Unidades de $\mathbb{Z}C_{2p}$ e aplicações

Renata Rodrigues Marcuz Silva

Tese apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Doutor em Ciências

Programa: Matemática

Orientador: Prof. Dr. Raul Antonio Ferraz

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CAPES e do CNPq

São Paulo, 13 abril de 2012

Unidades de $\mathbb{Z}C_{2p}$ e aplicações

Este exemplar corresponde à redação
final da tese devidamente corrigida
e defendida por Renata Rodrigues Marcuz Silva
e aprovada pela Comissão Julgadora.

Banca Examinadora:

- Prof. Dr. Raul Antonio Ferraz (orientador) - IME-USP.
- Prof. Dr. Jairo Zacarias Gonçalves - IME-USP.
- Prof. Dr. Antonio Paques - UFRGS.
- Prof. Dr. Osnel Broche Cristo - UFLA.
- Profa. Dra. Paula Murgel Veloso - UFF.

Dedicatória

Dedico esta tese à minha família, em especial, aos meus pais, Fernando e Terezinha, e irmãos, Rodrigo e Ricardo, que tanto me deram, que tão pouco retribuí e todos meus erros e defeitos compreenderam.

Agradecimentos

Durante estes cinco anos, muitas pessoas cruzaram meu caminho e deparei me com inúmeras situações que contribuiram para que o sonho de elaborar tal trabalho fosse concretizado.

Gostaria de começar agradecendo ao Departamento de Matemática da USP, pela oportunidade que me foi oferecida no momento em que me acolheram e por oferecer um ambiente extremamente estimulante e desafiador.

Em especial, gostaria de agradecer meu orientador, Prof. Dr. Raul Antonio Ferraz, pela sua paciência, dedicação com o ensino e a pesquisa, e acima de tudo pelo seu grande apoio em todas as etapas do nosso trabalho.

Também adoraria agradecer meus colegas de pós-graduação, que se uniram no início ou ao longo desta grande empreitada, e que me deram apoio incondicional, tornando minhas tarefas mais leves e alegres.

Um agradecimento especial aos meus amigos: John Castillo, que me ajudou a utilizar o GAP, facilitando a construção dos exemplos desta obra; Paula Olga Gneri e Patricia Massae Kitani, que travaram grandes batalhas durante o processo de formação acadêmica, nunca deixando o desânimo prevalecer; Alexander Holguín Villa e Luis Enrique Ramírez, por sempre estarem ao meu lado e me escutarem, não importando quantas vezes e horas fossem necessárias. A todos meus amigos queridos, obrigada pelo apoio emocional que proporcionaram.

Para terminar, gostaria de agradecer aos funcionários do Instituto de Matemática e Estátistica da USP pela esforço, paciência e infraestrutura oferecidas.

Resumo

Unidades de $\mathbb{Z}C_{2p}$ e aplicações

Seja p um número primo ímpar e seja θ uma raiz p - ésima primitiva da unidade. Considere os seguintes elementos $u_i := 1 + \theta + \theta^2 + \cdots + \theta^{i-1}$ para todo $1 \leq i \leq \frac{p+1}{2}$ do anel $\mathbb{Z}[\theta]$.

Nesta tese, nós descrevemos explicitamente um conjunto gerador para o grupo das unidades do anel de grupo integral $\mathbb{Z}C_{2p}$, representado por $\mathcal{U}(\mathbb{Z}C_{2p})$, onde C_{2p} representa o grupo cíclico de ordem $2p$ e p satisfaz as seguintes condições: $S_\theta := \{-1, \theta, u_2, \ldots, u_{\frac{p-1}{2}}\}$ gera $\mathcal{U}(\mathbf{Z}[\theta])$ e $\mathcal{U}(\mathbb{Z}_p) = \langle \overline{2} \rangle$ ou $\mathcal{U}(\mathbb{Z}_p)^2 = \langle \overline{2} \rangle$ e $\overline{-1} \notin \mathcal{U}(\mathbb{Z}_p)^2$, que para $p = 7, 11, 13, 19, 23, 29, 37, 53, 59, 61$ e 67 sabemos que são verificadas. Enquanto para outros valores de p não sabemos se as nossas hipóteses são válidas.

Com o intuito de estender tais ideias, encontramos um conjunto gerador para $\mathcal{U}(\mathbb{Z}(C_{2p} \times C_2)$ e $\mathcal{U}(\mathbb{Z}(C_{2p} \times C_2 \times C_2)$ onde p satisfaz as mesmas condições anteriores acrescidas de uma nova hipótese.

Finalmente, com o auxílio dos resultados anteriores, apresentamos um conjunto gerador das unidades centrais do anel de grupo $\mathbb{Z}(C_p \times Q_8)$, onde Q_8 representa o grupo dos quatérnios, ou seja, $Q_8 := \langle a, b : a^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1} \rangle$.

Palavras Chaves: Anéis de Grupo sobre os Inteiros, Unidades de Anéis de Grupo, Unidades Centrais de Anéis de Grupo Integral, Grupo dos Quatérnios.

Abstract

Units of $\mathbb{Z}C_{2p}$ and applications

Let p be an odd prime integer, θ be a p^{th} primitive root of unity, C_n be the cyclic group of order n, and $\mathcal{U}(\mathbb{Z}G)$ the units of the Integral Group Ring $\mathbb{Z}G$. Consider $u_i := 1+\theta+\theta^2+\ldots+\theta^{i-1}$ for $2 \leq i \leq \dfrac{p+1}{2}$. In our study we describe explicitly the generator set of $\mathcal{U}(\mathbb{Z}C_{2p})$, where p is such that $S_\theta := \{-1, \theta, u_2, \ldots, u_{\frac{p-1}{2}}\}$ generates $\mathcal{U}(\mathbb{Z}[\theta])$ and $\mathcal{U}(\mathbb{Z}_p)$ is such that $\mathcal{U}(\mathbb{Z}_p) = \langle \overline{2} \rangle$ or $\mathcal{U}(\mathbb{Z}_p)^2 = \langle \overline{2} \rangle$ and $\overline{-1} \notin \mathcal{U}(\mathbb{Z}_p)^2$, which occurs for $p = 7, 11, 13, 19, 23, 29, 37, 53, 59, 61$, and 67. For another values of p we don't know if such conditions hold.

In addition, under suitable hypotheses, we extend these ideas and build a generator set of $\mathcal{U}(\mathbb{Z}(C_{2p} \times C_2))$ and $\mathcal{U}(\mathbb{Z}(C_{2p} \times C_2 \times C_2))$.

Besides that, using the previous results, we exhibit a generator set for the central units of the group ring $\mathbb{Z}(C_p \times Q_8)$ where Q_8 represents the quaternion group.

Keywords: Group Rings over Integers, Units of Group Rings, Central Units of Integral Group Rings, Quaternion Group.

Índice

Introdução

Dado um grupo G e um anel R define-se um anel de grupo, representado por RG, como o conjunto de todas as somas formais quase nulas da seguinte forma: $\sum_{g\in G} a_g g$, com $a_g \in R$, munidos das seguintes operações:

(i) $+ : \sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G} (a_g + b_g) g;$

(ii) $\cdot : \left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) := \left(\sum_{g\in G}\sum_{h\in G} (a_g b_h) gh\right).$

Podemos também definir a multiplicação de elementos de RG por elementos do anel R :
$\cdot : \lambda.\left(\sum_{g\in G} a_g g\right) := \sum_{g\in G} (\lambda a_g) g.$

Com esta operação RG admite uma estrutura de R-módulo.

Acredita-se que este assunto começou a ser estudado implicitamente por A. Cayley em [5], e mais tarde explicitamente por T. Molien em 1897, e veio a adquirir enorme relevância a partir dos trabalhos de E. Noether, R. Brauer e I. Schur, que estabeleceram a relação que existe entre a teoria de estrutura de anéis e álgebras e as representações de grupos finitos.

Neste trabalho estudaremos o caso $\mathbb{Z}G$, conhecido como o anel de grupo integral. Descrever o grupo das unidades $\mathcal{U}(\mathbb{Z}G)$ para um grupo finito G é um problema clássico e difícil. A maioria das descrições de $\mathcal{U}(\mathbb{Z}G)$ na literatura matemática, ou dão uma descrição explícita das unidades, ou a estrutura geral de $\mathcal{U}(\mathbb{Z}G)$, ou ainda um subgrupo de $\mathcal{U}(\mathbb{Z}G)$ de índice finito. No caso em que G é um grupo finito, sabemos que o centro $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ de $\mathcal{U}(\mathbb{Z}G)$ é um grupo abeliano finitamente gerado, e portanto, deve ser da forma $T \times A$, onde T é um grupo abeliano finito e A é um subgrupo abeliano livre de $\mathcal{U}(\mathbb{Z}G)$. Berman em [4] e Higman em [9] provaram que $T = \pm\mathcal{Z}(G)$.

É claro que tal conjunto A não é unicamente determinado e, para determinar A, é suficiente determinar uma $\mathbb{Z}$ - base S para o $\mathbb{Z}$ - módulo livre A. Como a operação em A é a multiplicação, dizemos que S é um grupo multiplicativamente independente. A cardinalidade de S, ou seja, o posto de A é conhecido e é precisamente a diferença entre o número de componentes simples da álgebra $\mathbb{R}G$ e o número de componentes simples da álgebra $\mathbb{Q}G$. No entanto, em apenas alguns casos é possível determinar tal conjunto S.

Para alguns grupos específicos, pesquisadores já determinaram tais conjuntos. Aleev em [1] e Li & Parmenter em [16] determinaram o conjunto S para os subgrupos alternados A_5 e, no mesmo artigo, Aleev determinou tal conjunto para A_6. Aleev & Panina em [2] descreveram tal conjunto para os grupos cíclicos de ordem 7 e 9. Para grupos cíclicos de ordem 5 e 8 Polcino e Sehgal exibiram tais conjuntos.

Em outros artigos determinaram conjuntos multiplicativamente independentes que geram subgrupos de índice finito de $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. Entre estes artigos destacamos os seguintes: Jespers, Parmenter & Sehgal em [13], Polcino & Sehgal em [20] encontraram tal conjunto para grupos nilpotentes, Ferraz & Simón em [7] acharam tal conjunto para um tipo especial de grupo metacíclico, Hoechsmann em [10] e em [11] e Hoechsmann & Sehgal em [12] obtiveram alguns resultados quando o grupo é abeliano.

Bass fez um trabalho excepcional para anéis de grupos abelianos finitos. Para enunciar tal resultado introduzem-se as unidades cíclicas de Bass. Sejam g um elemento de um grupo abeliano G de ordem n e i um inteiro tal que $\mathrm{mdc}(i,n)=1$ com $1<i<n-1$. Sejam $\hat{g}=1+g+g^2+\ldots+g^{n-1}$, ϕ a função de Euler e $k=\dfrac{i^{\phi(n)}-1}{n}$. Define - se a unidade cíclica de Bass como:

$$b_i(g) := (1+g+g^2+\ldots+g^{i-1})^{\phi(n)} - k\hat{g}.$$

Bass em [3] provou que, se G é um grupo abeliano finito, então o grupo gerado por todas as unidades cíclicas de Bass de $\mathcal{U}(\mathbb{Z}G)$ é um subgrupo de índice finito de $\mathcal{U}(\mathbb{Z}G)$. Mais ainda, neste artigo Bass mostrou que se $G := \langle g\rangle$ é um grupo de cíclico de ordem prima ímpar p então o conjunto:

$$S_B := \left\{ b_i(g) : 2 \leq i \leq \frac{p-1}{2} \right\}$$

é um grupo multiplicativamente independente que gera um subgrupo de índice finito em $\mathcal{U}(\mathbb{Z}G)$.

Contudo este conjunto nunca gera um complemento para C_p em $\mathcal{U}_1(\mathbb{Z}C_p)$. Posteriormente Ferraz construiu um conjunto multiplicativamente independente que gera um complemento para C_p em $\mathcal{U}_1(\mathbb{Z}C_p)$, desde que satisfeita uma condição proveniente da teoria dos números. Para enunciar tal condição vamos definir alguns conceitos. Considere θ uma raiz p-ésima da unidade e $\mu_i = \sum_{j=0}^{i-1} \theta^j$. A condição é a seguinte: o conjunto $S_\theta := \{-1, \theta, \mu_2, \cdots, \mu_{\frac{p-3}{2}}\}$ deve gerar as unidades de $\mathbb{Z}[\theta]$.

No caso em que p é um primo ímpar tal que $5 \leq p \leq 67$ sabemos que esta condição é verificada. Já para $p \geq 68$ não sabemos se a condição é satisfeita. Como para determinar as unidades de $\mathbb{Z}C_{2p}$ fazemos uso das unidades de $\mathbb{Z}C_p$ então esta condição está atrelada aos nossos resultados.

A tese está dividida da seguinte forma, no Capítulo 1, nós apresentamos definições e resultados que são conhecidos da teoria de anéis, grupos e de anéis de grupos. Além disso, fixaremos as notações adotadas ao longo deste trabalho.

No Capítulo 2, fomos capazes de encontrar um conjunto multiplicativamente independente que gera o grupo de unidades do anel de grupo integral $\mathbb{Z}C_{2p}$. Em uma primeira tentativa, utilizando as unidades de $\mathbb{Z}C_p$ obtidas por Ferraz, conseguimos determinar as unidades de $\mathbb{Z}C_{2p}$. O conjunto gerador do grupo das unidades de $\mathbb{Z}C_{2p}$ está vinculado ao conhecimento do conjunto das unidades de $\mathbb{Z}C_p$ e a caracterização do núcleo do homomorfismo $\rho : \mathcal{U}(\mathbb{Z}C_p) \to \mathcal{U}(\mathbb{Z}_2C_p)$ definido por $\rho\left(\sum_{j=0}^{p-1} a_j g^j\right) = \sum_{j=0}^{p-1} \overline{a_j} g^j$.

Primeiramente, trabalhamos com as unidades para as quais $\overline{2}$ gera as unidades de $\mathbb{Z}_p$, e depois, passamos a considerar unidades tais que $\overline{2}$ gera $\mathcal{U}(\mathbb{Z}_p)^2$ e $-\overline{1}$ não pertence a $\mathcal{U}(\mathbb{Z}_p)^2$. No entanto, observamos através dos exemplos, que as contas ficavam mais difíceis conforme o p aumentava. Assim, na tentativa de minimizar estas contas, modificamos as unidades descritas por Ferraz em [6]. Tais unidades serão vistas com detalhes no Capítulo 2.

Nossa próxima intenção era generalizar o resultado obtido para o anel de grupo $\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}})$. Considere o homomorfismo de grupos $\phi : \mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}}) \to \mathbb{Z}_2(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}})$ definido da maneira usual e defina $\Phi = \phi|_{\mathcal{U}(\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}}))}$. Para se encontrar um conjunto gerador para $\mathcal{U}(\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}}))$ devemos conhecer as unidades de $\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}})$ e caracterizar o núcleo do homomorfismo Φ. Entretanto, descrever tal núcleo não é uma tarefa fácil, e por este motivo, não foi possível generalizar nosso resultado como gostaríamos.

No Capítulo 3, utilizando os resultados do Capítulo 2, conseguimos estender nosso resultado para o anel de grupo $\mathbb{Z}(C_{2p} \times C_2)$. Tal extensão depende diretamente do conjunto $\{\phi(\beta_1), \cdots, \phi(\beta_{\frac{p-3}{2}})\}$ ser linearmente independente. Tal hipótese resolve o problema de descrever o núcleo do homomorfismo $\Phi : \mathcal{U}(\mathbb{Z}C_{2p}) \to \mathcal{U}(\mathbb{Z}_2C_{2p})$.

