r,s},\ i \in I,\ 1 \leq r, s \leq k.$$

Indica-se por $\hat{F}_k(I)$ o fecho normal de $F_k(I)$, em relação a $SL_k(\mathbb{Z})$

Teorema 4.4.2. *Na notação de 4.4.1, valem as seguintes relações, para todo $k \geq 3$:*

1. $\left[SL_k(\mathbb{Z}) \ :\ \hat{F}_k(I)\right] < \infty$;
2. $\hat{F}_k(I^2) \subset F_k(I)$;
3. $[SL_k(\mathbb{Z}) \ :\ F_k(I)] < \infty$. □

Demonstração. *Cf. Lema 2.2 [11]*

Corolário 4.4.3. *Seja $\{r_{i,j}\}_{1 \leq i,j \leq k}$ uma família de inteiros. Seja G o subgrupo multiplicativo de $SL_k(\mathbb{Z})$ gerado pelas unidades elementares da forma:*

$$1 + r_{i,j}\delta_{i,j},\ r_{i,j} \in I,\ 1 \leq i, j \leq k.$$

Então, $[SL_k(\mathbb{Z}) \ :\ G] < \infty$

Demonstração. *1 — Seja* $n = mmc\left\{r_{i,j}\right\}_{1\leq i,j\leq k}$. *Então,*

$$F_k\left(n\mathbb{Z}\right) \subset G$$

2 — Segundo 4.4.2, tem-se

$$\begin{aligned} \left[SL_k\left(\mathbb{Z}\right) \ : \ \hat{F}_k\left(n\mathbb{Z}\right)\right] &< \infty \\ \Longrightarrow \left[SL_k\left(\mathbb{Z}\right) \ : \ G\right]\left[G \ : \ \hat{F}_k\left(n\mathbb{Z}\right)\right] &< \infty \\ \therefore \left[SL_k\left(\mathbb{Z}\right) \ : \ G\right] &< \infty \end{aligned}$$

4.5 A relação entre o índice da projeção e o do projetado.

Proposição 4.5.1. *Seja* G *grupo finito;* H, *grupo infinito;* $N < G \times H$. *Seja, ainda,* $\pi : N \longrightarrow H$ *a projeção de* N *em* H. *Se* $[H \ : \ \pi\left(N\right)] < \infty$, *então* $[G \times H \ : \ N] < \infty$.

Demonstração. *1 — Sejam* $h_1, ..., h_n$ *os representantes das classes laterais de* $\pi\left(N\right)$ *em relação a* H.

2 — Sejam os pares $z_{g,i} = (g, \ h_i)$, *definidos em função dos elementos de* G *e dos* h_i.

3 — Seja a união de classes laterais, não necessariamente disjuntas,

$$\cup_{g,i} z_{g,i} N \subset G \times H.$$

4 — Dado $(\phi, \ \psi) \in G \times H$, *deve haver* $\nu \in N$, $\nu = (\Gamma_\nu, \Delta_\nu)$, *e algum* h_i *dentre os representantes* $h_1, ..., h_n$, *que satisfaça* $h_i \Delta_n = \psi$.

5 — Seja, então, $g_\phi = \phi\Gamma_\nu^{-1} \in G$. *Então:*

$$\begin{aligned} z_{g_\phi,\ h_i}\nu &= (g_\phi,\ h_i)\,(\Gamma_\nu, \Delta_\nu) \\ &= \left(\phi\Gamma_\nu^{-1},\ h_i\right)(\Gamma_\nu, \Delta_\nu) \\ &= \left(\phi\Gamma_\nu^{-1}\Gamma_\nu,\ h_i\Delta_\nu\right) \\ &= (\phi,\ \psi) \quad \textit{cf. } \S 4. \end{aligned}$$

$$\therefore \cup_{g,i} z_{g,i} N = G \times H \quad \square$$

6 — Por 5, as classes laterais da forma $z_{g,i}N$ *recobrem* $G \times H$.

7 — Como por construção a quantidade dos $z_{g,i}$ *é finita, segue-se que o índice de* N *em* $G \times H$ *é finito.*

4.6 Reformulação do problema de tese.

Corolário 4.6.1. *Sejam* $\delta_{i,j},\ i \neq j,\ 1 \leq i, j \leq 2^n$ *as* $2^{2n} - 2^n$ *matrizes elementares contidas em* $M_{2^n}(\mathbb{Z})$; $\{r_{i,j}\}_{1 \leq i,j \leq k}$, *uma família de inteiros de tal natureza que* $r_{i,j}\delta_{i,j} \in \mathbb{Z}E_n$; $\mathcal{O}$, *o subgrupo de* $\mathcal{U}(\mathbb{Z}E_n)$ *gerado pelas unidades da forma*

$$1 + r_{i,j}\delta_{i,j},\ i \neq j,\ 1 \leq i, j \leq 2^n$$

Então, $[\mathcal{U}(\mathbb{Z}E_n)\ :\ \mathcal{O}] < \infty$

Demonstração. *1 — Por hipótese e por 4.3.4,*

$$\begin{aligned} \mathcal{O} &\subset \mathcal{U}(\mathbb{Z}E_n) \\ &\subset \oplus^{2^{2n}} \{\pm 1\} \oplus SL_{2^n}(\mathbb{Z}) \end{aligned}$$

2 — Por construção a projeção de $\mathcal{O}$ *em* $SL_{2^n}(\mathbb{Z})$ *é*

$$\pi_{2^{2n}+1}(\mathcal{O}) = \langle 1 + r_{i,j}\delta_{i,j} \rangle_{1 \leq i,j \leq 2^n}$$

3 — Segundo o corolário 4.4.3,

$$[SL_{2^n}(\mathbb{Z}) \ : \ \pi_{2^{2n}+1}(\mathcal{O})] < \infty$$

4 — Aplico o corolário 4.5.1 a $G = \oplus^{2^{2n}} \{\pm 1\}$ *e* $H = SL_{2^n}(\mathbb{Z})$*, para concluir que*

$$\left[\oplus^{2^{2n}} \{\pm 1\} \oplus SL_{2^n}(\mathbb{Z}) \ : \ \mathcal{O}\right] < \infty$$

$$\Longrightarrow \left[\oplus^{2^{2n}} \{\pm 1\} \oplus SL_{2^n}(\mathbb{Z}) \ : \ \mathcal{U}(\mathbb{Z}E_n)\right] [\mathcal{U}(\mathbb{Z}E_n) \ : \ \mathcal{O}] < \infty$$

$$\therefore [\mathcal{U}(\mathbb{Z}E_n) \ : \ \mathcal{O}] < \infty \quad \square$$

O corolário 4.6.1 contém em si a sugestão da estratégia de demonstração do teorema 1.4.2: o que vou mostrar nas próximas páginas é que o subgrupo $\langle b_1, ..., b_n, h_1, ..., h_n \rangle$ contém unidades da forma $1 \oplus 4^{*(i,j)}\delta_{i,j}, \ i \neq j, \ 1 \leq i, j \leq 2^n$.

Capítulo 5

Os geradores $\{b_1, ..., b_n, h_1, ..., h_n\}$

5.1 Os geradores.

Convém relembrar a apresentação do grupo E_n e introduzir nos seus geradores um índice a mais, para que possa empregar à frente o método de indução.

Definição 5.1.1. *Defina-se, em função de cada n, o grupo E_n pelas seguintes relações de apresentação:*

1. $E_n = \langle a_{n,1}, ..., \ a_{n,n}, \ b_{n,1}, ..., \ b_{n,n} \rangle$,

2. $a_{n,i}^2 = b_{n,i}^4 = 1_n, \ \forall \ i, \ 1 \leq i \leq n$,

3. $a_{n,i} b_{n,i} = b_{n,i}^3 a_{n,i}, \ \forall \ i, \ 1 \leq i \leq n$,

4. $a_{n,i} b_{n,j} = b_{n,j} a_{n,i}, \forall \ i, \ j, \ i \neq j$,

5. $a_{n,i}a_{n,j} = a_{n,j}a_{n,i}, \forall\ i,\ j,\ i \neq j,$

6. $b_{n,i}b_{n,j} = b_{n,j}b_{n,i}, \forall\ i,\ j,\ i \neq j,$

7. $b_{n,i}^2 = b_{n,j}^2, \forall\ i,\ j,\ i \neq j.$

5.2 A projeção na componente não linear.

Conforme demonstrei no capítulo 2, o centro de E_n é $Z(E_n) = \left\langle b_{n,1}^2 \right\rangle = \left\{1, b_{n,1}^2\right\}$. No último resultado do capítulo 3, tratei da decomposição em soma direta de $\mathbb{Q}E_n$:

$$\mathbb{Q}E_k = \oplus^{2^{2k}}\mathbb{Q} \oplus M_{2^k}(\mathbb{Q}) \tag{5.1}$$

Como isso é uma soma direta, cada $x \in \mathbb{Q}E_n$ pode ser escrito, na notação de 4.3.1, de maneira unívoca, como soma direta de projeções:

$$\begin{aligned} x &= \pi_1(x) + ... + \pi_{2^{2n}}(x) + \pi_{2^{2n}+1}(x) \\ \pi_i(x) &\in \mathbb{Q},\ \forall\ i,\ 1 \leq i \leq 2^{2n} \\ \pi_{2^{2n}+1}(x) &\in M_{2^n}(\mathbb{Q}) \\ \pi_i(x)\,\pi_j(x) &= \pi_j(x)\,\pi_i(x) \\ &= 0,\ \forall\ i,j,\ i \neq j. \end{aligned} \tag{5.2}$$

Em geral, se G for um grupo; se $\mathbb{Q}G = M_{n_1}(D_1) \oplus ... \oplus M_{n_r}(D_r)$ for a decomposição em soma direta da álgebra racional $\mathbb{Q}G$; e se $\rho_i(x)$ indicar a projeção na i-ésima componente; então, para cada parcela $M_{n_i}(D_i)$ haverá um idempotente central e_i que satisfaça:

$$\rho_i(x) = xe_i \tag{5.3}$$

De acordo com as observações do capítulo anterior, o que importa neste trabalho é a projeção $\pi_{2^{2n}+1}$ — cf. 4.3.1. Assim sendo, o teorema 3.3.1 já determina qual o idempotente que devo empregar:

Proposição 5.2.1. *A projeção $\pi_{2^{2n}+1}$ de $\mathbb{Q}E_n$ em $M_{2^n}(\mathbb{Q})$ obedece à seguinte lei*[1]

$$\begin{aligned}\pi_{2^{2n}+1} : \mathbb{Q}E_n &\longrightarrow M_{2^n}(\mathbb{Q}) \\ x &\longmapsto x\left(\frac{1-b_{n,1}^2}{2}\right)\end{aligned}$$

Demonstração. *1 — Seja $Z(E_n) = \left\{1, b_{n,1}^2\right\}$. Na notação de 3.3.1, $e_{Z(E_n)}$ deve valer:*

$$e_{Z(E_n)} = \frac{1+b_{n,1}^2}{2}.$$

2 — Conforme demonstrei no capítulo 2, $\mathbb{Q}\frac{E_n}{Z(E_n)} \cong \mathbb{Q}E_k e_{Z(E_n)} = \oplus^{2^{2k}}\mathbb{Q}$.

