UNIVERSIDADE FEDERAL
DO RIO DE JANEIRO

COTAS PARA O ÍNDICE DO SUBGRUPO GERADO PELAS UNIDADES BICÍCLICAS NO GRUPO DE UNIDADES DO ANEL DE GRUPO INTEIRO DE GRUPOS EXTRA-ESPECIAIS

Elaine Araujo da Silva

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

Orientador: Guilherme Augusto de La Rocque Leal

Rio de Janeiro
de 2017

COTAS PARA O ÍNDICE DO SUBGRUPO GERADO PELAS UNIDADES BICÍCLICAS NO GRUPO DE UNIDADES DO ANEL DE GRUPO INTEIRO DE GRUPOS EXTRA-ESPECIAIS

Elaine Araujo da Silva

TESE SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE MATEMÁTICA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM CIÊNCIAS. ÁREA DE CONCENTRAÇÃO: MATEMÁTICA.

Banca Examinadora:

Prof. Guilherme Augusto de La Rocque Leal, D.Sc.

Prof. Antônio Pacques - UFRGS, D.Sc.

Prof. Francisco César Polcino Milies - USP, D.Sc.

Prof. Ilir Snopche - IM/UFRJ, D.Sc.

Profa. Luciane Quoos Conte - IM/UFRJ, D.Sc.

Aprovada em 22 de dezembro de 2017.

RIO DE JANEIRO, RJ – BRASIL
DE 2017

Araujo da Silva, Elaine

Cotas para o índice do subgrupo gerado pelas unidades bicíclicas no grupo de unidades do anel de grupo inteiro de grupos extra-especiais/Elaine Araujo da Silva. – Rio de Janeiro: UFRJ/IM/DM, 2017.

VIII, 55 p. 29, 7cm.

Orientador: Guilherme Augusto de La Rocque Leal

Tese (doutorado) – UFRJ/IM/Programa de Matemática, 2017.

Referências Bibliográficas: p. 52 – 52.

I. Augusto de La Rocque Leal, Guilherme. II. Universidade Federal do Rio de Janeiro, IM, Programa de Matemática. III. Título.

"O que sabemos é uma gota,o
que ignoramos é um oceano.Mas
o que seria o oceano senão
infinitas gotas?"

Isaac newton

Agradecimentos

Gostaria de agradecer a Deus em primeiro lugar a minha família por todo o apoio. Agradeço muito ao meu orientador pela sua paciência e companheirismo. Não posso deixar de agradecer ao meu amigo Benaia pela sua prontidão em sempre me ajudar com o Latex e à Cristiane de Mello por toda a ajuda e troca de experiências. Finalmente agradeço a todos os professores desde a época do mestrado com quem tive contato que me influenciaram e inspiraram, ajudando portanto no meu crescimento profissional.

Resumo da Tese apresentada ao IM/UFRJ como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências (D.Sc.)

COTAS PARA O ÍNDICE DO SUBGRUPO GERADO PELAS UNIDADES BICÍCLICAS NO GRUPO DE UNIDADES DO ANEL DE GRUPO INTEIRO DE GRUPOS EXTRA-ESPECIAIS

Elaine Araujo da Silva

/2017

Orientador: Guilherme Augusto de La Rocque Leal

Programa: Matemática

No estudo de alguns subgrupos invertíveis do anel de grupo $\mathbb{Z}D_4$ Jespers e Leal construíram um isomorfismo de grupos que nos permite estudar as unidades bicíclicas em $M_2(\mathbb{Q})$,sendo as mesmas um conjunto de inversíveis em $\mathbb{Z}D_4$ D_4 é o grupo diedral. Considerando $\mathcal{B}_2$ o subgrupo em $\mathcal{U}(\mathbb{Z}D_4)$ gerado pela mesmas , segue que nesse caso $\mathcal{B}_2 \subset E_2$ é uma inclusão direta e trivial. Além disso temos que $E_4 \subset \mathcal{B}_2$, E_n é o subgrupo gerado pelas matrizes elementares em $Sl(\mathbb{Z})$ da forma $I_d + ne_{ij}$, $i \neq j$. Trabalhando então com $G = \dfrac{D_4 \times D_4^*}{I}$, D_4^* é um grupo isomorfo ao D_4 e $I \subset D_4 \times D_4^*$ é um subgrupo escolhido para que $Z(G) = G' = \{1, s\}$, vamos provar que a inclusão $\mathcal{B}_2 \subset E_2$ será preservada e além disso $E_{2^3} \subset \mathcal{B}_2$. Generalizando o resultado provaremos que sendo $G = \dfrac{D_4^1 \times D_4^2 \times \ldots \times D_4^n}{I}$, D_4^i são grupos isomorfos ao D_4 então $E_{2^n} \subset \mathcal{B}_2 \subset E_2$ onde $\mathcal{B}_2 \subset \mathcal{U}(\mathbb{Z}G)$.

Abstract of Thesis presented to IM/UFRJ as a partial fulfillment of the requirements for the degree of Doctor of Science (D.Sc.)

Elaine Araujo da Silva

/2017

Advisor: Guilherme Augusto de La Rocque Leal

Department: Mathematics

In the study of some invertible subgroups in ring of group $\mathbb{Z}D_4$ Jespers e Leal ,they built an isomorphism that allow to study the bicyclics units in its matrix form in $M_2(\mathbb{Q})$, being the same a set of inversions in $\mathbb{Z}D_4$, D_4 is the dihedral group. Whereas $\mathcal{B}_2$ the subgroup generated by the bicyclic units,follow that $\mathcal{B}_2 \subset E_2$ is an inclusion direct and trivial. Besides that $E_4 \subset \mathcal{B}_2$, E_n is the subgroup generated by the elementary matrices the form $I_d + ne_{ij}, i \neq j$. Working then with $G = \dfrac{D_4 \times D_4^*}{I}$, D_4^* is an isomorphic group to the D_4 and $I \subset D_4 \times D_4^*$ is a subgroup chosen for $Z(G) = \{1, s\}$, let's prove that the inclusion $\mathcal{B}_2 \subset E_2$ will be preserved and beyond that $E_{2^n} \subset \mathcal{B}_2$. Generalizing the result will prove que being $G = \dfrac{D_4^1 \times D_4^2 \times \ldots \times D_4^n}{I}$, D_4^i are isomorphic groups to the dihedral group follow that $E_{2^n} \subset \mathcal{B}_2 \subset E_2$ where $\mathcal{B}_2 \subset \mathcal{U}\mathbb{Z}G$.

Sumário

Introdução

Seja G um grupo, b um elemento em G e a qualquer elemento de ordem finita e então podemos construir um elemento inversível em $\mathbb{Z}(G)$ da forma:

$$\mu_{a,b} = 1 + (1-a)b\hat{a},\ \hat{a} = 1 + a + a^2 + \ldots + a^{n-1}$$

e caso definindo $\eta = (1-a)b\hat{a}$ é fácil ver que $\eta^2 = 0$ e portanto $(\mu_{a,b})^{-1} = 1 - (1-a)b\hat{a}$.

Esse elemento é chamado de uma unidade bicíclica de $\mathbb{Z}(G)$ e para maiores detalhes veja em(RITTER e K.SEHGAL [1]).

O célebre matemático, John Milmor, criou uma classe de inversíveis em $\mathbb{Z}(G)$ e, quando o grupo é abeliano, Hyman Bass (ver em H.BASS [2]) provou que esse conjunto tem índice finito em $U(\mathbb{Z}G)$. Esse elemento inversível em $\mathbb{Z}G$ é chamada de unidade cíclica de Bass sendo portanto definido por:

$$\mu_i = (1 + g + g^2 + \ldots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\hat{g},$$

onde g é um elemento de ordem n, i é um inteiro com $mdc(i,n) = 1$ e $\phi(n)$ é a função totiente de Euler.

Seja $\mathcal{B}$ o subgrupo gerado pelas unidades cíclicas e bicíclicas. Sehgal e Jurgen Ritter demonstraram que quando o grupo $\mathcal{B}$ é não abeliano ele é de índice finito em $\mathcal{U}(\mathbb{Z}G)$. .

Nesse trabalho,vamos considerar primeiramente um grupo G pertencente à família de 2-grupos extra especiais formado pelo produto central de 2 cópias isomorfas do grupo diedral D_4. Observe que nesse caso as unidades cíclicas são triviais e então $\mathcal{B}$ será formado apenas pelas unidades bicíclicas. Nós estimaremos então o índice de $\mathcal{B}$ em $U(\mathbb{Z}G)$.

Ao considerar $E = \dfrac{1-s}{2}$ um idempotente do anel de grupo $\mathbb{Q}G$, s está no centro de D_4 e $s^2 = 1$, por conseqüencia $\mathbb{Q}G = \mathbb{Q}GE \oplus \mathbb{Q}G(1-E)$, então nesse trabalho provaremos que $\mathbb{Q}GE \cong M_4(\mathbb{Q})$ e a partir disso estabeleceremos um monomorfismo φ de U_2 em $\varphi(U_2) \subset M_4(\mathbb{Q})$ com U_2 definido por:

$$U_2 = \mathcal{U}(\mathbb{Z}G) \cap \left(\mathbb{Q}G\left(\frac{1-s}{2}\right) + \left(\frac{1+s}{2}\right)\right)$$

O resultado que segue é encontrado em JESPERS [3] nos fornece propriedades importantes de U_2 em $\mathcal{U}\mathbb{Z}G$:

Proposição 0.1. *Com U_2 definido acima, temos que:*

(*i*) $U_2 = \{u = 1 + \alpha(1-s) |\, u \in \mathcal{U}(\mathbb{Z}G),\ \alpha \in \mathbb{Z}G\}$;

(*ii*) $V = \{u = 1 + \alpha\,(1-s) |\, u \in \mathcal{U}(\mathbb{Z}G),\ \alpha \in \mathbb{Z}G$ *e* $\varepsilon(\alpha)$ *é par*$\}$ *é um subgrupo livre de torsão de* U_2 *e* $V \cong U_2/G'$.

Pela proposição anterior se $u \in U_2$ então $u = \{1 + \alpha(1-s)/\alpha \in \mathbb{Z}(G)\}$ e então ao utilizar o monomorfismo φ segue que $V \cong \dfrac{(U_2)}{G'} \cong \dfrac{\varphi(U_2)}{\{I_d, -I_d\}}$.

No caso em que V é subgrupo de $\mathcal{U}(\mathbb{Z}D_4)$ verifica-se que $V \subset \Gamma_2(2)$ a menos de um isomorfismo pois $\dfrac{\varphi(U_2)}{\{I_d, -I_d\}} \subset \Gamma_2(2)$, sendo $\Gamma_n(m)$ o núcleo do homomorfismo $SL_n(\mathbb{Z}) \longrightarrow SL_n(\mathbb{Z}_m)$ induzido pela aplicação canônica $\mathbb{Z} \longrightarrow \mathbb{Z}_m$. Em NEWMAN [4] sabemos que $\Gamma_2(2) = E_2, E_p =< (I_d + pe_{ij})/i \neq j >, e_{ij}$ são as matrizes elementares em $M_n(\mathbb{Z})$ e segue então trivialmente que $\mathcal{B}_2 \subset V \subset \Gamma_2(2) = E_2, \mathcal{B}_2$ é o subgrupo de $\mathbb{Z}(D_4)$ gerado pelas unidades bicíclicas.

Nesse trabalho vamos então provar que a inclusão $\mathcal{B}_2 \subset E_2$, será preservada estudando $\mathcal{B}_2$ como subgrupo em $PLS_4(\mathbb{Q}) = \dfrac{SL_n(\mathbb{Q})}{\{I_d, -I_d\}}$ estando $\mathcal{B}_2$ em $\mathbb{Z}(G), G$, G é o produto central de 2 cópias isomorfas de D_4,visto que nesse caso a inclusão não é direta pois $\dfrac{\varphi(U_2)}{\{I_d, -I_d\}} \neq E_2$.

Em H.BASS [2] segue que $\left|\dfrac{SL_n(\mathbb{Z})}{E_p}\right| < +\infty$ para $n \geq 3$. Então provando que $E_8 \subset \varphi(\mathcal{B}_2) \subset E_2$ como subgrupo de $PLS_4(\mathbb{Q})$ estabeleceremos uma cota de índice superior e inferior para $\varphi(\mathcal{B}_2)$ em $SL_n(\mathbb{Z})$ de tal forma que $\left|\dfrac{SL_4(\mathbb{Z})}{E_2}\right| \leq \left|\dfrac{SL_4(\mathbb{Z}}{\varphi(\mathcal{B}_2)}\right| \leq \left|\dfrac{SL_4(\mathbb{Z})}{E_8}\right|$.

No capítulo 1 serão apresentados resultados relevantes sobre anéis de grupos e outros tópicos essenciais utilizados no desenvolvimento desse trabalho.

No capítulo 2 vamos apresentar as ferramentas necessárias para estudarmos as unidades bicíclicas em $\mathcal{U}(\mathbb{Z}G)$ na sua forma matricial em $M_4(\mathbb{Q})$. Para isso teremos o estudo da decomposição de $\mathbb{Q}(D_4)$ e $\mathbb{Q}G$ em componentes simples.

No capítulo 3 será então provado que $E_8 \subset \varphi(\mathcal{B}_2)$ e $\mathcal{B}_2 \subset E_2$ como um subgrupo do grupo projetivo $PLS_4(\mathbb{Q})$ e que por H.BASS [2] segue que $[E_2 : B_2] < +\infty$.

No capítulo 4 teremos um resultado mais generalizado onde será provado que $E_{2^{n+1}} \subset \varphi(\mathcal{B}_2)$ e $\mathcal{B}_2 \subset E_2$ ao considerar $\mathcal{B}_2$ um subgrupo de $\mathcal{U}(\mathbb{Z}G)$ onde G é o produto central de n cópias isomorfas de grupos isomorfos ao grupo diedral.

1 Resultados Preliminares

Neste primeiro capítulo, apresentaremos alguns tópicos básicos da *Teoria de Anéis de Grupo*, cujos detalhes de todas demonstrações podem ser encontrados em POLCINO [5]. Fixaremos algumas notações e estabeleceremos alguns resultados que serão utilizados ao longo do texto.

1.1 Anéis de grupo

Nesta primeira seção, introduziremos a definição de um anel de grupo RG, onde G é um grupo e R é um anel comutativo com identidade, e apresentaremos algumas de suas principais propriedades. Além disso, caracterizaremos os anéis de grupo RG no caso em que G é um produto direto de grupos.

Seja G um grupo (não necessariamente finito) e seja R um anel comutativo com identidade. Denotaremos por RG o conjunto de todas as combinações lineares da forma

$$\lambda = \sum_{g \in G} \lambda_g \, g,$$

onde $\lambda_g \in R$, para todo $g \in G$, e $\lambda_g = 0$ quase sempre, isto é, somente um número finito de coeficientes são diferentes de 0 em cada uma dessas somas.

Definição 1.1. *Dado um elemento $\lambda = \sum_{g \in G} \lambda_g g \in RG$, definimos o* ***suporte de*** *λ como sendo o subconjunto dos elementos de G cujos coeficientes em λ são não nulos e o denotaremos por $supp(\lambda)$, isto é:*

$$supp(\lambda) = \{g \in G;\ \lambda_g \neq 0\}.$$

Observação 1.1. *Dados $\lambda, \mu \in RG$, $\lambda = \sum_{g \in G} \lambda_g g$ e $\mu = \sum_{g \in G} \mu_g g$, temos $\lambda = \mu$ se, e somente se, $\lambda_g = \mu_g$, para todo $g \in G$.*

Definição 1.2. *Dados* $\alpha \in R$ *e* $\lambda, \mu \in RG$, $\lambda = \sum_{g\in G} \lambda_g g$ *e* $\mu = \sum_{g\in G} \mu_g g$, *definimos a soma* $\lambda + \mu$, *o produto* $\lambda\mu$ *e o produto por escalar* $\alpha \cdot \lambda$ *por:*

$$(i)\ \lambda + \mu = \sum_{g\in G} \lambda_g g + \sum_{g\in G} \mu_g g = \sum_{g\in G} (\lambda_g + \mu_g) g;$$

$$(ii)\ \lambda\mu = \Big(\sum_{g\in G} \lambda_g g\Big)\Big(\sum_{g\in G} \mu_g g\Big) = \sum_{g\in G} \nu_g g,\ \textit{onde}$$

$$\nu_g = \sum_{h\in G} \lambda_h \mu_{h^{-1}g} = \sum_{xy=g} \lambda_x\, \mu_y;$$

$$(iii)\ \alpha \cdot \lambda = \alpha\Big(\sum_{g\in G} \lambda_g g\Big) = \sum_{g\in G} (\alpha\lambda_g) g.$$

Com as operações de soma e produto definidos acima, RG é um anel com identidade 1, a saber

$$1 = \sum_{g\in G} u_g g,$$

onde o coeficiente correspondente ao elemento identidade do grupo é igual a 1 e $u_g = 0$ para todo $g \in G$, $g \neq 1$. Em relação à soma e ao produto por escalar, RG é um R-módulo.

Podemos definir uma imersão $i : G \to RG$ associando a cada elemento $a \in G$ o elemento

$$i(a) = \sum_{g\in G} \gamma_g g \in RG$$

tal que $\gamma_a = 1$ e $\gamma_g = 0$, se $g \neq a$. Deste modo, consideramos G como um subconjunto de RG. Com esta identificação, podemos afirmar que RG é um R-módulo livre com base G.

Também podemos definir uma aplicação $\upsilon : R \to RG$ dada por

$$\upsilon(\alpha) = \sum_{g\in G} \eta_g g \in RG,$$

onde $\eta_1 = \alpha$ e $\eta_g = 0$ para todo $g \in G$, $g \neq 1$. Claramente, υ é um monomorfismo de anéis e, desta maneira, podemos considerar R como um subanel de RG.

Com estas identificações, dados $\alpha \in R$ e $g \in G$, é claro que $\alpha g = g\alpha$ em RG. Portanto, denotando por $\mathcal{Z}(RG)$ o centro de RG, obtemos $R \subseteq \mathcal{Z}(RG)$.

Definição 1.3. *O conjunto* RG *com as operações definidas anteriormente, é chamado* ***Anel de Grupo*** *de* G *sobre* R.

Na sequência, apresentaremos uma descrição para o anel de grupo RG, no caso em que G é um grupo qualquer. Para tal, precisaremos da definição que segue.

Definição 1.4. *Sejam G um grupo finito e $\{\mathcal{C}_i\}_{i\in I}$ o conjunto das classes de conjugação de G. Para cada índice $i \in I$, os elementos*

$$C_i = \sum_{x\in\mathcal{C}_i} x.$$

são ditos ***Somas de Classe*** *de G sobre R.*

Teorema 1.1. *Se G é um grupo finito, então o conjunto $\{C_i\}_{i\in I}$, de todas as somas de classe de G sobre R, é uma base do centro $\mathcal{Z}(RG)$ de RG sobre R. Em particular, $\mathcal{Z}(RG)$ é um R-módulo livre cujo posto é igual ao número de classes de conjugação de G.*

O resultado seguinte mostra que podemos considerar RG um anel com involução.

Nosso próximo passo será definir a *Aplicação de Aumento* e o *Ideal de Aumento* de RG.

Definição 1.5. *O homomorfismo $\varepsilon : RG \to R$ definido por*

$$\varepsilon\Big(\sum_{g\in G} \lambda_g g\Big) = \sum_{g\in G} \lambda_g \in R$$

é chamado a ***Aplicação de Aumento*** *de RG. O núcleo de ε é chamado o* ***Ideal de Aumento*** *de RG e será denotado por $\Delta(G)$.*

Observação 1.2. *Dado um elemento* $\lambda = \sum_{g\in G} \lambda_g g \in \Delta(G)$, *temos que*

$$\varepsilon(\lambda) = \epsilon\Big(\sum_{g\in G} \lambda_g g\Big) = \sum_{g\in G} \lambda_g = 0.$$

Daí, podemos escrever λ *na forma*

$$\lambda = \sum_{g\in G} \lambda_g g - \sum_{g\in G} \lambda_g = \sum_{g\in G} \lambda_g (g-1).$$

É claro que $g-1 \in \Delta(G)$, *para todo* $g \in G$. *Logo, a igualdade acima mostra que* $\{g-1;\, g\in G,\, g\neq 1\}$ *é um conjunto de geradores de* $\Delta(G)$ *sobre* R. *Além disso, como os elementos de* G *são linearmente independentes sobre* R, *segue que este conjunto é linearmente independente.*

Proposição 1.1. *O conjunto* $\{g-1;\, g\in G,\, g\neq 1\}$ *é uma base de* $\Delta(G)$ *sobre* R. *Logo, podemos escrever*

$$\Delta(G) = \left\{\sum_{g\in G} \lambda_g (g-1);\, g\in G,\, g\neq 1,\, \lambda_g \in R\right\},$$

onde, como sempre, assumimos que somente um número finito de coeficientes λ_g *são diferentes de 0. Em particular, se* G *é um grupo finito, então* $\Delta(G)$ *é um* R*-módulo livre de posto* $|G|-1$.

Para finalizarmos esta seção, caracterizaremos os anéis de grupo RG no caso em que G é um produto direto de grupos.

Proposição 1.2. *Sejam* G *e* H *grupos e seja* R *um anel comutativo com identidade. Então,*

$$R(G\times H) \cong (RG)H \cong RG \otimes_R RH.$$

Demonstração. Primeiramente, observamos que, dados $g\in G$ e $h\in H$, gh é uma unidade do anel $(RG)H$: $ghg^{-1}h^{-1} = gg^{-1}hh^{-1} = 1$.

Agora, consideramos a aplicação $\overline{\varphi}$ do grupo $G\times H$ no grupo de unidades do anel $(RG)H$ definida por $\overline{\varphi}(g,h) = gh$.

Afirmamos que $\overline{\varphi}$ é um homomorfismo de grupos injetor.

De fato, dados $(g_1,h_1),(g_2,h_2)\in G\times H$, temos que:

• $\overline{\varphi}((g_1,h_1)\cdot(g_2,h_2)) = \overline{\varphi}(g_1g_2,h_1h_2) = g_1g_2h_1h_2 = g_1h_1g_2h_2 = \overline{\varphi}(g_1,h_1)\cdot \overline{\varphi}(g_2,h_2)$;

• $\overline{\varphi}(g_1,h_1) = \overline{\varphi}(g_2,h_2) \Rightarrow g_1h_1 = g_2h_2 \Rightarrow g_1 = g_2$ e $h_1 = h_2 \Rightarrow (g_1,h_1) = (g_2,h_2)$.

Logo, $\overline{\varphi}$ é um homomorfismo de grupos injetor.