No Capítulo 4, determinamos o núcleo da função Φ para o caso em que $n = 2$, e com isso, conseguimos exibir um conjunto de geradores para as unidades do anel de grupo integral $\mathbb{Z}(C_{2p} \times C_2 \times C_2)$. Além disso, descobrimos que a existência ou não de um idempotente não trivial no conjunto da imagem de ϕ modifica o núcleo de Φ. Com o auxílio destes núcleos encontrados, conseguimos também descrever um grupo gerador para as unidades centrais do anel de grupo $\mathbb{Z}(C_p \times Q_8)$, onde Q_8 representa o grupo dos quatérnios.

No caso em que tal idempotente não exista, estamos generalizando os resultados obtidos, e, em nossos trabalhos futuros, pretendemos descrever o conjunto gerador de suas unidades. Porém, no caso em que este idempotente existe, ainda precisamos trabalhar um pouco mais, uma vez que, os conjuntos tornam-se mais complexos do que inicialmente pensavamos.

Capítulo 1

Fundamentação Teórica

O propósito principal deste Capítulo é introduzir alguns conceitos que utilizaremos ao longo desta tese, enfatizando a definição de unidades de anéis de grupos, objeto de nossos estudos. Apresentaremos também as notações que serão utilizadas no decorrer do trabalho.

Em 1843 quando se descobriu a álgebra dos quatérnios, muitos matemáticos se aventuraram a estudar estruturas similares levando ao desenvolvimento da álgebra abstrata. Destacaremos algumas delas que utilizaremos ao longo desta tese.

1.1 Grupos

Definição 1. *Um* ***grupo*** *consiste em um conjunto não vazio G munido de uma operação binária $\mu : G \times G \to G$ definida por $\mu((g,h)) = gh$ que satisfaz os seguintes axiomas:*

(G1) $(gh)m = g(hm)$

(G2) Existe $e \in G$ *tal que* $eg = g = ge$ *para todo* $g \in G$

(G3) Para todo $g \in G$ *existe* $h \in G$ *tal que* $hg = e = gh$

Observe que enquanto o primeiro axioma garante que a operação μ é associativa, o segundo assegura a existência do elemento neutro, que no caso multiplicativo é chamado de identidade e representado por 1. Já o terceiro axioma afirma que todo elemento do grupo G tem inverso, que no caso multiplicativo é representado por g^{-1}.

Alguns grupos possuem uma propriedade adicional: a **comutatividade**, isto é, $gh = hg$, para todo $g, h \in G$. Este grupo especial é chamado de **grupo abeliano**.

Salvo indicações contrárias, todos os grupos aqui considerados serão multiplicativos.

Definição 2. *Um subconjunto H de um grupo G é dito um* ***subgrupo*** *de G se satisfaz:*

(S1) H é não vazio

(S2) Para todo $h, s \in H$ tem-se que $hs \in H$

(S3) Se $h \in H$ então $h^{-1} \in H$ para todo $h \in H$

Utilizamos a seguinte notação $H \leq G$ para representar que H é subgrupo de G.

Seja μ a operação binária que dá a G sua estrutura de grupo. A condição (S2) implica que podemos considerar a restrição desta operação sobre $H \times H$, enquanto (S1) garante que existe ao menos um elemento h em H e (S3) garante que $h^{-1} \in H$. Das condições (S1), (S2) e (S3) obtém-se que $1 \in H$.

Definição 3. *Seja S um subconjunto não vazio de um grupo G. Define-se o* ***subgrupo gerado por S*** *como $\langle S \rangle := \bigcap \{H : H \leq G \text{ e } S \subseteq H\}$.*

Perceba que $\langle S \rangle$ é o menor subgrupo de G que contém o subconjunto S. A fim de caracterizar os elementos de S pode-se escrever o subgrupo gerado por S como $\langle S \rangle = \{s_1 s_2 \cdots s_n : s_j \in S \text{ ou } s_j^{-1} \in S \ \forall\, 1 \leq j \leq n \text{ e } n \geq 1\}$.

Proposição 1.1.1. *Seja G um grupo e considere $g \in G$. Então:*

(1) $\langle g \rangle = \{\cdots, g^{-2}, g^{-1}, 1, g, g^2, \cdots\}$

(2) Se $g^n = 1$ para algum $n \geq 2$ e $\{1, g, g^2, \cdots, g^{n-1}\}$ forem distintos então $\langle g \rangle = \{1, g, g^2, \cdots, g^{n-1}\}$ e, além disso, $g^i = g^j$ se, e somente se, $i \equiv j \ (mod\, n)$.

A demonstração desta Proposição pode ser encontrada em [18] na página 16.

Definição 4. *Um grupo G é* ***cíclico*** *quando ele pode ser gerado por um único elemento,ou seja, quando $G = \langle g \rangle$ para algum $g \in G$. Quando $g^n = 1$ representamos $G = C_n$.*

Se um grupo G tem um número finito de elementos, então ele é chamado de **grupo finito** . Neste caso, $|G|$ representa o número de elementos do grupo G e é chamado de **ordem** de G. Diz-se que em elemento $g \in G$ é de **ordem finita** se o grupo $\langle g \rangle$ é finito. Representaremos a **ordem** de g como $\mathbf{ord}(g) = |\langle g \rangle|$.

Sabemos que $\langle g \rangle = \{\cdots, g^{-2}, g^{-1}, 1, g, g^2, \cdots\}$. Se $\mathbf{ord}(g) = n$ da Proposição 1.1.1 tem-se que n representa o menor inteiro positivo tal que $g^n = 1$ e então $\langle g \rangle = \{1, g, g^2, \cdots, g^{n-1}\}$. Quando este inteiro não existe dizemos que g tem **ordem infinita**.

Definição 5. *Seja G um grupo abeliano. Se todo elemento de G tem ordem finita então G é chamado de **grupo de torção**. Em contrapartida, G é dito um **grupo livre de torção** se todos os seus elementos, exceto o 1, têm ordem infinita.*

Definição 6. *Sejam G um grupo e H um subgrupo de G. Considere $g \in G$ e os subconjuntos da forma $gH := \{gh : h \in H\}$ e $Hg := \{hg : h \in H\}$. Tais conjuntos são chamados de **classe lateral** à esquerda e à direita de H determinados por g respectivamente.*

Definição 7. *A cardinalidade do conjunto das classes laterais à esquerda ou à direita é o índice de H em G e será representado por $[G : H]$*

Considere G um grupo e seja H um subgrupo de G. Queremos verificar se a operação de G induz de maneira natural uma operação sobre o conjunto das classes laterais à esquerda de H em G, ou seja, se a operação $(xH, yH) \mapsto xyH$ é bem definida. Para que tal operação seja bem definida precisamos definir um novo tipo de subgrupo.

Definição 8. *Um subgrupo H de um grupo G diz-se **normal** em G e representamos $H \lhd G$ se uma das condições equivalentes for satisfeita*

(H1) $Hg = gH$ *para todo* $g \in G$

(H2) $gHg^{-1} = H$ *para todo* $g \in G$

(H3) $g^{-1}Hg = H$ *para todo* $g \in G$

Quando H é um subgrupo normal do grupo G então a operação $(xH, yH) \mapsto xyH$ está bem definida e pode-se formular o seguinte conceito.

Definição 9. *Sejam G um grupo e H um subgrupo normal de G. O grupo das classes laterais com a operação induzida de G é o **grupo quociente** de G por H e será representado por $\dfrac{G}{H}$.*

Definimos agora um conceito fundamental na Teoria de Grupos.

Definição 10. *Sejam $(G, .)$ e $(H, *)$ dois grupos. Uma função*

$$\begin{array}{ccc} G & \stackrel{f}{\to} & H \\ g & \longmapsto & f(h) \end{array}$$

*satisfazendo $f(g_1.g_2) = f(g_1) * f(g_2)$ é chamada de **homomorfismo de grupos**. Se o homomorfismo for injetor dizemos que f é um **monomorfismo**, se f for sobrejetora o homomorfismo é chamado de **epimorfismo** e se este for uma bijeção diz-se que f é um **isomorfismo** entre G e H.*

Os subgrupos definidos abaixo são de grande importância.

Definição 11. *Sejam* $(G, .)$ *e* $(H, *)$ *grupos e considere o homomorfismo de grupos* $f : G \to H$*. O subconjunto* $Ker(f) := \{g \in G : f(g) = 1_H\}$*, onde* 1_H *representa o elemento neutro de* H *é chamado de* ***núcleo*** *de* f*.*

Definição 12. *Sejam* $(G, .)$ *e* $(H, *)$ *grupos e considere o homomorfismo de grupos* $f : G \to H$*. O subconjunto* $Im(f) := \{h \in H : \text{ existe } g \in G \text{ tal que } f(g) = h\}$*, é chamado de* ***imagem*** *de* f*.*

Teorema 1.1.1. *Sejam* $(G, .)$ *e* $(H, *)$ *grupos e seja* $f : G \to H$ *um homomorfismo de grupos. Então*

(i) $f(1_G) = 1_H$ *e* $f(g^{-1}) = f(g)^{-1}$ *para todo* $g \in G$

(ii) Se K *é um subgrupo de* G *então* $f(K) = \{f(k) : k \in K\}$ *é subgrupo de* H*.*

(iii) Se M *é um subgrupo de* H *então* $f^{-1}(M) := \{g \in G : f(g) \in M\}$ *é subgrupo de* G*. Em particular, se* $M = 1_H$ *então* $Ker(f)$ *é um subgrupo de* G*.*

(iv) $f(g) = f(h)$ *se, e somente se,* $gh^{-1} \in Ker(f)$*. Em particular,* f *é injetora se, e só se,* $Ker(f) = \{1_H\}$*.*

(v) Se M *é um subgrupo normal de* H *então* $f^{-1}(M)$ *é um subgrupo normal de* G*. Em particular,* $Ker(f)$ *é normal em* G*.*

Esta demonstração é um exercício fácil, conforme Martin diz em [18].

Em seguida enunciaremos um dos principais teoremas relacionados aos isomorfismos de grupos.

Teorema 1.1.2 (Teorema do Isomorfimo)**.** *Seja* $f : (G, .) \to (H, *)$ *um homomorfismo de grupos. Então a função* $\overline{f} : \frac{G}{Ker(f)} \to Im(f)$ *é um isomorfismo de grupos.*

A prova deste teorema pode ser encontrada em [8] na página 149.

Definição 13. *Sejam* H *e* K *dois subgrupos normais de um grupo* G*, tais que* $H \bigcap K = 1_G$ *e* $G = HK$*, dizemos que* G *é o* ***produto direto interno*** *de* H *e* K*.*

A definição acima implica que se $g \in G$ então g se escreve de maneira única como hk para algum $h \in H$ e algum $k \in K$.

Definição 14. *Sejam* $G_1, \cdots, G_n$ *grupos. O* ***produto direto externo*** *de* $G_1, \cdots G_n$*, representado por* $G_1 \times \cdots \times G_n$ *é definido como:*

$$G_1 \times \cdots \times G_n := \{(g_1, \cdots, g_n) : g_i \in Gi\}$$

com o produto definido componente a componente.

A seguir apresentaremos um resultado que nos dá condições para que um grupo G seja isomorfo ao produto direto de grupos $G_1, G_2, \cdots, G_n$.

Teorema 1.1.3. *Sejam $G, G_1, G_2, \cdots, G_n$ grupos. Então o grupo G é isomorfo ao grupo $G_1 \times G_2 \times \cdots \times G_n$ se, e somente se, G possui subgrupos $H_1 \cong G_1, \cdots, H_n \cong G_n$ tais que*

(i) $G = H_1 H_2 \cdots H_n$

(ii) H_i *é um subgrupo normal de* G *para todo* $1 \leq i \leq n$

(iii) $H_i \bigcap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{1\}$ *para todo* $1 \leq i \leq n$*.*

A demonstração deste resultado pode ser encontrada em [8] na página 180.

Vamos destacar agora o conjunto dos elementos $g \in G$ que comutam com todos os elementos do grupo.

Definição 15. *Seja G um grupo. Considere o conjunto*

$$\mathcal{Z}(G) := \{g \in G : hg = gh, \; \forall \; h \in G\}$$

*Tal conjunto é chamado de **centro** de G.*

Vamos nos concentrar agora nos grupos abelianos.

Definição 16. *Um grupo abeliano G é **finitamente gerado** se existirem $g_1, g_2, \cdots, g_n \in G$ tais que para todo $g \in G$ tem-se que $g = g_1^{r_1} g_2^{r_2} \cdots g_n^{r_n}$ com $r_i \in \mathbb{Z}$, para todo i e representamos por $G := \langle g_1, g_2, \cdots, g_n \rangle$.*

Ressalto aqui que estamos fazendo uso da notação multiplicativa.

Definição 17. *Dizemos que os elementos $g_1, g_2, \cdots g_k$ de G são **multiplicativamente independentes** sobre $\mathbb{Z}$ se a equação $g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k} = 1$ com $n_j \in \mathbb{Z}$ para todo $1 \leq j \leq k$ tiver solução apenas quando todos os n_j forem nulos.*

Observe que um conjunto $\{g_1, g_2, \cdots, g_k\}$ de elementos multiplicativamente independentes de G e que gera G é chamado de **base** de G.

Definição 18. *Um grupo abeliano que possui uma base com n elementos é chamado de **grupo abeliano livre de posto n**.*

Lema 1.1.1. *Seja G um grupo abeliano livre de posto n e seja H um subgrupo de G. Então $\dfrac{G}{H}$ é um grupo finito, se e somente se, H tiver posto n. Neste caso, se $\{g_1, g_2, \cdots, g_n\}$ e $\{h_1, h_2, \cdots, h_n\}$ forem bases de G e H respectivamente com $h_i = \prod_{j=0}^{n} g_j^{a_{ij}}$ para todo $1 \leq i \leq n$ então $[G : H] = |det(a_{ij})|$.*

A demonstração deste resultado pode ser encontrada em [18] na página 80.

1.2 Anéis

Definição 19. *Um **anel** é um conjunto não vazio R munido de duas operaçoẽs binárias, que representaremos por $+$ e $.$ e chamaremos de adição e multiplicação respectivamente, tais que para todos $r, s, t \in R$*

(A1) $r + (s + t) = (r + s) + t$

(A2) Existe um elemento $0 \in R$ *tal que* $r + 0 = 0 + r = r$

(A3) Existe um elemento $-r \in R$ *tal que* $r + (-r) = (-r) + r = 0$

(A4) $r + s = s + r$

(A5) $r.(s.t) = (r.s).t$

(A6) $r.(s + t) = r.s + r.t$

(A7) $(r + s).t = r.t + s.t$

Se, além destas condições, tal conjunto ainda satisfizer $r.s = s.r$ o anel é dito **comutativo**. Um anel R que contém um elemento $1 \neq 0$ tal que, para todo $r \in R$, $1.r = r.1 = r$ é chamado de **anel com unidade**. Além disso, um anel com unidade é chamado de **domínio** se para todos $r, s \in R$ tais que $r.s = 0$ tem-se que ou $r = 0$ ou $s = 0$. Elementos não nulos $r, s \in R$ tais que $r.s = 0$ são chamados de **divisores de zeros**. Portanto um domínio é um anel com unidade sem divisores de zeros. Definiremos agora o conjuntos dos elementos inversíveis de um anel.