3 — Segundo 3.3.1, vale

$$\begin{aligned}\mathbb{Q}E_k &= \oplus^{2^{2k}}\mathbb{Q} \oplus M_{2^k}(\mathbb{Q}) \\ &= \mathbb{Q}E_k e_{Z(E_n)} \oplus \mathbb{Q}E_k\left(1 - e_{Z(E_n)}\right) \\ \therefore \mathbb{Q}E_k\left(1 - e_{Z(E_n)}\right) &= M_{2^k}(\mathbb{Q}) \quad \square\end{aligned}$$

Já que $\pi_{2^{2n}+1}$ é a única projeção que importa a este trabalho, convém purgar da notação o índice:

[1] É preciso explicar o abuso da notação nesta proposição e, de fato, no restante do trabalho: segundo o teorema 3.4.2, vale o isomorfismo $\mathbb{Q}E_k \cong \oplus^{2^{2k}}\mathbb{Q} \oplus M_{2^k}(\mathbb{Q})$. Nesta proposição, assim como no restante do trabalho, as componentes irredutíveis da álgebra $\mathbb{Q}E_k$ são identificadas, por esse isomorfismo, com as parcelas da soma direta $\oplus^{2^{2k}}\mathbb{Q} \oplus M_{2^k}(\mathbb{Q})$. Para ser mais preciso, a cada componente irredutível duma álgebra de grupo KG corresponde um único elemento idempotente central. Assim sendo, se KG admitir n componentes irredutíveis, haverá n elementos idempotentes centrais, e_i, por essa razão, cada elemento $x \in KG$ pode ser escrito, de maneira única, pela expressão $x = \sum xe_i$ e as componentes irredutíveis de KG terão a forma KGe_i. No que se segue, pois, faço a identificação $M_{2^k}(\mathbb{Q}) = \mathbb{Q}E_k e_{2^{2k}+1}$ e calculo com precisão quem é o elemento idempotente $e_{2^{2k}+1}$.

Definição 5.2.2. *Por π_n indico $\pi_{2^{2n}+1}$*

Observação 5.2.3. *π_n é homomorfismo de álgebras.*

5.3 A representação irredutível de E_n por $M_{2^n}(\mathbb{Q})$.

À luz dessas observações, é fácil calcular a representação irredutível de E_n por $M_{2^n}(\mathbb{Q})$ que pretendo empregar doravante.

Proposição 5.3.1. *A representação irredutível de E_n por $M_{2^n}(\mathbb{Q})$ pode ser calculada, em função dos geradores do grupo E_n, pelas seguintes relações.*

$$\mathfrak{X}_1(a_{1,1}) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\mathfrak{X}_1(b_{1,1}) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$\mathfrak{X}_n(a_{n,i}) = \underbrace{1_1 \otimes ... \otimes \underbrace{\mathfrak{X}_1(a_{1,1})}_{i} \otimes 1_1 ... \otimes 1_1}_{n\ vezes}.$$

$$\mathfrak{X}_n(b_{n,i}) = \underbrace{1_1 \otimes ... \otimes \underbrace{\mathfrak{X}_1(b_{1,1})}_{i} \otimes 1_1 ... \otimes 1_1}_{n\ vezes}.$$

Demonstração. *1 — Segundo os §§16 e 17 da demonstração de 3.4.1, a representação $\mathfrak{X}_1$ indicada no enunciado é a representação irredutível de $E_1 \cong D_4$ por $M_2(\mathbb{Q})$.*

2 — Segundo 3.1.1, a representação irredutível $\mathfrak{Y}_2 : E_1 \times D_4 \longrightarrow M_2(\mathbb{Q}) \otimes M_2(\mathbb{Q}) = M_4(\mathbb{Q})$ é o produto tensorial de Kronecker $\mathfrak{Y}_2(x,y) = \mathfrak{X}_1(x) \otimes \mathfrak{X}_1(y)$.

3 — Se $C = A \otimes B$ forem espaços vetoriais, a dimensão de C é produto:

$$\dim C = \dim A \dim B$$

4 — À luz de 1.1.2 e do §3, o grau de $\mathfrak{Y}_2$ deve ser 4. Como, porém, $\mathbb{Q}D_4$ contém uma única componente de grau 4; $\mathfrak{Y}_2$ é a única maneira de construir representação irredutível de grau 4.

5 — Por 3.3.1, as componentes irredutíveis de $\mathbb{Q}E_2$ advêm, por exclusão, das de $\mathbb{Q}(E_1 \times D_4)$.

6 — Pelos §§3 e 5, posso assegurar a validade do teorema, no caso $n = 2$.

7 — Emprego, agora, 2.3.3: segundo 3.1.1, a representação irredutível $\mathfrak{Y}_{n+1}$: $E_n \times D_4 \longrightarrow M_{2^n}(\mathbb{Q}) \otimes M_2(\mathbb{Q}) = M_{2^{n+1}}(\mathbb{Q})$ é o produto tensorial de Kronecker $\mathfrak{Y}_{n+1}(x, y) = \mathfrak{X}_n(x) \otimes \mathfrak{X}_1(y)$.

8 — À luz de 1.1.2 e de §3, o grau de $\mathfrak{Y}_{n+1}$ deve ser 2^{2n+2}. Como, porém, $\mathbb{Q}D_4$ contém uma única componente de grau 4; e $\mathbb{Q}E_n$, uma única de grau 2^{2n}; segue-se que $\mathfrak{Y}_{n+1}$ é a única maneira de construir representação irredutível de grau 2^{2n+2}.

9 — Por 3.3.1, as componentes irredutíveis de $\mathbb{Q}E_{n+1}$ advêm, por exclusão, das de $\mathbb{Q}(E_n \times D_4)$.

10 — Pelos §§8 e 9, concluo a validade do resultado, no caso geral. □

Corolário 5.3.2. *A forma matricial da projeção π_n pode ser calculada pelas seguintes fórmulas:*

$$\pi_1(a_{1,1}) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\pi_1(b_{1,1}) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$\pi_n(a_{n,i}) = \underbrace{1_1 \otimes ... \otimes \underbrace{\pi_1(a_{1,1})}_{i} \otimes 1_1 ... \otimes 1_1}_{n\ vezes}.$$

$$\pi_n(b_{n,i}) = \underbrace{1_1 \otimes ... \otimes \underbrace{\pi_1(b_{1,1})}_{i} \otimes 1_1 ... \otimes 1_1}_{n\ vezes}.$$

Corolário 5.3.3. *A forma matricial da projeção π_n admite a seguinte definição recursiva:*

$$\pi_1(a_1) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\pi_1(b_1) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$\pi_n(a_i) = \pi_{n-1}(a_i) \otimes 1_1, \forall i,\ 1 \leq i \leq n-1$$

$$\pi_n(a_n) = 1_{n-1} \otimes \pi_1(a_1)$$

$$\pi_n(b_i) = \pi_{n-1}(b_i) \otimes 1_1, \forall i,\ 1 \leq i \leq n-1$$

$$\pi_n(b_n) = 1_{n-1} \otimes \pi_1(b_1)$$

Corolário 5.3.4. *A forma matricial da projeção π_n admite a seguinte definição*

recursiva:

$$\pi_1(a_1) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\pi_1(b_1) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$\pi_n(a_i) = 1_1 \otimes \pi_{n-1}(a_{i-1}) \otimes 1, \forall i,\ 2 \leq i \leq n$$

$$\pi_n(a_1) = \pi_1(a_1) \otimes 1_{n-1}$$

$$\pi_n(b_i) = 1_1 \otimes \pi_{n-1}(b_{i-1}), \forall i,\ 2 \leq i \leq n$$

$$\pi_n(b_n) = \pi_1(b_1) \otimes 1_{n-1}$$

5.4 Os geradores dum subgrupo de $\mathcal{U}(\mathbb{Z}E_n)$ de índice finito.

Definição 5.4.1. *Defino os elementos $h_n, h_{n,i} \in \mathbb{Z}E_n$, da seguinte forma:*

$$h_n = \left(1_n - b_{n,1}^2\right) \prod_{1 \leq i \leq n} (1_n - a_{n,i});$$

$$h_{n,i} = 1_n - h_n b_{n,i}.$$

Observação 5.4.2. *1 — Convém notar por que os elementos de 5.4.1 pertencem, de fato, ao anel $\mathbb{Z}E_n$: são produtos de combinações lineares dos elementos da base, com coeficientes ± 1.*

2 — Convém observar que à luz de 5.2.1, $h_n = 2\pi\left(\prod(1_n - a_i)\right)$

Proposição 5.4.3.

$$h_n = 2^{n+1} \underbrace{(\delta_{2,2} \otimes .... \otimes \delta_{2,2})}_{n\ vezes}$$

Demonstração. *1 — Segundo 5.4.1 e 5.4.2.2, deve valer:*

$$
\begin{aligned}
h_n &= \left(1_n - b_{n,1}^2\right) \prod \left(1_n - a_{n,i}\right) \\
&= 2\pi \left(\prod \left(1_n - a_{n,i}\right)\right) \quad \textit{cf. 5.4.2.2} \\
&= 2 \prod \left(\pi \left(1_n - a_{n,i}\right)\right) \quad \textit{cf. 5.2.3} \\
&= 2 \prod \left(\pi \left(1_n\right) - \pi \left(a_{n,i}\right)\right) \quad \textit{cf. 5.2.3} \\
&= 2 \left(\prod_{i \leq n-1} \left(\pi \left(1_{n-1}\right) \otimes 1_1 - \pi \left(a_{n-1,i}\right) \otimes 1_1\right) \right) \left(\pi \left(1_n\right) - \pi \left(a_{n,n}\right)\right) \quad \textit{cf. 5.3.3} \\
&= 2 \left(\prod_{i \leq n-1} \left(\left(\pi \left(1_{n-1}\right) - \pi \left(a_{n-1,i}\right)\right) \otimes 1_1\right) \right) \left(\pi \left(1_n\right) - \pi \left(a_{n,n}\right)\right) \quad \textit{cf. 3.2.1.1} \\
&= 2 \left(\prod_{i \leq n-1} \left(\left(\pi \left(1_{n-1} - a_{n-1,i}\right)\right) \otimes 1_1\right) \right) \left(\pi \left(1_n\right) - \pi \left(a_{n,n}\right)\right) \quad \textit{cf. 5.2.3} \\
&= 2 \left(\prod_{i \leq n-1} \left(\left(\pi \left(1_{n-1} - a_{n-1,i}\right)\right) \otimes 1_1\right) \right) \left(1_{n-1} \otimes \pi \left(1_1\right) - 1_{n-1} \otimes \pi \left(a_{1,1}\right)\right) \quad \textit{cf. 5.3.3} \\
&= 2 \left(\prod_{i \leq n-1} \left(\left(\pi \left(1_{n-1} - a_{n-1,i}\right)\right) \otimes 1_1\right) \right) \left(1_{n-1} \otimes \left(\pi \left(1_1\right) - \pi \left(a_{1,1}\right)\right)\right) \quad \textit{cf. 3.2.1.1} \\
&= 2 \left(\left(\prod_{i \leq n} \pi \left(1_{n-1} - a_{n-1,i}\right) \right) \otimes 1_1 \right) \left(1_{n-1} \otimes \left(\pi \left(1_1\right) - \pi \left(a_{1,1}\right)\right)\right) \quad \textit{cf. 3.2.1.3} \\
&= 2 \left(\prod_{i \leq n-1} \pi \left(1_{n-1} - a_{n-1,i}\right) \right) \otimes \left(\pi \left(1_1\right) - \pi \left(a_{1,1}\right)\right) \quad \textit{cf. 3.2.1.3}
\end{aligned}
$$

2 — Se o processo delineado no §1 for repetido $n-1$ vezes, o resultado será este:

$$h_n = 2 \underbrace{\left(\pi \left(1_1\right) - \pi \left(a_{1,1}\right)\right) \otimes ... \otimes \left(\pi \left(1_1\right) - \pi \left(a_{1,1}\right)\right)}_{n \text{ vezes}}$$

3 — Por 5.2.2 e por A.2.2,

$$\pi \left(1_1\right) - \pi \left(a_{1,1}\right) = 2\delta_{2,2}$$

4 — Pelo §2 e pelo §3,

$$h_n = 2^{n+1} \underbrace{\left(\delta_{2,2} \otimes .... \otimes \delta_{2,2}\right)}_{n \text{ vezes}} \quad \square$$

Proposição 5.4.4. *Sejam* $\aleph$ *e* $\beth \in \mathbb{Q}E_n$. *Se* $\aleph \in M_{2^n}(\mathbb{Q})$, *então,*

$$\aleph\beth = \aleph\pi_n(\beth)$$

Demonstração. *1 — Como* $\aleph \in M_{2^n}(\mathbb{Q})$, *então,* $\pi(\aleph) = \aleph$