Vamos estender $\overline{\varphi}$ linearmente da seguinte maneira:

$$\begin{array}{rccc} \varphi \ : & R(G\times H) & \longrightarrow & (RG)H \\ & \sum\limits_{g\in G,\, h\in H} \lambda_{gh}(g,h) & \longmapsto & \sum\limits_{h\in H}\Big(\sum\limits_{g\in G}\lambda_{gh}g\Big)h. \end{array}$$

Afirmamos que φ é um isomorfismo de anéis de grupo.

De fato, sejam $\lambda,\mu,\gamma \in R(G\times H)$, onde $\lambda = \sum\limits_{g\in G,\, h\in H}\lambda_{gh}(g,h)$, $\mu = \sum\limits_{j\in G,\, k\in H}\mu_{jk}(j,k)$ e $\gamma = \sum\limits_{g\in G,\, h\in H}\gamma_{gh}(g,h)$, e seja $\alpha\in R$, então:

- $\varphi(\lambda\cdot\mu) = \varphi\Big(\sum \lambda_{gh}\mu_{jk}(gj,hk)\Big) = \sum\limits_{h,k\in H}\Big(\sum\limits_{g,j\in G}\lambda_{gh}\mu_{jk}gj\Big)hk =$

$$= \sum_{h\in H}\Big(\sum_{g\in G}\lambda_{gh}g\Big)h \cdot \sum_{k\in H}\Big(\sum_{j\in G}\mu_{jk}j\Big)k =$$

$$= \varphi\Big(\sum_{g\in G,\, h\in H}\lambda_{gh}(g,h)\Big)\cdot\varphi\Big(\sum_{j\in G,\, k\in H}\mu_{jk}(j,k)\Big) = \varphi(\lambda)\cdot\varphi(\mu);$$

- $\varphi(\lambda+\gamma) = \varphi(\Big(\sum\limits_{g\in G,h\in H}\lambda_{gh}+\gamma_{gh}\Big)(g,h)) = \sum\limits_{h\in H}\Big(\sum\limits_{g\in G}(\lambda_{gh}+\gamma_{gh})g\Big)h =$

$$= \sum_{h\in H}\Big(\sum_{g\in G}\lambda_{gh}g\Big)h + \sum_{h\in H}\Big(\sum_{g\in G}\gamma_{gh}g\Big)h = \varphi(\lambda)+\varphi(\gamma);$$

Logo, φ é um homomorfismo de anéis de grupo. Resta mostrar que φ é bijetor.

Sejam $\lambda,\gamma\in R(G\times H)$, onde $\lambda = \sum\limits_{g\in G,\, h\in H}\lambda_{gh}(g,h)$ e $\gamma = \sum\limits_{g\in G,\, h\in H}\gamma_{gh}(g,h)$, então:

- $\varphi(\lambda) = \varphi(\gamma) \Rightarrow \sum\limits_{h\in H}\Big(\sum\limits_{g\in G}\lambda_{gh}g\Big)h = \sum\limits_{h\in H}\Big(\sum\limits_{g\in G}\gamma_{gh}g\Big)h \Rightarrow$

$$\Rightarrow \sum_{h\in H}\Big(\sum_{g\in G}\lambda_{gh}g\Big)h - \sum_{h\in H}\Big(\sum_{g\in G}\gamma_{gh}g\Big)h = 0 \Rightarrow$$

$$\Rightarrow \sum_{h\in H}\Big(\sum_{g\in G}(\lambda_{gh}-\gamma_{gh})g\Big)h = 0 \Rightarrow$$

$$\Rightarrow \textstyle\sum_{g\in G}(\lambda_{gh}-\gamma_{gh})g = 0 \Rightarrow \lambda_{gh} = \gamma_{gh},\ \forall\, g\in G \text{ e } \forall\, h\in H \Rightarrow$$

$$\Rightarrow \lambda = \gamma.$$

Segue que φ é injetor.

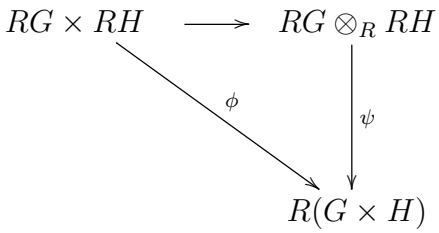
Por outro lado, temos que $GH\subseteq Im(\overline{\varphi})\subseteq Im(\varphi)$ e GH gera $(RG)H$ sobre

R. Daí, $(RG)H \subseteq Im(\varphi)$ e φ é sobrejetor.

Portanto, φ é um isomorfismo de anéis de grupo e $R(G \times H) \cong (RG)H$.

Agora vamos utilizar a *Propriedade Universal do Produto Tensorial* para mostrar que $R(G \times H) \cong RG \otimes_R RH$.

Consideremos o seguinte diagrama:



Seja $\phi : RG \times RH \to R(G \times H)$ definida por:

$$\phi\Big(\sum_{i=0}^{n} \alpha_i g_i, \sum_{j=0}^{m} \beta_j h_j\Big) = \sum_{i,j} \alpha_i \beta_j (g_i, h_j).$$

Afirmamos que ϕ é uma aplicação balanceada.

De fato, dados $\alpha \in R$, $\lambda, \mu \in RG$ e $\gamma, \eta \in RH$, onde $\lambda = \sum \alpha_i g_i$, $\mu = \sum \beta_i g_i$, $\gamma = \sum r_j h_j$ e $\eta = \sum s_j h_j$, temos que:

• $\phi(\lambda + \mu, \gamma) = \phi(\sum(\alpha_i + \beta_i)g_i, \sum r_j h_j) = \sum(\alpha_i + \beta_i)r_j(g_i, h_j) = \sum \alpha_i r_j(g_i, h_j) + \sum \beta_i r_j(g_i, h_j) = \phi(\lambda, \gamma) + \phi(\mu, \gamma)$;

• $\phi(\lambda, \gamma + \eta) = \phi(\sum \alpha_i g_i, \sum(r_j + s_j)h_j) = \sum \alpha_i(r_j + s_j)(g_i, h_j) = \sum \alpha_i r_j(g_i, h_j) + \sum \alpha_i s_j(g_i, h_j) = \phi(\lambda, \gamma) + \phi(\lambda, \eta)$;

• $\phi(\alpha \cdot \lambda, \gamma) = \phi(\sum \alpha\alpha_i g_i, \sum r_j h_j) = \sum \alpha\alpha_i r_j(g_i, h_j) = \alpha \sum \alpha_i r_j(g_i, h_j) = \alpha\phi(\lambda, \gamma)$;

• $\phi(\lambda, \alpha \cdot \gamma) = \phi(\sum \alpha_i g_i, \sum \alpha r_j h_j) = \sum \alpha_i \alpha r_j(g_i, h_j) = \alpha \sum \alpha_i r_j(g_i, h_j) = \alpha\phi(\lambda, \gamma)$.

Logo, ϕ é uma aplicação balanceada.

Pela *Propriedade Universal do Produto Tensorial*, segue que existe um único homomorfismo $\psi : RG \otimes_R RH \to R(G \times H)$ definido por

$$\psi\Big(\sum_{i=0}^{n} \alpha_i g_i \otimes \sum_{j=0}^{m} \beta_j h_j\Big) = \sum_{i,j} \alpha_i \beta_j (g_i, h_j)$$

que faz o diagrama acima comutar.

Afirmamos que ψ é bijetor.

De fato, seja $\tilde{\psi} : R(G \times H) \to RG \otimes_R RH$ definida por $\tilde{\psi}(\sum \alpha_{ij}(g_i, h_j)) = \sum \alpha_{ij} g_i \otimes h_j$. Temos que:

• $\psi(\tilde{\psi}(\sum \alpha_{ij}(g_i, h_j))) = \psi(\sum \alpha_{ij} g_i \otimes h_j) = \sum \alpha_{ij}(g_i, h_j)$;

• $\tilde{\psi}(\psi(\sum \alpha_i g_i \otimes \sum \beta_j h_j)) = \tilde{\psi}(\sum \alpha_i \beta_j (g_i, h_j)) = \sum \alpha_i \beta_j g_i \otimes h_j = \sum \alpha_i g_i \otimes \beta_j h_j$.

Daí, ψ e $\tilde{\psi}$ são aplicações inversas uma da outra e ψ é bijetor.

Portanto, ψ é um isomorfismo de anéis de grupo e $R(G \times H) \cong RG \otimes_R RH$. □

1.2 Semi-simplicidade e o Teorema de Maschke

Nesta seção apresentaremos condições sobre o anel R e o grupo G que nos permitam decompor o anel RG em uma soma direta de anéis simples. Nesta direção, nosso interesse principal é determinar condições necessárias e suficientes sobre R e G para que RG seja um anel semi-simples. Iniciaremos estudando algumas relações entre os subgrupos de G e ideais de RG. Estas relações são muito importantes no estudo de muitos problemas que envolvem a estrutura de RG.

Dados um grupo G e um anel R comutativo com identidade, denotaremos por $\mathcal{S}(G)$ o conjunto de todos os subgrupos de G e por $\mathcal{I}(RG)$ o conjunto de todos os ideais à esquerda de RG.

Definição 1.6. *Dado um subgrupo $H \in \mathcal{S}(G)$, denotaremos por $\Delta_R(G, H)$ o ideal à esquerda de RG gerado pelo conjunto $\{h - 1;\ h \in H\}$, isto é,*

$$\Delta_R(G, H) = \left\{ \sum_{h \in H} \alpha_h (h - 1);\ \alpha_h \in RG \right\}.$$

Para um anel R fixo, omitiremos o subscrito e denotaremos $\Delta_R(G, H)$ simplismente por $\Delta(G, H)$. Observamos que $\Delta(G, G) = \Delta(G)$.

Lema 1.1. *Seja H um subgrupo de G e seja S um conjunto de geradores de H. Então, o conjunto $\{s - 1;\ s \in S\}$ é um conjunto de geradores de $\Delta(G, H)$ como um ideal à esquerda de RG.*

Para uma melhor descrição de $\Delta(G, H)$, denotamos por $\mathcal{T} = \{q_i\}_{i \in I}$ um conjunto completo de representantes das classes laterais à esquerda de H em G, isto é, uma *transversal* de H em G, e vamos escolher, como representante da classe H em $\mathcal{T}$, o elemento identidade de G. Pela definição de transversal, todo elemento $g \in G$ pode ser escrito de maneira única na forma $g = q_i h_j$, onde $q_i \in \mathcal{T}$ e $h_j \in H$.

Proposição 1.3. *O conjunto $B_H = \{q(h - 1);\ q \in \mathcal{T},\ h \in H, h \neq 1\}$ é uma base de $\Delta_R(G, H)$ sobre R.*

Se H é um subgrupo normal de G, o homomorfismo canônico $\omega : G \to G/H$ pode ser estendido ao epimorfismo $\omega^* : RG \to R(G/H)$ tal que:

$$\omega^*\Big(\sum_{g\in G} \lambda_g g\Big) = \sum_{g\in G} \lambda_g\, \omega(g).$$

Neste caso, $\Delta(G,H)$ é o núcleo do epimorfismo ω^*:

Proposição 1.4. *Seja H um subgrupo normal de G. Então, com a notação acima, $Ker(\omega^*) = \Delta(G,H)$. Em particular, $\Delta(G)$ é o núcleo do epimorfismo ε induzido pela aplicação trivial*

$$G \to G/G = \{1\}.$$

Corolário 1.2. *Seja H um subgrupo normal de G. Então, $\Delta(G,H)$ é um ideal bilateral de RG e*

$$\frac{RG}{\Delta(G,H)} \cong R(G/H).$$

Assim, podemos definir uma aplicação de $\mathcal{S}(G)$ sobre $\mathcal{I}(RG)$ de modo que os subgrupos normais de G são levados em ideais bilaterais de RG. Por outro lado, dado um ideal à esquerda $I \in \mathcal{I}(RG)$, consideramos o conjunto

$$\nabla(I) = \{g \in G;\ g - 1 \in I\}$$

isto é,

$$\nabla(I) = G \cap (1 + I).$$

Afirmamos que $\nabla(I)$ é um subgrupo de G.

De fato, dados $g, h \in \nabla(I)$, temos que $gh - 1 = g(h-1) + g - 1 \in I$. Daí, $gh \in \nabla(I)$. Ainda, se $g \in \nabla(I)$, então $g^{-1} - 1 = -g^{-1}(g-1) \in I$. Logo, $g^{-1} \in \nabla(I)$. Portanto, $\nabla(I)$ é um subgrupo de G.

Se I é um ideal bilateral de RG, é fácil verificar que $\nabla(I)$ é um subgrupo normal de G.

A relação entre essas duas funções é dada da seguinte maneira:

Proposição 1.5. *Se $H \in \mathcal{S}(G)$, então $\nabla(\Delta(G,H)) = H$.*

Observação 1.3. *As aplicações Δ e ∇, ao contrário do que parece, não são inversas uma da outra.*

De fato, dado um ideal $I \in \mathcal{I}(RG)$, é fácil ver que $\Delta(G, \nabla(I)) \subset I$. Mas a igualdade pode não ser verdadeira: se $I = RG$, então $\nabla(RG) = \{g \in G;\ g - 1 \in RG\} = G$. No entanto, $\Delta(G, \nabla(RG)) = \Delta(G) \neq RG$.

Nosso próximo passo será apresentar condições sobre o anel R e o grupo G para que RG possa ser decomposto em uma soma direta de anéis simples.

Definição 1.7. *Sejam RG um anel de grupo e A um subconjunto finito de G. Então, $\widehat{A}$ denota o elemento de RG dado por:*

$$\widehat{A} = \sum_{a \in A} a.$$

Lema 1.2. *Se H é um subgrupo finito de G e $|H|$ é invertível em R, então $e_H = \frac{1}{|H|}\widehat{H}$ é um idempotente de RG. Além disso, se $H \triangleleft G$, então e_H é central.*

Definição 1.8. *Se G é finito e $|G|$ é invertível em R, então o idempotente $e_G = \frac{1}{|G|}\widehat{G}$ é denominado **idempotente principal** de RG.*

Proposição 1.6. *Seja H um subgrupo normal de G tal que $|H|$ é invertível em R. Então, tomando $e_H = \frac{1}{|H|}\widehat{H}$, temos a soma direta de anéis*

$$RG \cong RGe_H \oplus RG(1 - e_H),$$

onde $RGe_H \cong R(G/H)$ e $RG(1 - e_H) \cong \Delta(G, H)$.

Corolário 1.3. *Se G é finito e $|G|$ é invertível em R, então podemos decompor RG em uma soma direta de anéis*

$$RG \cong R \oplus \Delta(G).$$

Lema 1.3. *Se I é um ideal do anel de grupo RG, então o anel quociente RG/I é comutativo se, e somente se, $\Delta(G, G') \subset I$, onde G' denota o subgrupo derivado de G.*

Proposição 1.7. *Seja RG um anel de grupo semi-simples tal que $|G'|$ é invertível em R. Então,*

$$RG \cong RGe_{G'} \oplus \Delta(G, G'),$$

onde $RGe_{G'} \cong R(G/G')$ é a soma de todas as componentes simples comutativas de RG e $\Delta(G, G')$ é a soma de todas as outras.

Agora vamos determinar condições necessárias e suficientes sobre R e G para que RG seja um anel semi-simples. Para tal, precisaremos de alguns resultados sobre anuladores.

Definição 1.9. *Seja X um subconjunto do anel de grupo RG. O **anulador à esquerda** de X é o conjunto*

$$Ann_l(X) = \{\lambda \in RG;\ \lambda x = 0,\ \forall\, x \in X\}.$$

Analogamente, O ***anulador à direita*** *de X é o conjunto*

$$Ann_r(X) = \{\lambda \in RG;\ x\lambda = 0,\ \forall\, x \in X\}.$$

Lema 1.4. *Se H é um subgrupo de G, então $Ann_r(\Delta(G,H)) \neq 0$ se, e somente se, H é finito. Neste caso, temos*

$$Ann_r(\Delta(G,H)) = \widehat{H} \cdot RG.$$

Além disso, se $H \lhd G$, então o elemento $\widehat{H}$ é central em RG e

$$Ann_r(\Delta(G,H)) = Ann_l(\Delta(G,H)) = RG \cdot \widehat{H}.$$

Corolário 1.4. *Seja G um grupo finito. Então,*

(1) $Ann_r(\Delta(G)) = Ann_l(\Delta(G)) = R \cdot \widehat{G}$;

(2) $Ann_r(\Delta(G)) \cap \Delta(G) = \left\{a\widehat{G};\ a \in R,\ a\,|G| = 0\right\}$.

Lema 1.5. *Seja I um ideal de R e suponhamos que exista um ideal J de R tal que $R = I \oplus J$. Então, $J \subset Ann_r(I)$.*

Lema 1.6. *Se o ideal aumento $\Delta(G)$ é um somando direto de RG, como um RG-módulo, então G é finito e $|G|$ é invertível em R.*

Demonstração. Suponhamos que $\Delta(G)$ é um somando direto de RG, como RG-módulo. Então, pelo lema anterior, $Ann_r(\Delta(G)) \neq 0$. Daí, pelo *Lema 1.28* e pelo *Corolário 1.29*, G é finito e

$$Ann_r(\Delta(G)) = R \cdot \widehat{G}.$$

Escrevendo $RG = \Delta(G) \oplus J$, obtemos $1 = e_1 + e_2$, onde $e_1 \in \Delta(G)$ e $e_2 \in J$. Daí, $1 = \epsilon(e_1) + \epsilon(e_2) = \epsilon(e_2)$. Como $J \subset Ann_r(\Delta(G))$, pelo lema anterior, segue que $e_2 = \alpha\widehat{G}$, para algum $\alpha \in R$, $\alpha \neq 0$. Logo, $1 = \alpha\,\epsilon(\widehat{G}) = \alpha\,|G|$. Portanto, $|G|^{-1} = \alpha$ e $|G|$ é invertível em R. □

O resultado que segue determina condições necessárias e suficientes sobre R e G para que RG seja um anel semi-simples.

Teorema 1.5. *(**Teorema de Maschke**) O anel de grupo RG é semi-simples se, e somente se, as seguintes condições são verdadeiras:*

(*i*) *R é um anel semi-simples.*

(*ii*) *G é um grupo finito.*

(*iii*) *$|G|$ é invertível em R.*

Demonstração. Suponhamos, inicialmente, que RG é um anel semi-simples. Pelo *Corolário 1.17*, temos que $R \cong RG/\Delta(G)$. Como RG é semi-simples, segue que seu quociente também o é. Daí, a condição (i) é verdadeira. Ainda, como a semi-simplicidade de RG implica que $\Delta(G)$ é um somando direto de RG, o *Lema 1.31* mostra que as condições (ii) e (iii) também são verdadeiras.

Reciprocamente, suponhamos que as condições (i), (ii) e (iii) são verdadeiras.

Seja M um RG-submódulo de RG. Como R é semi-simples, temos que RG é semi-simples como R-módulo. Daí, existe um R-submódulo N de RG tal que

$$RG = M \oplus N.$$

Seja $\pi : RG \to M$ a projeção canônica associada a esta soma direta. Definimos $\pi^* : RG \to M$ como a média

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx), \text{ para todo } x \in RG.$$

Se provarmos que π^* é um RG-homomorfismo tal que $(\pi^*)^2 = \pi^*$ e $Im(\pi^*) = M$, então teremos que $Ker(\pi^*)$ é um RG-submódulo de RG tal que $RG = M \oplus Ker(\pi^*)$ e o teorema estará provado.

Como π^* é um R-homomorfismo, para mostrar que ele também é um RG-homomorfismo é suficiente mostrar que

$$\pi^*(ax) = a\pi^*(x), \text{ para todo } x \in G \text{ e para todo } a \in G.$$

Temos que

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x).$$

Quando g percorre todos os elementos de G, o produto ga também percorre todos os elementos de G. Daí,

$$\pi^*(ax) = a\,\frac{1}{|G|} \sum_{t \in G} t^{-1}\pi(tx) = a\pi^*(x).$$

Como π é uma projeção sobre M, sabemos que $\pi(m) = m$, para todo $m \in M$. Além disso, como M é um RG-módulo, temos que $gm \in M$, para todo $g \in G$. Logo,

$$\pi^*(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gm) = \frac{1}{|G|} \sum_{g \in G} g^{-1}gm = m.$$

Portanto, $M \subset Im(\pi^*)$. Por outro lado, dado um elemento $x \in RG$, temos que $\pi(gx) \in M$, para todo $g \in G$. Daí, $\pi^*(x) \in M$ e $Im(\pi^*) \subset M$. Consequentemente,

$$\pi^*(\pi^*(x)) = \pi^*(x), \text{ para todo } x \in RG, \text{ ou seja, } (\pi^*)^2 = \pi^*.$$

□

Um caso particularmente importante é aquele em que $R = K$ é um corpo. Neste caso, K é semi-simples e $|G|$ é invertível em K se, e somente se, $|G| \neq 0$ em K, isto é, se, e somente se, a característica de K não divide a ordem de G.

Corolário 1.6. *Sejam G um grupo finito e K um corpo. Então, KG é semi-simples se, e somente se, a característica de K não divide a ordem de G.*

Ainda neste caso, traduzimos fielmente o *Teorema de Wedderburn* e obtemos várias informações a respeito da estrutura do anel de grupo KG:

Teorema 1.7. *Sejam G um grupo finito e K um corpo tal que a característica de K não divide a ordem de G. Então:*

(*i*) *KG é uma soma direta de ideais bilaterais minimais $\{B_i\}_{1 \leq i \leq r}$, as componentes simples de KG.*

(*ii*) *Todo ideal bilateral de KG é uma soma direta de alguns membros da família $\{B_i\}_{1 \leq i \leq r}$.*

(*iii*) *Cada componente simples B_i é isomorfa a um anel de matrizes $M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia de K em seu centro, e o isomorfismo*

$$KG \cong \oplus_{i=1}^{r} M_{n_i}(D_i).$$

é um isomorfismo de K-álgebras.

(*iv*) *Em cada matriz $M_{n_i}(D_i)$, o conjunto*

$$I_i = \left\{ \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & & & \\ x_{n_i} & 0 & \cdots & 0 \end{pmatrix} ; \, x_1, x_2, \cdots, x_{n_i} \in D_i \right\}$$

é um ideal minimal à esquerda de KG.

Corolário 1.8. *Sejam G um grupo finito e K um corpo algebricamente fechado tal que a característica de K não divide a ordem de G. Então,*

$$KG \cong \oplus_{i=1}^{r} M_{n_i}(K),$$

e $|G| = n_1^2 + n_2^2 + \cdots + n_r^2$.

Utilizando a estrutura intrínseca do grupo G, é possível determinarmos o número de componentes simples de KG. É disso que trata o resultado a seguir.