Definição 20. *Seja R um anel. Um elemento r de R é chamado de inversível se existe um elemento, que denotaremos por $r^{-1} \in R$ e chamaremos de inverso, tal que $r \cdot 1 = 1 \cdot r = r$. O conjunto:*

$$\mathcal{U}(R) := \{r \in R : \exists s \in R \ \ \textit{tal que} \ \ rs = 1 = sr\}$$

*é chamado de grupo multiplicativo **das unidades**.*

De maneira análoga ao conceito de homomorfismo de grupos pode-se definir o conceito de homomorfismo de anéis.

Definição 21. *Seja R um anel. Um* ***homomorfismo de anéis*** *é uma aplicação $f : (A, +_A, ._A) \to (B, +_B, ._B)$ que satisfaz:*

(1) $f(a_1 +_A a_2) := f(a_1) +_B f(a_2)$

(2) $f(a_1 ._A a_2) := f(a_1) ._B f(a_2)$

para todos $a_1, a_2 \in A$

Um homomorfismo de anéis $f : R \to S$ é chamado de **monomorfismo** se f for injetor, isto é, se $f(r_1) = f(r_2)$ implica que $r_1 = r_2$, para todo $r_1, r_2 \in R$. Se f for sobrejetor, ou seja, $\mathrm{Im}(f) = S$ o homomorfismo é chamado de **epimorfismo**. Já se f for uma bijeção o homomorfismo é chamado de **epimorfismo**. Neste caso, dizemos que R e S são **isomorfos** e representamos por $R \cong S$. Um homomorfismo do anel R nele mesmo é chamado de **endomorfismo**. Se, além disso, ele for também um isomorfismo então será chamado de **automorfismo**.

A seguir, introduziremos o conceito de involução, uma aplicação de grande importância e utilidade na Teoria de Anéis, bem como na Teoria de Grupos.

Definição 22. *Seja R um anel. Uma* ***involução*** *$* : R \to R$ é uma bijeção que satisfaz:*

(1) $(r + s)^* := r^* + s^*$,

(2) $(rs)^* := s^* r^*$,

(3) $(r^*)^* := r$,

para todos $r, s \in R$

Observe que a involução nada mais é do que um anti-automorfismo de ordem 2.

Exemplo 1. *Considere $^* : \mathbb{C} \to \mathbb{C}$ definida como $z^* := \overline{z}$, o conjugado de z. Tal função é uma involução.*

De fato, temos que para todo $z_1 = a_1 + ib_1, z_2 = a_2 + ib_2 \in \mathbb{C}$:
$(z_1 + z_2)^* = \overline{z_1 + z_2} = \overline{(a_1 + a_2) + i(b_1 + b_2)} = (a_1 + a_2) - i(b_1 + b_2) = (a_1 - ib_1) + (a_2 - ib_2) = \overline{z_1} + \overline{z_2}$
$(z_1 z_2)^* = \overline{z_1 z_2} = \overline{(a_1 a_2 - b_1 b_1) + i(a_1 b_2 + a_2 b_1)} = (a_1 a_2 - b_1 b_1) - i(a_1 b_2 + a_2 b_1) = a_1(a_2 - ib_2) + -ib_1(a_2 - ib_2) = (a_1 - ib_1)(a_2 - ib_2) = \overline{(a_1 + ib_1)(a_2 + ib_2)} = \overline{z_1 z_2}$
$(z_1^*)^* = (\overline{z_1})^* = (a_1 - ib_1)^* = \overline{a_1 - ib_1} = a_1 + ib_1 = z_1$
logo * é um involução.

Exemplo 2. *Considere* $^*: M_n(K) \to M_n(K)$ *definida como* $A^* := A^t$, *a transporta da matriz* A. *Tal função é uma involução.*

O conceito de módulo, introduzido a seguir, foi apresentado implicitamente nos trabalhos de Richard Dedekind sobre Teoria dos Números.

Definição 23. *Seja* R *um anel com unidade. Um grupo abeliano* M *é chamado de* R***-módulo*** *à esquerda se para cada* r *de* R *e para cada elemento* m *de* M *o produto* $rm \in M$ *satisfaz*

1. $(r+s)m = rm + sm$, *para todos* $r, s \in R$ *e, para todo* $m \in M$;
2. $r(m_1 + m_2) = rm_1 + rm_2$, *para todo* $r \in R$ *e, para todos* $m_1, m_2 \in M$;
3. $r(sm) = (rs)m$, *para todos* $r, s, \in R$ *e, para todo* $m \in M$;
4. $1 \cdot m = m \cdot 1 = m$, *para todo* $m \in M$;

1.3 Anéis de Grupos

Nesta seção, iremos apresentar notações e propriedades clássicas dos anéis de grupos. Iniciaremos com a definição de anél de grupo.

Definição 24. *Sejam* R *um anel com unidade e* G *um grupo. Define-se um* ***anel de grupo***, *representado por* RG, *como o conjunto*

$$RG := \left\{ \sum_{g \in G} a_g g : a_g \in R \text{ e } a_g \neq 0 \textit{ para apenas um número finito de } g \right\}$$

Definimos em RG *as seguintes operações:*

(i) $+ : \sum_{g \in G} a_g g + \sum_{g \in G} b_g g := \sum_{g \in G} (a_g + b_g) g;$

(ii) $\cdot : \left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{h \in G} b_h h \right) := \left(\sum_{g \in G} \sum_{h \in G} (a_g b_h) gh \right).$

Podemos também definir a multiplicação de elementos de RG *por elementos do anel* R :

$\cdot : \lambda \cdot \left(\sum_{g \in G} a_g g \right) := \sum_{g \in G} (\lambda a_g) g,$

fazendo com que RG *admita uma estrutura de* R*-módulo.*

Nesta tese, estaremos sempre trabalhando com o chamado **anel de grupo integral**, ou seja, o anel R considerado será o anel dos inteiros $\mathbb{Z}$. A seguir definimos uma aplicação muito útil e importante na área de anéis de grupos.

Definição 25. *Sejam R um anel e G um grupo. Considere o anel de grupo associado a eles RG. O homomorfismo de anéis: $\epsilon : RG \to R$ definido por $\epsilon\left(\sum_{g\in G} a_g g\right) := \sum_{g\in G} a_g$ é chamado de* ***função de aumento*** *de RG. Seu núcleo, representado por, $\Delta(G)$ é chamado de* ***ideal de aumento*** *de RG.*

Observe que, um elemento $\alpha = \sum_{g\in G} a_g g \in \Delta(G)$ se, e somente se, $\epsilon(\alpha) = \sum_{g\in G} a_g = 0$. Portanto, todo elemento $\alpha \in \Delta(G)$ pode ser reescrito como $\alpha := \sum_{g\in G} a_g(g-1)$.

Logo, $\Delta(G) \subseteq \quad \langle g-1 : g \in G\rangle$, onde $\langle g-1 : g \in G\rangle$ denota o R-módulo livre gerado por $\{g-1 : g \in G\}$.

Por outro lado, temos que $\langle g-1 : g \in G\rangle \quad \subseteq \Delta(G)$ uma vez que $\epsilon(g-1) = 0$. Desta forma, podemos caracterizar o ideal de aumento como R- módulo livre cuja base é $\{g-1 : g \in G,\ g \neq 1\}$.

Outra aplicação bem conhecida e de grande utilidade é a involução. Restringiremos-nos aqui apenas a involução clássica, que está definida a seguir.

Definição 26. *Seja RG um anel de grupo. Considere a função $* : RG \to RG$ definida por $\left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1}$. Tal função é chamada de* ***involução clássica****.*

O resultado a seguir foi bastante utilizado no trabalho e por tal razão encontra-se aqui enunciado e demonstrado.

Proposição 1.3.1. *Seja R um anel comutativo com unidade e sejam G e H grupos. Então $R(G \times H) \cong (RG)H$.*

Demonstração:

Considere

$$\begin{array}{ccc} R(G\times H) & \stackrel{\phi}{\to} & (RG)H \\ \left(\sum_{\substack{g\in G\\ h\in H}} a_{(g,h)}(g,h)\right) & \longmapsto & \sum_{h\in H}\left(a_{(g,h)}g\right)h \end{array}$$

Primeiramente vejamos que ϕ está bem definida.

Sejam $\alpha = \sum_{\substack{g\in G\\ h\in H}} a_{(g,h)}(g,h)$ e $\beta = \sum_{\substack{g\in G\\ h\in H}} a_{(g,h)}(g,h) \in R(G\times H)$, tais que $\alpha = \beta$, então, para todo $g \in G$ e, para todo $h \in H$ $a_{(g,h)} = b_{(g,h)}$. Assim,

$\phi(\alpha) = \sum_{h\in H}\left(\sum_{g\in G} a_{(g,h)}g\right)h = \sum_{h\in H}\left(\sum_{g\in G} b_{(g,h)}g\right)h = \phi(\beta).$

Logo, a função está bem definida.

Vamos mostrar agora que ϕ é um homomorfismo de anéis. Sejam $\alpha = \sum_{\substack{g\in G\\ h\in H}} a_{(g,h)}(g,h)$ e $\beta = \sum_{\substack{g\in G\\ h\in H}} b_{(g,h)}(g,h) \in R(G\times H)$, então $\alpha+\beta = \sum_{\substack{g\in G\\ h\in H}}(a_{(g,h)} + b_{(g,h)})(g,h)$ e $\alpha\beta = \sum_{\substack{g_1,g_2\in G\\ h_1,h_2\in H}} a_{(g_1,h_1)}b_{(g_2,h_2)}(g_1g_2,h_1h_2)$. Logo,

$\phi(\alpha+\beta) = \sum_{h\in H}\left(\sum_{g\in G}(a_{(g,h)}+b_{(g,h)})g\right)h = \sum_{h\in H}\left(\sum_{g\in G} a_{(g,h)}g\right)h + \sum_{h\in H}\left(\sum_{g\in G} b_{(g,h)}g\right)h$
$= \phi(\alpha)+\phi(\beta).$

Sabe-se que,

$$\phi(\alpha\beta) = \sum_{h_1,h_2\in H}\left(\sum_{g_1,g_2\in G}(a_{(g_1,h_1)}b_{(g_2,h_2)})g_1g_2\right)h_1h_2$$

Por outro lado,

$$\phi(\alpha)\phi(\beta) = \left[\sum_{h\in H}\left(\sum_{g\in G} a_{(g,h)}g\right)h\right]\left[\sum_{g\in G}\sum_{h\in H}\left(b_{(g,h)}g\right)h\right],$$

ou seja,

$$\phi(\alpha)\phi(\beta) = \sum_{h_1,h_2\in H}\left(\sum_{g_1,g_2\in G}(a_{(g_1,h_2)}b_{(g_1,h_2)})g_1g_2\right)h_1h_2$$

e, portanto, $\phi(\alpha\beta)=\phi(\alpha)\phi(\beta)$. Logo, ϕ é um homomorfismo de anéis.

Demonstremos que ϕ é injetora. Seja $\alpha = \sum_{\substack{g\in G\\ h\in H}} a_{(g,h)}(g,h) \in R(G\times H)$, tal que $\phi(\alpha)=0$, então $\sum_{h\in H}\left(\sum_{g\in G} a_{(g,h)}g\right)h = 0$. Como H é uma RG - base de $(RG)H$, então $\sum_{g\in G} a_{(g,h)}g = 0$, para todo $h\in H$. Mas, G é uma R - base de RG, então $a_{(g,h)} = 0$, para todo $g\in G$. Logo, $\alpha = 0$ e, portanto, ϕ é injetora.

Verifiquemos que ϕ é sobrejetora. Seja $y\in(RG)H$. Como H é uma RG - base para $(RG)H$, então $y = \sum_{h\in H}\alpha_h h$. Como G é uma R - base para RG, para cada $h\in H$ tem-se que $\alpha_h = \sum_{g\in G} a_{(g,h)}g$.

Considere $x = \sum_{\substack{g \in G \\ h \in H}} a_{(g,h)}(g,h) \in R(G \times H)$, então $\phi(x) = \displaystyle\sum_{h \in H} \left(\sum_{g \in G} a_{(g,h)} g \right) h = \sum_{h \in H} \alpha_h h = y$. Portanto, ϕ é sobrejetora.

Desta forma, $R(G \times H) \cong (RG)H$.

■

Definição 27. *Sejam G um grupo, R um anel com unidade comutativo e $\{C_i\}_{i \in I}$ o conjunto das classes de conjugação de G que contêm apenas um número finito de elementos. Para todo $i \in I$ considere $\gamma_i = \widehat{C_i} = \displaystyle\sum_{x \in C_i} x$. Estes elementos são chamados de* ***somas de classe*** *de G sobre R.*

Teorema 1.3.1. *Seja G um grupo e seja R um anel com unidade comutativo. Então o conjunto $\{\gamma_i\}_{i \in I}$ de todas as somas de classes é uma base de $\mathcal{Z}(RG)$, o centro de RG, sobre R.*

A prova deste Teorema encontra-se em [19] na página 151.

1.4 Unidades de anéis de grupos

De maneira geral, é extremamente difícil descrever as unidades de um anel de grupo e muitos matemáticos trabalharam neste problema. Alguns conseguiram descrever tais conjuntos para determinados grupos, outros encontraram um subgrupo multiplicativamente independente das unidades e outros ainda encontraram um subgrupo de índice finito de $\mathcal{U}(\mathbb{Z}G)$.

Da definição 20 tem-se em particular que dado um grupo G e um anel R então $\mathcal{U}(RG)$ representa o grupo das unidades do anel de grupo RG. A seguir definiremos um subgrupo das unidades dos anéis de grupo que será de grande utilidade ao longo de nosso trabalho.

Definição 28. *O conjunto*

$$\mathcal{U}_1(RG) := \{u \in \mathcal{U}(RG) : \epsilon(u) = 1\}$$

é o subgrupo das unidades de aumento 1, conhecido como o grupo das ***unidades normalizadas****.*

Considere $u \in \mathcal{U}(\mathbb{Z}G)$. Então existe $v \neq 0 \in \mathbb{Z}G$ tal que $uv = 1 = vu$. Desta maneira $\epsilon(uv) = 1$ e como ϵ é um homomorfismo de anéis temos que $\epsilon(u)\epsilon(v) = 1$. Como $\epsilon(u), \epsilon(v) \in \mathbb{Z}$ segue que $\epsilon(u) = 1$ e $\epsilon(v) = 1$ ou $\epsilon(u) = -1$ e $\epsilon(v) = -1$. Assim $\mathcal{U}(\mathbb{Z}G) \subseteq \pm\mathcal{U}_1(\mathbb{Z}G)$. Portanto $\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G)$.

Sendo nosso objetivo o de determinar um conjunto multiplicativamente independente e gerador para as unidades do anel de grupo integral $\mathbb{Z}G$, do resultado acima basta determinar tal conjunto para as unidades normalizadas de $\mathbb{Z}G$. Desta forma, de agora em diante focaremos no grupo das unidades normalizadas.

Descreveremos abaixo algumas formas de construir unidades.