2 — Por conseguinte,

$$\begin{aligned}
\aleph\beth &= \pi_n(\aleph)\beth \\
&= \left(\frac{1-b_{n,1}^2}{2}\right)\aleph\beth \quad \textit{cf. 5.4.2.2} \\
&= \aleph\left(\frac{1-b_{n,1}^2}{2}\right)\beth \quad \textit{cf. 5.2.1} \\
&= \aleph\pi_n(\beth) \quad \textit{cf. 5.4.2.2}
\end{aligned}$$

Proposição 5.4.5. $(h_n b_{n,i})^2 = 0,\ \forall n, \forall\ i,\ 1 \leq i \leq n.$

Demonstração. *1 — Como* h_n *pertence a* $M_{2^{n+1}}(\mathbb{Q})$, *basta empregar a proposição 5.4.4.*

$$\begin{aligned}
h_n b_{n,i} &= h_n \pi_n(b_{n,i}) \\
&= 2^{n+1}\left(\underbrace{(\delta_{2,2}\otimes ....\otimes\delta_{2,2})}_{n\ vezes}\right)\left(\underbrace{\left(1_1\otimes ...\otimes\underbrace{\pi_1(b_{1,1})}_{i}\otimes ...\otimes 1_1\right)}_{n\ vezes}\right) \quad \textit{5.4.3, 2.2.1} \\
&= 2^{n+1}\left(\underbrace{\left(\delta_{2,2}\otimes ...\otimes\underbrace{\delta_{2,2}\pi_1(b_{1,1})}_{i}\otimes ...\otimes\delta_{2,2}\right)}_{n\ vezes}\right) \quad \textit{3.2.1.3} \\
&= 2^{n+1}\left(\underbrace{\left(\delta_{2,2}\otimes ...\otimes\underbrace{\delta_{2,1}}_{i}\otimes ...\otimes\delta_{2,2}\right)}_{n\ vezes}\right) \quad \textit{cf. A.4.1}
\end{aligned}$$

2 — Uso, agora, 3.2.1.3 para calcular o quadrado desta última expressão:

$$\underbrace{\left(\delta_{2,2}\otimes ...\otimes \underbrace{\delta_{2,1}}_{i}\otimes ...\otimes \delta_{2,2}\right)^{2}}_{n\ vezes} = \underbrace{\left(\delta_{2,2}\otimes ...\otimes \underbrace{\delta_{2,1}^{2}}_{i}\otimes ...\otimes \delta_{2,2}\right)}_{n\ vezes}$$

$$= 0 \quad cf.\ A.1.1$$

Corolário 5.4.6. *$h_{n,i} = 1_n - h_n b_{n,i}$ é elemento invertível de $\mathbb{Z}E_n,\ \forall n, \forall\ i,\ 1 \leq i \leq n$.*

5.5 Conjugação e comutadores.

É escusado dizer que conjugação e formação de comutadores multiplicativos são operações fechadas no subgrupo $\langle b_1, ..., b_n,\ h_{n,1}, ..., h_{n,n}\rangle < \mathcal{U}(\mathbb{Z}E_n)$. É preciso, no entanto, explicar como se calculam essas operações, em função dos geradores de $\langle b_1, ..., b_n,\ h_{n,1}, ..., h_{n,n}\rangle$.

Proposição 5.5.1. *Sejam $U_1, ..., U_n \in M_2(\mathbb{Q})$, então:*

$$(U_1 \otimes ... \otimes U_n)^{b_{n,1}^{j_1}...b_{n,n}^{j_n}} = U_1^{\pi_1(b_{1,1})^{j_1}} \otimes ... \otimes U_n^{\pi_1(b_{1,1})^{j_n}} \in M_{2^{k+1}}.$$

Demonstração. *1 — A relação de pertinência, a saber, $\in \mathbb{Z}E_n$, percebe-se de imediato, porque $\mathbb{Z}E_n$ é anel, portanto, fechado nas operações de soma e multiplicação.*

2 — A relação de igualdade pode ser demonstrada por indução. A demonstração do caso $n = 1$ é evidente por conta de 5.4.4.

3 — Seja $U = U_1 \otimes ... \otimes U_{n-1}$

4 — À luz de 3:

$$(U_1 \otimes ... \otimes U_n)^{b_{n,1}^{j_1}...b_{n,n}^{j_n}} = (U \otimes U_n)^{b_{n,1}^{j_1}...b_{n,n}^{j_n}}$$

$$= \left(b_{n,1}^{j_1}...b_{n,n}^{j_n}\right)(U \otimes U_n)\left(b_{n,1}^{j_1}...b_{n,n}^{j_n}\right)^{-1}$$

5 — Segundo 5.1.1, os $b_{n,i}$ comutam entre si, portanto, a ordem em que viesse a tomar as conjugações não alteraria o resultado final. Calculo primeiro a conjugação por $b_{n,n}^{j_n}$:

$$\begin{aligned} b_{n,n}^{j_n}\left(U\otimes U_n\right)b_{n,n}^{-j_n} &= \left(1_{n-1}\otimes\pi_1\left(b_{1,1}\right)\right)\left(U\otimes U_n\right)\left(1_{n-1}\otimes\pi_1\left(b_{1,1}\right)^{-1}\right) \quad \textit{cf. 5.3.2} \\ &= U\otimes\left(\pi_1\left(b_{1,1}\right)U_n\pi_1\left(b_{1,1}\right)^{-1}\right) \quad \textit{cf. 3.2.1.3} \\ &= U\otimes U_n^{\pi_1(b_{1,1})} \end{aligned}$$

6 — Segundo 5.3.2 e 5.4.4, deve valer, para todo $i,\ 1\leq i\leq n-1$

$$\begin{aligned} b_{n,i}^{j_i}\left(U\otimes U_n\right)b_{n,i}^{-j_i} &= \left(\pi_{n-1}\left(b_{n-1,i}\right)^{j_i}\otimes 1_1\right)\left(U\otimes U_n\right)\left(\pi_{n-1}\left(b_{n-1,i}\right)^{-j_i}\otimes 1_1\right) \\ &= \left(\pi_{n-1}\left(b_{n-1,i}\right)^{j_i}U\pi_{n-1}\left(b_{n-1,i}\right)^{-j_i}\otimes U_n\right) \\ &= U^{\pi_{n-1}(b_{n-1,i})^{j_i}}\otimes U_n \end{aligned}$$

7 — Neste ponto, poderia assumir uma hipótese indutiva, ou simplesmente supor que o processo esboçado no §6 fosse repetido $n-1$ vezes:

$$\left(U\otimes U_n\right)^{b_{n,1}^{j_1}\ldots b_{n,n-1}^{j_{n-1}}} = \left(U^{\pi(b_{n,1})^{j_1}\ldots\pi(b_{n,n-1})^{j_{n-1}}}\otimes U_n\right)$$

8 — Eis a aplicação ao §7 da conclusão do §5:

$$\left(U\otimes U_n\right)^{b_{n,1}^{j_1}\ldots b_{n,n-1}^{j_{n-1}}b_{n,n}^{j_n}} = \left(U^{\pi(b_{n,1})^{j_1}\ldots\pi(b_{n,n-1})^{j_{n-1}}}\otimes U_n^{\pi_1(b_{1,1})}\right)$$

9 — À luz de 5.4.4, é possível aplicar indução a $U^{\pi(b_{n,1})^{j_1}\ldots\pi(b_{n,n-1})^{j_{n-1}}}$:

$$\left(U_1\otimes\ldots\otimes U_n\right)^{b_{n,1}^{j_1}\ldots b_{n,n}^{j_n}} = U_1^{\pi_1(b_{1,1})^{j_1}}\otimes\ldots\otimes U_{n+1}^{\pi_1(b_{1,1})^{j_n}}$$

Teorema 5.5.2. *Sejam $\delta_{i,j}$ e $\delta_{j,k}$, matrizes elementares $\in M_{2^n}(\mathbb{Z})$ Se $i,\ j,\ k$ forem diferentes entre si, então:*

$$\left[1-a\delta_{i,j},\ 1-b\delta_{j,k}\right] = 1+ab\delta_{i,k}$$

$$[1 - b\delta_{j,k},\ 1 - a\delta_{i,j}] = 1 - ab\delta_{i,k}$$

Ademais, qualquer outra combinação de matrizes elementares produz comutador trivial.

Demonstração. *Cf. [8] lema 1.2*

Capítulo 6

Problema de contagem.

Dos dois últimos resultados arrolados no capítulo anterior, o único que se encontra na forma conveniente é a proposição 5.5.1. Com ela é possível conjugar, pelos geradores $b_{n,i}$, os elementos da forma $1 + aU_1 \otimes ... \otimes U_n$; contudo, o mesmo não se pode dizer de 5.5.2, porquanto ainda não expliquei como seria possível decompor $\delta_{i,k}$ num produto tensorial de Kronecker de matrizes elementares.

O primeiro resultado que exponho neste capítulo é a decomposição única de matrizes elementares em produto tensorial de matrizes elementares. Em particular, será possível dizer que

$$\begin{aligned} \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{p+1},j_{p+1}} &= \delta_{k_1,l_1} \otimes ... \otimes \delta_{k_{p+1},l_{p+1}} \\ \implies \delta_{i_s,j_s} &= \delta_{k_s,l_s} \\ \therefore i_s &= k_s \\ j_s &= l_s. \end{aligned}$$

De posse desse critério de igualdade vou delinear um algoritmo geral com que obtenha todas as matrizes elementares, de qualquer tamanho, a partir de das matrizes elementares de tamanho 2×2.

6.1 Fatoração única

A base de tudo o que farei doravante é esta como que fatoração única:

Lema 6.1.1. *Seja $p \in \mathbb{Z}$ primo; $\delta_{i,j} \in M_{p^{n+1}}(\mathbb{Z})$ matriz elementar. Então, há n+1 matrizes elementares $\delta_{i_k,j_k} \in M_p(\mathbb{Z})$, unicamente determinadas por $\delta_{i,j}$, que satisfazem a relação abaixo:*

$$\delta_{i,j} = \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{p+1},j_{p+1}}$$

Demonstração. *1. Se a e b forem inteiros diferentes, e se $X \in \mathbb{N}$ e $0 \leq a, b \leq X$; vale a desigualdade:*

$$1 \leq |a - b| \leq X - 1.$$

2. Suponho que $\delta_{i_k,j_k} \in M_p(\mathbb{Z})$ $1 \leq k \leq n+1$, sejam n+1 matrizes elementares. Pela consideração das dimensões, à luz de A.1.2, o resultado da equação abaixo, indicado por $\delta_{i,j}$, é matriz elementar:

$$\delta_{i,j} = \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}} \in M_{p^{n+1}}(\mathbb{Z}).$$

3. No que se segue, indico por $\delta_{i,j}$ uma matriz elementar. Em oposição ao §2, se $\delta_{i,j} \in M_{p^{n+1}}(\mathbb{Z})$ for dada, é possível realizar as seguintes divisões com resto:

$$i = p^n q + r;$$

$$j = p^n z + s;$$

4. Se nem i, nem j, forem $\equiv 0 \mod p^n$, sejam as matrizes

$$\delta_{q+1,\ z+1} \in M_p(\mathbb{Z});$$

$$\delta_{r,s} \in M_{p^n}(\mathbb{Z}).$$

$$\therefore \delta_{q+1,\ z+1} \otimes \delta_{r,s} \quad \textit{cf. A.1.2}$$

5. *Como i e j são índices de matrizes de $M_{p^n}(\mathbb{Z})$, se uma ou outra for $\equiv 0 \mod p^n$; deverá valer p. Nesse caso seja:*

$$\delta_{p-1,p^n}$$

6. *Como quer que seja, a matriz $\delta_{i,j} \in M_{p^{n+1}}(\mathbb{Z})$ poderá ser decomposta, na forma:*

$$\delta_{i,j} = \delta_{i_1,j_1} \otimes \delta_{\mu,\nu}$$

$$\delta_{i_1,j_1} \in M_p(\mathbb{Z})$$

$$\delta_{\mu,\nu} \in M_{p^n}(\mathbb{Z})$$

7. *Se repetir, diversas vezes, o processo que desenhei nos §§3-5, tomando por objeto o fator da direita, i.e., $\in M_{p^n}(\mathbb{Z})$, depois de α aplicações, terei decomposto $\delta_{i,j}$ na forma*

$$\delta_{i,j} = \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_\alpha,j_\alpha} \otimes \delta_{\mu_\alpha,\nu_\alpha}$$

$$\delta_{i_k,j_k} \in M_p(\mathbb{Z})$$

$$\delta_{\mu_\alpha,\nu_\alpha} \in M_{p^{n-\alpha}}(\mathbb{Z})$$

8. *Como se vê o critério de parada é delimitado exatamente pelo último fator da expressão, cujo tamanho, segundo o §6, se reduz, a cada aplicação do processo de decomposição, de $p^\alpha \times p^\alpha$ para $p^{\alpha-1} \times p^{\alpha-1}$.*