Teorema 1.9. *Sejam G um grupo finito e K um corpo algebricamente fechado tal que a característica de K não divide a ordem de G. Então, o número de componentes simples de KG é igual ao número de classes de conjugação de G.*

Finalizaremos esta seção, apresentando uma caracterização dos anéis de grupos KG, no caso em que G é um grupo abeliano finito e K é um corpo tal que a característica de K não divide a ordem de G. Tal caracterização foi dada por *S. Perlis* e *G. Walker*.

Teorema 1.10. ***(Perlis-Walker)****Seja G um grupo abeliano finito de ordem n e seja K um corpo tal que a característica de K não divide a ordem de G. Então,*

$$KG \cong \oplus_{d|n} a_d\, K(\zeta_d),$$

onde ζ_d denota uma raiz primitiva da unidade de ordem d e $a_d = \dfrac{n_d}{[K(\zeta_d) : K]}$. Nesta fórmula, n_d denota o número de elementos de ordem d em G.

Corolário 1.11. *Seja G um grupo abeliano finito de ordem n e seja K um corpo tal que a característica de K não divide a ordem de G. Se K contém um raiz primitiva da unidade de ordem n, então*

$$KG \cong \underbrace{K \oplus \cdots \oplus K}_{n}.$$

Corolário 1.12. *Seja G um grupo abeliano finito de ordem n. Então,*

$$\mathbb{Q}G \cong \oplus_{d|n} a_d \mathbb{Q}(\zeta_d),$$

onde ζ_d denota uma raiz primitiva da unidade de ordem d e a_d é o número de subgrupos cíclicos de ordem d de G.

Corolário 1.13. *Seja $G = \langle a \rangle$ um grupo cíclico finito de ordem n. Então,*

$$\mathbb{Q}\langle a \rangle \cong \oplus_{d|n} \mathbb{Q}(\zeta_d),$$

onde ζ_d denota uma raiz primitiva da unidade de ordem d.

1.3 Unidades bicíclicas e unidades cíclicas de Bass

Nesta seção, definiremos dois tipos especiais de unidades: unidades bicíclicas e unidade cíclicas de *Bass*. Apresentaremos algumas propriedades de extrema importância em unidades bicíclicas que serão utilizadas em todo desenvolvimento do trabalho.

Seja $\mathbb{Z}G$ um anel de grupo inteiro e seja $g \in G$ um elemento de ordem finita n. Denotando $\widehat{g} = 1 + g + g^2 + \cdots + g^{n-1} \in \mathbb{Z}G$, temos que $(1-g)\widehat{g} = 0$. Daí, dado $h \in G$, podemos construir a unidade

$$\mu_{g,h} = 1 + (1-g)h\widehat{g},$$

cujo inverso é $1 - (1-g)h\widehat{g}$. Em particular, se g e h comutam, se e somente se $\mu_{g,h} = 1$.

Seja RG um anel de grupo, R é um anel. Denotaremos $\mathcal{U}(R)$ o grupo das unidades do anel R e $\mathcal{U}(RG)$ o grupo das unidades de RG.

Definição 1.10. *Se $\gamma \in \mathcal{U}(RG)$ é tal que $\gamma = ag, a \in \mathcal{U}(R)$ e $g \in G$, então dizemos que γ é uma unidade trivial.*

Em particular as unidades triviais de $\mathbb{Z}G$ são os elementos da forma $\pm g$.

Definição 1.11. *Seja G um grupo e sejam $g, h \in G$, com $o(g) = n < \infty$. A unidade $\mu_{g,h}$ construída acima é chamada* ***Unidade Bicíclica*** *de $\mathbb{Z}G$.*

Denotaremos por $\mathcal{B}_2$ o subgrupo de $\mathcal{U}(\mathbb{Z}G)$ gerado por todas as unidades bicíclicas de $\mathbb{Z}G$.

O resultado a seguir caracteriza as unidades bicíclicas triviais.

Proposição 1.8. *Seja G um grupo e sejam $g, h \in G$, com $o(g) = n < \infty$. Então, a unidade bicíclica $\mu_{g,h}$ é trivial se, e somente se, h normaliza $\langle g \rangle$. Neste caso, $\mu_{g,h} = 1$.*

Demonstração. Suponhamos que h normaliza $\langle g \rangle$. Então, $h^{-1}gh = g^j$, para algum inteiro positivo j. Daí, $gh = hg^j$ e, como $g^j\,\widehat{g} = \widehat{g}$, temos que $gh\widehat{g} = h\widehat{g}$. Logo, $\mu_{g,h} = 1$.

Reciprocamente, suponhamos que $\mu_{g,h}$ é trivial. Como $\varepsilon(\mu_{g,h}) = 1$, existe $x \in G$ tal que $\mu_{g,h} = x$, ou seja, $1 + (1-g)h\widehat{g} = x$. Daí,

$$1 + h(1 + g + g^2 + \cdots + g^{n-1}) = x + gh(1 + g + g^2 + \cdots + g^{n-1}).$$

Se $x = 1$, então $h = ghg^i$, para algum inteiro positivo i e, daí, $h^{-1}gh = g^{-i}$. Por outro lado, se $x \neq 1$, então $h \notin \langle g \rangle$. Como 1 aparece no lado esquerdo da

equação, ele também deve aparecer do lado direito da mesma e, assim, existe um inteiro positivo i tal que $1 = ghg^i$. Daí, $h = g^{-(i+1)} \in \langle g \rangle$, um absurdo. □

Corolário 1.14. *Seja G um grupo finito. Então, o grupo $\mathcal{B}_2$ é trivial se todo subgrupo de G é normal.*

O próximo resultado garante que toda unidade bicíclica não-trivial de $\mathbb{Z}G$ possui ordem infinita.

Proposição 1.9. *Toda unidade bicíclica $\mu_{g,h}$ de $\mathbb{Z}G$, $\mu_{g,h} \neq 1$, tem ordem infinita.*

Demonstração. Dada $\mu_{g,h} = 1 + (1-g)h\widehat{g} \in \mathbb{Z}G$, temos que

$$\mu_{g,h}^s = (1 + (1-g)h\widehat{g})^s = 1 + s(1-g)h\widehat{g}.$$

Daí, $\mu_{g,h}^s = 1$ se, e somente se, $(1-g)h\widehat{g} = 0$, ou seja, se, e somente se, $\mu_{g,h} = 1$. □

Utilizaremos, agora, a função ϕ de *Euler* para definir outro tipo de unidade de $\mathbb{Z}G$: dado um inteiro positivo n, escrevemos n como um produto de fatores primos, a saber, $n = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$. Daí,

$$\phi(n) = p_1^{n_1-1}(p_1-1)p_2^{n_2-1}(p_2-1)\cdots p_t^{n_t-1}(p_t-1).$$

Lembramos, ainda, que uma propriedade importante dessa função é dada pelo chamado *Teorema de Euler*: se i e n são inteiros relativamente primos, então

$$i^{\phi(n)} \equiv 1 \,(\mathrm{mod}\, n).$$

Definição 1.12. *Seja G um grupo e seja $g \in G$ um elemento de ordem finita n. Uma **Unidade Cíclica de Bass** é um elemento de $\mathbb{Z}G$ da forma:*

$$\mu_i = (1 + g + \cdots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\,\widehat{g},$$

onde i é um inteiro tal que $1 < i < n-1$ e $(i,n) = 1$.

O subgrupo de $\mathcal{U}(\mathbb{Z}G)$ gerado por todas as unidades cíclicas de Bass é denotado por $\mathcal{B}_1$.

Observação 1.4. *É possível verificar que μ_i é de fato uma unidade de $\mathbb{Z}G$ e que sua inversa é*

$$\mu_i^{-1} = (1 + g^i + \cdots + g^{i(k-1)})^{\phi(n)} + \frac{1 - k^{\phi(n)}}{n}\,\widehat{g},$$

onde k é qualquer inteiro tal que $ik \equiv 1\,(mod\, n)$. Ainda, $\varepsilon(\mu_i) = 1$, ou seja, μ_i é uma unidade normalizada.

O último resultado dessa seção afirma que as unidades cíclicas de *Bass* de $\mathbb{Z}G$ não são triviais.

Proposição 1.10. *Sejam G um grupo, $g \in G$ um elemento de ordem finita n e s um inteiro tal que $1 < s < n-1$ e $(s,n) = 1$. Então, a unidade cíclica de Bass*

$$\mu_s = (1 + g + \cdots + g^{s-1})^{\phi(n)} + \frac{1 - s^{\phi(n)}}{n}\,\widehat{g}$$

é de ordem infinita.

Demonstração. Sabemos que

$$\mathbb{Q}\langle g\rangle \cong \oplus_{d/n}\mathbb{Q}(\zeta_d)$$

onde ζ é numa raiz primitiva n-ésima da unidade e os expoentes d são divisores de n. Além disso, nesse isomorfismo, temos que

$$g \longmapsto (1, \ldots, \zeta^d, \ldots, \zeta^d).$$

Vamos mostrar que a projeção $\mu_s(\zeta)$ de μ_s na última componente, ou seja,

$$\mu_s(\zeta) = (1 + \zeta + \cdots + \zeta^{s-1})^{\phi(n)},$$

é de ordem infinita.

Suponhamos, por absurdo, que tal projeção é de ordem finita. Então, $1 + \zeta + \cdots + \zeta^{s-1}$ deverá ser de ordem finita. Como o conjunto $\{\pm\zeta^t;\, 0 \leq t \leq n-1\}$ contém todas as raízes da unidade de $\mathbb{Q}(\zeta)$, segue que

$$1 + \zeta + \cdots + \zeta^{s-1} = \pm\zeta^t,$$

para algum inteiro positivo t. Multiplicando ambos os lados dessa equação por $1-\zeta$, obtemos $1 - \zeta^s = \pm\zeta^t(1-\zeta)$. Daí, $|1-\zeta^s| = |1-\zeta|$. Escrevendo $\zeta = \cos\theta + i\,\mathrm{sen}\,\theta$, com $i = \sqrt{-1}$, segue que $\zeta^s = \cos(s\theta) + i\,\mathrm{sen}(s\theta)$. Ainda,

$$|1-\zeta|^2 = |1 - (\cos\theta + i\,\mathrm{sen}\,\theta)|^2 = 2(1-\cos\theta) \quad \text{e}$$

$$|1-\zeta^s|^2 = |1 - (\cos(s\theta) + i\,\mathrm{sen}(s\theta))|^2 = 2(1-\cos(s\theta)).$$

Logo, $\cos\theta = \cos(s\theta)$ e $s\theta = \theta$ ou $s\theta = 2\pi - \theta$. Portanto, $\zeta^s = \zeta$ ou $\zeta^s = \zeta^{s-1}$, o que é um absurdo. □

2

O Grupo de Unidades de $\mathbb{Z}D_4$

Neste capítulo, apresentaremos as ferramentas necessárias para estudarmos as unidades bicíclicas em $U(\mathbb{Z}G)$ na sua forma matricial em $M_4(\mathbb{Q})$, bem como a descrição completa do grupo G extra-especial de ordem 32 com G sendo o produto central de 2 cópias isomorfas a D_4, D_4 é o grupo diedral. Iniciaremos com a decomposição do anel de grupo $\mathbb{Q}D_4$ em componentes simples e terminaremos com a descrição completa do anel de grupo $\mathbb{Q}G$.

2.1 Representações de grupos e a decomposição de $\mathbb{Q}D_4$

A teoria dos módulos se transformou em uma ferramenta muito importante em Álgebra, devido especialmente aos trabalhos de *Emmy Noether*. Em particular, no artigo NOETHER [6] de 1929, ela observou que este conceito poderia ser usado para relacionar duas teorias que, até então, tinham se desenvolvido separadamente: as representações lineares de grupos e o estudo da estrutura de álgebras. Inaugurou, assim, um novo estágio do desenvolvimento destas teorias.

Nesta seção, utilizaremos a teoria das representações lineares de um grupo para descrever a decomposição do anel de grupo $\mathbb{Q}D_4$. Tal decomposição é de extrema importância para o estudo do grupo de unidades de $\mathbb{Z}D_4$.

Proposição 2.1. *Sejam G um grupo e R um anel comutativo com identidade. Então, existe uma correspondência bijetora entre as representações de G e os RG-módulos de posto finito sobre R.*

Demonstração. Seja V um módulo livre de posto finito sobre R e seja $GL(V)$ o grupo dos R-automorfismos de V. A cada representação $T : G \to GL(V)$ de G sobre R podemos associar um módulo dando a V a estrutura de RG-módulo. Para

tal, dados $\lambda = \sum_{g \in G} \lambda_g \, g \in RG$ e $x \in V$, definimos o produto λx do seguinte modo:

$$\lambda x = \Big(\sum_{g \in G} \lambda_g \, g \Big) x = \sum_{g \in G} \lambda_g \, T_g(x).$$

Reciprocamente, se M é um RG-módulo de posto finito sobre R, definimos a representação $T : G \to GL(M)$ associando a cada elemento $g \in G$ a função R-linear $T_g : M \to M$ definida por:

$$T_g(x) = gx, \text{ para todo } x \in M.$$

É fácil verificar que as correspondências assim definidas são inversas uma da outra. □

A proposição que segue, de simples demonstração, POLCINO [5] estabele relações entre propriedades de módulos e propriedades das representações correspondentes.

Proposição 2.2. *Sejam G um grupo e K um corpo. Então,*

(*i*) *Duas representações T e T' de G sobre K são equivalentes se, e somente se, os KG-módulos correspondentes são isomorfos.*

(*ii*) *Uma representação é irredutível se, e somente se, o KG-módulo correspondente é simples.*

(*iii*) *Seja M um KG-módulo que admite uma decomposição em soma direta de submódulos*

$$M = \oplus_{i=1}^{t} M_i$$

e sejam T, T_i as representações associadas aos módulos M e M_i, $1 \leq i \leq t$, respectivamente. Então,

$$T = \oplus_{i=1}^{t} T_i.$$

(*iv*) *Uma representação de G sobre K é completamente redutível se, e somente se, o KG-módulo correspondente é semi-simples.*

Segue deste último resultado que todas as representações de um grupo finito G sobre um corpo K serão completamente redutíveis se, e somente se, todos os KG-módulos forem semi-simples, o que acontece se, e somente se, KG é um anel semi-simples. Do *Teorema de Maschke*, este último acontece se, e somente se, a característica de K não divide a ordem de G.

Outras consequências interessantes podem ser obtidas. No caso semi-simples, sabemos que todo módulo é soma direta de submódulos simples; em termos de representações, isto significa que toda representação é soma direta de representações irredutíveis. Assim, para conhecer todas as representações de G sobre K é suficiente conhecer todas as representações irredutíveis. Como todas as representações irredutíveis estão em correspondência bijetora com os módulos simples e estes estão determinados, a menos de isomorfismos, pelos ideais minimais à esquerda de KG, segue que determinar representações irredutíveis não-equivalentes se traduz em determinar os ideais minimais à esquerda não isomorfos de KG. Em particular, lembramos que o número de classes de isomorfismo é igual ao número de componentes simples de KG.

Dada uma componente simples $M_{n_i}(D_i)$, onde D_i denota um anel de divisão contendo uma cópia de K, qualquer ideal minimal à esquerda contido nela será um representante da classe de módulos simples. Conforme o *Teorema 1.34*, tal ideal é dado por

$$I_i = \left\{ \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & & & \\ x_{n_i} & 0 & \cdots & 0 \end{pmatrix} ;\, x_1, x_2, \cdots, x_{n_i} \in D_i \right\}$$

Se T_i é a representação de G associada, temos que o grau de T_i é igual a dimensão de I_i como espaço vetorial sobre K, isto é:

$$grau\,(T_i) = n_i \; dim_K(D_i). \qquad (*)$$

Agora, temos condições de apresentar a decomposição do anel de grupo $\mathbb{Q}D_4$, onde

$$D_4 = \langle b, v |\, b^2 = 1,\, v^4 = 1 \text{ e } bvbv = 1 \rangle.$$

Consideremos a representação T de D_4 sobre $\mathbb{Q}$ dada por:

$$T_b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad T_v = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

É fácil verificar que esta representação é irredutível. Ainda, podemos determinar quatro representações não-equivalentes de grau 1 de D_4 sobre $\mathbb{Q}$:

$$\begin{gathered} R_b = 1 \quad \text{e} \quad R_v = 1, \\ R'_b = -1 \quad \text{e} \quad R'_v = 1, \\ S_b = 1 \quad \text{e} \quad S_v = -1, \\ S'_b = -1 \quad \text{e} \quad S'_v = -1. \end{gathered}$$

A representação T corresponderá a um somando direto da forma $M_n(D)$ e, de $(*)$,

$$grau\,(T) = n\ dim_{\mathbb{Q}}(D).$$

Logo, $n = 1$ e $dim_{\mathbb{Q}}(D) = 2$ ou $n = 2$ e $dim_{\mathbb{Q}}(D) = 1$. Como $dim_{\mathbb{Q}}(\mathbb{Q}D_4) = 8$ e haverá quatro somandos iguais a $\mathbb{Q}$ correspondentes às representações de grau 1, se $n = 1$ e $dim_{\mathbb{Q}}(D) = 2$, então a decomposição do anel de grupo é:

$$\mathbb{Q}D_4 \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus D \oplus D',$$

onde D' é também um anel com divisão tal que $dim_{\mathbb{Q}}(D') = 2$. Daí, como toda extensão de grau 2 sobre $\mathbb{Q}$ é comutativa, o anel de grupo $\mathbb{Q}D_4$ também o é, o que é um absurdo. Portanto, $n = 2$ e $dim_{\mathbb{Q}}(D) = 1$, ou seja,

$$\mathbb{Q}D_4 \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}).$$

2.2 Alguns resultados sobre finitude de alguns índices

Seja O_i o anel dos inteiros de um corpo K_i.Considerando $S_i = M_n(K_i)_{n_i \times n_i}$, vamos denotar por Gl_i ou $GL_i(n_i, O_i)$ o grupo das matrizes inversíveis em $M_n(O_i)$ e por SL_i ou $SL_i(n, O_i)$ o subgrupo de matrizes de determinante 1.

Seja O um ideal de O_i. Definimos o subgrupo $E(O)$ de SL_i gerado por todas as matrizes elementares $I_d + qe_{im}, q \in O$ e $i \neq m$ de tal forma que $e_{il}e_{jk} = e_{ik}$ se $l = j$ e $e_{il}e_{jk} = 0$ se $l \neq K$. Denotamos também $\tilde{E}(O)$ seu fecho normal em SL_i.

Com essa notação de BACK [7],H.BASS [2] e J.P.SERRE [8] vale o seguinte teorema:

Teorema 2.1. *Seja K_i um corpo qualquer para $n_i \geq 3$ e considere $K_i \neq \mathbb{Q}$ da mesma forma que K_i não é um corpo quadrático imaginário para $n_i = 2$. Então:*
(1)$[SL_i : \tilde{E}(Q)]$ é finita para todo ideal O de O_i.
(2)Todo subgrupo não central de SL_i normalizado por um subgrupo de índice finito contém $\tilde{E}(O)$ para algum ideal não nulo O de O_i.

Devido a L.N.VASERSTEIN [9] temos também o seguinte teorema:

Teorema 2.2. *(1) Se $n_i \geq 3$, então $\tilde{E}(O^2) \subset E(O)$ e em particular $[SL_i : E(O)] < +\infty$*
(2)Se $n_i = 2$ e K_i não é racional ou quadrático imaginário, então
$[SL_i : E(O)] < +\infty$

Observação 2.1. *Tomando $K = \mathbb{Q}$ segue que $O_i = \mathbb{Z}$. Então para todo ideal O de $\mathbb{Z}$ segue que $[Sl_i : E(O)] < +\infty$. Note também que como todo ideal de $\mathbb{Z}$ é principal então existe um $d \in \mathbb{Z}$ onde $O = d\mathbb{Z}$ e conseqüentemente $E(O) = E_d = \langle I_d + e_{ij}, i \neq j\ e\ 1 \leq i, j \leq n \rangle$.*

Observação 2.2. *Considerando o homomorfismo canônico* $\mathbb{Z} \longrightarrow \mathbb{Z}_m$, *segue que o mesmo induz um homomorfismo em* $Sl_n(\mathbb{Z}) \longrightarrow Sl_n(\mathbb{Z}_m)$ *que terá como núcleo* $\Gamma_n(m)$ *(o m-th subgrupo de congruência principal).*

Segue que para $m = n = 2$ *temos que:*

$$\Gamma_2(2) = \frac{\begin{bmatrix} 2\mathbb{Z}+1 & 2\mathbb{Z} \\ 2\mathbb{Z} & 2\mathbb{Z}+1 \end{bmatrix}}{\{I_d, -I_d\}} = E_2$$

Ver I.MERZLJAKOV [10] e NEWMAN [4]

2.3 Subgrupos relevantes em $\mathbb{Z}G$

Definição 2.1. *Um p-grupo* G *é extra-especial se é não abeliano em que* $G' = Z(G)$ *e* $|Z(G)| = p$.

Vamos apresentar a definição de alguns subgrupos importantes de $U(\mathbb{Z}G)$, para o nosso trabalho onde G é um 2 grupo extra-especial. (detalhes veja JESPERS [3].)

Definição 2.2. U_2 *é o subgrupo de* $\mathcal{U}(\mathbb{Z}G)$ *definido por:*

$$U_2 = \mathcal{U}(\mathbb{Z}G) \cap \left(\mathbb{Q}G\Big(\frac{1-s}{2}\Big) + \Big(\frac{1+s}{2}\Big)\right).$$

A proposição abaixo que se encontra em JESPERS [3] nos fornece propriedades importantes do subgrupo U_2 de $\mathcal{U}(\mathbb{Z}G)$.

Proposição 2.3. *Com as notações acima, temos que:*

(*i*) $U_2 = \{u = 1 + \alpha(1-s) |\, u \in \mathcal{U}(\mathbb{Z}G),\ \alpha \in \mathbb{Z}G\}$;

(*ii*) $V = \{u = 1 + \alpha\,(1-s) |\, u \in \mathcal{U}(\mathbb{Z}G),\ \alpha \in \mathbb{Z}G$ *e* $\varepsilon(\alpha)$ *é par*$\}$ *é um subgrupo livre de torsão de* U_2 *e* $V \cong U_2/G'$.