Exemplo 3 (Unidades Triviais)**.** *Sejam g um elemento do grupo G e $r \in \mathcal{U}(R)$. O elemento $u = rg$ do anel de grupo RG é uma unidade e seu inverso é $u^{-1} = r^{-1}g^{-1}$. Os elementos desta forma são chamados de* ***unidades triviais*** *de RG.*

Exemplo 4 (Unidades Unipotentes)**.** *Seja r um elemento nilpotente do anel R, ou seja, $r^k = 0$ para algum $k \in \mathbb{N}$. Então temos que $1-r, 1+r \in \mathcal{U}(R)$ uma vez que $(1-r)(1+r+r^2+\cdots+r^{k-1}) = 1-r^k = 1$ e $(1+r)(1-r+r^2-\ldots+(-1)^{k-1}r^{k-1}) = 1-r^k = 1$. Os elementos $1 \pm r$ são chamados de* ***unidades unipotentes*** *de R.*

Exemplo 5 (Unidades Bicíclicas)**.** *Seja g um elemento de ordem finita n do grupo G, ou seja, $g^n = 1$ e seja $h \in G$. O elemento $u_{g,h} = 1 + (g-1)h\widehat{g}$ onde $\widehat{g} = 1 + g + g^2 + \ldots + g^{n-1}$ é uma unidade de RG chamada de* ***unidade bicíclica****.*

Note que estas unidades na verdade são um caso particular de unidades unipotentes, já que $[(g-1)h\widehat{g}]^2 = 0$.

Exemplo 6 (Unidade cíclica de Bass)**.** *Considere Φ a função de Euler. Sejam g um elemento de um grupo abeliano G de ordem n e i um inteiro tal que $mdc(i,n) = 1$ com $1 < i < n-1$. Sejam $\hat{g} = 1 + g + g^2 + \ldots + g^{n-1}$ e $k = \dfrac{i^{\phi(n)}-1}{n}$. Define - se a unidade cíclica de Bass como:*

$$b_i(g) := (1 + g + g^2 + \ldots + g^{i-1})^{\phi(n)} - k\hat{g}.$$

Exemplo 7 (Unidades de Hoechsmann)**.** *Seja $G = C_n = \langle g \rangle$ o grupo cíclico de ordem n. Então*

$$u = \frac{1 + g^j + \cdots + g^{j(i-1)}}{1 + g + \cdots + g^{i-1}}$$

onde $mdc(i,n) = 1$ e $mdc(j,n) = 1$ é uma unidade, chamada de ***unidade de Hoechsmann****.*

Vejamos que $\dfrac{1 + g^j + \cdots + g^{j(i-1)}}{1 + g + \cdots + g^{i-1}}$ é um elemento de $\mathbb{Z}G$.

De fato, seja $t \in \mathbb{Z}$ tal que $it \equiv 1 \pmod{n}$ e seja $k = \dfrac{it-1}{n}$. Como $it \equiv 1 \pmod{n}$ então $it = qn + 1$ para algum $q \in \mathbb{Z}$ e pela definição $k = q$. Repare que

$$\begin{aligned}(1 + g + \cdots + g^{i-1})(1 + g^i + g^{2i} + \cdots + g^{i(t-1)} - \frac{k}{i}\widehat{g}) &= 1 + g + g^2 + \cdots + g^{it-i+i-1} - q\widehat{g} \\ &= 1 + g + g^2 + \cdots + g^{it-1} - q\widehat{g}.\end{aligned}$$

Lembrando que $it - 1 = qn$ segue que

$$(1 + g + \cdots + g^{i-1})(1 + g^i + g^{2i} + \cdots + g^{i(t-1)} - \frac{k}{i}\widehat{g}) = 1 + q\widehat{g} - q\widehat{g} = 1.$$

Logo

$$(1 + g + \cdots + g^{i-1})^{-1} = 1 + g^i + g^{2i} + \cdots + g^{i(t-1)} - \frac{k}{i}\widehat{g}$$

e, portanto,

$$\frac{1 + g^j + \cdots + g^{j(i-1)}}{1 + g + \cdots + g^{i-1}} = (1 + g^j + \cdots + g^{j(i-1)})(1 + g^i + g^{2i} + \cdots + g^{i(t-1)}) - k\widehat{g} \in \mathbb{Z}G.$$

Em 1960 G. Higman formulou o seguinte Teorema:

Teorema 1.4.1. *Se G é um grupo arbitrário então $\mathcal{U}(\mathbb{Z}G) = \pm G \times F$, onde F é um grupo livre cujo posto é definido como:*

$$rank(F) := \begin{cases} \frac{1}{2}\left[|G_0| - 2l + m + 1\right] & se \quad G_0 \text{ é finito} \\ 0 & se \quad G_0^4 = 1 \text{ ou } G_0^6 = 1 \\ |G_0| & se \quad G_0 \text{ é infinito, } G_0^4 \neq 1 \text{ e } G_0^6 \neq 1 \end{cases}$$

Aqui G_0 é o subgrupo de torção de G, $G^n := \{g^n : g \in G\}$, m é o número de subgrupos cíclicos de G_0 de ordem 2 e l representa o número de subgrupos cíclicos de G_0.

A demostração do Teorema acima pode ser encontrada em [14] na página 139.

Iremos voltar nossa atenção para grupos de unidades especiais, as unidades simétricas e as unidades unitárias.

Definição 29. *O conjunto $\mathcal{U}^*(RG) := \{u \in \mathcal{U}(RG) : u^* = u\}$ é chamado de conjunto das* ***unidades simétricas*** *de RG, onde $*$ representa a involução clássica.*

Observe que se G é abeliano e R é comutativo então $\mathcal{U}^*(RG)$ é subgrupo de $\mathcal{U}(RG)$.

Definição 30 (Unidades Unitárias)**.** *Sejam G um grupo e RG o anel de grupo associado. Considere $*$ a involução clássica. O conjunto*

$$Un(RG) = \{u \in \mathcal{U}(RG) : uu^* = u^*u = 1\}$$

é chamado de conjunto das ***unidades unitárias.***

Proposição 1.4.1. *Seja $u \in \mathcal{U}(\mathbb{Z}G)$ tal que $u^*u = 1$. Então $u = \pm g$, para algum $g \in G$.*

Demonstração: Seja $u = \sum_{g \in G} \alpha_g g \in \mathcal{U}(\mathbb{Z}G)$. Então $u^* = \sum_{g \in G} \alpha_g g^{-1}$ e, sendo assim, tem-se que $uu^* = \sum_{g \in G} \alpha_g^2 + \sum_{g,h \in G h \neq g^{-1}} \alpha_g \alpha_h gh$. Como $uu^* = 1$ então $\sum_{g \in G} \alpha_g^2 = \pm 1$. Logo existe $g_0 \in G$ tal que $\alpha_{g_0} = 1$ e $\alpha_g = 0$ para todo $g \neq g_0 \in G$.

Desta forma, $u = \pm g_0$.

■

O Teorema abaixo caracteriza o grupo $\mathcal{U}_1(\mathbb{Z}G)$ para o caso em que G é um grupo abeliano de ordem ímpar.

Teorema 1.4.2. *Seja G um grupo abeliano finito de ordem ímpar. Então $\mathcal{U}_1(\mathbb{Z}G) = G \times \mathcal{U}_1^*(\mathbb{Z}G)$, onde $\mathcal{U}_1^*(\mathbb{Z}G)$ representa o grupo das unidades simétricas normalizadas e $*$ representa a involução clássica.*

Demonstração: Seja $u \in \mathcal{U}_1(\mathbb{Z}G)$. Observe que

$$(u^{-1}u^*)^* = (u^*)^*(u^{-1})^* = u(u^{-1})^* = (u^{-1})^*u = (u^{-1}u^*)^{-1},$$

ou seja, $(u^{-1}u^*)^*(u^{-1}u^*) = 1$. Como $u^{-1}u^* \in \mathcal{U}_1(\mathbb{Z}G)$ segue da proposição 1.4.1 que $u^{-1}u^* = g^{-1}$ para algum $g \in G$, isto é, $u = gu^*$. Como G tem ordem ímpar podemos escrever $g = (g^{\frac{o(g)+1}{2}})^2$. Considere $h = g^{\frac{o(g)+1}{2}}$. Logo $u = h^2u^*$, ou seja, $h^{-1}u = hu^*$. Vejamos que $hu^* \in \mathcal{U}^*(\mathbb{Z}G)$. Temos que $(hu^*)^* = (u^*)^*h^* = uh^* = h^*u = h^{-1}u = hu^*$ e portanto $hu^* \in \mathcal{U}_1^*(\mathbb{Z}G)$. Assim $u = h(hu^*)$, onde $h \in G$ e $hu^* \in \mathcal{U}_1^*(\mathbb{Z}G)$.

Vejamos agora que $G \cap \mathcal{U}_1^*(\mathbb{Z}G) = (1)$. Seja $g \in G \cap \mathcal{U}_1^*(\mathbb{Z}G)$. Temos que $g = g^* = g^{-1}$. Logo $g^2 = 1$, como a ordem de G é ímpar segue que $g = 1$. Portanto $G \cap \mathcal{U}^*(\mathbb{Z}G) = (1)$. Daí tem - se que $\mathcal{U}_1(\mathbb{Z}G) = G \times \mathcal{U}_1^*(\mathbb{Z}G)$.

■

Analogamente pode-se mostrar que $\mathcal{U}(\mathbb{Z}G) = G \times \mathcal{U}^*(\mathbb{Z}G)$. Assim, afim de descrever o grupo das unidades de $\mathbb{Z}G$, podemos delimitar nossa atenção apenas para o grupo das unidades simétricas normalizadas.

Em nossos estudos utilizamos as unidades provenientes das unidades descritas por Ferraz em [6] que iremos definir em seguida.

Definição 31. *Seja p um número primo e seja θ uma raíz p-ésima primitiva da unidade. Vamos definir:*

$$\mu_i := 1 + \theta + \theta^2 + \ldots + \theta^{i-1} \in \mathbb{Z}[\theta]$$

onde $i \geq 1 \in \mathbb{Z}$

Façamos algumas considerações iniciais.

(1) Se $i \equiv 0 \pmod{p}$ então $\mu_i = 0$;

De fato, vamos considerar o polinômio $f(x) = x^p - 1$. Temos que
$f(x) = (x-1)(x^{p-1} + x^{p-2} + \ldots + x + 1)$.
Como θ é uma raíz $p$ésima primitiva da unidade temos que θ é raíz do polinômio $x^{p-1} + x^{p-2} + \ldots + x + 1$, ou seja, $\theta^{p-1} + \theta^{p-2} + \ldots + \theta + 1 = 0$. Como $i \equiv 0 \pmod{p}$ então $i = qp$ para algum $q \in \mathbb{Z}$. Deste modo,
$\mu_i = 1+\theta+\theta^2+\ldots+\theta^{p-1}+\theta^p+\theta^{p+1}+\ldots+\theta^{2p-1}+\theta^{2p}+\ldots+\theta^{(q-1)p}+\theta^{(q-1)p}+1\ldots+\theta^{qp-1}$
ou seja,
$\mu_i = \underbrace{(1 + \theta + \theta^2 + \ldots + \theta^{p-1}) + (1 + \theta + \ldots + \theta^{p-1}) + (1 + \theta \ldots + \theta^{p-1})}_{q \text{ vezes}}$
isto é,
$\mu_i = 0$.

(2) Se $1 \leq i \leq p-1$ então $\mu_i = -\theta^i \mu_{p-i}$;

Pelo item anterior temos que $\mu_p = 0$. Como $\mu_p = 1+\theta+\theta^2+\ldots+\theta^{i-1}+\theta^i+\theta^{i+1}+\ldots+\theta^{p-1}$ segue que:
$1 + \theta + \theta^2 + \ldots + \theta^{i-1} = -(\theta^i + \theta^{i+1} + \ldots + \theta^{p-1}) = -\theta^i(1 + \theta + \ldots + \theta^{p-i-1})$
ou seja,
$\mu_i = -\theta^i \mu_{p-i}$.

(3) Se $i + j \equiv 0 \pmod{p}$ então $\mu_i = -\theta^i \mu_j$;

Por (1) temos que $\mu_{i+j} = 0$. Vamos supor sem perda de generalidade que $i < j$ então temos que
$1 + \theta + \ldots + \theta^{i-1} + \theta^i + \theta^{i+1} + \ldots + \theta^{j-i-1} = -\theta^i(1 + \theta + \ldots + \theta^{j-1})$
ou seja,
$\mu_i = -\theta^i u_j$.

(4) Se $i \equiv j \pmod{p}$ então $\mu_i = \mu_j$;

Vamos supor sem perda de generalidade que $i < j$. Como $i \equiv j \pmod{p}$ então $j = qp + i$ para algum $q \in \mathbb{Z}$. Portanto:

$\theta^j = \theta^{qp+1} = \theta^{qp}\theta^i = \theta i$ uma vez que $\theta^p = 1$.

Como $j - i \equiv 0 \pmod{p}$ segue por (i) que $\mu_{j-i} = 0$. Assim temos que:

$1 + \theta + \theta^2 + \ldots + \theta^{i-1} = -(\theta^i + \theta^{i+1} + \ldots + \theta^{j-i-1}) = \theta^j + \theta^{j+1} + \ldots + \theta^{p-1}$.

Lembrando que

$u_p = 1 + \theta + \ldots + \theta^{j-1} + \theta^j + \theta^{j+1} + \ldots + \theta^{p-1} = 0$

temos que

$1 + \theta + \theta^2 + \ldots + \theta^{i-1} = 1 + \theta + \theta^2 + \ldots + \theta^{j-1}$,

ou seja,

$\mu_i = \mu_j$.

(5) Se $1 \leq i \leq p - 1$ então $\mu_i \in \mathcal{U}(\mathbb{Z}[\theta])$;

Seja $j \in \mathbb{Z}$ tal que $ij \equiv 1 \pmod{p}$. Considere:

$\alpha = 1 + \theta^i + \theta^{2i} + \ldots + \theta^{(j-1)i} \in \mathbb{Z}[\theta]$. Temos que:

$\alpha\mu_i = (1 + \theta^i + \theta^{2i} + \ldots + \theta^{(j-1)i})(1 + \theta + \theta^2 + \ldots + \theta^{i-1})$

$\Rightarrow$

$\alpha\mu_i = 1 + \theta + \ldots + \theta^{i-1} + \theta^i + \theta^{i+1} + \ldots + \theta^{2i-1} + \ldots + \theta^{(j-1)i} + \theta^{(j-1)i+1} + \ldots + \theta^{(j-1)i+i-1}$

$\Rightarrow$

$\alpha\mu_i = 1 + \theta + \theta^2 + \ldots + \theta^{ji-i+i-1} = 1 + \theta + \theta^2 + \ldots + \theta^{ji-1}$

Como $ji - 1 \equiv 0 \pmod{p}$ temos que $ji - 1 = qp$ para algum $q \in \mathbb{Z}$. Assim:

$\alpha\mu_i = \underbrace{(1 + \theta + \theta^2 + \ldots \theta^{p-1}) + \ldots + (1 + \theta + \theta^2 + \ldots \theta^{p-1})}_{q \text{ vezes}} + 1 = q\mu_p + 1$

Por (1) segue que $\alpha\mu_i = 1$. Portanto $\mu_i \in \mathcal{U}(\mathbb{Z}[\theta])$.

Esta unidade originou um tipo especial de unidade, descrita por Ferraz em [6] que faremos uso no próximo Capítulo.