9. *Por conseguinte, após $n+1$ repetições obterei algo da forma:*

$$\delta_{i,j} = \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}}$$

$$\delta_{i_k,j_k} \in M_p(\mathbb{Z})$$

10. Sejam agora $\delta_{i,j},\ \delta_{k,l},\ \delta_{m,n},\ \delta_{r,s} \in M_p(\mathbb{Z})$. *Suponho que*

$$\delta_{i,j} \otimes \delta_{k,l} = \delta_{m,n} \otimes \delta_{r,s}$$

$$\therefore \delta_{p(i-1)+k,\ p(j-1)+l} = \delta_{p(m-1)+r,\ p(n-1)+s} \quad \textit{cf. A.1.2}$$

$$\iff p(i-1)+k = p(m-1)+r$$

$$p(j-1)+l = p(n-1)+s$$

11. Se, por contradição, eu supuser que $\delta_{i,j} \neq \delta_{m,n}$ *e* $\delta_{k,l} \neq \delta_{r,s}$, *as relações do §10 implicariam, à luz do §1, estoutras:*

$$p|i-m| = |k-r|$$

$$\implies p \leq p|i-m| = |k-r| \leq p-1$$

$$p|j-n| = |l-s|$$

$$\implies p \leq p|j-n| = |l-s| \leq p-1$$

12. A hipótese de contradição do §11 é, portanto, absurda. Deve-se concluir que

$$i = m,\ j = n$$

$$k = r,\ l = s$$

$$\therefore \delta_{i,j} = \delta_{m,n}$$

$$\delta_{k,l} = \delta_{r,s}$$

13. Se, por indução, eu supuser que

$$\delta_{i_1,j_i} \otimes ... \otimes \delta_{i_k,j_k} = \delta_{r_1,s_i} \otimes ... \otimes \delta_{r_k,s_k}$$

$$\implies \delta_{i_l,j_l} = \delta_{r_l,s_l},\ \forall l,\ 1 \leq l \leq k;\ \forall k,\ 3 \leq k \leq n;$$

14. posso propor, como acima, a seguinte equação:

$$\delta_{i_1,j_1} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}} = \delta_{r_1,s_1} \otimes \delta_{r_2,s_2} \otimes ... \otimes \delta_{r_{n+1},s_{n+1}}$$

$$\delta_{i_l,j_l}, \delta_{r_k,s_k} \in M_p(\mathbb{Z})$$

15. Seja

$$\delta_{i_2,j_2} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}} = \delta_{i,j} \in M_{p^n}(\mathbb{Z})$$

$$\delta_{r_2,s_2} \otimes ... \otimes \delta_{r_{n+1},s_{n+1}} = \delta_{r,s} \in M_{p^n}(\mathbb{Z}).$$

16. Em função dessas relações, reescrevo a expressão proposta no §14:

$$\delta_{i_1,j_1} \otimes \delta_{i,j} = \delta_{r_1,s_1} \otimes \delta_{r,s}$$

$$\implies \delta_{p^n(i_1-1)+i,\ p^n(j_1-1)+j} = \delta_{p^n(r_1-1)+r,\ p^n(s_1-1)+s} \quad \textit{cf. A.1.2.}$$

17. Da qual igualdade se seguem estas:

$$p^n |i_1 - r_1| = |i - r|$$

$$p^n |j_1 - s_1| = |j - s|$$

18. Se, por absurdo, eu supusesse que $\delta_{i_1,j_1} \neq \delta_{r_1,s_1}$ e $\delta_{i,j} \neq \delta_{r,s}$, poderia empregar a lição do §1:

$$\implies p^n \leq p^n |i_1 - r_1| = |i - r| \leq p^n - 1$$

$$\implies p^n \leq p |j_1 - s_1| = |j - s| \leq p^n - 1$$

19. Por contradição, devo concluir que,

$$\delta_{i_1,j_1} = \delta_{r_1,s_1}$$

$$\delta_{i,j} = \delta_{r,s}$$

$$\iff \delta_{i_1,j_1} \otimes \delta_{i,j} = \delta_{r_1,s_1} \otimes \delta_{r,s}$$

$$\iff \delta_{i_1,j_1} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}} = \delta_{r_1,s_i} \otimes \delta_{r_2,s_2} \otimes ... \otimes \delta_{r_{n+1},s_{n+1}}$$

$$\therefore \delta_{i_k,j_k} = \delta_{r_k,s_k},\ \forall k,\ 1 \leq k \leq n+1. \quad \square$$

Corolário 6.1.2. *Sejam* $\delta_{i_1,j_1}...\delta_{i_n,j_n}, \delta_{k_1,l_1}...\delta_{k_n,l_n}$ *matrizes elementares* $\in M_p(\mathbb{Z})$. *Então,* $\forall n$ *vale*

$$\delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{p+1},j_{p+1}} = \delta_{k_1,l_1} \otimes ... \otimes \delta_{k_{p+1},l_{p+1}}$$

$$\implies \delta_{i_s,j_s} = \delta_{k_s,l_s}$$

$$\therefore i_s = k_s$$

$$j_s = l_s.$$

6.2 Novamente os comutadores, agora tratados da forma adequada.

Proposição 6.2.1. *Seja* $\{\delta_{k,l}\}$ *família de matrizes elementares* $\in M_p(\mathbb{Z})$. *Seja, ainda,* C *o comutador da forma*

$$C = [1 - a\delta_{i_1,j_1} \otimes ... \otimes \delta_{i_n,j_n},\ 1 - b\delta_{r_1,s_1} \otimes ... \otimes \delta_{r_n,s_n}]$$

C *será não trivial se, e somente se, uma das duas relações abaixo for observada:*

$$j_k = r_k \ e\ i_k \neq j_k \neq s_k \neq i_k$$

$$i_k = s_k \ e\ i_k \neq j_k \neq r_k \neq i_k$$

No primeiro caso, o resultado será:

$$1 - ab\delta_{i_1,s_1} \otimes ... \otimes \delta_{i_n,s_n}.$$

No segundo,

$$1 + ab\delta_{r_1,j_1} \otimes ... \otimes \delta_{r_n,j_n}$$

Como quer que seja, um caso pode ser obtido do outro pela permutação da ordem em que se forma o comutador.

Demonstração. *1. Reescrevo, à luz do lema 6.1.1, as expressões do enunciado.*

$$\delta_{i,j} = \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_n,j_n} \in M_{p^n}(\mathbb{Z})$$

$$\delta_{r,s} = \delta_{r_1,s_1} \otimes ... \otimes \delta_{r_n,s_n} \in M_{p^n}(\mathbb{Z})$$

2. Segundo 5.5.2, e o apêndice A.1.1, o enunciado desta proposição posso reformulá-lo da seguinte maneira:

$$[1 - a\delta_{i,j},\ 1 - b\delta_{r,s}] \neq 1 \Longleftrightarrow \delta_{i,j}\delta_{r,s} \neq 0 \text{ ou } \delta_{r,s}\delta_{i,j} \neq 0.$$

3. Para demonstrar a conclusão da proposição, é suficiente verificar a condição $\delta_{i,j}\delta_{r,s} \neq 0$, pois que a outra se pode obter pela permuta da ordem em que se forma o comutador — cf. 5.5.2.

$$\begin{aligned}
\delta_{i,j}\delta_{r,s} \neq 0 &\Longleftrightarrow (\delta_{i_1,j_1} \otimes ... \otimes \delta_{i_n,j_n})(\delta_{r_1,s_1} \otimes ... \otimes \delta_{r_n,s_n}) \neq 0 \\
&\Longleftrightarrow \delta_{i_1,j_1}\delta_{r_1,s_1} \otimes ... \otimes \delta_{i_n,j_n}\delta_{r_n,s_n} \neq 0 \quad \textit{cf. 3.2.1.3} \\
&\Longleftrightarrow \delta_{i_k,j_k}\delta_{r_k,s_k} \neq 0,\ \forall\ k \quad \textit{cf. 3.2.1.1} \\
&\Longleftrightarrow j_k = r_k,\ \forall\ k \quad \textit{cf. apêndice A.1.1}
\end{aligned}$$

4. Eis o resultado da operação:

$$\begin{aligned}
&[1 - a\delta_{i_1,j_1} \otimes ... \otimes \delta_{i_n,j_n},\ 1 - b\delta_{j_1,s_1} \otimes ... \otimes \delta_{j_n,s_n}] \\
&= [1 - a\delta_{i,j},\ 1 - b\delta_{j,s}] \\
&= 1 - ab\delta_{i,s} \quad \textit{cf. A.1.1} \\
&= 1 - ab\delta_{i_1,s_1} \otimes ... \otimes \delta_{i_n,s_n}. \quad \textit{cf. 6.1.1 e 6.1.2.} \quad \square
\end{aligned}$$

Corolário 6.2.2. *Seja $\{\delta_{k,l}\}$ família de matrizes elementares $\in M_p(\mathbb{Z})$ que contenha ao menos um elemento δ_{i_k,j_k} que satisfaça $i_k \neq j_k$. Sejam, ainda, os produtos*

tensoriais:

$$\delta_{i,i} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}}$$

$$\delta_{i,j} \otimes \delta_{j_2,j_2} \otimes ... \otimes \delta_{j_{n+1},j_{n+1}}$$

$$i \neq j$$

Então, vale:

$$\left[1 - a\delta_{i,i} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}}, 1 - b\delta_{i,j} \otimes \delta_{j_2,j_2} \otimes ... \otimes \delta_{j_{n+1},j_{n+1}}\right]$$

$$= 1 + ab\delta_{i,j} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}}$$

$$\neq 1$$

Corolário 6.2.3. *Seja* $\{\delta_{k,l}\}$ *família de matrizes elementares* $\in M_p(\mathbb{Z})$*, que contenha ao menos um elemento* δ_{i_k,j_k} *que satisfaça* $i_k \neq j_k$*.*

$$\delta_{i,i} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}}$$

$$\delta_{i,i} \otimes \delta_{j_2,k_2} \otimes ... \otimes \delta_{j_{n+1},k_{n+1}}.$$

Seja, ainda,

$$C = \left[1 - a\delta_{i_2,j_2} \otimes ... \otimes \delta_{i_{n+1},j_{n+1}},\ 1 - b \otimes \delta_{j_2,k_2} \otimes ... \otimes \delta_{j_{n+1},k_{n+1}}\right]$$

Vale:

$$C = 1 + ab \otimes \delta_{i_2,k_2} \otimes ... \otimes \delta_{i_{n+1},k_{n+1}}$$

$$\neq 1$$

6.3 O conjunto das matrizes elementares.

A partir de agora, passo a centrar a atenção no modo de produzir matrizes elementares.

Definição 6.3.1. *Por* $\daleth^n$ *denoto o conjunto das matrizes elementares* $\delta_{i,j}$, $i \neq j$ *contidas em* $M_{2^n}(\mathbb{Q})$.