Observação 2.3. *Se* G *é um 2-grupo é fácil ver que* $\mathcal{B}_2 \subset V$, *pois tomando* $\mu_{a,b} = 1 + (a-1)b\hat{a}$ *então se* $ab = sba$ *segue que* $\mu_{a,b} = 1 + (a-1)b\hat{a} = 1 + (sba - b)\hat{a} = 1 - b\hat{a}(1-s)$. *Então é fácil ver que* $b\hat{a}$ *possui função aumento par. Da mesma forma que se* $ab = ba$ *então* $\mu_{a,b} = 1$ *e é trivial.*

Para identificar V na sua forma matricial, JESPERS [3] estabeleceu o seguinte monomorfismo $\varphi : U_2 \longrightarrow \varphi(U_2) \subset M_2(\mathbb{Q})$ onde se $u = 1 + \alpha(1-s) \in U_2$ então $\varphi(u) = I_d + 2F(\alpha E)$ onde F é um isomorfismo de $\mathbb{Q}(D_4E)$ em $M_2(\mathbb{Q}), E = \left(\frac{1-s}{2}\right)$ cuja existência provém da seguinte proposição:

Proposição 2.4. *Com a mesma notação da proposição* 2.5 *o anel de grupo* $\mathbb{Q}D_4$ *admite a seguinte decomposição:*

$$\mathbb{Q}D_4 = \mathbb{Q}D_4\Big(\frac{1+s}{2}\Big) \oplus \mathbb{Q}D_4\Big(\frac{1-s}{2}\Big),$$

onde $\mathbb{Q}G\Big(\frac{1+s}{2}\Big) \cong \oplus^4 \mathbb{Q}$ *e* $\mathbb{Q}D_4\Big(\frac{1-s}{2}\Big) \cong M_2(\mathbb{Q})$ *onde denotaremos esse último isomorfismo por* F.

Como $F(sE) = F(-E) = -I_d$ e $s = 1+s(1-s) \in U_2$, então $\varphi(s) = I_d - 2I_d = -I_d$ e conseqüentemente:

$$V \cong \frac{U_2}{D_4'} \cong \frac{\varphi(U_2)}{\{I_d, -I_d\}}$$

Para finalizarmos esta seção, provaremos um resultado que será necessário para o decorrer do texto.

Proposição 2.5. *Seja* G *um* 2*-grupo finito extra-especial, com* $G' = \mathcal{Z}(G) = \{1, s\}$. *Então,* $\mathbb{Q}G(E)$ *é simples, onde* $E = \Big(\frac{1-s}{2}\Big)$.

Demonstração. Seja G um 2-grupo finito extra-especial, com $G' = \mathcal{Z}(G) = \{1, s\}$. Queremos mostrar que $\mathbb{Q}G(E)$ é simples, onde $E = \Big(\frac{1-s}{2}\Big)$. Para tal, seja e um idempotente central de $\mathbb{Q}G(E)$. Então,

$$e = \sum_{g \in \mathcal{Z}(G)} \alpha_g g + \sum_{g \notin \mathcal{Z}(G)} \alpha_g C_g, \qquad (*)$$

onde $C_g = \sum_{x \in \mathcal{C}_g} x$.

Como $G' = \{1, s\}$, se $g \in G$ não é central, então $\mathcal{C}_g = \{g, gs\}$. Daí, de $(*)$, obtemos

$$e = \sum_{g \in \mathcal{Z}(G)} \alpha_g g + \sum_{g \notin \mathcal{Z}(G)} \alpha_g (g + gs) = \sum_{g \in \mathcal{Z}(G)} \alpha_g g + (1+s) \sum_{g \notin \mathcal{Z}(G)} \alpha_g g.$$

Como e é um idempotente de $\mathbb{Q}G(E)$, temos que $eE = e$. Ainda, $(1+s)E = 0$. Logo,

$$e = \Big(\sum_{g \in \mathcal{Z}(G)} \alpha_g g \Big) E$$

e $e \in \mathbb{Q}(\mathcal{Z}(G))$. Como $\mathcal{Z}(G) = \{1, s\}$, as únicas possibilidades são

$$0, 1, \frac{1+s}{2} \quad \text{e} \quad \frac{1-s}{2}.$$

Portanto, $e = E$ e $\mathbb{Q}G(E)$ é simples, como queríamos provar. □

Seja D_4 o grupo diedral de ordem 8, isto é,

$$D_4 = \langle x, v |\, x^2 = 1,\ v^4 = 1 \text{ e } xvxv = 1 \rangle.$$

Vamos adotar a seguinte notação para os elementos de D_4:

$1 = x^2 = v^4$	$b = xv^2$	b	$s = v^2$
$y = bv$	$u = vb$	v	$w = v^3$

Sejam D e D^* grupos isomorfos a D_4. Denotaremos por $D \times D^*$ os elementos da forma xy^*, onde $x \in D$ e $y^* \in D^*$ é tal que seu correspondente em D é y. Assim, definimos o grupo

$$G \cong \frac{D \times D^*}{I},$$

onde $I_1 = \{1, ss^*\}$.

Os elementos de G serão denotados do seguinte modo:

1	x	b	s
y	u	v	w
x^*	b^*	y^*	u^*
v^*	w^*	bx^*	bb^*
by^*	bu^*	bv^*	bw^*
ux^*	ub^*	uy^*	uu^*
uv^*	uw^*	vx^*	vb^*
vy^*	vu^*	vv^*	vw^*

Então, G é um 2-grupo extra-especial de ordem 32, produto central de duas cópias de D_4, e $G' = \mathcal{Z}(G) = \{1, s\}$. Ainda, os elementos de G/G' serão denotados do seguinte modo:

$$G/G' = \begin{array}{|c|c|c|c|} \hline \overline{1} & \overline{b} & \overline{u} & \overline{v} \\ \hline \overline{b^*} & \overline{u^*} & \overline{v^*} & \overline{bb^*} \\ \hline \overline{bu^*} & \overline{bv^*} & \overline{ub^*} & \overline{uu^*} \\ \hline \overline{uv^*} & \overline{vb^*} & \overline{vu^*} & \overline{vv^*} \\ \hline \end{array}$$

Na sequência, apresentamos a decomposição do anel de grupo $\mathbb{Q}G$.

Proposição 2.6. *O anel de grupo $\mathbb{Q}G$ admite a seguinte decomposição:*

$$\mathbb{Q}G = \mathbb{Q}G\Big(\frac{1+s}{2}\Big) \oplus \mathbb{Q}G\Big(\frac{1-s}{2}\Big),$$

onde $\mathbb{Q}G\Big(\frac{1+s}{2}\Big) \cong \oplus^{16}\mathbb{Q}$ *e* $\mathbb{Q}G\Big(\frac{1-s}{2}\Big) \cong M_4(\mathbb{Q})$.

Demonstração. A decomposição segue da *Proposição 1.8*,juntamente com o isomorfismo $\mathbb{Q}G\Big(\frac{1+s}{2}\Big) \cong \mathbb{Q}(G/G')$ onde $e_{G'} = \frac{1+s}{2}$ e $\mathbb{Q}(G/G')$ é a soma de todas as componentes simples comutativas de $\mathbb{Q}G$ e $\mathbb{Q}G\Big(\frac{1-s}{2}\Big)$ é a soma de todas as outras. Daí, a decomposição de $\mathbb{Q}D_4$, apresentada no capítulo anterior onde $(\mathbb{Q}D_4)E \cong M_2(\mathbb{Q})$, unida à proposição que nos fornece que $R(G\times H) \cong RG\otimes_R RH$, onde G e H são grupos e R um anel comutativo com unidade segue o resultado desejado em concordância com a proposição 2.5. □

Através do isomorfismo $\mathbb{Q}GE \cong M_4(\mathbb{Q})$ sendo representado por F podemos construir o seguinte monomorfismo $\varphi : U_2 \to M_4(\mathbb{Q})$,onde:

$$\varphi(u_2) = I_d + 2F(\alpha E),\ u_2 = 1 + \alpha(1-s)$$

Sendo $\varphi(s) = I_d + 2F(sE) = -I_d$ e $\varphi(1) = I_d$ e sabendo que $V \cong \frac{U_2}{\{1,s\}}$ então $V \cong \frac{\varphi(U_2)}{\{I_d, -I_d\}}$.

Note que: $\varphi(U_2) \subset \begin{bmatrix} 2\mathbb{Z}+1 & 2\mathbb{Z} & 2\mathbb{Z} & 2\mathbb{Z} \\ 2\mathbb{Z} & 2\mathbb{Z}+1 & 2\mathbb{Z} & 2\mathbb{Z} \\ 2\mathbb{Z} & 2\mathbb{Z}+1 & 2\mathbb{Z} & 2\mathbb{Z} \\ 2\mathbb{Z} & 2\mathbb{Z} & 2\mathbb{Z}+1 & 2\mathbb{Z} \end{bmatrix}$

3

Estudo sobre unidades bicíclicas

Seja G um 2 grupo extra-especial. Como foi citado no capítulo anterior, segue que se $\mu_{a,b} = 1+(a-1)b\hat{a}$ é uma unidade bicíclica, então $\mu_{a,b} = 1-b\hat{a}(1-s)$ o que garante que $\mu_{a,b} \in V$ e por consequência $\mathcal{B}_2 \subset V$. Da mesma forma que $\Gamma_2(2) = E_2$ cuja igualdade é encontrada na observação da página 23. Logo ao tomar V como subgrupo de $\mathcal{U}(\mathbb{Z}D_4)$ temos que $\mathcal{B}_2 \subset V$ e $V \subset \Gamma_2(2) = E_2$ a menos de um isomorfismo.

Considerando $D_4 = \langle x, v \; x^2 = v^4 = 1, \; /x^{-1}vx = v^{-1}\rangle$, trabalharemos com G sendo o produto central de 2 cópias isomorfas de D_4, o que implica que $G = \frac{D_4 \times D_4^*}{I}$, $I_1 = \{1, (s, s^*)\}$. Note que nesse caso $Z(G) = G' = \{1, s\}$ pois $Z(D_4) = D_4' = \{1, s\}$. Iremos então mostrar que a inclusão será preservada no sentido de que $\varphi(\mathcal{B}_2) \subset E_2$ como subgrupo de $PSL_4(\mathbb{Q})$ e também $E_8 \subset \varphi(\mathcal{B}_2)$ sendo φ um monomorfismo de U_2 em $M_4(\mathbb{Q})$ visto na seção 2.3. Observe que nesse caso $E_2 \subsetneq \Gamma_4(2)$.

Para tal objetivo iniciaremos com alguns lemas importantes:

Lema 3.1. *Seja μ_{z_1,z_2} uma unidade bicíclica em $\mathcal{U}(\mathbb{Z}G)$. Se z_1 é qualquer elemento de G e $\circ(z_1) = 4$ então $\mu_{z_1,z_2} = 1$.*

Demonstração. Seja $\mu_{z_1,z_2} = (z_1 - 1)z_2\hat{z_1}$ uma unidade bicíclica. Se $\circ(z_1) = 4$ é fácil ver que $\langle z_1\rangle = \{1, z_1, s, sz_1\}$ pois $z_1^2 = s$. Como G'=$Z(G)$=$\{1, s\}$ segue que:

$$z_2^{-1}z_1z_2z_1^{-1} = 1 \text{ ou } z_2^{-1}z_1z_2z_1^{-1} = s.$$

Portanto $z_2^{-1}z_1z_2 = z_1$ ou $z_2^{-1}z_1z_2 = sz_1$. Em qualquer dos casos temos que $z_2^{-1}z_1z_2 \in \langle z_1\rangle$ ocorrendo $\mu_{z_1,z_2} = 1$. □

Lema 3.2. *Seja μ_{z_1,z_2} uma unidade bicíclica não trivial em G. Então:*

$$\mu_{z_1,z_2} = 1 + (z_1z_2 - z_2)(1 - s), \textit{ onde } G' = \{1, s\}$$

Demonstração. Sendo $\mu_{z_1,z_2} \neq 1$ então pelo lema 3.1, $\circ(z_1) = 2$ e $z_2z_1z_2^{-1} \notin \langle z_1\rangle$.

Particularmente $z_2 z_1 z_2^{-1} \neq z_1$ segue então que :

$$z_2 z_1 z_2^{-1} z_1^{-1} = s \Rightarrow z_2 z_1 = s z_1 z_2.$$

Logo:

$$\begin{aligned}
\mu_{z_1,z_2} &= 1 + (z_1 - 1)z_2(1 + z_1) = 1 + (z_1 z_2 - z_2)(1 + z_1) \\
&= 1 + (z_1 z_2 + (z_1 z_2)z_1 - z_2 - (z_2 z_1)) \\
&= 1 + (z_1 z_2 + z_1(s z_1 z_2) - z_2 - s(z_1 z_2)) \\
&= 1 + ((1 - s)z_1 z_2 - z_2(1 - s)) \\
&= 1 + (z_1 z_2 - z_2)(1 - s).
\end{aligned}$$

□

Observação 3.1. *Para* $E = \dfrac{1-s}{2}$ *e sabendo pela proposição* 2.4 *que* $\mathbb{Q}(D_4 E) \cong M_2(\mathbb{Q}), D_4$ *é o grupo diedral definido por* $D_4 = \langle x, v / x^2 = v^4 = 1 \, e \, x^{-1} v x = v^{-1} \rangle$. *Considere um isomorfismo* F_1 *obtido através de uma representação irredutível de* D_4 *que chamaremos de*T *e conseqüentemente* $F_1 : \mathbb{Q}D_4 E \to M_2(\mathbb{Q})$ *será determinado por:*

$$xE \to \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = T(x)$$

$$vE \to \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = T(v)$$

Pela proposição 2.6 temos que $\mathbb{Q}GE \cong M_4(\mathbb{Q})$, onde $E = \dfrac{1-s}{2}$. Vamos trabalhar com o seguinte isomorfismo $F : \mathbb{Q}GE \to M_4(\mathbb{Q})$ onde $\otimes$ é o produto de kroneker de matrizes definido pela seguinte representação:

$$\begin{aligned}
(x, 1^*)E &\to T(x) \otimes I_d \\
(v, 1^*)E &\to T(v) \otimes I_d \\
(1, x^*)E &\to I_d \otimes T(x) \\
(1, v^*)E &\to I_d \otimes T(v)
\end{aligned}$$

Segue diretamente da representação acima que para qualquer $w = (x, y^*)E \in GE$ onde x e y^* são elementos em D_4 e D_4^* respectivamente. Então $w = xE \otimes y^* E$ ao identificarmos xE com $T(x)$ e $y^* E$ com $T(y)$. Além disso, dadas duas matrizes elementares e_{ij} e e_{lk} em $M_2(\mathbb{Q})$,podemos obter em $M_4(\mathbb{Q})$ a matriz elementar:

$$e'_{i_1 j_1} = e_{ij} \otimes e_{lk}, \; i_1 = (2(-1 + i) + l) \, e \, j_1 = (2(-1 + j) + k)$$

Então se $wE \in GE \Rightarrow wE = xE \otimes y^* E = (a_1 e_{1l_1} + a_2 e_{2l_2}) \otimes (b_1 e_{1k_1} + b_2 e_{2k_2}), |a_1 a_2| = |b_1 b_2| = 1$ onde as 4 constantes são inteiras e $l_1 = 1$ e $l_2 =$

2 ou $l_1 = 2$ e $l_2 = 1$. Raciocínio análogo vale para k_1 e k_2. Para efeitos de simplificação considere $wE = (xE).(y^*E)$. Com isto vemos que wE em $M_4(\mathbb{Q})$ é combinação linear de quatro matrizes elementares utilizando a distributividade do produto tensorial. Sendo $w^2 = 1$ ou $w^2 = s$, segue que $(wE)^2 = E = I_d$ ou $(wE)^2 = -E = -I_d$ visto que $sE = -E$. Portanto temos duas configurações possíveis para wE:
$wE = a_1e'_{ij} + a_2e'_{ji} + a_3e'_{lk} + a_4e'_{kl}$ ou $wE = a_1e'_{11} + a_2e'_{22} + a_3e'_{33} + a_4e'_{44}$

Tomando e_{ij} e e_{lk} matrizes elementares em $M_2(\mathbb{Q})$, podemos formar a matriz elementar $e'_{i_1j_1}$ em $M_4(\mathbb{Q})$ da seguinte maneira:

$$e'_{i_1j_1} = e_{ij} \otimes e_{lk}$$

onde $i_1 = (2(-1+i)+l)$ e $j_1 = ((-1+j)+k)$. Sabendo que $1 \leq l, k \leq 2$ então o índice de $e'_{i_1j_1}$ representa uma posição na diagonal, ou seja:

$$i_1 = j_1 \Leftrightarrow i = j \text{ e } l = k$$

o que nos garante que apenas essas 2 configurações são possíveis para wE, pois sendo $wE = xE \otimes y^*E$ como estamos utilizando a representação irredutível T em D_4 onde todo elemento $T(x)$ está na diagonal principal ou na diagonal secundária $\forall x \in D_4$, então se xE e yE estiverem ambos na diagonal principal em $M_2(\mathbb{Q})$ segue que todos os termos de wE estarão na diagonal principal em $M_4(\mathbb{Q})$. Caso contrário se pelo menos xE ou yE estiveram na diagonal secundária, então todos os termos de wE estarão fora da diagonal principal.

Observação 3.2. *Do isomorfismo F, os elementos de $A = \{gE/g \in G\}$ se agrupam em blocos onde os elementos de cada bloco se caracterizam da forma:*
se g_1E e g_2E estão no mesmo bloco e $g_1E = \sum_{i=1}^{4} a_ie_{ij_i}$ então $g_2E = \sum_{i=1}^{4} b_ie_{ij_i}$, $\forall\, i$ onde $1 \leq i \leq 4$.

Teorema 3.1. *Através do isomorfismo F, existem exatamente 4 blocos disjuntos D_i, $1 \leq i \leq 4$ onde se divide o conjunto A,sendo que em cada bloco D_i fora da diagonal, existe exatamente 4 elementos de ordem 2 e 4 elementos de ordem 4.*

Demonstração. É fácil ver que se $wE \in GE \Rightarrow wE = (xE).(y^*E), xE$ e $y^*E \in M_2(\mathbb{Q})$. Então existem duas possibilidades de posições para xE e duas possibilidades para yE (diagonal principal e diagonal secundária), existindo portanto 4 possibilidades de posições diferentes e disjuntas para wE em $M_4(\mathbb{Q})$. A saber, as possibilidades de posições dadas pelos respectivos conjuntos: $A_1 = \{(1,1),(2,2),(3,3),(4,4)\}, A_2 = \{(1,2),(2,1),(3,4),(4,3)\}, A_3 =$

$\{(1,3),(3,1),(2,4),(4,2)\}, A_4 = \{(1,4),(4,1),(2,3),(3,2)\}$.

Note agora que se $\circ(wE) = 2, wE = xE.yE$ e $xE = e_{11} - e_{22}$ e $yE = e_{12} + e_{21}$ então as outras possibilidades para wE tal que xE e yE estão nessas mesmas posições (diagonal principal e diagonal secundária) são:

$wE = xE.(syE)$ pois $syE = -yE; wE = E.(yE)$ e $wE = E.(syE)$ sendo $E = e_{11} + e_{22}$

tendo portanto 4 possibilidades para wE de ordem 2.

Considerando agora $\circ(wE) = 4$ onde xE e yE estão nas mesmas posições que no caso anterior devemos ter nessas condições $\circ(yE) = 4$ ou seja $yE = e_{12} - e_{21}$ ou $yE = -e_{12} + e_{21}$. Fixando uma das possibilidades para yE temos então outras 4 possibilidades para wE de ordem 4 a seguir:

$$wE = xE.yE, wE = xE.(syE), wE = E.(yE) \text{ ou } wE = E.(syE).$$

Apenas note que para $wE = xE.yE$, xE e yE estão na diagonal temos 7 possibilidades para wE onde o mesmo apenas terá ordem 2 tal que:

$$wE = xE.yE,\ wE = xE.(syE),\ wE = xE.(E),\ wE = (sxE).E,$$

$$wE = E.(yE),\ wE = E.(syE) \text{ e } wE = E.(sE)$$

Raciocínio análogo vale para xE e yE ambos fora da diagonal. Apenas note que nesse caso se $\circ(wE) = 2$ então $\circ(xE) = \circ(yE) = 2$ ou $\circ(xE) = \circ(yE) = 4$. □

Pela formação também do monomorfismo $\varphi : U_2 \to \varphi(U_2)$,como na seção 2.3 considerando a unidade bicíclica $\mu_{z_1,z_2} \neq 1$ onde z_1 e $z_2 \in G$, pelo resultado 1.1, $\circ(z_1) = 2$ e além disso:

$$\begin{aligned}\mu_{z_1,z_2} &= 1 + (z_1 - 1)z_2(z_1 + 1)\\ &= 1 + (z_1z_2 - z_2)(1 - s)\end{aligned}$$

Definindo então $a = (z_1 - 1)z_2(z_1 + 1)$, sabemos que $a^2 = 0$ e consequentemente $\varphi(\mu_{z_1,z_2}) = I_d + 2F(a/2)$, $(2F(a/2))^2 = 4(F(a/2))^2 = 0$ pois F é um isomorfismo e $(a/2)^2 = 0$.

Proposição 3.1. *Através do isomorfismo F se $g \in G$ e sendo $gE = \sum_{i=1}^{4} a_i e_{ij_i}, a_i = \pm 1\ \forall\ 1 \leq i \leq 2^2$, segue que todos os $a_i's$ ou possuem o mesmo sinal ou metade deles é positiva e a outra metade é negativa.*

Demonstração. Veja que para $n = 1$ se $u \in D_4$ então $uE = \sum_{i=1}^{2} a_i e_{ij_i}$ e $a_i > 0$ ou $a_i < 0 \; \forall 1 \leq i \leq 2$ ou $a_1 a_2 < 0$ pela representação T em D_4 . Se $wE \in GE$ então $wE = xE \otimes yE$, xE e yE estão em D_4E. Então supondo válido para $n = 1$ vale o resultado também para wE. □

Observação 3.3. *Como conseqüência temos que sendo* $gE = \sum_{i=1}^{4} a_i e_{ij_i}$,*e* $a_i = \pm 1$,*então* $\sum_{i=1}^{4} a_i = 2^2, -2^2$ *ou* 0, *o que implica que* $4/\sum_{i=1}^{4} a_i$.