Definição 32. *Seja $G = C_p = \langle g \rangle$ o grupo cíclico de ordem prima $p \geq 5$. Para cada i com $1 \leq i \leq \frac{p-3}{2}$ definimos:*

$$u_i := \left(\sum_{j=0}^{r-1} g^{tj}\right)\left(\sum_{j=0}^{t-1} g^{jt^i}\right) - k\widehat{g} = \left(1 + g^t + \ldots + g^{t(r-1)}\right)\left(1 + g^{t^i} + \ldots + g^{t^i(t-1)}\right) - k\widehat{g}$$

onde $t \in \mathbb{Z}$ tal que $\overline{t}$ gera $\mathcal{U}(\mathbb{Z}_p)$, r é o menor inteiro positivo tal que $tr \equiv 1 \pmod{p}$ e $k = \frac{rt-1}{p}$.

Com base nas unidades acima Ferraz em [6] conseguiu encontrar um conjunto gerador e multiplicativamente independente para o anel de grupo integral $\mathbb{Z}C_p$. Mais precisamente,

Teorema 1.4.3. *Sempre que o conjunto* $\left\langle -1, \theta, \mu_2, \cdots, \mu_{\frac{p-3}{2}} \right\rangle$ *gera* $\mathcal{U}(\mathbb{Z}[\theta])$ *temos que o conjunto* $S := \left\langle \mu_2, \mu_3, \cdots, \mu_{\frac{p-3}{2}} \right\rangle$ *é um subconjunto multiplicativamente independente de* $\mathcal{U}_1(\mathbb{Z}C_p)$ *tal que*

$$\mathcal{U}_1(\mathbb{Z}C_p) = \langle g \rangle \times \langle S \rangle .$$

Capítulo 2

Unidades de $\mathbb{Z}C_{2p}$

2.1 Introdução

Seja p um primo ímpar. Neste Capítulo temos como objetivo descrever um conjunto multiplicativamente independente de geradores das unidades do anel de grupo integral $\mathbb{Z}G$, onde $G := C_{2p}$. Tal primo p deve satisfazer algumas condições que especificaremos mais adiante, e além disso, ser tal que ou 2 gera $\mathcal{U}(\mathbb{Z}_p)$, ou que 2 gera $\mathcal{U}(\mathbb{Z}_p)^2$ e que $-1 \notin \mathcal{U}(\mathbb{Z}_p)^2$.

Sabemos que $\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G)$, portanto é suficiente determinarmos um conjunto multiplicativamente independente para $\mathcal{U}_1(\mathbb{Z}C_{2p})$.

Neste trabalho, sempre consideraremos que $C_2 \cong \langle a : a^2 = 1 \rangle$ e $C_p \cong \langle g : g^p = 1 \rangle$. Como $\mathbb{Z}C_{2p} \cong (\mathbb{Z}C_p)\, C_2$ então temos que qualquer elemento u de $\mathbb{Z}C_{2p}$ pode ser escrito como $u = \alpha + \beta a$, onde $\alpha, \beta \in \mathbb{Z}C_p$.

Seja $u \in \mathbb{Z}C_{2p}$. Logo, u será uma unidade se, e somente se, existe $v \neq 0 \in \mathbb{Z}C_{2p}$ tal que $uv = 1 = vu$. Como $u, v \in \mathbb{Z}C_{2p}$ existem $\alpha, \beta, \gamma, \delta \in \mathbb{Z}C_p$ tais que $u = \alpha + \beta a$ e $v = \gamma + \delta a$.

Assim, $uv = (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)a = 1$, de onde obtemos o seguinte sistema

$$\begin{cases} \alpha\gamma + \beta\delta = 1 \\ \alpha\delta + \beta\gamma = 0 \end{cases}$$

Somando e subtraindo tais equações obtemos que:

$$\begin{cases} (\alpha + \beta)(\gamma + \delta) = 1 \\ (\alpha - \beta)(\gamma - \delta) = 1 \end{cases}$$

isto é, $\alpha + \beta, \alpha - \beta \in \mathcal{U}(\mathbb{Z}C_p)$.

Portanto, existem $u_1, u_2 \in \mathcal{U}(\mathbb{Z}C_p)$ tais que $u_1 = \alpha + \beta$ e $u_2 = \alpha - \beta$. Desta forma: $\alpha = \dfrac{u_1 + u_2}{2}$ e $\beta = \dfrac{u_1 - u_2}{2}$, ou ainda, $\alpha = u_1\left(\dfrac{1 + u_1^{-1}u_2}{2}\right)$ e $\beta = u_1\left(\dfrac{1 - u_1^{-1}u_2}{2}\right)$, com $u_1, u_2 \in \mathcal{U}(\mathbb{Z}C_p)$.

Como $\alpha, \beta \in \mathbb{Z}C_p$, então $\dfrac{1 \pm u_1^{-1}u_2}{2} \in \mathbb{Z}C_p$. Sendo assim: $1 \pm u_1^{-1}u_2 \equiv 0 \pmod{\langle 2\rangle}$, ou seja, $u_1^{-1}u_2 \equiv 1 \pmod{\langle 2\rangle}$.

Assim,

$$u \in \mathcal{U}(\mathbb{Z}C_{2p}) \Rightarrow u = u_1\left[\left(\frac{1+u_2}{2}\right) + \left(\frac{1-u_2}{2}\right)a\right],$$

onde $u_1, u_2 \in \mathcal{U}(\mathbb{Z}C_p)$ e $u_2 \equiv 1 \pmod{\langle 2\rangle}$.

Vejamos agora que,se $u = u_1\left[\left(\dfrac{1+u_2}{2}\right) + \left(\dfrac{1-u_2}{2}\right)a\right]$ tal que $u_1, u_2 \in \mathcal{U}(\mathbb{Z}C_p)$ e $u_2 \equiv 1 \pmod{\langle 2\rangle}$, então $u \in \mathcal{U}(\mathbb{Z}C_{2p})$.

Como u_1 e $u_2 \in \mathcal{U}(\mathbb{Z}C_p)$, então existem u_1^{-1} e $u_2^{-1} \in \mathbb{Z}C_p$. Mas $1 \pm u_2 \in 2\mathbb{Z}C_p$, então $u \in \mathbb{Z}C_{2p}$. Falta mostrar que $u \in \mathcal{U}(\mathbb{Z}C_{2p})$. Para isso, vamos exibir $v \in \mathbb{Z}C_{2p}$ tal que $uv = 1 = vu$. Considere:

$$\begin{aligned} v &= u_1^{-1}u_2^{-1}\left[\left(\frac{1+u_2}{2}\right) - \left(\frac{1-u_2}{2}\right)a\right] \\ &= u_1^{-1}\left[\left(\frac{1+u_2^{-1}}{2}\right) + \left(\frac{1-u_2^{-1}}{2}\right)a\right]. \end{aligned}$$

Logo,

$$\begin{aligned} uv &= u_2^{-1}\left[\left(\frac{1+u_2}{2}\right)^2 - \left(\frac{1-u_2}{2}\right)^2\right] \\ &= u_2^{-1}\left[\frac{1 + 2u_2 + u_2^2 - (1 - 2u_2 + u_2^2)}{4}\right] \\ &= 1 \end{aligned}$$

Novamente, como $u_2 \equiv 1 \pmod{\langle 2\rangle}$, então $v \in \mathcal{U}(\mathbb{Z}C_{2p})$ e assim, concluímos que:

$$u \in \mathcal{U}(\mathbb{Z}C_{2p}) \Leftrightarrow u = u_1\left[\left(\frac{1+u_2}{2}\right) + \left(\frac{1-u_2}{2}\right)a\right],$$

onde $u_1, u_2 \in \mathcal{U}(\mathbb{Z}C_p)$ e $u_2 \equiv 1 \pmod{\langle 2\rangle}$.

Considere o seguinte homomorfismo de anéis $\psi : \mathbb{Z}C_p \to \mathbb{Z}_2C_p$ definido da maneira usual, isto é,

$$\psi\left(\sum_{i=0}^{p-1} a_i g^i\right) := \sum_{i=0}^{p-1} \overline{a}_i g^i.$$

Desta forma,

$$u \in \mathcal{U}(\mathbb{Z}C_{2p}) \Leftrightarrow u = u_1\left[\left(\frac{1+u_2}{2}\right) + \left(\frac{1-u_2}{2}\right)a\right],$$

com $u_1, u_2 \in \mathcal{U}(\mathbb{Z}C_p)$ e $u_2 \in \mathrm{Ker}(\psi|_{\mathcal{U}(\mathbb{Z}C_p)})$.

Nosso trabalho agora está em determinar o núcleo de $\psi|_{\mathcal{U}(\mathbb{Z}C_p)}$. Observe que $\mathrm{Ker}(\psi|_{\mathcal{U}(\mathbb{Z}C_p)}) \subseteq \mathcal{U}^*(\mathbb{Z}C_p)$.

De fato, seja $u \in \mathrm{Ker}(\psi|_{\mathcal{U}(\mathbb{Z}C_p)})$, então $u \in \mathcal{U}(\mathbb{Z}C_p)$ e do Teorema 1.4.2 tem-se $u = g^i v$, onde $v \in \mathcal{U}^*(\mathbb{Z}C_p)$. Além disso, $\psi(u) = g^i\psi(v) = \overline{1}$. Como $\psi(v), \psi(u) \in \mathcal{U}^*(\mathbb{Z}_2C_p)$, tem-se que $i = 0$ e assim $u = v \in \mathcal{U}^*(\mathbb{Z}C_p)$. Logo, $\mathrm{Ker}(\psi|_{\mathcal{U}(\mathbb{Z}C_p)}) \subseteq \mathcal{U}^*(\mathbb{Z}C_p)$.

Considere

$$\rho := \psi|_{\mathcal{U}_1^*(\mathbb{Z}C_p)}.$$

Vejamos que $\mathrm{Im}(\rho) \subseteq \mathcal{U}^*(\mathbb{Z}_2C_p)$.

Seja $u \in \mathcal{U}_1^*(\mathbb{Z}C_p)$, isto é, $u \in \mathcal{U}_1(\mathbb{Z}C_p)$ e $u = u^*$, sendo que $*$ representa a involução clássica. Como ψ é um homomorfismo de anéis, então $\rho(u) \in \mathcal{U}_1(\mathbb{Z}_2C_p)$. Como $u = \sum_{i=0}^{p-1} a_i g^i$, da condição de que $u = u^*$, tem-se que $a_i = a_{p-i}$, $1 \leq i \leq \frac{p-1}{2}$ e, sendo assim, $\overline{a_i} = \overline{a_{p-i}}$ que resulta em $\rho(u) = \rho(u)^*$. Portanto, $\mathrm{Im}(\rho) \subseteq \mathcal{U}^*(\mathbb{Z}_2C_p)$.

Como $\mathcal{U}^*(\mathbb{Z}C_p)) = \langle -1 \rangle \times \mathcal{U}_1^*(\mathbb{Z}C_p)$ e $-1 \in \mathrm{Ker}(\rho)$, então $\mathrm{Ker}(\psi|_{\mathcal{U}^*(\mathbb{Z}C_p)}) = \langle -1 \rangle \times \mathrm{Ker}(\rho)$. Assim nos concentraremos agora em determinar o núcleo de ρ.

Low em [17], utiliza um resultado um pouco mais geral para calcular certos grupos de unidades. Ele calculou explicitamente $\mathcal{U}(\mathbb{Z}C_{10})$.

Na próxima seção descreveremos um método sistemático para determinar o núcleo de ρ a partir das unidades definidas em [6] (citadas na página 20).

2.2 Núcleo de ρ

Relembremos que, para determinar um conjunto gerador do grupo das unidades do anel de grupo $\mathbb{Z}C_{2p}$, precisamos caracterizar o núcleo do homomorfismo de grupos

$$\rho : \mathcal{U}(\mathbb{Z}C_p) \longrightarrow \mathcal{U}(\mathbb{Z}_2C_p).$$

Caso 1. Suponha que 2 gera $\mathcal{U}(\mathbb{Z}_p)$.

Para todo $1 \leq i \leq \frac{p-1}{2}$, considere

$$u_i := (1 + g^2 + g^4 + g^6 + \cdots + g^{p-1})(1 + g^{2^i}) - \widehat{g}.$$

Temos que u_i é uma unidade normalizada de $\mathbb{Z}C_p$.

De fato, seja

$$m_i := (1 + g^{2^{i+1}} + g^{2\cdot 2^{i+1}} + g^{3\cdot 2^{i+1}} + \cdots + g^{(\frac{p-1}{2})\cdot 2^{i+1}})(1 + g) - \widehat{g}.$$

Temos que:

$u_i m_i = (1 + g^2 + g^4 + g^6 + \cdots + g^{p-1})(1 + g)(1 + g^{2^{i+1}} + g^{2\cdot 2^{i+1}} + g^{3\cdot 2^{i+1}} + \cdots + g^{(\frac{p-1}{2})\cdot 2^{i+1}})(1 + g^{2^i}) +$
$-2\left(\dfrac{p+1}{2}\right)\widehat{g} - 2\left(\dfrac{p+1}{2}\right)\widehat{g} + p\widehat{g},$

de onde,

$u_i m_i = (1 + g^2 + g^4 + \cdots + g^{p-1} + g + g^3 + g^5 + \cdots + g^{p-2} + 1)(1 + g^{2\cdot 2^i} + g^{4\cdot 2^i} + g^{6\cdot 2^i} + \cdots + g^{(p-1)\cdot 2^i}) +$
$+(1 + g^{2^i}) - (p+2)\widehat{g},$

ou seja,

$u_i m_i = (1 + \widehat{g})(1 + g^{2\cdot 2^i} + g^{4\cdot 2^i} + g^{6\cdot 2^i} + \cdots + g^{(p-1)\cdot 2^i} + g^{2^i} + g^{3\cdot 2i} + g^{5\cdot 2^i} + \cdots + g^{(p-1)\cdot 2^i} + 1) +$
$-(p+2)\widehat{g},$

isto é,

$$u_i m_i = (1 + \widehat{g})(1 + \widehat{g}) - (p+1)\widehat{g} = 1 + (p+2)\widehat{g} - (p+2)\widehat{g} = 1.$$

Logo

$$u_i^{-1} = (1 + g^{2^{i+1}} + g^{2\cdot 2^{i+1}} + g^{3\cdot 2^{i+1}} + \cdots + g^{(\frac{p-1}{2})\cdot 2^{i+1}})(1 + g) - \widehat{g}.$$

Observe que as unidade u_i nada mais são do que as unidades descritas por Ferraz em [6] e apresentadas aqui na Definição 32.