Por $\beth^n$ *denoto o conjunto das matrizes elementares* $\delta_{i,i}$, *contidas em* $M_{2^n}(\mathbb{Q})$.

Observação 6.3.2. *1 — A diferença entre* $\daleth^n$ *e* $\beth^n$ *é importante:* $\beth^n$ *contém somente elementos diagonais;* $\daleth^n$ *os exclui.*

2 — A cardinalidade de $\daleth^n$ *calcula-se facilmente: basta contar o número de entradas duma matriz* $2^n \times 2^n$ *e descontar desse número a quantidade de matrizes diagonais da forma* $\delta_{i,i}$*:* $2^n 2^n - 2^n = 2^{2n} - 2^n$.

Conforme expliquei na demonstração do lema 6.1.1, a matriz elementar $\delta_{i,j} \in M_{2^n}(\mathbb{Q})$ pode ser decomposta num produto tensorial da forma $\delta_{i,j} = \delta_{i_1,j_1} \otimes \delta$, $\delta_{i_1,j_1} \in M_2(\mathbb{Q}), \delta \in M_{2^{n-1}}(\mathbb{Q})$. Como os índices da matriz $\delta_{i_1,j_1} \in M_2(\mathbb{Q})$ variam entre 1 e 2; a decomposição acima referida divide a matriz em quatro quadrantes diferentes. A próxima definição reparte de modo disjunto o conjunto $\daleth^n$ em quatro partes.

Definição 6.3.3. *Seja, em função de cada inteiro* n, *e de cada par* $u,\ v$, *sendo* $u,\ v = 1,\ 2$, *o conjunto:*

$$\daleth^n_{u,v} = \left\{ \delta_{i,j} \in \daleth^n \ : \ \delta_{i,j} = \delta_{u,v} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_n,j_n};\ \delta_{a,b} \in \beth^1 \cup \daleth^1,\ \exists k,\ \delta_{i_k,j_k} \in \daleth^1 \right\}$$

Observação 6.3.4. *1 — O conjunto fica bem definido por conta de 6.1.1.*

2 — A cardinalidade de cada $\daleth^n_{u,v}$ *conta-se como a de* $\daleth^n$*:* $2^{2(n-1)} - 2^{n-1}$.

3 — Os quatro conjuntos que com a regra 6.3.3 se podem formar são disjuntos, porque a decomposição em produtos tensoriais de matrizes elementares é única, conforme deixei dito em 6.1.2, e por definição o primeiro elemento do produto tensorial é diferente, em cada conjunto.

4 — A união desses quatro conjuntos ainda não recobre o conjunto $\urcorner^n$*, visto que as matrizes da forma abaixo indicada não estão contidas em nenhum dos quatro, todavia, pertencem a* $\urcorner^n$*.*

$$\delta_{u,v} \otimes \delta_{i_2,i_2} \otimes ... \otimes \delta_{i_n,i_n},\ u \neq v.$$

Na próxima definição dou conta das matrizes que faltam à partição as quais matrizes mencionei em 6.3.4.4.

Definição 6.3.5. *Seja, em função de cada inteiro* n*, e de cada par* $u,\ v$*, sendo* $u,\ v = 1,\ 2,\ u \neq v$*, o conjunto:*

$$\lrcorner^n_{u,v} = \left\{\delta_{i,j} \in \urcorner^n\ :\ \delta_{i,j} = \delta_{u,v} \otimes \delta_{i_2,i_2} \otimes ... \otimes \delta_{i_n,i_n},\ \delta_{u,v} \in \urcorner^1,\ \delta_{i_k,i_k} \in \lrcorner^1\right\}$$

Observação 6.3.6. *1 — A contagem dos elementos de cada grupo dessa forma é fácil de realizar: são duas possibilidades por distribuir em* $n-1$ *fatores, ou seja,* 2^{n-1}

2 — Por definição são disjuntos entre si os conjuntos da forma $\urcorner^n_{u,v}$ *e da forma* $\lrcorner^n_{u,v}$*.*

3 — Da forma $\urcorner^n_{u,v}$ *são quatro os conjuntos, de cardinalidade* $2^{2(n-1)} - 2^{n-1}$*: no total somam* $2^2\left(2^{2(n-1)} - 2^{n-1}\right) = 2^{2n} - 2^{n+1}$ *elementos.*

4 — Dois são os conjuntos $\lrcorner^n_{u,v}$*, que, pelo §1, somam ao todo,* 2^n *elementos.*

5 — Tudo somado, encontram-se $2^{2n} - 2^{n+1} + 2^n = 2^{2n} - 2^n$ *elementos na união disjunta desses seis conjuntos*[1]*.*

[1] As matrizes quadradas e, sobretudo, aquelas cujo tamanha seja potência de 2 podem ser dividas, de modo natural, em quadrantes. Por exemplo, seja matriz $\delta_{8,8} \in M_8(\mathbb{Z})$. Segundo o que tenho demonstrado essa matriz pode ser decomposta da seguinte maneira: $\delta_{8,8} = \delta_{2,2} \otimes \delta_{4,4}$, sendo $\delta_{2,2} \in M_2(\mathbb{Z})$ e $\delta_{4,4} \in M_4(\mathbb{Z})$. Os quadrantes a que me refiro são determinados pelo fator

Corolário 6.3.7.

$$\urcorner_{1,1}^n \cup \urcorner_{1,2}^n \cup \lrcorner_{1,2}^n \cup \urcorner_{2,2}^n \cup \urcorner_{2,1}^n \cup \lrcorner_{2,1}^n = \urcorner^n$$

6.4 Obtenção de matrizes elementares.

Convém lembrar que o foco do estudo são as matrizes que pertencem a $\urcorner^n$. Eventualmente, como já o disse, vou retraduzir as idéias aqui delineadas em termos de noções típicas do anel $\mathbb{Z}E_n$. Para o que pretendo fazer à frente, posso desconsiderar metade desses conjuntos, com a ajuda da próxima proposição, que à primeira pode parecer uma arbitrariedade, contudo, as funções que nela defino encontram correspondentes exatos na álgebra $\mathbb{Z}E_n$.

Proposição 6.4.1. *Defino as funções ϕ_n, ψ_n e χ_n como se segue:*

$$\phi_n : \urcorner_{2,2}^n \longrightarrow \urcorner_{1,1}^n$$

$$\delta_{2,2} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_n,j_n} \longmapsto \delta_{1,1} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_n,j_n}$$

$$\psi_n : \urcorner_{2,1}^n \longrightarrow \urcorner_{1,2}^n$$

$$\delta_{2,1} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_n,j_n} \longmapsto \delta_{1,2} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_n,j_n}$$

$$\chi_n : \lrcorner_{2,1}^n \longrightarrow \lrcorner_{1,2}^n$$

$$\delta_{2,1} \otimes \delta_{i_2,i_2} \otimes ... \otimes \delta_{i_n,i_n} \longmapsto \delta_{1,2} \otimes \delta_{i_2,i_2} \otimes ... \otimes \delta_{i_n,i_n}$$

à esquerda do produto tensorial, ou seja, $\delta_{2,2}$, o quarto quadrante. Assim sendo, as matrizes contidas, por exemplo, em $\lrcorner_{2,1}^n$ são as diagonais do terceiro quadrante; aquelas em $\lrcorner_{1,2}^n$, as do segundo quadrante. Já as matrizes contidas em $\urcorner$ são as matrizes elementares, não diagonais, do primeiro, segundo terceiro ou quarto quadrantes, conforme os índices subscritos.

Então, ϕ_n, ψ_n e χ_n são bijetivas.

Demonstração. *1 — Se permutasse os índices do domínio e do contradomínio, obteria a inversa bilateral.* □

Não há dúvida de que semelhante bijeção se poderia encontrar entre os conjuntos $\urcorner_{2,2}^n$ e $\urcorner_{2,1}^n$. Todavia, não se pode perder de vista o objeto deste trabalho, o anel $\mathbb{Z}E_n$. Na próxima proposição demonstro a existência de certa bijeção que, mais à frente, poderá ser convenientemente retraduzida em termos de $\mathbb{Z}E_n$.

Proposição 6.4.2. *Sejam dados os conjuntos $\urcorner_{2,2}^n$ e $\llcorner_{2,1}^n$. Então,*

1. *Para cada $x \in \urcorner_{2,2}^n$ há um único $y_x \in \llcorner_{2,1}^n$ de tal natureza que o comutador $[1-x,\ 1-y_x]$ **não** seja trivial.*

2. *A função ζ abaixo definida é bijetiva.*

$$\begin{aligned} \zeta \ : \ \urcorner_{2,2}^n &\longrightarrow \urcorner_{2,1}^n \\ x &\longmapsto [1-x,\ 1-y_x]-1 \end{aligned}$$

Demonstração. *1 — Seja $x \in \urcorner_{2,2}^n$, então, por 6.3.3, x admite uma única decomposição da forma:*

$$x = \delta_{2,2} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_n,j_n},\ \delta_{i_\alpha,j_\alpha} \in \urcorner^1 \cup \llcorner^1,\ \exists \alpha,\ \delta_{i_\alpha,j_\alpha} \in \urcorner^1.$$

2 — Diga-se o mesmo de $y \in \llcorner_{2,1}^n$:

$$y = \delta_{2,1} \otimes \delta_{k_2,k_2} \otimes ... \otimes \delta_{k_n,k_n},\ \delta_{k_\alpha,k_\alpha} \in \llcorner^1$$

3 — Seja C o comutador $[1-x,\ 1-y]$. Segundo 6.2.1, C será não trivial se, e somente se,

$$j_\alpha = k_\alpha,\ \forall\ \alpha,\ 2 \leq \alpha \leq n.$$

4 — Seja, pois, $y_x \in \beth_{2,1}^n, y_x = \delta_{2,1} \otimes \delta_{j_2,j_2} \otimes ... \otimes \delta_{j_n,j_n},\ \delta_{k_\alpha,k_\alpha} \in \beth^1$.

5 — Em 4 fica demonstrada a existência. Quanto à unicidade, esta decorre de 6.1.2.

6 — Por 4 e por 5, a função ζ *é bem definida.*

7 — Novamente, por 6.2.1, é possível calcular o valor da função ζ*, saber:*

$$\zeta(x) = \delta_{2,1} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_n,j_n},\ \delta_{i_\alpha,j_\alpha} \in \daleth^1 \cup \beth^1,\ \exists\alpha,\ \delta_{i_\alpha,j_\alpha} \in \daleth^1.$$

8 — Dado $z \in \daleth_{2,1}^n$*, como no §1,* z *pode ser decomposto na forma:*

$$\delta_{2,1} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_n,j_n},\ \delta_{i_\alpha,j_\alpha} \in \daleth^1 \cup \beth^1,\ \exists\alpha,\ \delta_{i_\alpha,j_\alpha} \in \daleth^1.$$

9 — Seja, pois, $x = \delta_{2,2} \otimes \delta_{i_2,j_2} \otimes ... \otimes \delta_{i_n,j_n},\ \delta_{i_\alpha,j_\alpha} \in \daleth^1 \cup \beth^1,\ \exists\alpha,\ \delta_{i_\alpha,j_\alpha} \in \daleth^1$*, então,* $x \in \daleth_{2,2}^n$.

10 — Conforme expliquei nos §§1-6, $\zeta(x)$ *é bem definido e vale* $\zeta(x) = z$

12 — Por 8-10, ζ *é sobrejetiva.*

13 — Quanto à injetividade, segundo 6.1.2, há um único modo de construir x*, que satisfaça* $\zeta(x) = z$. □

Observação 6.4.3. *1. Fixado n, sejam dados* $\daleth_{2,2}^n$ *e* $\beth_{2,1}^n$.

2. Pela aplicação da função ζ *da proposição 6.4.2, posso descobrir que* $\zeta\left(\daleth_{2,2}^n\right) = \daleth_{2,1}^n$.

3. Pela aplicação das funções ϕ_n*,* ψ_n *e* χ_n*, posso estimar que*

(a) $\phi_n\left(\daleth_{2,2}^n\right) = \daleth_{1,1}^n$;

(b) $\psi_n\left(\daleth_{2,1}^n\right) = \daleth_{1,2}^n$;

(c) $\chi_n\left(\beth_{2,1}^n\right) = \beth_{1,2}^n$.