Considerando então a unidade bicíclica $\varphi(\mu_{z_1,z_2}) = I_d + \alpha, \alpha^2 = 0$ *e* α *possui imagem em apenas um mesmo blocoD*$_j$ *então utilizando também a observação acima, temos que* $\varphi(\mu_{z_1,z_2}) = I_d + 2a_1 e_{ij} + 2b_1 e_{lk}, \; (l,k) \neq (j,i)$

Lema 3.3. *Não existe unidade bicíclica não trivial com imagem não nula apenas no bloco* $\mathcal{D}_1$ *que aparece na diagonal.*

Demonstração. Suponha por contradição que exista uma unidade bicíclica μ_{z_1,z_2} onde z_1 e $z_2 \in G$ tal que possui imagem não nula apenas em $\mathcal{D}_1$. Então:

$$\varphi(\mu_{z_1,z_2}) = I_d + 2F(a/2), \; 2F(a/2) = a_1 e_{11} + a_2 e_{22} + a_3 e_{33} + a_4 e_{44}$$

Como $\mu_{z_1,z_2} \neq 1$, segue que $\varphi(\mu_{z_1,z_2}) \neq \varphi(1) = I_d$ e então existe $a_i \neq 0$, $1 \leq i \leq 4$.Portanto $(2F(a/2))^2 \neq 0$ o que contradiz a observação anterior. □

Lema 3.4. *Se* μ_{z_1,z_2} *é uma unidade bicíclica, então* $\varphi(\mu_{z_1,z_2}) = [a_{ij}]_{4\times 4}$, *onde* $\forall$ *i onde* $1 \leq i, j \leq 4$ *segue que* $a_{ij} \in \mathbb{Z}$ *e* $-4 \leq a_{ij} \leq 4$.

Demonstração. Se $\mu_{z_1,z_2} = 1$ então é trivial. Caso contrario pelo resultado 1.1 e observação anterior segue que:

$$\mu_{z_1,z_2} = 1 + (z_1 z_2 - z_2)(1 - s)$$

onde $z_1 z_2 = g_1$ ou $z_1 z_2 = g_1 s$ e $z_2 = g_2$ ou $z_2 = g_2 s$, g_1 e $g_2 \in B_1$ e $s \in Z(G)$.

Sendo $sE = -E$ disto decorre que:

$$F(z_1 z_2 E) = \begin{cases} F(g_1 E), & \text{se } z_1 z_2 = g_1 \\ -F(g_1 E), & \text{se } z_1 z_2 = s g_1 \end{cases}$$

Da mesma forma que:

$$F(z_2 E) = \begin{cases} F(g_2 E), & \text{se } z_2 = g_2 \\ -F(g_2 E), & \text{se } z_2 = s g_2 \end{cases}$$

Podemos então analisar $\varphi(\mu_{z_1,z_2})$ em três casos sendo:

$$\varphi(\mu_{z_1,z_2}) = I_d + 2F(z_1 z_2 E) - 2F(z_2 E) \tag{3.1}$$

Caso 1.1: Unidade bicíclica com imagem não nula em apenas um único bloco:

Podemos supor sem perda de generalidade da observação anterior que: $F(z_1z_2E) = a_1e_{il} + a_2e_{li} + a_3e_{jk} + a_4e_{kj}$ e $F(z_2E) = b_1e_{il} + b_2e_{li} + b_3e_{jk} + b_4e_{kj}$, i, j, k, l são elementos distintos do conjunto $A_1 = \{1, 2, 3, 4\}$ e além disso $|a_i| = |b_i| = 1$ onde $1 \leq i \leq 4$. Segue então que para $2(a_i - b_i) \neq 0 \Rightarrow 2(a_i - b_i) = 4$ ou $2(a_i - b_i) = -4$.

Caso 1.2: Unidade bicíclica com imagem não nula em 2 blocos disjuntos fora da diagonal:

Nesse caso $F(z_1z_2E) = a_1e_{il} + a_2e_{li} + a_3e_{jk} + a_4e_{kj}$ e $F(z_2E) = b_1e_{ik_1} + b_2e_{k_1i} + b_3e_{l_1l_2} + b_4e_{l_2l_1}$, $W_1 \cap W_2 = \emptyset$ onde $W_1 = \{(i, l), (l, i), (j, k), (k, j)\}$ e $W_2 = \{(i, k_1), (k_1, i)(l_1, l_2)(l_2, l_1)\}$. De acordo com isso de (1.1) segue que respectivamente $2F(z_1z_2E)$ e $2F(z_2E)$ possui todas as entradas na forma $2a_i = 2$ ou $2a_i = -2$ e $2b_i = 2$ ou $2b_i = -2$, . Então $\varphi(\mu_{z_1,z_2}) = [a_{ij}]_{4\times4}$, $\forall\ 1 \leq i, j \leq 4$ segue que $-2 \leq a_{ij} \leq 2$.

Caso 1.3: Unidade bicíclica com imagem não nula no bloco da diagonal e fora da diagonal:

Podemos supor que $F(z_1z_2E) = a_1e_{11} + a_2e_{22} + a_3e_{33} + a_4e_{44}$ e $F(z_2E) = b_1e_{1l_1} + b_2e_{l_11} + b_3e_{jk} + b_4e_{kj}$, $1, l_1, j, k$ são elementos distintos entre si e componentes de, $A_1 = \{1, 2, 3, 4\}$, então de (1.1) em cada entrada na diagonal de $\varphi(\mu_{z_1,z_2})$ aparece uma expressão da forma: $1 + 2a_i$, $1 \leq i \leq 4$. Sendo $|a_i| = |b_i| = 1$ segue que $1 + 2a_i = 3$ ou $1 + 2a_i = -1$. Em contrapartida a imagem de $\varphi(\mu_{z_1,z_2})$ fora da diagonal será representada por $2F(z_2E)$ que assumirá valores iguais a $2b_i = 2$ ou $2b_i = -2$. Analisando os três casos segue o resultado.

□

Lema 3.5. *Se u_1 e u_2 são dois elementos de G com $\circ(u_1) = 2$ e $\circ(u_2) = 4$ e além disso $F(u_1E)$ e $F(u_2E)$ ocupam as mesmas posições não nulas e fora da diagonal em $M_4(Q)$ então $u_1u_2 \neq u_2u_1$*

Demonstração. Por hipótese temos que $F(u_1E) = a_1'e_{il} + a_2'e_{li} + a_3'e_{jk} + a_4'e_{kj}$ e $F(u_2E) = b_1'e_{il} + b_2'e_{li} + b_3'e_{jk} + b_4'e_{kj}$, a_i' e $b_i' \in \mathbb{Z}\ \forall\ 1 \leq i \leq 4$. Sendo $u_1^2 = 1$ e $u_2^4 = 1$ temos $(F(u_1E))^2 = F((u_1E)^2) = F(E) = I_d$ e $F(u_2E))^2 = F((u_2E)^2) = F(sE) = -I_d$ visto que $u_2^2 = s$. De acordo com isso concluimos que $a_1'a_2' = a_3'a_4' = 1$ e $b_1'b_2' = b_3'b_4' = -1$ Sendo $F(u_1E)F(u_2E) = a_1'b_2'e_{ii} + a_2'b_1'e_{ll} + a_3'b_4'e_{jj} + a_4'b_3'e_{kk}$ e $F(u_2E)F(u_1E) = b_1'a_2'e_{ii} + b_2'a_1'e_{ll} + a_3'a_4'e_{jj} + b_4'a_3'e_{kk}$ é fácil ver que $a_1'b_2' \neq b_1'a_2'$ pois se $a_1'b_2' = 1$ de $(a_1'a_2')(b_1'b_2') = -1$ segue que $b_1'a_2' = -1$. Da mesma forma ,se $a_1'b_2' = -1$ então $b_1'a_2' = 1$.

Logo $F(u_1E)F(u_2E) \neq F(u_2E)F(u_1E)$ e conseqüentemente $u_1u_2E \neq u_2u_1E$ o que implica que $u_1u_2 \neq u_2u_1$. □

Proposição 3.2. *Dados 2 elementos u_1 e $u_2 \in G = \frac{D_4 \times D_4^*}{I}$ com $\circ(u_1) = 2$ e $\circ(u_2) = 4$,e além disso $F(u_1E)$ e $F(u_2E)$ possuem imagens no mesmo bloco D_j em $M_4(\mathbb{Q})$. Então existe uma unidade bicíclica μ_{z_1,u_1} onde:*

$$\varphi(\mu_{z_1,u_1}) = I_d + 2F(u_2E) - 2F(u_1E)$$

Demonstração. Considerando $z_1 = u_2u_1$ é fácil ver pela proposição 3.1 que $z_1^2 = 1$ e além disso $u_1^{-1}z_1u_1 \notin < z_1 >$. Então pelo lema 1.3 $\mu_{z_1,u_1} \neq 1$ e $\mu_{z_1,u_1} = 1 + (u_2 - u_1)(1 - s)$ seguindo o resultado. A recíproca também é verdadeira, pois tomando $\mu_{z_1,w_1} = 1 + (z_1w_1 - w_1)(1 - s)$ uma unidade bicíclica não trivial se $\circ(z_1w_1) = 2$ então $\circ(w_1) = 4$, ou seja $w_1^2 = s$ pois se $\circ(w_1) = 2$ usando o fato que $\circ(z_1) = 2$ e que $z_1w_1 = sw_1z_1$ então teríamos $\circ(z_1w_1) = 4$ o que gera uma contradição. De maneira análoga se $\circ(z_1w_1) = 4$ então $\circ(w_1) = 2$.

Caso $\circ(u_1) = 4$ e $\circ(u_2) = 2$ basta considerar a unidade bicíclica $\mu_{z_2,u_1}, z_2 = u_1u_2$ e de maneira análoga verifica-se que $\varphi(\mu_{z_2,u_1}) = I_d + 2F(u_2E) - 2F(u_1E)$. □

Observação 3.4. *Na proposição abaixo vamos trabalhar com as unidades bicíclicas $\varphi(\mu_{z_1,w_1}) = I_d + \alpha, \alpha = 2F(z_1w_1E) - 2F(w_1E), F(z_1w_1E)$ mboxe $F(w_1E)$ possuem imagem em um mesmo bloco fora da diagonal. Ou seja se $F(z_1w_1E) = \sum_{i=1}^{4} a_ie_{ij_i}$ então $F(w_1E) = \sum_{i=1}^{4} a_ie_{ij_i}$.*

Proposição 3.3. *Dada uma unidade bicíclica $\mu_{z_1,w_1} \neq 1$ em $\mathcal{U}(\mathbb{Z}(D_4))$ onde $\varphi(\mu_{z_1,w_1}) = I_d + \alpha, \alpha = 2F(z_1w_1E) - 2F(w_1E)$. Tomando então qualquer elemento $u_1' \in D_4$, então existe uma unidade bicíclica μ'_{z_2,w_2} em $\mathcal{U}(\mathbb{Z}(G))$ onde:*

$$\varphi(\mu'_{z_2,w_2}) = I_d + \alpha \otimes (u_1'E)$$

Demonstração. Sabendo que em $\mathcal{U}(\mathbb{Z}(D_4))$ temos que $\varphi(\mu_{z_1,w_1}) = I_d + 2F_1(z_1w_1E) - 2F_1(w_1E), F_1$ é o isomorfismo citado no início do capítulo $\mathbb{Q}D_4E$ em $M_{2^1}(\mathbb{Q})$. Para efeitos de simplificação considere $2F_1(z_1w_1E) - 2F_1(w_1E) = 2(z_1w_1E) - 2(w_1E) = \alpha$. Então $\alpha(u_1'E) = 2((z_1w_1)u_1'E) - 2((w_1)u_1'E)$. Suponha sem perda de generalidade que $\circ(z_1w_1) = 4$ e $\circ(w_1) = 2$. Se $\circ(u_1') = 1$ ou 2 então $\circ((z_1w_1)u_1') = 4$ e $\circ((w_1)u_1') = 2$. Caso contrário se $\circ(u_1') = 4$ então $\circ((z_1w_1)u_1') = 2$ e $\circ(w_1u_1') = 4$. Pela proposição anterior existe então uma unidade bicíclica, μ_{z_2,w_2} em $\mathcal{U}(\mathbb{Z}(G_1))$ onde:

$$\varphi(\mu_{z_2,w_2}) = I_d + 2((z_1w_1)u_1'E) - 2((w_1)u_1'E) = I_d + \alpha(u_1'E)$$

□

Diante das proposições expostas acima é possível provar o teorema abaixo:

Teorema 3.2. $E_8 \subset \varphi(\mathcal{B}_2)$.

Demonstração. Utilizando o isomorfismo F_1 de $\mathbb{Q}(D_4)E \cong M_2(\mathbb{Q})$ e considerando $y = xv$ é fácil ver que $\circ(y) = 2$ e $\mu_{x,y} \neq 1$. Segue então que $\mu_{x,y} = 1 + (v - y)(1 - s)$ e conseqüentemente:

$$\varphi(\mu_{x,y}) = I_2 + 2(vE) - 2(yE) = I_2 - 4e_{12} \text{ e}$$

$$\varphi(\mu_{sx,y}) = I_2 + 2(svE) - 2(yE) = I_2 - 4e_{21}$$

o que implica que $E_4 \subset \varphi(\mathcal{B}_2)$ em $\mathcal{U}(\mathbb{Z}(D_4))$.

Tome agora $e_{ij}, i \neq j$ uma matriz elementar em $M_4(\mathbb{Q})$. Vamos provar que $I_4 + 8e_{ij} \in \varphi(\mathcal{B}_2)$.

Sabendo que $e_{ij} = e_{i_1j_1} \otimes e_{i_2j_2}$. Suponha que i é ímpar e j é par, o que implica que $e_{ij} = e_{i_1j_1} \otimes e_{12}$. Vamos dividir então em dois casos:

Caso 1: Tome $i_1 \neq j_1$,ou seja $(i_1, j_1) = (1, 2)$ ou $(i_1, j_1) = (2, 1)$:

Como $I_2 + 4e_{12}$ e $I_2 + 4e_{21}$ são unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(D_4))$ então considerando $(svE) = e_{12} - e_{21}$ e $(xvE) = e_{12} + e_{21}$ pela proposição anterior segue que: $(I_4 + ((4e_{i_1j_1})) \otimes (e_{12} - e_{21}))$ e $(I_4 + ((4e_{i_1j_1})) \otimes (e_{12} + e_{21}))$ são unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(G))$. Pela a distributividade do produto tensorial temos que:
$(I_4 + ((4e_{i_1j_1})) \otimes (e_{12} - e_{21})) = I_4 + 4e_{ij} - 4e_{(i+1,j-1)}$ e $(I_4 + ((4e_{i_1j_1})) \otimes (e_{12} + e_{21})) = (I_4 + 4e_{ij} + 4e_{(i+1,j-1)})$.
Observando que $j \neq (i + 1)$ e$(j - 1) \neq i$ então $I_4 + 8e_{ij}$ é o produto das duas unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(G))$.

Caso 2: Tome $i_1 = j_1$ e sabendo que $(I_4 + 4e_{12})$ é uma unidade bicíclica em $\mathcal{U}(\mathbb{Z}(D_4))$, então considerando $xE = e_{11} - e_{22}$ e $E = e_{11} - e_{22}$ e fazendo a multiplicação pela esquerda segue que:
$I_4 + ((e_{11} + e_{22})(4e_{12}))$ e $I_4 + ((e_{11} - e_{22})(4e_{12}))$ são unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(G))$.
Suponha que $i_1 = j_1 = 1$ e pela distributividade no produto tensorial reescrevemos as unidades acima da seguinte forma:
$I_4 + (4e_{ij} + 4e_{(i+2)(j+2)})$ e $I_4 + (4e_{ij} - 4e_{(i+2)(j+2))})$. Sabendo que $j \neq (i + 2)$ então: $(I_4 + 8e_{ij})$ é o produto de ambas e conseqüentemente provamos que cada gerador de E_8 está em $\varphi(\mathcal{B}_2)$. □

Observação 3.5. *Tendo μ_{z_1,z_2} uma unidade bicíclica não trivial, então sabemos que $\mu_{z_1z_2} = 1 + (z_1z_2 - z_2)(1 - s) = 1 + 2(z_1z_2 - z_2)(1 - s)/2$ e $\varphi(\mu_{z_1,z_2}) = I_d + 2F(z_1z_2E) - 2F(z_2E), E = (1 - s)/2$. Definindo $\alpha = 2F(z_1z_2E)$ e $\beta = 2F(z_2E)$ segue que α e β em relaçao à matriz $M_4(\mathbb{Q})$ ou possuem imagens em posições disjuntas entre si ou imagens nas mesmas posições. Visto que $\alpha^2 = I_d$ ou $\alpha^2 = -I_d$ então se $ae_{ij}, a \in \mathbb{Z}$ é um termo de α então $\exists\ b \in \mathbb{Z}$ onde be_{ji} também é um termo*

de α. Observação análoga vale para β.

Explicitaremos os lemas a seguir que permitirão provar que $\mathcal{B}_2) \subset E_2$ considerando $\mathcal{B}_2$ como subgrupo de $PSL_n(\mathbb{Q})$.

Lema 3.6. *Seja μ_{z_1,z_2} uma unidade bicíclica não nula. Se $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$, onde α e β possuem imagens em posições disjuntas em $M_4(\mathbb{Q})$ ambas fora da diagonal então $\alpha\beta$ e $\beta\alpha$ não possuem termos na diagonal.*

Demonstração. Por hipótese segue que $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$ onde $\alpha = a_1e_{1l_1} + a_2e_{2l_1} + a_3e_{3l_3} + a_4e_{4l_4}, \beta = b_1e_{1k_1} + b_2e_{2k_2} + b_3e_{3k_3} + b_4e_{4k_4}$, e $l_i \neq k_i, 1 \leq i \leq 4$.

Suponha por contradição que $\alpha\beta$ possui um termo dado por c_ie_{ii} na diagonal.Então $c_ie_{ii} = (a_ie_{il_i})(b_ie_{jk_j})$ em $\alpha\beta$ que pela definição de multiplicação de matrizes elementares segue que $l_i = j$ e $k_j = i$. Isto significa que β possuindo um termo na posição (l_i, i) possuirá um termo na posição (i, l_i) da mesma forma que α, o que contradiz a hipótese . Resultado análogo vale para $\beta\alpha$. □

Lema 3.7. *Tomando a unidade bicíclica como no lema anterior,então $\alpha\beta + \beta\alpha = 0, \alpha\beta \neq 0$.*

Demonstração. Note que se por contradição $\alpha\beta = 0$, então considerando $a^{'}e_{ij} \in \alpha\beta$ deve existir $(-a^{'}e_{ij})$ em $\alpha\beta$ tal que $(a^{'}e_{ij} - a^{'}e_{ij}) = 0$.Logo temos $a^{'}e_{ij} = (a_1e_{ik_1})(b_1e_{k_1j})$ e $(-a^{'}e_{ij}) = (-d_1e_{ik_1^{'}})(d_2e_{k_1^{'}j})$, $k_1^{'} \neq k_1, a_1b_1 = d_1d_2 = a^{'}$ onde $a_1e_{ik_1}$ e $-d_1e_{ik_1^{'}}$ são termos de α da mesma forma que $b_1e_{k_1j}$ e $d_2e_{k_1^{'}j}$ são termos de β. Sendo $k_1^{'} \neq k_1$ teríamos em α dois termos em uma mesma linha, o que é um absurdo.

De $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$ e utilizando a propriedade já vista de unidade bicíclica sabemos que $(\alpha+\beta)^2 = (\alpha+\beta)(\alpha+\beta) = 0$. Fazendo um cálculo algébrico é fácil ver que α^2e β^2 possuem imagem apenas na diagonal, logo $(\alpha + \beta)^2 = \alpha^2 + \alpha\beta + \beta\alpha + \beta^2$, $\alpha^2 + \beta^2 = 0$ consequëntementeo$\alpha\beta + \beta\alpha = 0$. □

Observação 3.6. *Sendo $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$ onde $\alpha = a_1e_{1l_1} + a_2e_{2l_1} + a_3e_{3l_3} + a_4e_{4l_4}$ e $\beta = b_1e_{1k_1} + b_2e_{2k_1} + b_3e_{3k_3} + b_4e_{4k_4}, l_i \neq k_i$ e $1 \leq i \leq 4$, podemos decompor α da seguinte forma:*
$\alpha = \alpha_1 + \alpha_2, \alpha_1 = a_1e_{1l_1} + a_ie_{il_i}, 1 < i \leq 4$ e $(i, l_i) \neq (l_1, 1)$. De acordo com isso $\alpha_2 = a_ke_{l_11} + a_k^{'}e_{l_ii}$ onde k e $k^{'} \in A_1 = \{1, 2, 3, 4\} - \{1, i\}$. Como sabemos que na primeira e i-ésima linhas existem também termos de β então podemos tomar $\beta = \beta_1 + \beta_2$, $\beta_1 = b_1e_{1k_1} + b_ie_{ik_i}, 1 < i \leq 4$ onde $(i, k_i) \neq (k_1, 1)$. Logo $\beta_2 = b_ke_{k_11} + b_k^{'}e_{k_ii}$ de tal forma que k e $k^{'} \in A_1 = \{1, 2, 3, 4\} - \{1, i\}$.

Note que essas decomposições com tais características serão sempre possíveis,pois se $(i, k_i) \doteq (k_1, 1)$ escolhemos então $\alpha_1 = a_1e_{1l_1} + a_i^{'}e_{l_ii}$ e então consideramos $\beta_1 = b_1e_{1k_1} + b_i^{'}e_{l_ij}, j \neq i$. Nesse caso temos que $(l_i, j) \neq (k_1, 1)$,pois se fossem iguais teríamos que $l_i = k_1 = i$ e $a_i^{'}e_{l_ii} = a_i^{'}e_{ii}$ o que contradiz o fato de

que α *não possui termos na diagonal.*

É de fácil verificação também que $\alpha_1\beta_1 = \beta_1\alpha_1 = \alpha_2\beta_2 = \beta_2\alpha_2 = 0$*, portanto de* $\alpha\beta + \beta\alpha = 0$ *temos que* $(\alpha_1+\alpha_2)(\beta_1+\beta_2)+(\beta_1+\beta_2)(\alpha_1+\alpha_2) = 0$ *o que implica que* $\alpha_1\beta_2 + \alpha_2\beta_1 + \beta_1\alpha_2 + \beta_2\alpha_1 = 0$*.*

Lema 3.8. *Em relação às decomposições anteriores segue que* $\alpha_1\beta_2 + \beta_1\alpha_2 = 0$ *e* $\alpha_2\beta_1 + \beta_2\alpha_1 = 0$*.*

Demonstração. Tomando um termo de_{ij} de $\alpha_1\beta_2$ então o mesmo também é um termo de $\alpha\beta$ e pelo lema anterior existe $-de_{ij} \in \beta\alpha = \beta_1\alpha_2+\beta_2\alpha_1, (deij+(-de_{ij})) = 0$.

Segue então que $-de_{ij} \in \beta_1\alpha_2$ pois se $-de_{ij} \in \beta_2\alpha_1$ então $-de_{ij} = (d^{'}e_{ik})(d_1^{'}e_{kj}), (-d) = (d^{'}d_1^{'}), d^{'}e_{ik} \in \beta_2$ e $d_1^{'}e_{kj} \in \alpha_1$. Da mesma forma que sendo $de_{ij} \in \alpha_1\beta_2$ então $de_{ij} = (d_1e_{il})(d_2e_{lj})$, $d = d_1d_2$, $d_1e_{il} \in \alpha_1$ e $d_2e_{lj} \in \beta_2$.