Vamos definir $v_1 := u_1$ e $v_i := u_i u_{i-1}^{-1}$, $2 \leq i \leq \dfrac{p-1}{2}$. Então,

$$\begin{aligned} v_i \;=\;& (1 + g^2 + g^4 + \cdots + g^{p-1})(1 + g)(1 + g^{2^i} + g^{2\cdot 2^i} + \cdots + g^{(\frac{p-1}{2})\cdot 2^i})(1 + g^{2^i}) - 2\left(\frac{p+1}{2}\right)\widehat{g} + \\ & -2\left(\frac{p+1}{2}\right)\widehat{g} + p\widehat{g}, \end{aligned}$$

ou seja,

$$v_i = (1+\widehat{g})(1+g^{2^i}+g^{2\cdot 2^i}+\cdots+g^{(\frac{p-1}{2})\cdot 2^i})(1+g^{2^i})-(p+2)\widehat{g},$$

isto é,

$$v_i = (1+g^{2^i}+g^{2\cdot 2^i}+\cdots+g^{(\frac{p-1}{2})\cdot 2^i})(1+g^{2^i})+2\left(\frac{p+1}{2}\right)\widehat{g}-(p+2)\widehat{g},$$

ou ainda,

$$v_i = (1+g^{2^i}+g^{2\cdot 2^i}+\cdots+g^{(\frac{p-1}{2})\cdot 2^i})(1+g^{2^i})-\widehat{g},$$

e, portanto,

$$v_i = (1+g^{2\cdot 2^{i-1}}+g^{4\cdot 2^{i-1}}+\cdots+g^{(p-1)\cdot 2^{i-1}})(1+g^{2\cdot 2^{i-1}})-\widehat{g},$$

que pode ser escrito como

$$v_i = (1+2g^{2\cdot 2^{i-1}}+2g^{4\cdot 2^{i-1}}+\cdots+2g^{(p-1)\cdot 2^{i-1}}+g^{2^{i-1}})-\widehat{g}$$

e, desta forma,

$$v_i = g^{2\cdot 2^{i-1}}-g^{3\cdot 2^{i-1}}+g^{4\cdot 2^{i-1}}-g^{5\cdot 2^{i-1}}+\cdots+g^{(p-1)\cdot 2^{i-1}},$$

logo,

$$v_i = g^{2\cdot 2^{i-1}}(1-g^{2^{i-1}}+g^{2\cdot 2^{i-1}}+\cdots-g^{(p-4)\cdot 2^{i-1}}+g^{(p-3)\cdot 2^{i-1}}),\ \forall\, 2\leq i\leq \frac{p-1}{2}.$$

Como u_i é uma unidade normalizada, então v_i também é uma unidade normalizada. Seja

$$\begin{aligned} w_i \;:=\; & g^{(\frac{p-1}{2})\cdot 2^{i-1}}v_i=(-1)^{(\frac{p-3}{2})}(1-g^{2^{i-1}}+g^{2\cdot 2^{i-1}}+\cdots+(-1)^{(\frac{p-3}{2})}g^{(\frac{p-3}{2})\cdot 2^{i-1}}+ \\ & +(-1)^{(\frac{p-3}{2})}g^{(\frac{p+3}{2})\cdot 2^{i-1}}+\cdots+g^{(p-2)\cdot 2^{i-1}}-g^{(p-1)\cdot 2^{i-1}}), \end{aligned}$$

$1\leq i\leq \dfrac{p-1}{2}$

Novamente como v_i é uma unidade normalizada, então w_i também o é. Mais ainda, pela definição de w_i, tem-se que w_i é uma unidade simétrica normalizada.

Caso 2. Estudemos agora o caso em que $\overline{2}$ gera $\mathcal{U}(\mathbb{Z}_p)^2$ e, além disso, $\overline{-1} \notin \mathcal{U}(\mathbb{Z}_p)^2$.

Teorema 2.2.1. *Considere p um número primo ímpar e seja $\mathcal{U}(\mathbb{Z}_p) = \langle h \rangle$. Então*

i) $z \in \mathcal{U}(\mathbb{Z}_p)^2$ se, e somente se, $z^{\frac{p-1}{2}} \equiv 1 \ (mod\, p)$

ii) $z \in \mathcal{U}(\mathbb{Z}_p) \setminus \mathcal{U}(\mathbb{Z}_p)^2$ se, e somente se, $z^{\frac{p-1}{2}} \equiv -1 \ (mod\, p)$

Demonstração:

(i) $(\Rightarrow)$ Se $z \in \mathcal{U}(\mathbb{Z}_p)^2$, como $\mathcal{U}(\mathbb{Z}_p) = \langle h \rangle$, então $z = h^{2k}$. Assim $z^{\frac{p-1}{2}} = h^{(p-1)k}$ e pelo Pequeno Teorema de Fermat segue que $z^{\frac{p-1}{2}} = (h^k)^{p-1} \equiv 1^k = 1 \pmod p$

(ii) $(\Rightarrow)$ Se $z \in \mathcal{U}(\mathbb{Z}_p) \setminus \mathcal{U}(\mathbb{Z}_p)^2$, como $\mathcal{U}(\mathbb{Z}_p) = \langle h \rangle$, então $z = h^{2k+1}$. Assim $z^{\frac{p-1}{2}} = (h^k)^{p-1} h^{\frac{p-1}{2}}$, e portanto $z^{\frac{p-1}{2}} \equiv 1(-1) = -1 \pmod p$

Demonstremos agora a recíproca do item (i)

$(\Leftarrow)$ Considere $z^{\frac{p-1}{2}} \equiv 1 \ (mod\, p)$. Suponha, por absurdo, que $z \notin \mathcal{U}(\mathbb{Z}_p)^2$, então $z \in \mathcal{U}(\mathbb{Z}_p) \setminus \mathcal{U}(\mathbb{Z}_p)^2$. Pelo item (ii) segue que $z^{\frac{p-1}{2}} \equiv -1 \pmod p$ o que contradiz a hipótese. Logo $z \in \mathcal{U}(\mathbb{Z}_p)$.

Vamos provar agora a recíproca do item (ii)

$(\Leftarrow)$ Considere $z^{\frac{p-1}{2}} \equiv -1 \pmod p$; do item (i) segue que $z \notin \mathcal{U}(\mathbb{Z}_p)^2$ e, portanto, $z \in \mathcal{U}(\mathbb{Z}_p) \setminus \mathcal{U}(\mathbb{Z}_p)^2$.

■

Vejamos que $\mathcal{U}(\mathbb{Z}_p) = \left\langle \overline{-2} \right\rangle$.

Lema 2.2.1. *Considere p um número primo tal que $\mathcal{U}(\mathbb{Z}_p)^2 = \left\langle \overline{2} \right\rangle$ e $-\overline{1} \notin \mathcal{U}(\mathbb{Z}_p)^2$. Então $\mathcal{U}(\mathbb{Z}_p) = \left\langle \overline{-2} \right\rangle$.*

Demonstração:

Temos que $-2 \notin \mathcal{U}(\mathbb{Z}_p)^2$, porque, se $-2 \in \mathcal{U}(\mathbb{Z}_p)^2$, então, como $-2 = -1(2)$, tem-se que $-1 \in \mathcal{U}(\mathbb{Z}_p)^2$, contradizendo a hipótese. Logo $-2 \notin \mathcal{U}(\mathbb{Z}_p)^2$. Pelo Teorema 2.2.1 segue que $(-2)^{\frac{p-1}{2}} \equiv -1 \pmod p$; assim $-1 \in \langle -2 \rangle$. Além disso, $2 = (-1)(-2) \in \langle -2 \rangle$, o que implica que, $\langle 2 \rangle \subsetneq \langle -2 \rangle$ e, portanto, $1 < [\langle -2 \rangle : \langle 2 \rangle] \leq [\mathcal{U}(\mathbb{Z}_p) : \langle 2 \rangle] = 2$, ou seja, $[\langle -2 \rangle : \langle 2 \rangle] = 2$. Desta forma, concluímos que $\mathcal{U}(\mathbb{Z}_p) = \left\langle \overline{-2} \right\rangle$.

■

Nas condições do Lema acima e da Definição 32, podemos reescrever as unidades de $\mathbb{Z}C_p$ da seguinte forma

$$u_i := (\widehat{g} - g^2(1 + g^2 + g^4 + \cdots + g^{p-1}))(\widehat{g} - (g^{(p-2)(-2)^i} + g^{(p-1)(-2)^i})) - \widehat{g}$$

para todo $1 \leq i \leq \frac{p-3}{2}$.

De fato, por hipótese tem-se que $\mathcal{U}(\mathbb{Z}_p)^2 = \langle \overline{2} \rangle$ e $\overline{-1} \notin \mathcal{U}(\mathbb{Z}_p)^2$ e, pelo Lema 2.2.1, segue que $\mathcal{U}(\mathbb{Z}_p) = \langle \overline{-2} \rangle$.

Da Definição 31 segue que

$$u_i := \left(\sum_{j=0}^{r-1} g^{tj}\right)\left(\sum_{j=0}^{t-1} g^{jt^i}\right) - k\widehat{g} = \left(1 + g^t + \ldots + g^{t(r-1)}\right)\left(1 + g^{t^i} + \ldots + g^{t^i(t-1)}\right) - k\widehat{g},$$

sendo t o gerador de $\mathcal{U}(\mathbb{Z}_p)$, r é o menor inteiro positivo tal que $tr \equiv 1$ (mod p) e $k = \frac{rt-1}{p}$.

Como no nosso caso $t = p - 2$, tem-se que $r = \frac{p-1}{2}$ e portanto $k = \frac{p-3}{2}$. Assim

$$\begin{aligned} u_i &= \left(\sum_{j=0}^{\frac{p-3}{2}} g^{(-2)\cdot j}\right)\left(\sum_{j=0}^{p-3} g^{(-2)^i\cdot j}\right) - k\widehat{g} \\ &= \left(1 + g^t + \ldots + g^{(r-1)\cdot j}\right)\left(1 + g^{t^i} + \ldots + g^{(t-1)\cdot t^i}\right) + \\ &\quad -(\frac{p-3}{2})\widehat{g}, \end{aligned}$$

ou seja,

$$\begin{aligned} u_i &= [1 + g^{-2} + g^{-4} + \cdots + g^{(-2)\cdot(\frac{p-5}{2})} + g^{(-2)\cdot(\frac{p-3}{2})}][1 + g^{(-2)^i} + g^{2\cdot(-2)^i} + g^{3\cdot(-2)^i} + \cdots + \\ &\quad + g^{(-2)^i\cdot(p-4)} + g^{(-2)^i\cdot(p-3)}] - (\frac{p-3}{2})\widehat{g}, \end{aligned}$$

isto é,

$$u_i = \left(1 + g^{p-2} + g^{p-4} + \cdots + g^5 + g^3\right)\left(1 + g^{(-2)^i} + g^{(-2)^i\cdot 2} + g^{(-2)^i\cdot 3} + \cdots + g^{(-2)^i\cdot(p-4)} + g^{(-2)^i\cdot(p-3)}\right) + -(\frac{p-3}{2})\widehat{g},$$

que pode ser escrito como,

$$u_i = \left(\widehat{g} - g^2(1 + g^2 + g^4 + \cdots + g^{p-3} + g^{p-1})\right)\left(\widehat{g} - g^{(-2)^i\cdot(p-2)}(1 + g^{(-2)^i})\right) - (\frac{p-3}{2})\widehat{g}.$$

Pode-se reescrever u_i da seguinte forma

$$u_i \;=\; g^{(-2)^i\cdot(p-2)+2}[(1+g^2+g^4+\cdots+g^{p-3}+g^{p-1})(1+g^{(-2)^i})+\left(p-2-(\frac{p+1}{2})-(\frac{p-3}{2})\right)\widehat{g}],$$

e portanto,

$$u_i = g^{((-2)^i-1)\cdot(p-2)}[(1+g^2+g^4+\cdots+g^{p-3}+g^{p-1})(1+g^{(-2)^i})-\widehat{g}].$$

Para todo $1 \leq i \leq \dfrac{p-1}{2}$, considere

$$x_i := (1+g^2+g^4+g^6+\cdots+g^{p-1})(1+g^{(-2)^i})-\widehat{g}.$$

Temos que x_i é uma unidade normalizada de $\mathbb{Z}C_p$, uma vez que $x_i = g^{-((-2)^i-1)\cdot(p-2)}u_i$ e temos que

$$x_i^{-1} := (1+g^{(-2)^{i+1}}+g^{(-2)^{i+1}\cdot 2}+g^{(-2)^{i+1}\cdot 3}+\cdots+g^{(-2)^{i+1}\cdot(\frac{p-1}{2})})(1+g)-\widehat{g}.$$

Vamos definir $y_1 := x_1$ e $y_i := x_i x_{i-1}^{-1}$, para todo $2 \leq i \leq \frac{p-1}{2}$. Então

$$\begin{aligned} y_i \;=\; & (1+g^2+g^4+\cdots+g^{p-1})(1+g)(1+g^{(-2)^i}+g^{(-2)^i\cdot 2}+\cdots+g^{(-2)^i\cdot(\frac{p-1}{2})})(1+g^{(-2)^i})+ \\ & -2\left(\frac{p+1}{2}\right)\widehat{g}-2\left(\frac{p+1}{2}\right)\widehat{g}+p\widehat{g}, \end{aligned}$$

$\Longrightarrow$

$$y_i = (1+\widehat{g})(1+g^{(-2)^i}+g^{(-2)^i\cdot 2}+\cdots+g^{(-2)^i\cdot(\frac{p-1}{2})})(1+g^{(-2)^i})-(p+2)\widehat{g},$$

$\Longrightarrow$

$$y_i = (1+g^{(-2)^i}+g^{(-2)^i\cdot 2}+\cdots+g^{(-2)^i\cdot(\frac{p-1}{2})})(1+g^{(-2)^i})+2\left(\frac{p+1}{2}\right)\widehat{g}-(p+2)\widehat{g},$$

$\Longrightarrow$

$$y_i = (1+g^{(-2)^i}+g^{(-2)^i\cdot 2}+\cdots+g^{(-2)^i\cdot(\frac{p-1}{2})})(1+g^{(-2)^i})-\widehat{g},$$

$\Longrightarrow$

$$y_i = (1+g^{(-2)^{i-1}\cdot 2}+g^{(-2)^{i-1}\cdot 4}+\cdots+g^{(-2)^{i-1}\cdot(p-1)})(1+g^{(-2)^{i-1}\cdot 2})-\widehat{g},$$

$\Longrightarrow$

$$y_i = (1 + 2g^{(-2)^{i-1}\cdot 2} + 2g^{(-2)^{i-1}\cdot 4} + \cdots + 2g^{(-2)^{i-1}\cdot(p-1)} + g^{(-2)^{i-1}}) - \widehat{g},$$

$\Longrightarrow$

$$\begin{aligned} y_i &= g^{(-2)^{i-1}\cdot 2} - g^{(-2)^{i-1}\cdot 3} + g^{(-2)^{i-1}\cdot 4} - g^{(-2)^{i-1}\cdot 5} + \cdots + g^{(-2)^{i-1}\cdot(p-1)} \\ &= g^{(-2)^{i-1}\cdot 2}(1 - g^{(-2)^{i-1}} + g^{(-2)^{i-1}\cdot 2} + \cdots - g^{(-2)^{i-1}\cdot(p-4)} + g^{(-2)^{i-1}\cdot(p-3)}),\ \forall\, 1 \leq i \leq \frac{p-1}{2}. \end{aligned}$$

Como x_i é uma unidade normalizada, então y_i também é uma unidade normalizada. Seja $z_i := g^{(-2)^{i-1}(\frac{p-1}{2})}y_i$. Assim

$$\begin{aligned} z_i &= (-1)^{(\frac{p-3}{2})}(1 - g^{(-2)^{i-1}} + g^{(-2)^{i-1}\cdot 2} + \cdots + (-1)^{(\frac{p-3}{2})}g^{(-2)^{i-1}\cdot(\frac{p-3}{2})} + (-1)^{(\frac{p-3}{2})}g^{(-2)^{i-1}\cdot(\frac{p+3}{2})} + \\ &\quad + \cdots + g^{(-2)^{i-1}\cdot(p-2)} - g^{(-2)^{i-1}\cdot(p-1)}), \end{aligned}$$

para todo $1 \leq i \leq \frac{p-1}{2}$.

Novamente como y_i é uma unidade normalizada, então z_i também o é. Mais ainda, tal unidade é simétrica. É claro que $z_i = w_i$, uma vez que $z_i = w_i^*$ e w_i é uma unidade simétrica.