4. Segundo 6.3.7, a união disjunta dos seis conjuntos produzidos em 1-3 é $\daleth^n$

Proposição 6.4.4. *Para obter* $\daleth^n$*, basta o conhecimento dos conjuntos* $\daleth^n_{2,2}$ *e* $\beth^n_{2,1}$ *e das funções* $\zeta_n,\ \phi_n,\ \psi_n,\ \chi_n$.

6.5 Algoritmo geral de obtenção de matrizes elementares.

Convém apresentar um estudo de caso.

1. Sejam dados os conjuntos $\beth^3_{2,1}$, $\delta_{2,2} \otimes \beth^2_{2,1}$ e $\delta_{2,2} \otimes \daleth^2_{2,2}$.
2. Como se vê, por construção; vale: $\beth^3_{2,1}$, $\delta_{2,2} \otimes \beth^2_{2,1}$, $\delta_{2,2} \otimes \daleth^2_{2,2} \subset \daleth^3$.
3. Aplico à expressão $\delta_{2,2} \otimes \daleth^2_{2,2}$ a função $id \otimes \zeta_2$. A imagem, por essa função, do conjunto $\delta_{2,2} \otimes \daleth^2_{2,2}$ será $\delta_{2,2} \otimes \daleth^2_{2,1}$.
4. Aplico à $\delta_{2,2} \otimes \daleth^2_{2,2}$ a função $id \otimes \phi_2$. A imagem, por essa função, do conjunto $\delta_{2,2} \otimes \daleth^2_{2,2}$ será $\delta_{2,2} \otimes \daleth^2_{1,1}$.
5. Aplico à $\delta_{2,2} \otimes \daleth^2_{2,1}$, obtido em 3, a função $id \otimes \psi_2$. A imagem, por essa função, do conjunto $\delta_{2,2} \otimes \daleth^2_{2,1}$ será $\delta_{2,2} \otimes \daleth^2_{1,2}$.
6. Aplico à $\delta_{2,2} \otimes \beth^2_{2,1}$ a função $id \otimes \chi_2$. A imagem, por essa função, do conjunto $\delta_{2,2} \otimes \beth^2_{2,1}$ será $\delta_{2,2} \otimes \beth^2_{1,2}$.
7. Segundo declarei no §1, suponho conhecidos os conjuntos $\delta_{2,2} \otimes \beth^2_{2,1}$ e $\delta_{2,2} \otimes \daleth^2_{2,2}$. Nos §§3-6, obtive os seguintes quatro conjuntos: $\delta_{2,2} \otimes \daleth^2_{2,1}$, $\delta_{2,2} \otimes \daleth^2_{1,1}$, $\delta_{2,2} \otimes \daleth^2_{1,2}$ e $\delta_{2,2} \otimes \beth^2_{1,2}$.
8. À luz de 6.3.7, determino a reunião disjunta:

$$\begin{aligned}
&\delta_{2,2} \otimes \beth^2_{2,1} \cup \delta_{2,2} \otimes \daleth^2_{2,2} \cup \delta_{2,2} \otimes \daleth^2_{2,1} \cup \delta_{2,2} \otimes \daleth^2_{1,1} \cup \delta_{2,2} \otimes \daleth^2_{1,2} \cup \delta_{2,2} \otimes \beth^2_{1,2} \\
&= \delta_{2,2} \otimes \daleth^2 \\
&= \daleth^3_{2,2}
\end{aligned}$$

9. Aplico ao conjunto dado em 1, $\beth_{2,1}^3$, e ao obtido em 8, $\daleth_{2,2}^3$, a proposição 6.4.4, conforme delineei em 6.4.3, a fim de obter $\daleth^3$.

Em geral, trocando-se 3 por n, e 2 por $n-1$, é possível concluir:

Proposição 6.5.1. *Para obter $\daleth^n$, basta o conhecimento dos conjuntos $\beth_{2,1}^n$, $\delta_{2,2} \otimes \beth_{2,1}^{n-1}$ e $\delta_{2,2} \otimes \daleth_{2,2}^{n-1}$ e das funções $\zeta_{n-1},\ \phi_{n-1},\ \psi_{n-1},\ \chi_{n-1}$.*

Para arrematar este capítulo, apresento do algoritmo a formulação que me é mais conveniente à aplicação que tenho em vista.

Lema 6.5.2. *Seja $\delta_{i,j}$ uma matriz elementar contida em $M_2(\mathbb{Q})$, i.e., $\delta_{i,j} \in \daleth^1 \cup \beth^1$. Fixado n, se os objetos abaixo arrolados forem conhecidos:*

1. $\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{k} \otimes \beth_{2,1}^{n-k},\ 0 \leq k \leq n-2$;
2. $\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \daleth_{2,2}^2$;
3. $\zeta_k,\ \phi_k,\ \psi_k,\ \chi_k,\ \forall k,\ 1 \leq k \leq n-1$

Então, será possível gerar $\daleth^n$.

Demonstração. 1. *Segundo 6.5.1, para construir $\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \daleth^2$ basta o conhecimento de $\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \beth_{2,1}^2$ e $\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \daleth_{2,2}^2$, que são dados no enunciado.*

2. *Como, pela definição 6.3.3, $\delta_{2,2} \otimes \daleth^2 = \daleth_{2,2}^3$, é lícito dizer que:*

$$\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-3} \otimes \left(\delta_{2,2} \otimes \daleth^2\right) = \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-3} \otimes \daleth_{2,2}^2.$$

3. *Suponho, então, por indução, que o processo acima delineado tenha sido efetuado k vezes, $1 \leq k \leq n-1$. Então o resultado esperado é a lista dos conjuntos:*

(a) $\beth_{2,1}^{n}$, *dado no enunciado.*

(b) $\delta_{2,2} \otimes \beth_{2,1}^{n-1}$, *igualmente dado no enunciado.*

(c) $\delta_{2,2} \otimes \daleth_{2,2}^{n-1}$, *obtido na* $n-1$*-ésima iteração.*

4. Segundo 6.5.1, com esses conjuntos poderei construir $\daleth^{n}$.

Capítulo 7

Solução do problema.

7.1 Observações preliminares.

De volta ao problema de tese: segundo demonstrei em 5.4.3, a forma do elemento h_n é

$$2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{n}\right) \tag{7.1}$$

À luz de 5.4.1 e de 5.4.5, poderia escrever

$$\begin{aligned} h_{n,i} &= 1_n - h_n b_{n,i} \\ &= 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{n}\right)\left(\underbrace{1_1\otimes ...\otimes\underbrace{\pi_1\left(b_{1,1}\right)}_{i}\otimes ...\otimes 1_1}_{n}\right) \\ &= 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\underbrace{\delta_{2,2}\pi_1\left(b_{1,1}\right)}_{i}\otimes ...\otimes\delta_{2,2}}_{n}\right) \\ &= 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\underbrace{\delta_{2,1}}_{i}\otimes ...\otimes\delta_{2,2}}_{n}\right) \end{aligned} \tag{7.2}$$

Em particular, quando $n = 2$, vale:

$$\begin{aligned} h_{2,1} &= 1_2 - 8\,(\delta_{2,1} \otimes \delta_{2,2}) \\ h_{2,2} &= 1_2 - 8\,(\delta_{2,2} \otimes \delta_{2,1}) \end{aligned} \tag{7.3}$$

Aplicando à última equação a proposição 5.5.1, posso calcular o efeito da conjugação de $h_{2,2}$ e $h_{2,1}$ por $b_{2,2}$:

$$\begin{aligned} h_{2,1}^{b_{2,2}} &= 1_2 - 8\left(\delta_{2,1} \otimes \delta_{2,2}^{\pi_1(b_{1,1})}\right) \\ &= 1_2 - 8\,(\delta_{2,2} \otimes \delta_{1,1}) \quad \text{cf. A.5.2} \\ h_{2,2}^{b_{2,2}} &= 1_2 - 8\left(\delta_{2,2} \otimes \delta_{2,1}^{\pi_1(b_{1,1})}\right) \\ &= 1_2 + 8\,(\delta_{2,2} \otimes \delta_{1,2}) \quad \text{cf. A.5.2} \end{aligned} \tag{7.4}$$

Como se sabe o inverso duma unidade da forma $1 + \alpha,\ \alpha^2 = 0$, é $1 - \alpha$. Tomando, pois, o inverso dessas, posso colocar o resultado das operações acima, em dois conjuntos disjuntos:

$$\begin{aligned} &1_2 \pm 8\beth_{2,1}^2 \\ &1_2 \pm 8\gimel_{2,2}^2 \end{aligned} \tag{7.5}$$

Se é para empregar as idéias do capítulo anterior, sugere o 6.4.3 que conheça os equivalentes, no presente contexto, das funções ϕ_2, ψ_2, χ_2 e ζ_2. Ao definir a função ζ_2 em 6.4.2, comentei que sua fórmula pareceria arbitrária, contudo, ela já estava perfeitamente adaptada à finalidade a que a destinara: poderia empregar 6.2.2 para calcular individualmente dois comutadores diferentes e certamente posso aplicar-lhes o 6.4.3, a fim de estimar o resultado:

$$1_2 \pm 64\gimel_{2,1}^2 \tag{7.6}$$

A própria equação 7.4 acima fornece o meio por que identificar o equivalente das funções ϕ_2, ψ_2 e χ_2: a conjugação por $b_{2,1}$

$$\begin{aligned} h_{2,1}^{b_{2,1}} &= 1_2 - 8\left(\delta_{2,1}^{\pi_1(b_{1,1})} \otimes \delta_{i,j}\right) \\ &= 1_2 + 8\,(\delta_{1,2} \otimes \delta_{i,j}) \quad \text{cf. A.5.2} \\ h_{2,1}^{b_{2,1}} &= 1_2 - 8\left(\delta_{2,2}^{\pi_1(b_{1,1})} \otimes \delta_{i,j}\right) \\ &= 1_2 - 8\,(\delta_{1,1} \otimes \delta_{i,j}) \quad \text{cf. A.5.1} \end{aligned}$$

Por conseguinte, fica demonstrado como obter as unidades elementares da forma $1_2 \pm 2^*\delta_{i,j}$. Convém, no entanto, formalizar o que acabo de expor.

7.2 A contra-partida de ⅃ e a de ⅂.

Definição 7.2.1. *Seja* α, $\alpha^2 = 0$, $\alpha \in M^{2^n}(\mathbb{Q})$. *Seja, ainda,* $r \in \mathbb{Q}$. *Chamo parte nilpotente da unidade* $1 - r\alpha$, *à parcela* $r\alpha$ *que figura nessa expressão. Seja, agora,* N *o conjunto das unidades da forma* $\{1 + r\alpha\}_{r\in\mathbb{Q},\ \alpha\in M^{2^n}(\mathbb{Q})}$.

Seja, ademais, f *uma das funções* ϕ, χ, ζ *ou* ψ, *então,* $f(1 - r\alpha) = 1 - s\beta, \beta^2 = 0$.

Por efeito de f *na parte nilpotente dum elemento* $1 - r\alpha \in N$ *quero aludir à parte nilpotente da imagem* $f(1 - r\alpha)$, *a saber,* $s\beta$.

Por exemplo, o efeito de ψ_2 *na parte nilpotente de* $1 - 2\delta_{2,1} \otimes \delta_{1,2}$ *é* $\delta_{1,2} \otimes \delta_{1,2}$, *ou seja, altera o primeiro fator do produto.*

Definição 7.2.2. *Sejam as unidades* $h_{n,i}$ *como em 5.4.1. Seja, ainda,* $\mathcal{O}(h_{n,i})$ *definido como se segue, em função de* i, $1 \leq i \leq n-1$ *:*

$$\mathcal{O}(h_{n,i}) = \left\{ \left(h_{n,i}^{\pm 1}\right)^{b_{n,j}} \right\}_{j>i}.$$

Ou seja, $\mathcal{O}(h_{n,i})$ *é a órbita de* $h_{n,i}^{\pm 1}$ *relativa à conjugação pelos elementos* $b_{n,j}$, $j > i$.