Como $d_1e_{il} \in \alpha_1$ e pela maneira que β_1 foi definido $\exists\, d_2^{'}e_{il_1}, l \neq l_1 \in \beta_1$. Sendo $d^{'}e_{ik} \in \beta_2$ e como β_1 e β_2 não possuem termos na mesma posição então $k \neq l_1$. De $d_2^{'}e_{il_1}$ e $d^{'}e_{ik} \in \beta$ temos então uma contradição pois numa mesma linha existe apenas um termo de β.

Dessa maneira prova-se que $-\alpha_1\beta_2 \subset \beta_1\alpha_2$ e de maneira análoga verifica-se que $-\beta_1\alpha_2 \subset \alpha_1\beta_2$ chegando ao resultado. □

Teorema 3.3. *Seja* μ_{z_1,z_2} *uma unidade bicíclica em* G *então* $\varphi(\mu_{z_1,z_2}) \in E_2$ *como elemento de* $PSL_n(\mathbb{Q})$

Demonstração. Se $\mu_{z_1,z_2} = 1$ então é trivial. Suponha então $\mu_{z_1,z_2} \neq 1$ e vamos dividir em três casos:

Caso 1: Seja $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$, α e β possuem imagens disjuntas. Pela observação da página 35 anterior podemos representar:

$$\alpha = \alpha_1 + \alpha_2 \quad \text{e} \quad \beta = \beta_1 + \beta_2$$

Além disso como $\alpha^2 + \beta^2 = 0$ segue que:

$$\begin{cases} (\alpha_1+\alpha_2)^2 + (\beta_1+\beta_2)^2 = 0 \\ (\alpha_1+\alpha_2)(\beta_1+\beta_2) + (\beta_1+\beta_2)(\alpha_1+\alpha_2) = 0 \end{cases}$$

É fácil ver que $\alpha_1^2 = \alpha_2^2 = \beta_1^2 = \beta_2^2 = 0$ então da primeira equação temos:

$$\alpha_1\alpha_2 + \alpha_2\alpha_1 + \beta_1\beta_2 + \beta_2\beta_1 = 0$$

Sendo $\alpha_1 = a_1e_{1l_1} + a_ie_{il_i}, \alpha_2 = a_ke_{l_11} + a_k^{'}e_{l_ii}, \beta_1 = b_1e_{1k_1} + b_ie_{ik_i}$ e $\beta_2 = b_ke_{k_11} + b_k^{'}e_{k_ii}, (i,l_i) \neq (l_1,1)$ e $(i,k_i) \neq (k_1,1)$, segue que $\alpha_1\alpha_2$ e $\beta_1\beta_2$ possuem ima-

gens na diagonal e nas mesmas posições dadas por $(1,1)$ e (i,i) então:

$$\alpha_1\alpha_2 + \beta_1\beta_2 = 0 \tag{3.2}$$

$$\begin{aligned} \text{e portanto } \varphi(\mu_{z_1,z_2}) &= I_d + (\alpha+\beta) \\ &= (I_d + (\alpha_1+\alpha_2) + (\beta_1+\beta_2)) = (I_d + (\alpha_1+\beta_1) + (\alpha_2+\beta_2)) \\ &= (I_d + (\alpha_1+\beta_1))(I_d + (\alpha_2+\beta_2)) \\ &= (I_d+\alpha_1)(I_d+\beta_1)(I_d+\alpha_2)(I_d+\beta_2) \end{aligned}$$

visto que $(\alpha_1+\beta_1)(\alpha_2+\beta_2) = (\alpha_1\alpha_2 + \alpha_1\beta_2 + \beta_1\alpha_2 + \beta_1\beta_2) = 0$ de (3.3) e do lema 3.12.

Observe ainda que $(I_d+\alpha_1) = (I_d + a_1e_{1l_1})(I_d + a_2e_{il_i})$ e $(I_d+\beta_1) = (I_d + b_1e_{1k_1})(I_d + b_ie_{ik_i})$,pois $l_1 \neq i$ e $k_1 \neq i, |a_i| = |b_i| = |a_1| = |b_1| = 2$. Raciocínio análogo vale para $(I_d + a_2)$ e $(I_d + b_2)$.

Logo $\varphi(\mu_{z_1,z_2}) = (I_d+\alpha_1)(I_d+\beta_1)(I_d+\alpha_2)(I_d+\beta_2) \in E_2$

Caso2: Seja $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$, α possui imagem na diagonal e β fora da diagonal, então $\varphi(\mu_{z_1,z_2}) = (I_d+\alpha+\beta)$, $\alpha = a_1e_{ii}+a_2e_{ll}+a_3e_{kk}+a_4e_{jj}$ e $\beta = b_1e_{il}+b_2e_{li}+b_3e_{jk}+b_4e_{kj}$ onde i,l,j,k são distintos entre si no conjunto $A_1 = \{1,2,3,4\}$.

Das equações $\alpha^2+\beta^2 = 0$ e $\alpha\beta+\beta\alpha = 0$ seguem os seguintes resultados: $a_1^2{=}a_2^2{=}{-}(b_1b_2)$,$a_3^2{=}a_4^2{=}{-}(b_3b_4)$, $a_1{=}{-}a_2$ e $a_3{=}{-}a_4$. Sendo $|a_i|{=}|b_i| = 2$, $1 \leq i \leq 4$ então $b_1b_2{=}b_3b_4 = -4$ onde α em $M_4(\mathbb{Q})$ terá duas entradas positivas e duas negativas.

Suponha sem perda de generalidade que:

$$\alpha = 2e_{ii} - 2e_{ll} + 2e_{kk} - 2e_{jj}$$

$$\begin{aligned} \text{Logo } \varphi(\mu_{z_1,z_2}) &= (I_d + (\alpha+\beta)) = ((I_d+\alpha)+\beta) \\ &= (3e_{ii} - e_{ll} + 3e_{kk} - e_{jj}) + (b_1e_{il} + b_2e_{li} + b_3e_{jk} + b_4e_{kj}) \\ \text{então} -(\varphi(\mu_{z_1,z_2})) &= (-3e_{ii} + e_{ll} - 3e_{kk} + e_{jj}) - (b_1e_{il} + b_2e_{li} + b_3e_{jk} + b_4e_{kj}) \end{aligned}$$

Observando que:

$$(I_d - b_1e_{il} - b_4e_{kj})(I_d - b_2e_{li} - b_3e_{jk}) = (I_d - \beta + (b_1b_2)e_{ii} + (b_4b_3)e_{kk}) =$$

$$(-3eii + e_{ll} - 3e_{kk} + e_{jj} - \beta) = \varphi(\mu_{z_1,z_2})$$

Logo $-(\varphi(\mu_{z_1,z_2})) = (I_d - b_1e_{il})(I_d - b_4e_{kj})(I_d - b_2e_{li})(I_d - b_3e_{jk})$ visto que $l \neq k$ e $i \neq j$. De $|b_i| = 2 \ \forall\ 1 \leq i \leq 4$, segue o resultado.

Caso 3: Seja $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$, α e β possuem imagens nas mesmas posições.Sabemos que nesse caso temos que:

$$\varphi(\mu_{z_1,z_2}) = I_d + a_1 e_{il} + a_2 e_{jk},\ |a_1| = |a_2| = 4 \text{ e } (i,l) \neq (k,j)$$

Esse fato segue diretamente da observação 3.3 e de que $(\alpha + \beta)^2 = 0$. Segue então que $\varphi(\mu_{z_1,z_2}) = (I_d + a_1 e_{il})(I_d + a_2 e_{jk}) \in E_2$ desde que $l \neq k$ □

4

Resultado estendido

Nesse capítulo explicitaremos o resultado generalizado e para isso vamos considerar a seguinte definição:

Definição 4.1. *Dizemos que G é o produto central dos seus subgrupos G_i para $1 \leq i \leq n$ se:*
a- G=$\langle G_i; 1 \leq i \leq n \rangle$,com $[G_i, G_j] = 1$;
b-$Z(G) = Z(G_i)$, para todo $1 \leq i \leq n$.

Tome então $G_1 = D_4^1 \times D_4^2 \times D_4^2 \ldots \times D_4^n$ onde D_4^i são cópias isomorfas de D_4 onde $1 \leq i \leq n$ e defina I um subgrupo de G_1 formado pela unidade e pelos elementos da seguinte forma:
$w = \prod s_{i_1} s_{i_2} s_{i_3} \ldots s_{i_l}, 1 \leq s_{i_1} < s_{i_2} < \ldots < s_{i_l} \leq n$ onde l percorre todos os números pares entre 1 e n. É fácil ver então que $|I| = 2^{n-1}$ e nesse caso trabalharemos com $G = \dfrac{G_1}{I}$ e nesse caso $G' = Z(G) = \{1, s\}$ sendo portanto G o produto central de n cópias isomorfas de D_4.

Para o resultado generalizado precisaremos da seguinte proposição:

Proposição 4.1. *Sendo G o grupo citado acima, então o anel de grupo $\mathbb{Q}G$ admite a seguinte decomposição:*

$$\mathbb{Q}G = \mathbb{Q}G\left(\frac{1+s}{2}\right) \oplus \mathbb{Q}G\left(\frac{1-s}{2}\right)$$

onde $\mathbb{Q}G\left(\dfrac{1+s}{2}\right) \cong \oplus^{2^{2n}}\mathbb{Q}$ e $\mathbb{Q}G\left(\dfrac{1-s}{2}\right) \cong M_{2^n}(\mathbb{Q})$

Demonstração. A primeira parte da igualdade segue da proposição 1.8. Usando o fato que $e_{G'} = \dfrac{1+s}{2}$ a primeira congruência segue da proposição 1.9 sendo portanto a parte comutativa do anel de grupo. A segunda congruência vem da decomposição de $\mathbb{Q}D_4$ juntamente com as proposições 2.5 e 1.2. □

Observação 4.1. *Sejam 2 matrizes elementares e_{ij} e $e'_{i_1 j_1}$ que estão respectivamente em $M_{2^n}(\mathbb{Q})$ e $M_2(\mathbb{Q})$. Utilizando produto de kroneker entre as matrizes po-*

demos obter uma matriz elementar em $M_{2^{n+1}}(\mathbb{Q})$ *da forma:*

$$e_{lk} = e_{ij} \otimes e_{i_1 j_1}, e_{lk} \in M_{2^{n+1}}(\mathbb{Q}), l = 2(i-1) + i_1 \text{ e } k = 2(j-1) + j_1.$$

É fácil ver que e_{lk} *estará na diagonal,ou seja* $l = k \Leftrightarrow i_1 = j_1$ *e* $i = j$.

Sendo $D_4^i = \left\langle x_i, v_i / x_i^{-1} v_i x_i = v_i^{-1} \right\rangle$ considere o isomorfismo $F : \mathbb{Q}(G)E \to M_{2^n}(\mathbb{Q})$ definido pela representação:

$$(1, \ldots, 1, x_i, \ldots, 1) \to I_d \ldots \otimes I_d \otimes T(x_i) \ldots \otimes I_d$$

$$(1, \ldots, 1, v_i, \ldots, 1) \to I_d \ldots \otimes I_d \otimes T(v_i) \ldots \otimes I_d$$

Devido à representação acima é fácil ver que $gE = \sum_{i=1}^{2^n} a_i e_{ij_i}, a_i = \pm 1$ identificando $F(gE)$ com gE. Do isomorfismo F sabendo que $F(gE)^2 = I_d$ ou $F(gE)^2 = -I_d$ então dado $a_i e_{ij}$ em gE existe por sua vez um único termo $a_j e_{ji}$ em gE onde $a_i a_j = \pm 1$. Podemos descrever dessa forma os termos de gE como elementos do conjunto $A_1 = \{a_i e_{ij_i} / j_i \neq F(i^{'})$ sempre que $i \neq i^{'}$ para todo $1 \leq i, i^{'} \leq 2^n\}$

Considerando o conjunto A_2=$\{(i, F(i)), 1 \leq i \leq 2^n\}$ formado pelos índices dos elementos de A_1 existe sempre uma decomposição $A_2 = A_1^{'} \cup A_2^{'}$, $A_1^{'}$=$\{(i_k, F(i_k))$, onde se $k_1 \neq k_2$ então $(F(i_{k_1}), i_{k_1}) \neq (i_{k_2}, F(i_{k_2}))\}$ e $A_2^{'} = \{(F(i_k), i_k)\}$. Tomando a função bijetora $H : A_1 \to A_1$ onde $H((i, F(i))) = (F(i), i)$ é fácil ver que $H_2 = H/_{A_1^{'}}$ é uma bijeção de $A_1^{'}$ em $A_2^{'}$ tornando fácil concluir que $\circ\left(A_1^{'}\right) = \circ\left(A_2^{'}\right) = 2^{n-1}$.

Proposição 4.2. *Seja* $gE \in GE$. *Então* $F(gE)$ *possui imagem apenas na diagonal ou completamente fora da diagonal.*

Demonstração. Vamos provar por indução sobre n:
Seja G_n e G_{n+1} respectivamente grupos que são produtos centrais de n e $n+1$ cópias isomorfas de D_4. Considerando então $gE \in G_{n+1}E$ segue que $gE = (g_1 E) \otimes (u_{n+1}E), g_1 E \in (G_n)E$ e $u_{n+1}E \in D_4 E$. Por hipótese de indução temos dois casos a considerar:

$$\begin{aligned} g_1 E &= \left(\sum_{i=1}^{2^n} a_i e^{'}_{ij_i)}\right), i = j_i \ \forall\ 1 \leq j \leq 2^n \text{ ou} \\ g_1 E &= \left(\sum_{i=1}^{2^n} a_i e^{'}_{ij_i)}\right), i \neq j_i \ \forall\ 1 \leq j \leq 2^n \end{aligned}$$

Considere primeiramente $u_{n+1}E$=$\left(\sum_{i=1}^{2} a_i e_{ii}\right)$ e então tomando $g_1 E$ na diagonal temos que:

$$(g_1E)\otimes(u_{n+1}E_{n+1}) = \left(\sum_{i=1}^{2^n} a_i a_1 e^{'}_{ij_i)} e_{11}\right) + \left(\sum_{i=1}^{2^n} a_i a_2 e^{'}_{ij_i)} e_{22}\right) = \left(\sum_{i=1}^{2^n} a_i a_1 e^{''}_{(2(-1+i)+1)(2(-1+i_j)+1}\right) + \left(\sum_{i=1}^{2^n} a_i a_1 e^{''}_{(2(-1+i)+2)(2(-1+i_j))+2}\right).$$

Logo gE possui imagem na diagonal sendo $j = f(j)$.

Caso contrário se $u_{n+1}E$ está fora da diagonal e g_1E na diagonal então:

$$(g_1E)\otimes(u_{n+1}E) = \left(\sum_{i=1}^{2^n} a_i a_1 e^{'}_{ij_i} e_{12}\right) + \left(\sum_{i=1}^{2^n} a_i a_2 e^{'}_{ij_i)} e_{21}\right)$$

concluindo-se que gE tem imagem fora da diagonal. Os outros dois casos são análogos aos anteriores seguindo o resultado.

Como consequência segue que dados u_1E e u_2E elementos de gE então ambos os elementos possuem imagens nas mesmas posições ou em posições completamente disjuntas em $M_{2^n}(\mathbb{Q})$. □

Proposição 4.3. *Seja Se $g \in GE$ e sendo $gE = \sum_{i=1}^{2^n} a_i e_{ij_i)}, a_i = \pm 1 \ \forall \ 1 \leq i \leq 2^n$, segue que todos os $a_i^{'}s$ ou possuem o mesmo sinal ou metade deles é positiva e a outra metade é negativa.*

Demonstração. Prova-se por indução assim como na proposição 4.3. Observando também que para $n = 1$ se $g \in D_4$ então segue que $gE = \sum_{i=1}^{2} a_i e_{ij_i)}, a_i > 0$ ou $a_i < 0 \ \forall 1 \leq i \leq 2$ ou $a_1 a_2 < 0$ □

Observação 4.2. *Como conseqüência temos que sendo $gE = \sum_{i=1}^{2^n} a_i e_{ij_i}$,e $|a_i| = 1$,então $\sum_{i=1}^{2^n} a_i = 2^n, -2^n$ ou 0, o que implica que $2^n / \sum_{i=1}^{2^n} a_i$*

Com os resultados então obtidos anteriormente é possível adaptarmos tudo que foi visto no capítulo anterior para provamos que $\mathcal{B}_2 \subset E_2$ em $PSL_n(\mathbb{Q})$.

Considerando $U_2, U_2 = \{1 + \alpha(1-s)/\alpha \in \mathbb{Z}(G)\}$ e $V = \{1 + \alpha(1-s)\}, \varepsilon(\alpha)$ é par subgrupos em $U(\mathbb{Z}(G))$. Sendo G um grupo extra-especial sabemos que $\mathcal{B}_2$ está em V e sendo $V \cong \dfrac{U_2}{\{I_d, -I_d\}}$ vamos estudar as unidades bicíclicas como subgrupo em $PSL_n(\mathbb{Q}) = \dfrac{SL_n\mathbb{Q}}{Z(SL_n(\mathbb{Q}))}$.

Através do isomorfismo $F : \mathbb{Q}(G)E \to M_{2_n}(\mathbb{Q})$ é possível definir um monomorfismo $\varphi : U_2 \to \varphi(U_2)$ de tal forma que se $u = 1 + \sum a_g g(1-s), \sum a_g g \in \mathbb{Z}(G) \in U_2$então$\varphi(u) = I_d + 2\sum a_g F(gE), E = \dfrac{(1-s)}{2}$ em $SL_n(\mathbb{Z})$.

Sabendo que $\mathcal{B}_2 \subset V$, o lema a seguir nos fornece uma maneira direta de expressarmos $z = \mu_{z_1,z_2} \in \mathcal{B}_2$,como elemento de U_2.

Lema 4.1. *Se μ_{z_1,z_2} é uma unidade bicíclica em $\mathcal{U}(\mathbb{Z}\ (G))$ não nula então:*

$$\mu_{z_1,z_2} = 1 + (z_1 z_2 - z_2)(1-s)$$

Demonstração. Basta observar que sendo $z_1 = u_1u_2\dots u_nI \in G$ então $\circ(z_1) = 4 \Leftrightarrow$ existe um número ímpar de termos $u_i, 1 \leq i \leq n, \circ(u_i) = 4$. Logo $< z_1 >= \{1, z_1, s, sz_1\}$ e neste caso sendo G extra-especial ,segue que :

$$z_2^{-1}z_1z_2z_1^{-1} = 1 \text{ ou } z_2^{-1}z_1z_2z_1^{-1} = s$$

o que implica a trivialidade da unidade bicíclica.Caso contrário se $\circ(z_1) = 2$ e $\mu_{z_1,z_2} \neq 1$ então $z_2^{-1}z_1z_2z_1^{-1} \neq 1$, o que implica que $z_2^{-1}z_1z_2z_1^{-1} = s$.Logo $z_1z_2 = sz_2z_1$ e o resultado segue análogo ao capítulo anterior. □

Observação 4.3. *Sabendo que* $\mu_{z_1,z_2} = 1 + (z_1z_2 - z_2)(1 - s), \alpha_1 = (z_1z_2 - z_2)(1 - s)$ *então* $\varphi(\mu_{z_1,z_2}) = I_d + F(\alpha_1), F(\alpha_1)^2 = 0$ *e além disso* $F(\alpha_1) = \alpha + \beta$, *onde* $\alpha = 2F(z_1z_2E)$ *e* $\beta = -2F(z_2E)$.

De acordo com as notações acima seguem os dois lemas abaixo de demonstrações análogas ao capítulo anterior.

Lema 4.2. *Seja* $\mu_{z_1z_2}$ *uma unidade bicíclica não nula.Se* $\varphi(\mu_{z_1,z_2}) = I_d+\alpha+\beta$, *onde* α *e* β *possuem imagens em posições disjuntas em* $M_{2^n}(\mathbb{Q})$ *ambas fora da diagonal então* $\alpha\beta$ *e* $\beta\alpha$ *não possuem termos na diagonal.*

Lema 4.3. *Tomando a unidade bicíclica como no lema anterior,então* $\alpha^2 + \beta^2 = 0$ *e* $\alpha\beta + \beta\alpha = 0, \alpha\beta \neq 0$.

Lema 4.4. *Dados* $\alpha = F(gE) = \sum_{i=1}^{2^n} a_ie_{il_i}$ *e* $\beta = (g_1E) = \sum_{i=1}^{2^n} a_ie_{ib_i}$ *elementos em posições disjuntas em* $M_{2^n}(\mathbb{Q})$ *segue que* $b_i \neq l_i, 1 \leq i \leq 2^n$. *Considere agora* $A_1 = \{(i, l_i)/1 \leq i \leq 2^n\}$ *e* $B_1 = \{(i, b_i)/1 \leq i \leq 2^n\}$ *conjuntos de índices que representam respectivamente as posições de cada termo de* α *e* β.*Então existem subconjuntos* $A_1^k \subset A_1$ *e* $B_1^k \subset B_1, A_1^k = \{(i_k, l_k)/1 \leq k \leq 2^{n-1}$ *e* $(i_k, l_k) \neq (l_j, i_j), k \neq j\}$ *e* $B_1^k = \{(i_k, b_k)/1 \leq k \leq 2^{n-1}$ *e* $(i_k, b_k) \neq (b_j, i_j), k \neq j\}$

Demonstração. Sabemos que existe um subconjunto $A_1^{'}$=$\{(i_k, l_k)$ $/1 \leq k \leq 2^{n-1}$ e $(i_k, l_k) \neq (l_j, i_j), k \neq j\} \subset A_1$. Como os termos de β percorrem todas as linhas de $M_{2^n}(\mathbb{Q})$ então para cada $i_k, 1 \leq k \leq 2^n$ existe $P_1 = (i_k, b_k)$ que denota a posição de um termo de β. À partir disso formamos o conjunto $B_1 = \{(i_k, b_k)\ /\ 1 \leq k \leq 2^{n-1}\}$.