Seja o isomorfismo de anéis $\delta : \mathbb{Z}C_p \to \mathbb{Z}C_p$ definido como

$$\delta\left(\sum_{j=0}^{p-1} a_j g^j\right) = \sum_{j=0}^{p-1} a_j g^{2j},$$

isto é, δ é a extensão linear do automorfismo de grupos $\delta' : C_p \to C_p$ que leva g em g^2.

Estes resultados motivam a seguinte definição:

Definição 33. *Considere θ uma p-ésima raiz primitiva da unidade. Seja p um primo ímpar tal que $\left\langle 1, \theta, \mu_1, \cdots, \mu_{\frac{p-3}{2}} \right\rangle$ gera $\mathcal{U}(\mathbb{Z}[\theta])$, onde $\mu_i = 1 + \theta + \theta^2 + \cdots + \theta^{i-1}$ e*

(i) ou $\overline{2}$ gera $\mathcal{U}(\mathbb{Z}_p)$

(ii) ou $\overline{2}$ gera $\mathcal{U}(\mathbb{Z}_p)^2$ e $-\overline{1} \notin \mathcal{U}(\mathbb{Z}_p)^2$.

*Tal p será chamado de **primo ótimo**.*

Vamos descrever as unidades w_i em função do homomorfismo δ e da unidade w_1.

Lema 2.2.2. *Seja p um primo ótimo. Para todo $2 \leq n \leq \frac{p-1}{2}$, tem-se que $\delta^{n-1}(w_1) = w_n$.*

Demonstração:

Façamos esta prova por indução sobre n. Como

$$w_1 = (-1)^{\frac{p-3}{2}}(1 - g + g^2 + \cdots + (-1)^{(\frac{p-3}{2})} g^{(\frac{p-3}{2})} + (-1)^{(\frac{p-3}{2})} g^{(\frac{p+3}{2})} + \cdots + g^{(p-2)} - g^{(p-1)})$$

então

$\delta(w_1) = (-1)^{(\frac{p-3}{2})}(1 - g^2 + g^4 + \cdots + (-1)^{(\frac{p-3}{2})} g^{(\frac{p-3}{2})\cdot 2} + (-1)^{(\frac{p-3}{2})} g^{(\frac{p+3}{2})\cdot 2} + \cdots + g^{(p-2)\cdot 2} - g^{(p-1)\cdot 2})$
$= w_2$.

Vamos supor que, para $n = k$, vale que $\delta^{k-1}(w_1) = w_k$ e vamos mostrar que, $\delta^k(w_1) = w_{k+1}$. Sabe-se que $\delta^k(w_1) = \delta(\delta^{k-1}(w_1))$ e, pela hipótese indutiva, pode-se concluir que $\delta^k(w_1) = \delta(w_k)$. Pela definição vamos ter que

$$\begin{aligned}
\delta^k(w_1) &= \delta((-1)^{(\frac{p-3}{2})}(1 - g^{2^{k-1}} + g^{2\cdot 2^{k-1}} + \cdots + (-1)^{(\frac{p-3}{2})} g^{(\frac{p-3}{2})\cdot 2^{k-1}} + \\
&\quad +(-1)^{(\frac{p-3}{2})} g^{(\frac{p+3}{2})\cdot 2^{k-1}} + \cdots + g^{(p-2)\cdot 2^{k-1}} - g^{(p-1)\cdot 2^{k-1}}),
\end{aligned}$$

ou seja,

$$\begin{aligned}
\delta^k(w_1) &= (-1)^{(\frac{p-3}{2})}(1 - g^{2^{k-1}\cdot 2} + g^{2\cdot 2^{k-1}\cdot 2} + \cdots + (-1)^{(\frac{p-3}{2})} g^{(\frac{p-3}{2})\cdot 2^{k-1}\cdot 2} + (-1)^{(\frac{p-3}{2})} g^{(\frac{p+3}{2})\cdot 2^{k-1}\cdot 2} \\
&\quad + \cdots + g^{(p-2)\cdot 2^{k-1}\cdot 2} - g^{(p-1)\cdot 2^{k-1}\cdot 2}),
\end{aligned}$$

isto é,

$$\begin{aligned}
\delta^k(w_1) &= (-1)^{(\frac{p-3}{2})}(1 - g^{2^k} + g^{2\cdot 2^k} + \cdots + (-1)^{(\frac{p-3}{2})} g^{(\frac{p-3}{2})\cdot 2^k} + (-1)^{(\frac{p-3}{2})} g^{(\frac{p+3}{2})\cdot 2^k} + \cdots + \\
&\quad +g^{(p-2)\cdot 2^k} - g^{(p-1)\cdot 2^k}) \\
&= w_{k+1}.
\end{aligned}$$

Portanto $\delta^{n-1}(w_1) = w_n$.

■

Relembrando temos que

$$\begin{aligned}
w_i &:= g^{(\frac{p-1}{2})\cdot 2^{i-1}} v_i = (-1)^{(\frac{p-3}{2})}(1 - g^{2^{i-1}} + g^{2\cdot 2^{i-1}} + \cdots + (-1)^{(\frac{p-3}{2})} g^{(\frac{p-3}{2})\cdot 2^{i-1}} + \\
&\quad +(-1)^{(\frac{p-3}{2})} g^{(\frac{p+3}{2})\cdot 2^{i-1}} + \cdots + g^{(p-2)\cdot 2^{i-1}} - g^{(p-1)\cdot 2^{i-1}}),
\end{aligned}$$

para todo $1 \leq i \leq \dfrac{p-1}{2}$

Vamos considerar a imagem através de ρ destas unidades.

$$\rho(w_i) = \overline{1} + g^{2^{i-1}} + g^{2 \cdot 2^{i-1}} + \cdots + g^{(\frac{p-3}{2}) \cdot 2^{i-1}} + g^{(\frac{p+3}{2}) \cdot 2^{i-1}} + \cdots + g^{(p-2) \cdot 2^{i-1}} + g^{(p-1) \cdot 2^{i-1}},$$

que pode enxergado como,

$$\rho(w_i) = \widehat{g} + g^{(\frac{p-1}{2}) \cdot 2^{i-1}} + g^{(\frac{p+1}{2}) \cdot 2^{i-1}},$$

ou seja,

$$\rho(w_i) = \widehat{g} + g^{(\frac{p-1}{2}) \cdot 2^{i-1}}(1 + g^{2^{i-1}}).$$

Lema 2.2.3. *Seja p um primo ótimo. Para todo $n \in \mathbb{N}$, tem-se que* $\rho(w_1)^{2^n} = \widehat{g} + g^{(\frac{p-1}{2}) \cdot 2^n}(\overline{1} + g^{2^n})$

Demonstração:

Façamos a demonstração por indução sobre n.

Quando $n = 1$ temos que:

$$\rho(w_1)^2 = [\widehat{g} + g^{(\frac{p-1}{2})}(\overline{1} + g)]^2 = \widehat{g}^2 + [g^{(\frac{p-1}{2})}(\overline{1} + g)]^2,$$

ou seja,

$$\rho(w_1)^2 = p\widehat{g} + g^{2 \cdot (\frac{p-1}{2})}(\overline{1} + g^2),$$

e, sendo que p é ímpar, acarreta que

$$\rho(w_1)^2 = \widehat{g} + g^{2 \cdot (\frac{p-1}{2})}(\overline{1} + g^2).$$

Logo a afirmação é verdadeira para $n = 1$.

Vamos supor que a igualdade seja verificada para $n = k - 1$, isto é, $\rho(w_1)^{2^{k-1}} = \widehat{g} + g^{(\frac{p-1}{2}) \cdot 2^{k-1}}(\overline{1} + g^{2^{k-1}})$ e, vamos mostrar que, a fórmula é válida para $n = k$.

Como:

$$\rho(w_1)^{2^k} = [\rho(w_1)^{2^{k-1}}]^2,$$

da hipótese de indução, segue que:

$$\rho(w_1)^{2^k} = [\widehat{g} + g^{(\frac{p-1}{2}) \cdot 2^{k-1}}(\overline{1} + g^{2^{k-1}})]^2,$$

isto é,

$$\rho(w_1)^{2^k} = \widehat{g}^2 + [g^{(\frac{p-1}{2})\cdot 2^{k-1}}(\overline{1} + g^{2^{k-1}})]^2$$

ou seja,

$$\rho(w_1)^{2^k} = p\widehat{g} + g^{(\frac{p-1}{2})\cdot 2^k}(\overline{1} + g^{2^{k-1}})^2,$$

ou ainda,

$$\rho(w_1)^{2^k} = \widehat{g} + g^{(\frac{p-1}{2})\cdot 2^k}(\overline{1} + g^{2^k})$$

Portanto, para todo $n \in \mathbb{N}$, vale que $\rho(w_1)^{2^n} = \widehat{g} + g^{(\frac{p-1}{2})\cdot 2^n}(\overline{1} + g^{2^n})$.

■

A seguir, descrevemos as imagem das unidades w_i através do homomorfismo ρ em função de $\rho(w_1)$.

Corolário 2.2.1. *Seja p um primo ótimo. Tem-se que $\rho(w_1)^{2^n} = \rho(w_{n+1})$, $1 \leq n \leq \frac{p-3}{2}$. Em particular, $Im(\rho) = \langle \rho(w_1) \rangle$.*

Demonstração:

Do Lema 2.2.3 tem-se que $\rho(w_1)^{2^{n+1}} = \widehat{g} + g^{(\frac{p-1}{2})\cdot 2^{n+1}}(\overline{1} + g^{2^{n+1}})$ e, da definição de w_i tem-se que $\rho(w_1)^{2^{n+1}} = \rho(w_n)$, $1 \leq n \leq \frac{p-3}{2}$.

Como $\mathcal{U}_1^*(\mathbb{Z}C_p) = \left\langle \{w_i : 1 \leq i \leq \frac{p-3}{2}\} \right\rangle$, segue que $\mathrm{Im}(\rho) = \left\langle \{\rho(w_i) : 1 \leq i \leq \frac{p-3}{2}\} \right\rangle$, porque ρ um homomorfismo de grupos. Pelo que acabamos de mostrar, tem-se que, $\mathrm{Im}(\rho) = \langle \rho(w_1) \rangle$.

■

Deste resultado tem-se que $\rho(w_1^{2^{j-1}} w_j^{-1}) = \overline{1}$, isto é, $w_1^{2^{j-1}} w_j^{-1} \in \mathrm{Ker}(\rho)$.

Lema 2.2.4. *Seja p um primo ótimo. Então $\rho(w_1)^{2^{\frac{p-1}{2}}-1} = \overline{1}$.*

Demonstração:

Sabe-se que

$$\rho(w_1)^{2^n} = \widehat{g} + g^{(\frac{p-1}{2})\cdot 2^n}(\overline{1} + g^{2^n}),$$

logo,

$$\rho(w_1)^{2^{\frac{p-1}{2}}} = \widehat{g} + g^{(\frac{p-1}{2})\cdot 2^{\frac{p-1}{2}}}(\overline{1} + g^{2^{\frac{p-1}{2}}})$$

Como $\mathrm{mdc}(2, p) = 1$, então pelo Pequeno Teorema de Fermat tem-se $2^{p-1} \equiv 1 \pmod{p}$, ou ainda, $(2^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$, isto é, $(2^{\frac{p-1}{2}})^2 - 1 \equiv 0 \pmod{p}$. Entretanto $(2^{\frac{p-1}{2}})^2 - 1 = (2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1)$, o que implica que ou $2^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$, ou $2^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$.

Caso 1) Suponhamos que $2^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$.

Logo $2^{\frac{p-1}{2}} = pq + 1$, com $q \in \mathbb{Z}$. Assim

$$\rho(w_1)^{2^{\frac{p-1}{2}}} = \widehat{g} + g^{(\frac{p-1}{2})\cdot(pq+1)}(\overline{1} + g^{pq+1}),$$

ou seja,

$$\rho(w_1)^{2^{\frac{p-1}{2}}} = \widehat{g} + g^{(\frac{p-1}{2})}(\overline{1} + g),$$

isto é,

$$\rho(w_1)^{2^{\frac{p-1}{2}}} = \rho(w_1).$$

Como $\rho(w_1)$ é inversível segue que $\rho(w_1)^{2^{\frac{p-1}{2}}-1} = \overline{1}$.

Caso 2) Suponhamos que $2^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$.

Neste caso, $2^{\frac{p-1}{2}} \equiv -1 = p - 1 \pmod{p}$, e assim, $2^{\frac{p-1}{2}} = pq + (p-1)$, para algum $q \in \mathbb{Z}$. Então

$$\rho(w_1)^{2^{\frac{p-1}{2}}} = \widehat{g} + g^{(\frac{p-1}{2})\cdot(pq+p-1)}(\overline{1} + g^{pq+p-1}),$$

ou ainda,

$$\rho(w_1)^{2^{\frac{p-1}{2}}} = \widehat{g} + g^{(\frac{p+1}{2})}(1 + g^{p-1}),$$

de onde,

$$\rho(w_1)^{2^{\frac{p-1}{2}}} = \widehat{g} + g^{(\frac{p+1}{2})} + g^{(\frac{p-1}{2})}$$

e, portanto,

$$\rho(w_1)^{2^{\frac{p-1}{2}}} = \widehat{g} + g^{(\frac{p-1}{2})}(\overline{1} + g) = \rho(w_1).$$

Como $\rho(w_1)$ é inversível segue que $\rho(w_1)^{2^{\frac{p-1}{2}}-1} = \overline{1}$.

$\blacksquare$

Do Lema acima concluímos que $w_1^{2^{\frac{p-1}{2}}-1} \in \mathrm{Ker}(\rho)$ e que $\mathbf{ord}(\rho(w_1)) \leq 2^{\frac{p-1}{2}} - 1$. Seja

$$S_1 := \left\{ w_1^2 w_2^{-1}, w_1^4 w_3^{-1}, w_1^8 w_4^{-1}, \cdots, w_i^{2^i} w_{i+1}^{-1}, \cdots, w_1^{2^{\frac{p-3}{2}}} w_{\frac{p-1}{2}}^{-1} \right\}$$

Tal conjunto gera um subgrupo do núcleo do homomorfismos ρ.

Observe que $v_1 v_2 \cdots v_i = u_1(u_2 u_1^{-1})(u_3 u_2^{-1}) \cdots (u_{i-2} u_{i-1}^{-1})(u_i u_{i-1}^{-1}) = u_i$. Portanto, como $\{g, u_1, u_2, \cdots, u_{\frac{p-1}{2}}\}$ gera $\mathcal{U}(\mathbb{Z}C_p)$, então $\{g, v_1, v_2, \cdots, v_{\frac{p-1}{2}}\}$ também vai gerar $\mathcal{U}(\mathbb{Z}C_p)$. Mais ainda, como $\{u_1, u_2, \cdots, u_{\frac{p-1}{2}}\}$ é multiplicativamente independente, então $\{v_1, v_2, \cdots, v_{\frac{p-1}{2}}\}$ também o é.