Por $\mathcal{O}$ denoto a união $\cup_i \mathcal{O}(h_{n,i})$

Proposição 7.2.3. *Para todo* i, $1 \leq i \leq n-1$, *vale*

$$\mathcal{O}(h_{n,i}) = 1_n \pm 2^{n+1} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes ⅃_{2,1}^{n-i+1} \right)$$

Demonstração. *1 — Fixados n, i e j, é fácil verificar isto:*

$$h_{n,i}^{b_{n,j}} = 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ... \otimes \underbrace{\delta_{2,1}}_{i} \otimes ... \otimes \delta_{2,2}}_{n}\right)^{b_{n,j}} \quad , \text{ cf. equação 7.2}$$

$$= 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ... \otimes \underbrace{\delta_{2,1}}_{i} \otimes .. \otimes \underbrace{\delta_{2,2}^{\pi_1(b_{1,1})}}_{j} \otimes ... \otimes \delta_{2,2}}_{n}\right), \quad \text{cf. 5.5.1}$$

$$= 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ... \otimes \underbrace{\delta_{2,1}}_{i} \otimes .. \otimes \underbrace{\delta_{1,1}}_{j} \otimes ... \otimes \delta_{2,2}}_{n}\right) \quad \text{cf. apêndice A.5.1}$$

2 — Seja $\{k_{i-1}, ..., k_n\}$ uma lista de números contidas em $\{0, 1\}$. Por 5.5.1, é lícito concluir que, se for $j > i$, então

$$h_{n,i}^{b_{n,i-1}^{k_{i-1}}...b_{n,n}^{k_n}} = 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ... \otimes \underbrace{\delta_{2,1}}_{i} \otimes \delta_{2,2}^{\pi_1^{k_{i-1}}(b_{1,1})} \otimes ... \otimes \delta_{2,2}^{\pi_1^{k_n}(b_{1,1})}}_{n}\right)$$

3 — Como, pela construção em 2, $k_\beta \in \{k_{i-1}, ..., k_n\}$ vale 0 ou 1; então, $k_\beta + 1$ deve valer 1 ou 2. Explicado esse detalhe, posso reescrever a expressão que obtive em 2, do seguinte modo:

$$h_{n,i}^{b_{n,i-1}^{k_{i-1}}...b_{n,n}^{k_n}} = 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ... \otimes \underbrace{\delta_{2,1}}_{i} \otimes \delta_{k_{i-1}+1,k_{i-1}+1} \otimes ... \otimes \delta_{k_n+1,k_n+1}}_{n}\right)$$

4 — Segundo a definição 6.3.5, vê-se que o efeito da conjugação de $h_{n,i}$ por $b_{n,i-1}^{k_{i-1}}...b_{n,n}^{k_n}$ na sua parte nilpotente é $\underbrace{\delta_{2,2}\otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \beth_{2,1}^{n-i+1}$.

5 — Levando em conta os inversos, posso dizer, portanto, que $\mathcal{O}(h_{n,i}) = 1_n \pm$

$2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{i-1}\otimes\beth_{2,1}^{n-i+1}\right)$.

6 — Como no §1 deixei i fixo, e não fiz, sobre esse número, nenhuma hipótese, é-me lícito concluir que a igualdade vale para todo i. □

Quem inspecionar o enunciado, verá que excluí das hipóteses a possibilidade de ser $i = n$, não digo que isso não faça sentido, tão-somente quero destacar esse caso particular, porque assume uma forma bem peculiar.

Proposição 7.2.4.

$$\mathcal{O}\left(h_{n,n}\right) = 1_n \pm 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{n-2}\otimes\daleth_{2,2}^{2}\right)$$

Demonstração. *1 — Fixado n, posso empregar a equação 7.2:*

$$\begin{aligned} h_{n,n} &= 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{n-1}\otimes\delta_{2,1}\right) \\ &= 1_n - 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{n-2}\otimes\delta_{2,2}\otimes\delta_{2,1}\right) \end{aligned}$$

2 — Pela igualdade obtida no §1 e pelo apêndice A.5.2, posso estimar o seu conjugado por $b_{n,n}$ — data venia, registro somente o o resultado.

$$h_{n,n}^{b_{n,n}} = 1_n + 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{n-2}\otimes\delta_{2,2}\otimes\delta_{1,2}\right)$$

3 — Se considerar os inversos, é-me forçoso concluir que

$$\mathcal{O}\left(h_{n,n}\right) = 1_n \pm 2^{n+1}\left(\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{n-2}\otimes\daleth_{2,2}^{2}\right) \quad \square$$

No lema 6.5.2, descobria que, a fim de produzir todas as matrizes elementares de $\daleth^n$, suficiente seria conhecer os conjuntos

$$\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{k}\otimes\beth_{2,1}^{n-k},\ 0\leq k\leq n-2;$$

$$\underbrace{\delta_{2,2}\otimes ...\otimes\delta_{2,2}}_{n-2}\otimes\daleth_{2,2}^{2}.$$

e as funções

$$\zeta_k,\ \phi_k,\ \psi_k,\ \chi_k,\ \forall k, 2 \leq k \leq n.$$

Nas proposições 7.2.3 e 7.2.4, encontrei a contra-partida em $\mathbb{Z}E_n$ dos conjuntos listados em 7.2. Resta-me, pois, fazer o mesmo às funções $\zeta_k,\ \phi_k,\ \psi_k,\ \chi_k$ e, sobretudo, estudar, à luz de 7.2.1, o efeito que nas unidades da forma $h_{n,i}$ produzem os seus equivalentes.

7.3 As funções $\zeta_n,\ \phi_n,\ \psi_n,\ \chi_n$ em nova perspectiva.

Proposição 7.3.1. *Seja $x \in \urcorner_{2,2}^n$. Fixem-se inteiros a e b e indique-se, por $y_x \in \llcorner_{2,1}^n$, o único elemento de $\llcorner_{2,1}^n$ que não trivialize a expressão:*

$$[1 - ax,\ 1 - by_x]$$

Seja, agora, a função Z definida como se segue[1]*:*

$$Z : \urcorner_{2,2}^n \longrightarrow \urcorner_{2,1}^n$$

$$x \longmapsto [1 - ax,\ 1 - by_x] - 1$$

Então, o efeito de $[1 - ax,\ 1 - by_x]$ na parte nilpotente é idêntico ao da função ζ_n, conforme definida em 6.4.2.

Demonstração. *O resultado é válido pela própria definição de ζ_n* $\square$.

Corolário 7.3.2. *Seja $x \in \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \urcorner_{2,1}^{n-i+1}$. Fixem-se inteiros a e b e indique-se, por $y_x \in \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \llcorner_{2,1}^{n-i+1}$, o único elemento que não trivialize a*

[1]Note-se: a função Z transforma as matrizes não triviais do quarto quadrante em matrizes não triviais do terceiro quadrante. O elemento y_x é, por construção, matriz diagonal do terceiro quadrante. Para ver que esse elemento é de fato único, consulte-se o 5.5.2. cf. nota de rodapé da página 59.

expressão:

$$[1 - ax,\ 1 - by_x]$$

Então, o efeito de $[1 - ax,\ 1 - by_x]$ *na parte nilpotente é idêntico ao da função* $\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \zeta_i$.

Lema 7.3.3.

$$h_{n,i}^{b_{n,i}} = 1_n + 2^{n+1} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \underbrace{\delta_{1,2}}_{i} \otimes ... \otimes \delta_{2,2}}_{n} \right)$$

Demonstração. *1 — A demonstração desse resultado é o caso particular do parágrafo primeiro de 7.2.3, no qual caso* $i = j$.

Corolário 7.3.4. *Seja a função* $\phi_{n,i}$, *definida como se segue em função de cada* $i,\ 1 \leq i \leq n-1$ *e dum inteiro* r *qualquer.*

$$\phi_{n,i} \ :\ 1_n \pm r \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \urcorner_{2,2}^{n-i+1} \longrightarrow 1_n \pm r \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \urcorner_{1,1}^{n-i+1}.$$

$$x \longmapsto x^{b_{n,i}}$$

Então, na parte nilpotente de x, $\phi_{n,i}$ *produz o mesmo efeito que* $\underbrace{id \otimes ... \otimes id}_{i-1} \otimes \phi_i$.

Demonstração. *1 — Se* $x \in 1_n \pm r \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \urcorner_{2,2}^{n-i+1}$; *então,*

$$\begin{aligned} x^{b_{n,i}} &= 1_n \pm r \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \delta_{2,2} \underbrace{\otimes \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{n-i},j_{n-i}}}_{n-i} \right)^{b_{n,i}} \\ &= 1_n \pm r \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \delta_{2,2}^{\pi_1(b_{1,1})} \underbrace{\otimes \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{n-i},j_{n-i}}}_{n-i} \right) \\ &= 1_n \pm r \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \delta_{1,1} \underbrace{\otimes \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{n-i},j_{n-i}}}_{n-i} \right) \end{aligned}$$

Corolário 7.3.5. *Seja a função $\psi_{n,i}$, definida como se segue em função de cada $i,\ 1 \leq i \leq n-1$ e dum inteiro r qualquer.*

$$\psi_{n,i} \ : \ 1_n \pm r \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \urcorner_{2,1}^{n-i+1} \longrightarrow 1_n \pm r \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \urcorner_{1,2}^{n-i+1}.$$

$$x \longmapsto x^{b_{n,i}}$$

Então, na parte nilpotente de x, $\psi_{n,i}$ produz o mesmo efeito que $\underbrace{id \otimes ... \otimes id}_{i-1} \otimes \psi_i$.

Demonstração. *1 — Se $x \in 1_n \pm r \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \urcorner_{2,1}^{n-i+1}$; então,*

$$\begin{aligned} x^{b_{n,i}} &= 1_n \pm r \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \delta_{2,1} \underbrace{\otimes \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{n-i},j_{n-i}}}_{n-i} \right)^{b_{n,i}} \\ &= 1_n \pm r \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \delta_{2,1}^{\pi_1(b_{1,1})} \underbrace{\otimes \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{n-i},j_{n-i}}}_{n-i} \right) \\ &= 1_n \pm r \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \delta_{1,2} \underbrace{\otimes \delta_{i_1,j_1} \otimes ... \otimes \delta_{i_{n-i},j_{n-i}}}_{n-i} \right) \end{aligned}$$

Corolário 7.3.6. *Seja a função $\chi_{n,i}$, definida como se segue em função de cada $i,\ 1 \leq i \leq n-1$ e dum inteiro r qualquer.*

$$\chi_{n,i} \ : \ 1_n \pm r \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \rfloor_{2,1}^{n-i+1} \longrightarrow 1_n \pm r \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \rfloor_{1,2}^{n-i+1}.$$

$$x \longmapsto x^{b_{n,i}}$$

Então, na parte nilpotente de x, $\chi_{n,i}$ produz o mesmo efeito que $\underbrace{id \otimes ... \otimes id}_{i-1} \otimes \chi_i$.