Vamos considerar então em B_1 2 subconjuntos dados por:
$B_1^{'}$=$\{(i_{k_l}, b_{k_l})/\ 1 \leq l \leq m, (i_{k_{l_1}}, b_{k_{l_1}}) \neq (b_{k_{l_2}}, i_{k_{l_2}})$ sempre que $l_1 \neq l_2\}$ e $B_2^{'} = \{(i_{k_j}, b_{k_j})/m < j \leq 2^{n-1}, (i_{k_l}, b_{k_l}) = (b_{k_{l+1}}, i_{k_{l+1}}), m + 1 \leq l \leq (2^{n-1} - 1)$ onde m denota o número de elementos de $B_1^{'}$. Para feitos de simplificação tome $B_1^{'} = \{(i_k, b_k), 1 \leq k \leq m\}$ e $B_2^{'} = \{(i_j, b_j)/m + 1 \leq j \leq 2^{n-1}\}$.Por sua vez a decomposição de B_1 gera uma decomposição em $A_1^{'}$ da seguinte forma:

$$A_1^{''} = \{(i_k, l_k)/1 \leq k \leq m\} \text{ e } A_2^{''} = \{(i_j, l_j)/m+1 \leq j \leq 2^{n-1}\}$$

.

Afirmação : Considerando $A_1^{''} \subset A_1^{'}, A_1^{''} = \{(i_k, l_k)/1 \leq k \leq m < 2^{n-1}$ e $B_1^{'} \subset B_1, B_1^{'} = \{(i_k, b_k)/1 \leq k \leq m < 2^{n-1}$, então tomando $(i_{m+1}, l_{m+1}) \in A_1^{'}$ é possível com $A_1^{''}$ e $B_1^{'}$ encontrarmos 2 novos conjuntos:

$A_1^{k^{'}} = \{(i_k, l_k)/1 \leq k \leq m+1\}$ e $B_1^{k^{'}} = \{(i_k, b_k)/1 \leq k \leq m+1$ e $(i_k, b_k) \neq (b_j, i_j)$ para $k \neq j\}$

Demonstração: Se (i_{m+1}, l_{m+1})é um elemento de $A_1^{'}$ existe (i_{m+1}, b_{m+1}) um elemento de B_1 e consideramos os novos conjuntos :

$$A_1^{1^{'}} = \{(i_1, l_1), (i_2, l_2), \ldots (i_k, l_k) \ldots (i_m, l_m), (i_{m+1}, l_{m+1})\}$$

$$B_1^{1^{'}} = \{(i_1, b_1), (i_2, b_2), \ldots (i_k, b_k) \ldots (i_m, b_m), (i_{m+1}, b_{m+1})\}$$

Se $(b_{m+1}, i_{m+1}) \neq (i_k, b_k)$,$1 \leq k \leq m$ então está provado. Caso contrário se $(b_{m+1}, i_{m+1}) \doteq (i_k, b_k)$ para algum k e sabendo que na (l+1)-ésima linha existe um termo de β na posição $(l_{m+1}, b_{m+1}^{'})$ tome então:

$$A_1^{2^{'}} = \{(i_1, l_1), (i_2, l_2), \ldots (i_k, l_k) \ldots (i_m, l_m), (l_{m+1}, i_{m+1})\}$$

$$B_1^{2^{'}} = \{(i_1, b_1), (i_2, b_2), \ldots (i_k, b_k) \ldots (i_m, b_m), (l_{m+1}, b_{m+1}^{'})\}$$

Veja que $(l_{m+1}, b_{m+1}^{'}) \neq (b_k, i_k)$ pois se $(l_{m+1}, b_{m+1}^{'}) \doteq (b_k, i_k) \Rightarrow l_{m+1} = b_k = i_{m+1}$ o que gera uma contradição.Se $(l_{m+1}, b_{m+1}^{'}) \neq (b_j, i_j), j \neq k$ então está provado.Caso contrário se $(l_{m+1}, b_{m+1}^{'}) \doteq (b_j, i_j)$ que sem perda de generalidade tome $(b_j, i_j) = (b_2, i_2)$ obtemos então:

$$A_1^{3^{'}} = \{(i_1, l_1), (l_2, i_2), \ldots (i_k, l_k) \ldots (i_m, l_m), (l_{m+1}, i_{m+1})\}$$

$$B_1^{3^{'}} = \{(i_1, b_1), (l_2, b_2^{'}), \ldots (i_k, b_k) \ldots (i_m, b_m), (l_{m+1}, b_{m+1}^{'})\}$$

Analogamente $(b_2^{'}, l_2) \neq (l_{m+1}, b_{m+1}^{'})$ pois se $(b_2^{'}, l_2) \doteq (l_{m+1}, b_{m+1}^{'}) \Rightarrow b_{m+1}^{'} = l_2 = i_2$ o que gera uma contradição .Da mesma forma que $(l_2, b_2^{'}) \neq (b_k, i_k)$ pois se $(l_2, b_2^{'}) \doteq (b_k, i_k) \Rightarrow b_k = l_2 = i_{m+1}$ o que também é uma contradição.

Como temos um número finito de termos então o processo termina após k passos, obtendo os conjuntos $A_1^{k^{'}}$ e $B_1^{k^{'}}$ desejados.

De acordo com isso, tomando $A_1^1 = A_1^{''} \cup A_1^*, A_1^* = \{(i_{m+1}, l_{m+1}), (i_{m+2}, l_{m+2})\}$ observando que $A_1^{'}$ gera o conjunto $B_1^* = \{(i_{m+1}, b_{m+1}), (i_{m+2}, b_{m+2})\} \subset$

$B_2^{'}$ é possível encontramos $B_1^1 = \{(i_k, b_k), 1 \leq k \leq m+2 \text{ e } (i_k, b_k) \neq (b_j, i_j), k \neq j\}$

Da mesma forma considerando $A_1^2 = A_1^1 \cup A_2^{'}$, $A_2^{'} = \{(i_{m+3}, l_{m+3}), (i_{m+4}, l_{m+4})\}$ notando que $A_2^{'}$ gera o conjunto $B_2^{''} = \{(i_{m+3}, b_{m+3}), (i_{m+4}, b_{m+4})\} \subset B_2^{'}$ então obtemos $B_1^2 = \{(i_k, b_k), 1 \leq k \leq m+4 \text{ e } (i_k, b_k) \neq (b_j, i_j), k \neq j\}$

Após um número finito de k passos, obtemos então $A_1^k = \{(i_j, l_j)/1 \leq j \leq 2^{n-1}$ e $B_1^k = \{(i_j, b_j)/1 \leq j \leq 2^{n-1}\}$ os conjuntos então desejados , $k = \dfrac{2^{n-1} - m}{2}$ □

Desse jeito definindo $A_1^{k^{'}} = \{(l_j, i_j)/1 \leq j \leq 2^{n-1}\}$ e $B_1^{k^{'}} = \{(b_j, i_j)/1 \leq j \leq 2^{n-1}\}$ e tomando α_1 como a soma dos temos de α que tem como índices os elementos de A_1^k e β_1 como a soma dos termos de β que possui como índices os elementos de B_1^k, temos a seguinte decomposição:

$$\alpha = \alpha_1 + \alpha_2 \text{ e } \beta = \beta_1 + \beta_2$$

É fácil ver que α_2 e β_2 são formados respectivamente da soma de termos cujos índices fazem parte dos conjuntos $A_1^{k^{'}}$ e $B_1^{k^{'}}$ respectivamente. Também por uma verificação rápida seguem as igualdades:

$$\alpha_1^2 = \beta_1^2 = \alpha_2^2 = \beta_2^2 = 0 \text{ e } \alpha_1\beta_1 = \alpha_2\beta_2 = \beta_1\alpha_1 = \beta_2\alpha_2 = 0$$

De $\alpha^2 + \beta^2 = 0$ e $\alpha\beta + \beta\alpha = 0$ temos:

$$\begin{cases} (\alpha_1 + \alpha_2)(\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)(\beta_1 + \beta_2) = 0 \\ (\alpha_1 + \alpha_2)(\beta_1 + \beta_2) + (\beta_1 + \beta_2)(\alpha_1 + \alpha_2) = 0 \end{cases}$$

Disto utilizando as igualdades acima obtemos:

$$\begin{cases} \alpha_1\alpha_2 + \alpha_2\alpha_1 + \beta_1\beta_2 + \beta_2\beta_1 = 0 \\ \alpha_1\beta_2 + \alpha_2\beta_1 + \beta_1\alpha_2 + \beta_2\alpha_1 = 0 \end{cases}$$

Temos então o seguinte lema cuja demonstração é análoga ao capítulo anterior:

Lema 4.5. *Seja* $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta, \alpha$ *e* β *possuem imagens disjuntas e fora da diagonal. Então de acordo com a decomposição anterior segue que* $\alpha_1\beta_2 + \beta_1\alpha_2 = 0$ *e* $\alpha_2\beta_1 + \beta_2\alpha_1 = 0$.

De acordo com os resultados preliminares segue o teorema principal do capítulo.

Teorema 4.1. *Sendo* $\mathcal{B}_2 \subset \mathcal{U}(\mathbb{Z}G))$. *Então* $\mathcal{B}_2 \subset E_2$ *como subgrupo de* $PSL_n(\mathbb{Q})$ *através do monomorfismo* $\varphi : U_2 \to \varphi(U_2) \subset M_{2^n}(\mathbb{Q})$.

Demonstração. **Caso 1 :** Seja $\mu_{z_1,z_2} \in \mathcal{B}_2, \varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$ onde α e β ocupam posições disjuntas em $M_{2^n}(\mathbb{Q})$ então:

$$\varphi(\mu_{z_1,z_2}) = I_d + (\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)$$

Observemos que $(\alpha_1 + \beta_1)(\alpha_2 + \beta_2) = \alpha_1\alpha_2 + \alpha_1\beta_2 + \beta_1\alpha_2 + \beta_1\beta_2 = 0$, pois $\alpha_1\alpha_2 + \beta_1\beta_2 = 0$ e $\alpha_1\beta_2 + \beta_1\alpha_2 = 0$ e portanto:

$$I_d + \alpha + \beta = (I_d + \alpha_1 + \beta_1)(I_d + \alpha_2 + \beta_2) =$$

$$(I_d + \alpha_1)(I_d + \beta_1)(I_d + \alpha_2)(I_d + \beta_2)$$

Pela formação de $\alpha_1, \alpha_2, \beta_1$ e β_2 segue que:

$$\alpha_1 = \left(I_d + \sum_{i=1}^{2^{n-1}} a_i e_{il_i}\right) = \prod_{i=1}^{2^{n-1}} (I_d + a_i e_{il_i}),$$
$$\alpha_2 = \left(I_d + \sum_{i=1}^{2^{n-1}} a_i^{'} e_{l_i i}\right) = \prod_{i=1}^{2^{n-1}} (I_d + a_i^{'} e_{l_i i}),$$
$$\beta_1 = \left(I_d + \sum_{i=1}^{2^{n-1}} d_i e_{ib_i}\right) = \prod_{i=1}^{2^{n-1}} (I_d + d_i e_{ib_i}),$$
$$\beta_2 = \left(I_d + \sum_{i=1}^{2^{n-1}} d_i^{'} e_{b_i i}\right) = \prod_{i=1}^{2^{n-1}} (I_d + d_i e_{b_i i}),$$

visto que $(i, l_i) \neq (l_j, j)$ e $(i, b_i) \neq (b_i, i)$ sempre que $i \neq j$. Sendo $|a_i| = |a_i^{'}| = |d_i| = |d_i^{'}| = 2$ resulta que $\varphi(\mu_{z_1,z_2}) \subset E_2$.
Caso2: Seja μ_{z_1,z_2} $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$, onde α e β ocupam respectivamente suas posições na diagonal e fora da diagonal em $M_{2^n}(\mathbb{Q})$ então:

$$\beta = b_1 e_{i_1 l_1} + b_2 e_{l_1 i_1} + + b_3 e_{i_2 l_2} + b_4 e_{l_2 i_2} + \ldots + b_{2^n} e_{l_{2^{n-1}} i_{2^{n-1}}} \text{ e}$$
$$\alpha = a_1 e_{i_1 i_1} + a_2 e_{l_1 l_1} + a_3 e_{i_2 i_2} + a_4 e_{l_2 l_2} + \ldots + a_{2^n} e_{l_{2^{n-1}} l_{2^{n-1}}}$$

De $(\alpha + \beta)^2 = 0$ temos as seguintes igualdades:

$$\alpha^2 + \beta^2 = 0 \text{ e} \tag{4.1}$$

$$\alpha\beta + \beta\alpha = 0 \tag{4.2}$$

De (2.1) segue que:

$$\begin{cases} a_1^2 = -(b_1 b_2) \\ a_3^2 = -(b_3 b_4) \\ \vdots \ = \ \vdots \\ a_{2k+1} = -(b_{2k+1} b_{2k+2}), 0 \leq k \leq (2^{n-1} - 1) \end{cases}$$

Da mesma forma que de (2.2) temos:

$$\begin{cases} a_1 b_1 + b_1 a_2 = 0 \\ a_3 b_3 + b_3 a_4 = 0 \\ a_5 b_5 + b_5 a_6 = 0 \\ \vdots \ + \ \vdots \ = \vdots \\ a_{2k+1} b_{2k+1} + b_{2k+1} a_{2k+2} = 0, 0 \leq k \leq (2^{n-1} - 1) \end{cases}$$

Das equações acima sendo $|a_i|=|b_i| = 2, 1 \leq i \leq 2^n \Rightarrow (b_{2k+1} b_{2k+2}) = -4, 0 \leq k \leq (2^{n-1} - 1)$ e também $a_{2k+1} = -a_{2k+2}, 0 \leq k \leq (2^{n-1} - 1)$. Portanto α terá metade de termos positivos e metade de termos negativos. Suponha então sem perda de generalidade que:
$\alpha = 2e_{i_1 i_1} - 2e_{l_1 l_1} + 2e_{i_2 i_2} - 2e_{l_2 l_2} + 2e_{i_3 i_3} - 2e_{l_3 l_3} + \ldots 2e_{i_{2^{n-1}} i_{2^{n-1}}} - 2e_{l_{2^{n-1}} l_{2^{n-1}}}$.

Logo $I_d + \alpha + \beta = 3e_{i_1 i_1} - e_{l_1 l_1} + 3e_{i_2 i_2} - e_{l_2 l_2} + 3e_{i_3 i_3} - e_{l_3 l_3} + \ldots + 3e_{i_{2^{n-1}} i_{2^{n-1}}} - e_{l_{2^{n-1}} l_{2^{n-1}}} + \beta$

Sendo $\overline{I_d + \alpha + \beta} = \overline{-(I_d + \alpha + \beta)}$ segue que:

$$I_d + \alpha + \beta = -3e_{i_1 i_1} + e_{l_1 l_1} - 3e_{i_2 i_2} + e_{l_2 l_2} - 3e_{i_3 i_3} + e_{l_3 l_3} + \ldots - 3e_{i_{2^{n-1}} i_{2^{n-1}}} + e_{l_{2^{n-1}} l_{2^{n-1}}} - \beta$$

.

Veja então que:

$(I_d - b_1 e_{i_1 l_1} - b_3 e_{i_2 l_2} - b_5 e_{i_3 l_3} + \ldots + (-b_{2^n - 1} e_{i_{2^{n-1}} l_{2^{n-1}}}))$.
$(I_d - b_2 e_{l_1 i_1} - b_4 e_{l_2 i_2} - b_6 e_{l_3 i_3} + \ldots + (-b_{2^n} e_{l_{2^{n-1}} i_{2^{n-1}}})) =$
$(I_d - \beta + (b_1 b_2) e_{i_1 i_1} + (b_3 b_4) e_{i_2 i_2} + (b_5 b_6) e_{i_3 i_3} + \ldots + (b_{2^n - 1} b_{2^n} e_{i_{2^{n-1}} i_{2^{n-1}}})) =$
$(-3e_{i_1 i_1} + e_{l_1 l_1} - 3e_{i_2 i_2} + e_{l_2 l_2} - 3e_{i_3 i_3} + \ldots - 3e_{i_{2^{n-1}} i_{2^{n-1}}} + e_{l_{2^{n-1}} l_{2^{n-1}}} - \beta) =$
$(I_d + \alpha + \beta)$.

Note que:

$\left(I_d - \sum_{k=0}^{2^{n-1}-1} b_{2k+1} e_{i_{(k+1)} l_{(k+1)}}\right) = \prod_{k=0}^{2^{n-1}-1} (I_d - b_{2k+1} e_{i_{(k+1)} l_{(k+1)}})$ e
$\left(I_d - \sum_{k=1}^{2^{n-1}} b_{2k} e_{i_k l_k}\right) = \prod_{k=1}^{2^{n-1}} (I_d - b_{2k} e_{i_k l_k})$

pois $(i_j, l_j) \neq (l_k, i_k)$ sempre que $j \neq k$. Sendo $|b_i| = 2 \; \forall \; 1 \leq i \leq 2^n$ segue que $\varphi(\mu_{z_1,z_2}) \subset E_2$.

Caso 3: Seja μ_{z_1,z_2} $\varphi(\mu_{z_1,z_2}) = I_d + \alpha + \beta$, onde α e β ocupam respectivamente as mesmas posições em $M_{2^n}(\mathbb{Q})$. Sabendo que $(\alpha + \beta)^2 = 0$ então:
$\varphi(\mu_{z_1,z_2}) = I_d + b_1 e_{i_1 l_1} + b_2 e_{i_2 l_2} + + b_3 e_{i_3 l_3} + \ldots + b_k e_{i_k l_k}$ onde $k = 2^{n-1}$ pela proposição 4.5 e $(i_j, l_j) \neq (l_k, i_k)$ para $j \neq k$.

Logo $\varphi(\mu_{z_1,z_2}) = \prod_{j=1}^{k}(I_d + b_j e_{i_j l_j})$ e como nesse caso $|b_j| = 4 \; \forall 1 \leq j \leq k$ então $\varphi(\mu_{z_1,z_2}) \subset E_2$, provando o resultado para todos os casos. □

Definição:Dizemos que $u_1 E = \sum_{i=1}^{2^n} a_i e_{ij_i}$ e $u_2 E = \sum_{i=1}^{2^n} b_i e_{ij_i'}$ estão no mesmo bloco sempre que $j_i = j_i^{'} \; \forall \; 1 \leq i \leq 2^n$.

Podemos dizer então que dois elementos u_1 e u_2 estão no mesmo bloco se as suas imagens ocupam as mesmas posições na matriz $M_{2^n}(\mathbb{Q})$.

Teorema 4.2. *Teorema da generalização dos blocos:Existem exatamente* 2^n *blocos disjuntos onde se divide o conjunto* $A = \{gE/g \in G\}$ *através do isomorfismo* $F \rightarrow mathbbQ(GE) \cong M_{2^n}(\mathbb{Q})$*, incluindo a diagonal. Além disso em cada bloco fora da diagonal existem* 2^n *elementos de ordem* 2 *e* 2^n *elementos de ordem* 4.

Demonstração. Suponha válido para n e vamos mostrar que vale para $n+1$:
Seja $u \in G_{n+1}$, então $uE = (wE).(u_1 E), w$ e u_1 estão respectivamente em G_n e D_4. Pela hipótese de indução segue que wE possui 2^n possibilidades de posições disjuntas em $M_{2^n}(\mathbb{Q})$. Sendo $u_1 E = a_1 e_{11} + a_2 e_{22}$ ou $u_1 E = b_1 e_{12} + b_2 e_{21}$ e sabendo que $wE = \sum_{i=1}^{2^n} a_i e_{ij_i}$ então $uE = (wE).(u_1 E)$ possuirá 2 posições disjuntas para cada wE fixo. Como temos 2^n possibilidades para wE teremos no total 2^{n+1} possibilidades de posições disjuntas para uE possuindo portanto 2^{n+1} blocos disjuntos onde se divide o conjunto A.

Fixando um bloco D_j e tomando wE cuja posição em $M_{2^n}(\mathbb{Q})$ esteja em D_j, então $wE = (u_1 E)(u_2 E), u_2 E \in D_4 E$. Temos então 2 posições a considerar:
Caso1: Considere $u_2 E$ está na diagonal:

Veja que nesse caso temos então 2 possibilidades a considerar: $u_2 E = I_d$ ou $u_1 E = a_1 e_{11} + a_2 e_{22}, a_1 a_2 = -1$. Então se $\circ(wE) = 2$ e $wE = (u_1 E)(u_2 E)$ segue que $\circ(u_1 E) = 2$ e por hipótese de indução temos 2^{n-1} possibilidades para $u_1 E$ e tendo 2 possibilidades para $u_2 E$ segue então temos 2^n possibilidades para wE. Se $\circ(wE) = 4$ implica que $\circ(u_1 E) = 4$ e de maneira análoga temos 2^n possibilidades para wE.
Caso 2: Considere$u_2 E$ está fora da diagonal:

Então $\circ(u_2 E) = 2$ ou $\circ(u_2 E) = 4$. Se $\circ(wE) = 2$ com $\circ(u_1 E)$ fora da diagonal então utilizando a hipótese de indução temos 2^{n-1} possibilidades para $u_1 E$

fixando qualquer uma das duas ordens para u_2E temos portanto 2^n possibilidades para wE. Raciocínio análogo vale para quando $\circ(wE) = 4$.

Quando u_1E está na diagonal podemos escrever $wE = (u_1'E)(w_1E)\ u_1'E \in D_4E$ e $w_1E \in G_n$ e novamente utilizando a hipótese de indução para w_1E vemos que wE possui 2^n possibilidades tendo ordem 2 e tendo ordem 4. □

As proposições e teoremas posteriores terão como objetivo provar que $E_{2^{n+1}} \subset \varphi(\mathcal{B}_2)$, sendo $\mathcal{B}_2$ um subgrupo em $\mathcal{U}(\mathbb{Z}(G)$.

Proposição 4.4. *Dados 2 elementos u_1 e $u_2 \in G$ onde $\circ(u_1) = 2$ e $\circ(u_2) = 4$, e além disso $F(u_1E)$ e $F(u_1E)$ estão no mesmo bloco D_j e fora da diagonal em $M_{2^n}(\mathbb{Q})$. Então existe uma unidade bicíclica μ_{z_1,u_1} onde:*

$$\varphi(\mu_{z_1,u_1}) = I_d + 2F(u_2E) - 2F(u_1E)$$

Demonstração. Considerando $z_1 = u_2u_1$ é fácil ver que $z_1^2 = 1$ e além disso $u_1^{-1}z_1u_1 \notin < z_1 >$. Então pelo lema 1.3 $\mu_{z_1,u_1} \neq 1$ e $\mu_{z_1,u_1} = 1 + (u_2 - u_1)(1 - s)$ seguindo o resultado.

Veja também que se $\circ(u_1) = 4$ e $\circ(u_2) = 2$, considerando a unidade bicíclica $\mu_{z_2,u_2s}, z_2 = u_1u_2$ de maneira análoga verifica-se que a mesma é não trivial e conseqüentemente

$$\varphi(\mu_{z_2,u_2s}) = I_d + 2F(u_2E) - 2F(u_1E)$$

.