Demonstração. *1 — Se* $x \in 1_n \pm r \underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \beth_{2,2}^{n-i+1}$*; então,*

$$x^{b_{n,i}} = 1_n \pm r \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \delta_{2,1} \underbrace{\otimes \delta_{i_1,i_1} \otimes ... \otimes \delta_{i_{n-i},i_{n-i}}}_{n-i} \right)^{b_{n,i}}$$

$$= 1_n \pm r \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \delta_{2,1}^{\pi_1(b_{1,1})} \underbrace{\otimes \delta_{i_1,i_1} \otimes ... \otimes \delta_{i_{n-i},i_{n-i}}}_{n-i} \right)$$

$$= 1_n \pm r \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \delta_{1,2} \underbrace{\otimes \delta_{i_1,i_1} \otimes ... \otimes \delta_{i_{n-i},i_{n-i}}}_{n-i} \right)$$

7.4 O algoritmo — ou a prova do problema de tese.

Teorema 7.4.1. *O subgrupo* $\langle b_1, ..., b_n,\ h_{n,1}, ..., h_{n,n} \rangle < U(\mathbb{Z}E_n)$ *tem índice finito.*

Demonstração. *1 — São dados os elementos* $b_1, ..., b_n,\ h_{n,1}, ..., h_{n,n}$*. É-me lícito considerar qualquer operação de grupo, em particular, a formação de inversos, a conjugação de elementos e os comutadores multiplicativos.*

2 — Em particular, segundo a definição 7.2.4, ser-me-ia possível construir o conjunto:

$$\mathcal{O}(h_{n,n}) = 1_n \pm 2^{n+1} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \beth_{2,2}^2 \right)$$

3 — Semelhantemente, pelas mesmas razões, com as mesmas ferramentas, construiria, à luz de 7.2.3:

$$\mathcal{O}(h_{n,i}) = 1_n \pm 2^{n+1} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{i-1} \otimes \beth_{2,1}^{n-i+1} \right), \forall\ i,\ 1 \leq i \leq n-1.$$

4 — Em particular, posso fixar, no §3, o valor $i = n - 1$

$$\mathcal{O}(h_{n,n-1}) = 1_n \pm 2^{n+1} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \beth_{2,1}^2 \right)$$

5 — Se seguir a receita delineada em 7.3.2; obterei como resultado o conjunto:

$$1_n \pm 2^{2(n+1)} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \urcorner^2_{2,1} \right)$$

6 — Se no conjunto que no §2 descrevi empregar o corolário 7.3.4, conseguirei adicionar mais um à lista:

$$1_n \pm 2^{n+1} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \urcorner^2_{1,1} \right)$$

7 — Mais dois conjuntos poderei construir, se no §4 empregar o corolário 7.3.6; e no §5, o 7.3.5:

$$1_n \pm 2^{n+1} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \lrcorner^2_{1,2} \right)$$

$$1_n \pm 2^{2(n+1)} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \urcorner^2_{1,2} \right)$$

8 — Convém notar que na última expressão as potências de 2 que aparecem na equação, à frente da parte nilpotente, são diferentes.

9 — O cálculo do quadrado dos elementos do grupo é uma das operações lícitas sobre as quais discuti no §1. O quadrado de cada elemento de $1_n \pm 2^{n+1} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \lrcorner^2_{1,2} \right)$, *forma este conjunto:*

$$1_n \pm 2^{2(n+1)} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \lrcorner^2_{1,2} \right)$$

10 — Considerando, pois, os quadrados, à maneira do §9, é-me possível determinar, à luz 6.3.7, a união disjunta dos seis conjuntos até agora obtidos.

$$1_n \pm 2^{2(n+1)} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-2} \otimes \urcorner^2 \right) = 1_n \pm 2^{2(n+1)} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-3} \otimes \delta_{2,2} \otimes \urcorner^2 \right)$$

$$= 1_n \pm 2^{2(n+1)} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-3} \otimes \urcorner^3_{2,2} \right).$$

11 — Fixando $i = n - 2$, no §3, o conjunto abaixo descrito posso obtê-lo; e a construção acima esboçada, repeti-la.

$$1_n \pm 2^{n+1} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-3} \otimes \beth_{1,2}^3 \right)$$

12 — À luz de 7.3.4, 7.3.6, 7.3.5 e 7.3.2, posso propor a seguinte hipótese de indução, de que, para todo $n - 1 \geq k \geq 1$, após $n - k$ repetições, o resultado do processo delineado nos §§1-11 seja o conjunto

$$1_n \pm 2^{(n-k)(n+1)} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-k} \otimes \urcorner^k \right) = 1_n \pm 2^{(n-k)(n+1)} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-k-1} \otimes \delta_{2,2} \otimes \urcorner^k \right)$$
$$= 1_n \pm 2^{(n-k)(n+1)} \left(\underbrace{\delta_{2,2} \otimes ... \otimes \delta_{2,2}}_{n-k-1} \otimes \urcorner_{2,2}^{k+1} \right).$$

13 — Segundo essa mesma hipótese de indução, na $n-1$-ésima repetição, o resultado será

$$1_n \pm 2^{(n-1)(n+1)} \left(\delta_{2,2} \otimes \urcorner^{n-1} \right) = 1_n \pm 2^{(n-1)(n+1)} \urcorner_{2,2}^n$$

14 —Mutatis mutandis: Posso fixar, em 3, o valor $i = 1$

$$\mathcal{O}\left(h_{n,1}\right) = 1_n \pm 2^{n+1} \beth_{2,1}^n$$

15 — Se seguir a receita delineada em 7.3.2, obterei como resultado o conjunto:

$$1_n \pm 2^{n(n+1)} \urcorner_{2,1}^n$$

16 — Se no conjunto descrito na hipótese de indução empregar o corolário 7.3.4, conseguirei adicionar mais um conjunto à lista:

$$1_n \pm 2^{(n-1)(n+1)} \urcorner_{1,1}^{n-1}$$

17 — Mais dois conjuntos poderei construir, se no §15 empregar o corolário 7.3.6; e no §14, o 7.3.5:

$$1_n \pm 2^{(n-1)(n+1)} \beth_{1,2}^n$$

$$1_n \pm 2^{n(n+1)} \urcorner_{1,2}^n$$

18 — Em analogia com os §§8 e 9, é necessário calcular a n-ésima potência dos conjuntos da forma $1_n \pm 2^{n+1} (\delta_{2,2} \otimes *)$*, a fim de determinar a união disjunta entre eles.*

$$1_n \pm 2^{n(n+1)} \urcorner^n$$

19 — Segundo 4.6.1, o subgrupo $\langle b_1, ..., b_n,\ h_{n,1}, ..., h_{n,n} \rangle < U(\mathbb{Z}E_n)$ *tem índice finito.*

Apêndice A

Cálculos explícitos.

Neste apêndice arrolo os cálculos matriciais que me foram necessários ao longo do trabalho.

A.1 Propriedades elementares das matrizes elementares.

Em primeiro lugar dois lembretes: como efetuar cálculos com matrizes elementares, e como descobrir os índices do produto tensorial de matrizes elementares.

Teorema A.1.1. *Seja* $\Delta(r,s)$ *o* Δ *de Kronecker*

$$\delta_{i,j}\delta_{k,l} = \Delta(k,i)\,\delta_{i,l} \tag{A.1}$$

Teorema A.1.2. *Sejam* $\delta_{i,j} \in M_n(\mathbb{Z})$ *e* $\delta_{k,l} \in M_m(\mathbb{Z})$, *matrizes elementares. Então:*

$$\delta_{i,j} \otimes \delta_{k,l} = \delta_{m(i-1)+k,\ m(j-1)+l}.$$

Em particular, o produto de Kronecker de matrizes elementares é matriz elementar.

A.2 a

Proposição A.2.1.

$$a = \delta_{1,1} - \delta_{2,2}$$

Demonstração. *cf. §16 da demonstração de 3.4.1.*

Proposição A.2.2.

$$1 - a = 2\delta_{2,2}$$

Demonstração.

$$\begin{aligned} 1 - a &= \delta_{1,1} + \delta_{2,2} - (\delta_{1,1} - \delta_{2,2}) \\ &= \delta_{1,1} + \delta_{2,2} - \delta_{1,1} + \delta_{2,2} \\ &= 2\delta_{2,2} \end{aligned}$$

A.3 b

Proposição A.3.1.

$$b = -\delta_{1,2} + \delta_{2,1}$$

$$b^2 = -1$$

Demonstração. *cf. §16 da demonstração de 3.4.1.*

A.4 h

Proposição A.4.1.

$$(1 - a)\, b = 2\delta_{2,1}$$

Demonstração.

$$(1-a)\,b = 2\delta_{2,2}b \quad \textit{cf. A.2.2}$$

$$2\delta_{2,2}\left(-\delta_{1,2}+\delta_{2,1}\right) \quad \textit{cf. A.3.1}$$

$$= 2\delta_{2,1} \quad \textit{cf. A.1.1}$$

A.5 Conjugados.

Proposição A.5.1.

$$(1-a)^b = 2\delta_{1,1}$$

Demonstração.

$$b\,(1-a)\,b^3 = -b\,(1-a)\,b \quad \textit{cf. A.3.1}$$

$$= -b\,(2\delta_{2,2})\,b \quad \textit{cf. A.2.2}$$

$$= -b\,(2\delta_{2,2}b)$$

$$= -b\,(2\delta_{2,1}) \quad \textit{cf. A.4.1}$$

$$= -2b\delta_{2,1}$$

$$= -2\left(-\delta_{1,2}+\delta_{2,1}\right)\delta_{2,1} \quad \textit{cf. A.3.1}$$

$$= -2-\delta_{1,1} \quad \textit{cf. A.1.1}$$

$$= 2\delta_{1,1}$$

Proposição A.5.2.

$$((1-a)\,b)^b = -2\delta_{1,2}$$

Demonstração.

$$\begin{aligned}
((1-a)\,b)^b &= b\,(1-a)\,b^4 \\
&= b\,(1-a) \\
&= (-\delta_{1,2}+\delta_{2,1})\,(1-a) \quad \textit{cf. A.3.1} \\
&= 2\,(-\delta_{1,2}+\delta_{2,1})\,\delta_{2,2} \quad \textit{cf. A.2.2} \\
&= -2\delta_{1,2}
\end{aligned}$$

Referências Bibliográficas

[1] BERTRAM HUPPERT, *Endliche Gruppen I*, GWM, 134, Springer Verlag, Heidelberg, 1967.

[2] CÉSAR P. MILIES E SEDARSHAN K. SEHGAL, *An Introduction to Group Rings*, Kluwer Academic Press, 2002.

[3] CHARLES W. CURTIS, *Linear Algebra, an Introductory Approach*, Springer Verlag, Nova Iorque, 1984.

[4] DANIEL GORENSTEIN, *Finite Groups*, Chelsea Publishing Company, Nova Iorque, 1980.

[5] GRAHAM HIGMAN, *The units of group rings*, Proc. London Mat. Soc. 46, 2, 231-248, 1940.

[6] IRVING REINER, *Maximal Orders*, Clarendon Press, Oxford, 2003.

[7] ISRAEL M. ISAACS, *Character Theory of Finite Groups*, Academic Press, 1976.

[8] HYMAN BASS, *K-theory and stable algebra*, Publications mathématiques de l'I.H.É.S., 22, 5-60, 1964.

[9] HYMAN BASS, JOHN MILNOR E JEAN-PIERRE SERRE, *Solution of the congruence subgroup problem for $SL_n\,(n \geq 3)$ and $Sp_{2n}\,(n \geq 2)$* , Publications mathématiques de l'I.H.É.S., 33, 59-137, 1964.

[10] JÜRGEN RITTER E SUDARSHAN K. SEHGAL, *Certain normal subgroups of units in group rings*, J. reine angew. 381, 214-220, 1987.

[11] JÜRGEN RITTER E SUDARSHAN K. SEHGAL, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. 324, 2, 603-621, abril de 1991.

[12] JÜRGEN RITTER E SUDARSHAN K. SEHGAL, *Generators of Subgroups of* $U\,(ZG)$, Cont. Math. 93, 1989.

[13] JÜRGEN RITTER E SUDARSHAN K. SEHGAL, *Integral group rings with trivial central units*, Proc. Amer. Math. Soc. 20, 2, fevereiro de 1989.

[14] SUDARSHAN K. SEHGAL, *Topics in Group Rings*, Pure and applied mathematics 50, Marcel Dekker, Nova Iorque, 1978.

[15] SUDARSHAN K. SEHGAL, *Units in Integral Group Rings*, Pitman monographs and surveys in pure and applied mathematics 69, Longman scientific and technical, Bath, 1993.

[16] TSIT Y. LAM, *A First Course in Noncommutative Rings*, GTM 131, Springer Verlag, Nova Iorque, 1991.