A recíproca também é verdadeira, pois tomando $\mu_{z_1,w_1} = 1+(z_1w_1-w_1)(1-s)$ uma unidade bicíclica não trivial se $\circ(z_1w_1) = 2$ então $\circ(w_1) = 4$, pois se $\circ(w_1) = 2$ usando o fato que $\circ(z_1) = 2$ e que $z_1w_1 = sw_1z_1$ então teríamos $\circ(z_1w_1) = 4$ o que gera uma contradição. De maneira análoga se $\circ(z_1w_1) = 4$ então $\circ(w_1) = 2$. □

Observação 4.4. *As unidades bicíclicas que trabalharemos abaixo são da forma $\varphi(\mu_{z_1,u_1})=I_d + \alpha, \alpha=2F(z_1u_1E) - 2F(u_1E)$ onde $2F(z_1u_1E) = 2(\Sigma_{i=1}^{2^n} a_ie_{ij_i})$ e $2F(u_1E) = 2(\Sigma_{i=1}^{2^n} b_ie_{ij_i})i \neq j_i$ e $|a_i| = |b_i| = 1 \forall 1 \leq i \leq 2^n$. Usando a propriedade elementar de unidades bicíclicas que $\alpha^2 = 0$ e pela proposição 4.5 segue que:*
$\alpha = 2(\Sigma_{i=1}^{2^{n-1}} c_{i_k}e_{i_kj_{i_k}}), c_{i_k} \neq 0$ e $c_{i_k} = (a_{i_k} - b_{i_k})$. Além disso para cada k_1 fixo temos que $j_{i_{k_1}} \neq i_k\ \forall\ 1 \leq k \leq 2^{n-1}$.

.

A partir de agora consideraremos G_n como o grupo G formado pelo produto central de n cópias isomorfas de D_4.

Proposição 4.5. *Dada uma unidade bicíclica $\mu_{z_1,w_1} \neq 1$ em $\mathcal{U}(\mathbb{Z}(G_n))$ onde $\varphi(\mu_{z_1,w_1}) = I_d + \alpha$ como citado acima. Tomando então qualquer elemento $u_1' \in D_4$,*

então existe uma unidade bicíclica μ'_{z_2,w_2} *em* $\mathcal{U}(\mathbb{Z}(G_{n+1}))$ *onde:*

$$\varphi(\mu'_{z_2,w_2}) = I_d + \alpha \otimes (u'_1 E)$$

Demonstração. Sabendo que em $\mathcal{U}(\mathbb{Z}(G_n))$ temos que $\varphi(\mu_{z_1,w_1}) = I_d + 2F(z_1w_1E) - 2F(w_1E), F$ é o isomorfismo de $\mathbb{Q}(G_nE)$ em $M_{2^n}(\mathbb{Q})$. Para efeitos de simplificação considere $2F(z_1w_1E) - 2F(w_1E) = 2(z_1w_1E) - 2(w_1E) = \alpha$. Então $\alpha(u'_1E) = 2((z_1w_1)u'_1E) - 2(w_1u'_1E)$. Suponha sem perda de generalidade que $\circ(z_1w_1) = 4$ e $\circ(w_1) = 2$. Se $\circ(u'_1) = 1$ ou 2 então $\circ((z_1w_1)u'_1) = 4$ e $\circ(w_1u'_1) = 2$. Caso contrário se $\circ(u'_1) = 4$ então $\circ((z_1w_1)u'_1) = 2$ e $\circ(w_1u'_1) = 4$. Pela proposição anterior existe então uma unidade bicíclica, μ_{z_2,w_2} em $\mathcal{U}(\mathbb{Z}(G_{n+1}))$ onde:

$$\varphi(\mu_{z_2,w_2}) = I_d + 2((z_1w_1)u'_1E) - 2(w_1u'_1E) = I_d + \alpha(u'_1E)$$

□

Observação 4.5. *Note então que o produto de* n *unidades bicíclicas da forma* $\varphi(\mu_i) = I_d + \alpha_i, 1 \leq i \leq n$ *onde os* $\alpha'_i s$ *ocupam as mesmas posições em* $M_{2^n}(\mathbb{Q})$ *isto é* $\alpha_i = \sum_{k=1}^{2^{n-1}} a_k^i e_{kj_k} \forall 1 \leq i \leq n$ *gerará um produto de* n *unidades bicíclicas em* $\mathcal{U}(\mathbb{Z}(G_{n+1}))$*,pois além disso como* $\alpha_i\alpha_j = 0$ *segue que:*
$\varphi(\mu_1)\varphi(\mu_2)\ldots\varphi(\mu_n) = (I_d + \alpha_1)(I_d + \alpha_2)\ldots(I_d + \alpha_n) = (I_d + (\alpha_1 + \alpha_2 + \ldots + \alpha_n))$.

Tomando $u \in D_4$ *um elemento qualquer temos que* $(\alpha_1 + \alpha_2 + \ldots + \alpha_n)u_1E = (\alpha_1u_1E + \alpha_2u_1E + \ldots + \alpha_nu_1E)$ *em* $\mathbb{Q}(G_{n+1})E)$.

Em seguida considerando a identidade I_d *em* $M_{2^{n+1}}(\mathbb{Q})$ *resulta em* $(I_d + \alpha_1u_1E + \alpha_2u_1E + \ldots + \alpha_nu_1E) = (I_d + \alpha_1u_1E)(I_d + \alpha_2u_1E)\ldots(I_d + \alpha_nu_1E)$
visto que pela proposição anterior $(I_d + \alpha_iu_1E)$ *são unidades bicíclicas em* $\mathcal{U}(\mathbb{Z}(G_{n+1}))$ *onde conseqüentemente* α_iu_1E *ocupam as mesmas posições em* $M_{2^{n+1}}(\mathbb{Q})$*,onde* $1 \leq i \leq n$.

Teorema 4.3. *Seja* $\mathcal{B}_2$ *o subgrupo gerado pelas unidades bicíclicas em* $\mathcal{U}(\mathbb{Z}(G_n))$. *Então* $E_{2^{n+1}} \subset \varphi(\mathcal{B}_2)$.

Demonstração. Vamos provar por indução a seguinte afirmação: $(I_d + 2^{n+1}e_{i_1j_1}), i_1 \neq j_1$ é o produto de 2^{n-1} unidades bicíclicas da forma $\varphi(\mu_i) = I_d + \alpha_i, \alpha_i = 2F(u_1E) - 2F(u_2E)$ onde u_1E e u_2E ocupam as mesmas posições em um mesmo bloco D_j fora da diagonal em $M_{2^n}(\mathbb{Q})$.

Sabemos por produto tensorial que dado e''_{ij} um elemento da base matricial em $M_{2^{n+1}}(\mathbb{Q})$, segue que $e''_{ij} = e_{i_1j_1} \otimes e^*_{l_1l_2}$, $e_{i_1j_1}$ e $e^*_{l_1l_2}$ são respectivamente elementos das bases matriciais em $M_{2^n}(\mathbb{Q})$ e $M_2(\mathbb{Q})$. Suponha sem perda de generalidade que i é ímpar e j é par e então $e''_{ij} = e_{i_1j_1}.e^*_{12}$.

<u>**Caso 1:**</u> Suponha que $i_1 \neq j_1$. Tomando então um elemento $u \in D_4, uE = e^*_{12} + e^*_{21}$, então pela observação anterior e pela hipótese de indução temos que:

$(I_d+((2^{n+1}e_{i_1j_1})u_1E)) = (I_d+((2^{n+1}e_{i_1j_1})(e^*_{12}+e^*_{21})) = (I_d+2^{n+1}e''_{ij}+2^{n+1}e''_{(i+1)(j-1)})$. Sendo portanto o produto de 2^{n-1} unidades bicíclicas $\varphi(\mu'_i) = I_d + \alpha'_i, \alpha'_i$ ocupam as mesmas posições em $M_{2^{n+1}}(\mathbb{Q})$.

De maneira análoga tomando $u_1E = e^*_{12} - e^*_{21}$ em D_4 então $(I_d + ((2^{n+1}e_{i_1j_1})(e^*_{12} - e^*_{21})) = (I_d + 2^{n+1}e''_{ij} - 2^{n+1}e''_{(i+1)(j-1)})$. Sendo também o produto de 2^{n-1} unidades bicíclicas $\varphi(\mu''_i) = I_d + \alpha''_i$ onde tanto α''_i quanto α'_i ocupam as mesmas posições em $M_{2^{n+1}}(\mathbb{Q})$.

Logo $(I_d + 2^{n+1}e''_{ij} + 2^{n+1}e''_{(i+1)(j-1)})(I_d + 2^{n+1}e''_{ij} - 2^{n+1}e''_{(i+1)(j-1)}) = (I_d + 2^{n+2}e''_{ij})$ é o produto de 2^n unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(G_{n+1}))$

Caso 2: Suponha agora que $i_1 = j_1$ e então $e''_{ij} = e_{i_1j_1}e^*_{12}, i_1 = j_1$ e $e_{i_1j_1}$ é um elemento da base matricial em $M_{2^n}(\mathbb{Q})$.

Utilizando produto tensorial de matrizes sabemos que $e_{i_1j_1} = e'_{ll} \otimes e^*_{kk}, e'_{ll}$ e e^*_{kk} são elementos respectivamente das bases matriciais em $M_2(\mathbb{Q})$ e $M_{2^n}(\mathbb{Q})$. Segue então que $e''_{ij} = (e'_{ll}.e^*_{kk})e^*_{12}$, chamando $e_{l_1l_2} = e^*_{kk}e^*_{12}$ que é um elemento de $M_{2^n}(\mathbb{Q})$. Por hipótese de indução temos que $(I_d + (2^{n+1})e_{l_1l_2}$ é o produto de 2^{n-1} unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(G_n)), \varphi(\mu_i) = I_d + \alpha_i, \alpha_i$ ocupam as mesmas posições em $M_{2^n}(\mathbb{Q})$. Suponha sem perda de generalidade que $e'_{ll} = e'_{11}$ e tome u_1 e $u_2 \in D_4, u_1 = e'_{11} + e'_{22}$ e $u_2 = e'_{11} - e'_{22}$. Por raciocínio análogo ao caso anterior segue $(I_d + ((e'_{11} + e'_{22})(2^{n+1}e_{l_1l_2}))$ e $(I_d + ((e'_{11} + e'_{22}).(2^{n+1}e_{l_1l_2})$ são respectivamente o produto de 2^{n-1} unidades bicíclicas em $M_{2^{n+1}}(\mathbb{Q})$ com imagens na mesma posição. Sabendo que $e'_{11}e_{l_1l_2} = e''_{ij}$ e $e'_{22}(e_{l_1l_2}) = e''_{(2^n+i)(2^n+j)}$ então $(I_d + 2^{n+1}e''_{ij} + 2^{n+1}e''_{(2^n+i)(2^n+j)})(I_d+2^{n+1}e''_{ij}-2^{n+1}e''_{(2^n+i)(2^n+j)})$ é o produto de 2^n unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(G_{n+1}))$, o que conclui-se que $((I_d + 2^{n+2}e''_{ij}) \in \mathcal{B}_2$.

Vamos provar que é válido para $n = 1$:

Sabemos do isomorfismo $\mathbb{Q}(G_1)E \cong M_2(\mathbb{Q})$ que existe um elemento de ordem 2 e outro de ordem 4 dados respectivamente por $u_1 = e_{12} + e_{21}$ e $u_2 = e_{12} - e_{21}$.

Pela proposição 4.6 existe uma unidade bicíclica $\mu_{z_1,u_1} \in \mathcal{U}(\mathbb{Z}(G_1))$ onde:

$$\varphi(\mu_{z_1,u_1}) = I_d + 2F(u_2E) - 2F(u_1E)$$

Chamando $\alpha = 2F(u_2E) - 2F(u_1E)$ sabendo que $\alpha^2 = 0$ da propriedade elementar de unidades bicíclicas então $\alpha = \pm 4e_{12}$ ou $\alpha = \pm 4e_{21}$. Suponha sem perda de generalidade que $\alpha = 4e_{12}$. Calculando, temos também que $\varphi(\mu_{sz_1,u_1}) = I_d - 4e_{21}$. Disto conclui-se então que:

$$E_{2^2} \subset \mathcal{B}_2 \subset \mathcal{U}(\mathbb{Z}(G_1))$$

. □

Referências Bibliográficas

[1] RITTER, J., K.SEHGAL, S. "Construction of units in integral Group rings of finite nilpotent groups", *Math Zeitsch*, v. 324, 1991.

[2] H.BASS, J. M. E. J. S. "Solution of the congruence subgroup problem for $Sln(n \geq 3)eS_{p^{2^n}}(n \geq 2)$", *Publ.Math. Hautes Etudes Sci*, v. 33, pp. 59–137, 1967.

[3] JESPERS, E.;LEAL, G. "Describing Units of Integral Groups Rings of Some 2-Groups", *Comm. Álgebra*, v. 19, n. 6, pp. 1809–1827, 1991.

[4] NEWMAN, N. *Integral Matrices*. 1 ed. New York, Academic Press, 1972.

[5] POLCINO, FRANCISCO CÉSAR ; SEHGAL, S. K. . *An Introduction to Group Rings*. 2 ed. Netherlands,USA, Academic Publishers, 2002.

[6] NOETHER, E. "Hypercomplexe Grossen Und Darstellungstheorie", *Math Zeitsch*, v. 30, pp. 641–692, 1929.

[7] BACK, A. "subgroups of the general linear groups normalized by relative elementary groups". In: Springer (Ed.), *Algebric K-theory*, Lecture Nite in Math.

[8] J.P.SERRE. "Le probléme des groupes de congruence pour SL_2", *Ann of Math-92*, pp. 489–527.

[9] L.N.VASERSTEIN. "On the group Sl_2 over Dedeking rings of arithmetic tipe", *Math. USSR-Sb*, v. 18, pp. 321–332, 1973.

[10] I.MERZLJAKOV, M. *Fundamentals of the Theory of Groups*. New York, Berlim, Springer Verlag, 1979.

Apêndice

Seja μ_{z_1,z_2} uma unidade bicíclica não trivial em $\mathcal{U}(\mathbb{Z}(G))$ onde G é grupo-extra especial de ordem 32. Vamos considerar então a imagem de algumas unidades bicíclicas $\varphi(\mu_{z_1,z_2}) = I_d+\alpha+\beta$ mediante os três casos possíveis com suas respectivas decomposições:

Caso1: Quando α e β possuem imagens nas mesmas posições e fora da diagonal:

$$\mu_{a,u}\longmapsto \begin{bmatrix} 1 & 0 & -4 & 0 \\ 0 & 1 & 0 & -4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -4 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\mu_{a,u}\longmapsto \begin{bmatrix} 1 & 0 & -4 & 0 \\ 0 & 1 & 0 & -4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -4 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\mu_{a,uw^*}\longmapsto \begin{bmatrix} 1 & 0 & 0 & -4 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & -4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Caso 2: Quando α e β possuem imagens em que uma delas está na diagonal e a outra fora da diagonal.

$$\mu_{t,b}\longmapsto \begin{bmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 2 & 0 & -3 & 0 \\ 0 & 2 & 0 & -3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\mu_{t,bb^*}\longmapsto \begin{bmatrix} 1 & 0 & -2 & 0 \\ 0 & -3 & 0 & 2 \\ 2 & 0 & -3 & 0 \\ 0 & -2 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 1 \end{bmatrix}$$

$$\mu_{t^*,b^*} \longmapsto \begin{bmatrix} 1 & -2 & 0 & 0 \\ 2 & -3 & 0 & 0 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 2 & -3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\mu_{bt^*,w^*} \longmapsto \begin{bmatrix} -3 & 2 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & -2 & -3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Caso 3 : Quando α e β possuem ambas imagens fora da diagonal e em posições disjuntas.

$$\mu_{t,bw^*} \longmapsto \begin{bmatrix} 1 & -2 & 0 & 2 \\ 2 & 1 & -2 & 0 \\ 0 & -2 & 1 & 2 \\ 2 & 0 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -2 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 0 & -2 & 1 \end{bmatrix}$$

$$\mu_{t^*,ub^*} \longmapsto \begin{bmatrix} 1 & 0 & -2 & 2 \\ 0 & 1 & -2 & 2 \\ -2 & 2 & 1 & 2 \\ -2 & 2 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -2 & 2 \\ 0 & 1 & -2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & 2 & 1 & 0 \\ -2 & 2 & 0 & 1 \end{bmatrix}$$

$$\mu_{ut^*,w^*} \longmapsto \begin{bmatrix} 1 & -2 & 2 & 0 \\ 2 & 1 & 0 & -2 \\ 2 & 0 & 1 & -2 \\ 0 & -2 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & -2 \\ 2 & 0 & 1 & -2 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -2 & 2 & 1 \end{bmatrix}$$

Formação das unidades bicíclicas $\mathcal{B}_2 \subset \mathcal{U}(\mathbb{Z}(G_1))$ através das unidades bicíclicas $\mathcal{B}_2 \subset \mathcal{U}(\mathbb{Z}(D_4))$, o que nos permite provar que $I_d + 8e_{ij}, i \neq j \in \mathcal{B}_2$ em $\mathcal{U}(\mathbb{Z}(G_1))$. Para isso vamos dividir o estudo em 3 blocos onde de divide o conjunto de índices fora da diagonal:

Caso1: Bloco formado pelas posições $(1,3),(3,1),(2,4)$ e $(4,2)$:

Sendo $D_4 = \langle x, v, x^2 = v^4 = 1/x^{-1}vx = v^3 \rangle, z(D_4) = D_4^{'} = \{1, v^2 = s\}$, considere o isomorfismo $F(\mathbb{Q}(D_4E \to M_2(\mathbb{Q}), E = \dfrac{1-s}{2}$ onde:

$F(xE) = I_d + e_{11} - e_{22}$ e $F(vE) = I_2 + e_{12} - e_{21}$.

De acordo com isso $\varphi(\mu_{x,sv}) = I_2 + 2F(xvE) - 2F(svE) = I_2 + 4e_{21}$. Então:

$\mu_1 = I_4 + (4e_{21} \otimes (e_{11}^* + e_{22}^*)) = I_4 + 4e_{31}^{'} + 4e_{42}^{'}$ e

$\mu_2 = I_4 + (4e_{21} \otimes (e_{11}^* - e_{22}^*)) = I_4 + 4e_{31}^{'} - 4e_{42}^{'}$

são unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(G_1))$.

Conclusão: $\mu_1.\mu_2 = I_4 + 8e_{31}^{'}$ e $\mu_1.(\mu_2)^{-1} = I_4 + 8e_{42}^{'} \in \mathcal{B}_2$

Da mesma forma sendo $\varphi(\mu_{sx,v}) = I_2 + 2F(sxvE) - 2F(vE) = I_d + 4e_{12}$, então:

$\mu_1^{'} = I_4 + (4e_{12} \otimes (e_{11}^* + e_{22}^*)) = I_4 + 4e_{13}^{'} + 4e_{24}^{'}$e

$\mu_2^{'} = I_4 + (4e_{12} \otimes (e_{11}^* + e_{22}^*)) = I_4 + 4e_{13}^{'} - 4e_{24}^{'}$ são unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(G_1))$.

Logo $\mu_1^{'}.\mu_2^{'} = I_4 + 8e_{13}^{'}$ e $\mu_1.(\mu_2)^{-1} = I_4 + 8e_{24}^{'} \in \mathcal{B}_2$

Caso2: Bloco formado pelas posições $(1,4),(4,1),(2,3)$ e $(2,3)$:

Veja que $e_{14}^{'} = e_{12} \otimes e_{12}^{*}$. Tomando então $u_1 = e_{12} + e_{21}$ e $u_2 = e_{12} - e_{21}$,elementos de D_4E é fácil ver que:

$\mu_3 = I_4 + (4e_{21} \otimes (e_{12}^{*} + e_{21}^{*})) = I_4 + 4e_{32}^{'} + 4e_{41}^{'}$,

$\mu_4 = I_4 + (4e_{21} \otimes (e_{12}^{*} - e_{21}^{*})) = I_4 + 4e_{32}^{'} - 4e_{41}^{'}$,

$\mu_3^{'} = I_4 + (4e_{12} \otimes (e_{12}^{*} + e_{21}^{*})) = I_4 + 4e_{14}^{'} + 4e_{23}^{'}$,

$\mu_4^{'} = I_4 + (4e_{12} \otimes (e_{12}^{*} - e_{21}^{*})) = I_4 + 4e_{14}^{'} - 4e_{23}^{'}$

Logo $\mu_3.\mu_4 = I_4 + 8e_{32}^{'}$, $\mu_3.\mu_4^{-1} = I_4 + 8e_{41}^{'}$, $\mu_3^{'}.\mu_4^{'} = I_4 + 8e_{14}^{'}$, e $\mu_3^{'}.\mu_4^{-1} = I_4 + 8e_{23}^{'} \in \mathcal{B}_2$.

Caso 3: Bloco formado pelas posições $(1,2),(2,1),(3,4)$ e $(4,3)$:

Note que $e_{12} = e_{11} \otimes e_{12}$ então considerando $\varphi(\mu_{s^*x^*,v^*}) = I_2 + 4e_{12}$, segue que tomando 2 elementos em D_4 dados por $I_2 = u_1 = e_{11} + e_{22}$ e $x = e_{11} - e_{22}$ temos que:

$\mu_1^{''} = \mu_{s^*x^*,v^*} = I_4 + ((e_{11} + e_{22})(4e_{12}^{*})) = I_4 + e_{12}^{'} + 4e_{34}^{'}$,

$\mu_2^{''} = \mu_{s^*x^*,xv^*} = I_4 + ((e_{11} - e_{22})(4e_{12}^{*})) = I_4 + e_{12}^{'} - 4e_{34}^{'}$

$\mu_3^{''} = \mu_{x^*,s^*v^*} = I_4 + ((e_{11} + e_{22})(4e_{21}^{*})) = I_4 + e_{12}^{'} + 4e_{43}^{'}$

$\mu_4^{''} = \mu_{x^*,xs^*v^*} = I_4 + ((e_{11} - e_{22})(4e_{21}^{*})) = I_4 + e_{12}^{'} - 4e_{43}^{'}$

são unidades bicíclicas em $\mathcal{U}(\mathbb{Z}(G_1))$. Logo $\mu_1^{''}.\mu_2^{''} = I_4 + 8e_{12}^{'}, \mu_1^{''}.(\mu_2^{''})^{-1} = I_4 + 8e_{34}^{'}, \mu_3^{''}.\mu_4^{''} = I_4 + e_{43}^{'}$ e $\mu_3^{''}.(\mu_4^{''})^{-1} = I_4 + 8e_{43}^{'}$ estão em $\mathcal{B}_2$.