Lema 2.2.5. *Seja p um primo ótimo. Temos que* $w_1 w_2 \cdots w_{\frac{p-1}{2}} = 1$

Demonstração:

Sabemos que $w_i = g^{(\frac{p-1}{2})\cdot 2^{i-1}} v_i,\ v_i = u_{i+1}u_i^{-1}$, para todo $2 \leq i \leq \dfrac{p-1}{2}$, e que $v_1 = u_1$. Portanto

$$w_1 w_2 \cdots w_{\frac{p-1}{2}} = g^{(\frac{p-1}{2})\cdot(1+2+2^2+\cdots+2^{\frac{p-3}{2}})} v_1 v_2 \cdots v_{\frac{p-1}{2}}.$$

Pela observação acima temos:

$$\begin{aligned} w_1 w_2 \cdots w_{\frac{p-1}{2}} &= g^{(\frac{p-1}{2})\cdot(2^{\frac{p-1}{2}}-1)} v_{\frac{p-1}{2}} \\ &= (1+g^2+g^4+\cdots+g^{p-1})(1+g^{2^{\frac{p-1}{2}}}) - \widehat{g} \end{aligned}$$

Lembre-se que, ou $2^{\frac{p-1}{2}} \equiv -1 = p-1 \pmod p$, ou $2^{\frac{p-1}{2}} \equiv 1 \pmod p$. Desta maneira:

Caso 1. $2^{\frac{p-1}{2}} \equiv -1 = p-1 \pmod p$

Nestas condições vamos ter que:

$$w_1 w_2 \cdots w_{\frac{p-1}{2}} = g^{(\frac{p-1}{2})(p-2)}(1+g^2+g^4+\cdots+g^{p-1})(1+g^{p-1}) - \widehat{g},$$

ou seja,

$$w_1 w_2 \cdots w_{\frac{p-1}{2}} = g(1+g^2+g^4+\cdots+g^{p-1}+g^{p-1}+g+g^3+\cdots+g^{p-2}) - \widehat{g},$$

isto é,

$$w_1 w_2 \cdots w_{\frac{p-1}{2}} = g(g^{p-1}+\widehat{g}) - \widehat{g} = 1.$$

Caso 2. $2^{\frac{p-1}{2}} \equiv 1 \pmod p$

Com estas hipóteses tem-se que:

$$w_1 w_2 \cdots w_{\frac{p-1}{2}} = (1+g^2+g^4+\cdots+g^{p-1})(1+g) - \widehat{g},$$

de onde,

$$w_1 w_2 \cdots w_{\frac{p-1}{2}} = (1+g^2+g^4+\cdots+g^{p-1}+g+g^3+g^5+\cdots+g^{p-2}+1) - \widehat{g},$$

ou ainda,

$$w_1 w_2 \cdots w_{\frac{p-1}{2}} = 1 + \widehat{g} - \widehat{g} = 1.$$

■

Considere o seguinte conjunto

$$S_2 := \left\{ w_1^2 w_2, w_1^4 w_3^{-1}, \cdots, w_1^{2^i} w_{i+1}^{-1}, \cdots, w_1^{2^{(\frac{p-3}{2})}+1} w_2 w_3 \cdots w_{\frac{p-3}{2}} \right\}$$

Pelo Lema 2.2.5 segue que $w_{\frac{p-1}{2}}^{-1} = w_1 w_2 \cdots w_{\frac{p-3}{2}}$ e, portanto, $\langle S_1 \rangle = \langle S_2 \rangle$.

Obseve que

$$(w_1^2 w_2^{-1})(w_1^4 w_3^{-1}) \cdots (w_1^{2^{\frac{p-5}{2}}} w_{\frac{p-3}{2}}^{-1})(w_1^{2^{\frac{p-3}{2}}} w_{\frac{p-1}{2}}^{-1}) = w_1^{2(1+2+\cdots+2^{\frac{p-5}{2}})+1},$$

ou ainda,

$$(w_1^2 w_2^{-1})(w_1^4 w_3^{-1}) \cdots (w_1^{2^{\frac{p-5}{2}}} w_{\frac{p-3}{2}}^{-1})(w_1^{2^{\frac{p-3}{2}}} w_{\frac{p-1}{2}}^{-1}) = w_1^{2(2^{\frac{p-3}{2}}-1)+1}$$

de onde, concluímos que,

$$(w_1^2 w_2^{-1})(w_1^4 w_3^{-1}) \cdots (w_1^{2^{\frac{p-5}{2}}} w_{\frac{p-3}{2}}^{-1})(w_1^{2^{\frac{p-3}{2}}} w_{\frac{p-1}{2}}^{-1}) = w_1^{2^{\frac{p-1}{2}}-1}.$$

Considere o conjunto

$$S_3 := \left\{ w_1^2 w_2^{-1}, w_1^4 w_3^{-1}, \cdots, w_1^{2^i} w_{i+1}^{-1}, \cdots, w_1^{2^{\frac{p-5}{2}}} w_{\frac{p-3}{2}}^{-1}, w_1^{2^{\frac{p-1}{2}}-1} \right\}$$

Pela observação acima segue que $\langle S_1 \rangle = \langle S_3 \rangle$.

Lema 2.2.6. *Se* $\boldsymbol{ord}(\rho(w_1)) = 2^{\frac{p-1}{2}} - 1$, *tem-se que* S_1 *gera o núcleo de* ρ.

Demonstração:

Do Lema 1.1.1 obtemos que $[\mathcal{U}^*(\mathbb{Z}C_p) : \langle S_3 \rangle] = |\det(A)|$, onde A é a matriz definida abaixo.

$$A = \begin{pmatrix} 2 & 4 & 8 & \cdots & 2^{\frac{p-5}{2}} & 2^{\frac{p-3}{2}} & 2^{\frac{p-1}{2}} - 1 \\ -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & -1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 & 0 \end{pmatrix}$$

Para calcular o determinante da matriz A vamos considerar a seguinte submatriz:

$$A_{1p-3} = \begin{pmatrix} -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & -1 \end{pmatrix}$$

Assim $|\det(A)| = (2^{\frac{p-1}{2}} - 1)|\det(A_{1\frac{p-3}{2}})|$. Como $|\det(A_{1\frac{p-3}{2}})| = 1$, então $|\det(A)| = 2^{\frac{p-1}{2}} - 1$.

Pelo Corolário 2.2.1 temos $\mathrm{Im}(\rho) = \langle \rho(w_1) \rangle$ e da hipótese vale que $|\mathrm{Im}(\rho)| = 2^{\frac{p-1}{2}} - 1$.

Como $\langle S_1 \rangle = \langle S_3 \rangle$, então $[\,\mathcal{U}^*(\mathbb{Z}C_p) : \langle S_1 \rangle] = 2^{\frac{p-1}{2}} - 1$ e sendo $\langle S_1 \rangle \subseteq \mathrm{Ker}(\rho)$ tem-se $\mathrm{Ker}(\rho) = \langle S_1 \rangle$.

■

Considere o conjunto

$$S_4 := \left\{ w_1^2 w_2^{-1}, w_2^2 w_3^{-1}, \cdots, w_i^2 w_{i+1}^{-1}, \cdots, w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1} \right\}$$

Vejamos que $\langle S_1 \rangle = \langle S_4 \rangle$.

Para todo $1 \leq i \leq \frac{p-1}{2}$ tem-se que:

$$(w_1^{2^{i-1}} w_i^{-1})^{-2}(w_1^{2^i} w_{i+1}^{-1}) = (w_1^{-2^i} w_i^2)(w_1^{2^i} w_{i+1}^{-1}) = w_i^2 w_{i+1}^{-2}.$$

Assim $\langle S_4 \rangle \subseteq \langle S_1 \rangle$.

Analogamente, para todo $1 \leq i \leq \frac{p-1}{2}$, vale que:

$$(w_1^2 w_2^{-1})^{2^{i-1}}(w_2^2 w_3^{-1})^{2^{i-2}} \cdots (w_{i-1}^2 w_i^{-1})^2 (w_i^2 w_{i+1}^{-1}) = (w_1^{2^i} w_2^{-2^{i-1}})(w_2^{2^{i-1}} w_3^{-2^{i-2}}) \cdots (w_{i-1}^4 w_i^{-2})(w_i^2 w_{i+1}^{-1}),$$

então,

$$(w_1^2 w_2^{-1})^{2^{i-1}}(w_2^2 w_3^{-1})^{2^{i-2}} \cdots (w_{i-1}^2 w_i^{-1})^2 (w_i^2 w_{i+1}^{-1}) = w_1^{2^i} w_{i+1}^{-1}.$$

Logo, $\langle S_1 \rangle \subseteq \langle S_4 \rangle$. Portanto, $\langle S_1 \rangle = \langle S_4 \rangle$.

O conjunto S_4 é bem interessante, uma vez que, cada elemento é levado no seu sucessor via o isomorfismo

$$\begin{array}{ccc} \mathbb{Z}C_p & \stackrel{\delta}{\to} & \mathbb{Z}C_p \\ \displaystyle\sum_{j=0}^{p-1} a_j g^j & \longmapsto & \displaystyle\sum_{j=0}^{p-1} a_j g^{2j} \end{array}$$

De fato, $\delta^i(w_1^2 w_2^{-1}) = \delta^i(w_1)^2 \delta^i(w_2)^{-1}$. Pelo Lema 2.2.2 $\delta^i(w_1)^2\delta^i(w_2)^{-1} = w_{i+1}^2 \delta^i(\delta(w_1))^{-1} = w_{i+1}^2 \delta^{i+1}(w_1)^{-1} = w_{i+1}^2 w_{i+2}^{-1}$, para todo $1 \leq i \leq \frac{p-5}{2}$. Sendo assim, ao calcular o primeiro elemento fica fácil determinar os demais.

Corolário 2.2.2. *Se* $\boldsymbol{ord}(\rho(w_1)) = 2^{\frac{p-1}{2}} - 1$, *então* $Ker(\rho) = \langle S_4 \rangle$.

Demonstração:

Como $\langle S_1 \rangle = \langle S_4 \rangle$ segue do Lema 2.2.6 que $\mathrm{Ker}(\rho) = \langle S_4 \rangle$.

■

Pela maneira que descrevemos as unidades de $\mathbb{Z}C_{2p}$, precisamos saber como multiplicar certo tipos de elementos, e como escrever seus inversos. Os dois próximos resultados tratam disso.

Lema 2.2.7. *Sejam* $C_2 \cong \langle a \rangle$ *e* $b_i \in \mathbb{Z}C_p$ *tal que* $b_i \equiv 1 \ (mod \ \langle 2 \rangle)$, $1 \leq i \leq n$. *Para todo* $n \geq 2 \in \mathbb{N}$, *tem-se:*

$$\frac{1 + b_1 b_2 \cdots b_n}{2} + \left(\frac{1 - b_1 b_2 \cdots b_n}{2}\right) a = \left[\frac{1+b_1}{2} + \left(\frac{1-b_1}{2}\right) a\right] \cdots \left[\frac{1+b_n}{2} + \left(\frac{1-b_n}{2}\right) a\right].$$

Em particular,

$$\frac{1+b_1^n}{2}+\left(\frac{1-b_1^n}{2}\right)a=\left[\frac{1+b_1}{2}+\left(\frac{1-b_1}{2}\right)a\right]^n.$$

Demonstração:

Façamos a prova por indução sobre n.

Para $n=2$, temos que

$$\begin{aligned}\left[\frac{1+b_1}{2}+\left(\frac{1-b_1}{2}\right)a\right]\left[\frac{1+b_2}{2}+\left(\frac{1-b_2}{2}\right)a\right] &= \frac{(1+b_1+b_2+b_1b_2)+(1-b_1-b_2+b_1b_2)}{4}+\\ &+\left(\frac{(1+b_1-b_2-b_1b_2)+(1-b_1+b_2-b_1b_2)}{4}\right)a,\end{aligned}$$

ou seja,

$$\left[\frac{1+b_1}{2}+\left(\frac{1-b_1}{2}\right)a\right]\left[\frac{1+b_2}{2}+\left(\frac{1-b_2}{2}\right)a\right] = \frac{2+2b_1b_2}{4}+\left(\frac{2-2b_1b_2}{4}\right)a,$$

isto é,

$$\left[\frac{1+b_1}{2}+\left(\frac{1-b_1}{2}\right)a\right]\left[\frac{1+b_2}{2}+\left(\frac{1-b_2}{2}\right)a\right]=\frac{1+b_1b_2}{2}+\left(\frac{1-b_1b_2}{2}\right)a.$$

Suponhamos que a igualdade se verifica para $n=k$, o que significa que,

$$\frac{1+b_1b_2\cdots b_k}{2}+\left(\frac{1-b_1b_2\cdots b_k}{2}\right)a=\left[\frac{1+b_1}{2}+\left(\frac{1-b_1}{2}\right)a\right]\cdots\left[\frac{1+b_k}{2}+\left(\frac{1-b_k}{2}\right)a\right]$$

e vamos mostrar que a fórmula vale para $n=k+1$. Pela hipótese indutiva, tem-se que:

$$\left[\frac{1+b_1}{2}+\left(\frac{1-b_1}{2}\right)a\right]\left[\frac{1+b_2}{2}+\left(\frac{1-b_2}{2}\right)a\right]\cdots\left[\frac{1+b_k}{2}+\left(\frac{1-b_k}{2}\right)a\right]\left[\frac{1+b_{k+1}}{2}+\left(\frac{1-b_{k+1}}{2}\right)a\right]=$$
$$\left[\frac{1+b_1b_2\cdots b_k}{2}+\left(\frac{1-b_1b_2\cdots b_k}{2}\right)a\right]\cdot\left[\frac{1+b_{k+1}}{2}+\left(\frac{1-b_{k+1}}{2}\right)a\right]$$

e, como provamos que a igualdade se verifica para $n=2$, segue que

$$\frac{1+b_1b_2\cdots b_kb_{k+1}}{2}+\left(\frac{1-b_1b_2\cdots b_kb_{k+1}}{2}\right)a,$$

$1\leq i\leq\dfrac{p-1}{2}$.

Tomando $b_1=b_2=\cdots=b_n$ segue o caso particular.

$\blacksquare$

Lema 2.2.8. *Seja $C_2 \cong \langle a \rangle$. Se b é uma unidade de $\mathbb{Z}C_p$, então*

$$\left[\frac{1+b}{2} + \left(\frac{1-b}{2}\right)a\right]^{-1} = \frac{1+b^{-1}}{2} + \left(\frac{1-b^{-1}}{2}\right)a.$$

Demonstração:

Observe que:

$$\begin{aligned}\left[\frac{1+b}{2} + \left(\frac{1-b}{2}\right)a\right]\left[\frac{1+b^{-1}}{2} + \left(\frac{1-b^{-1}}{2}\right)a\right] &= \frac{(1+b+b^{-1}+1)+(1-b-b^{-1}+1)}{4} + \\ &+ \left(\frac{(1-b+b^{-1}-1)-(1+b-b^{-1}-1)}{4}\right)a,\end{aligned}$$

ou seja,

$$\left[\frac{1+b}{2} + \left(\frac{1-b}{2}\right)a\right]\left[\frac{1+b^{-1}}{2} + \left(\frac{1-b^{-1}}{2}\right)a\right] = 1.$$

Portanto:

$$\left[\frac{1+b}{2} + \left(\frac{1-b}{2}\right)a\right]^{-1} = \frac{1+b^{-1}}{2} + \left(\frac{1-b^{-1}}{2}\right)a$$

■

2.3 Construção das unidades

Como determinamos o núcleo da função ρ podemos, enfim, descrever as unidades de $\mathbb{Z}C_{2p}$. Retomando,

$$\begin{aligned} w_i &:= g^{(\frac{p-1}{2})\cdot 2^{i-1}} v_i = (-1)^{(\frac{p-3}{2})}(1 - g^{2^{i-1}} + g^{2\cdot 2^{i-1}} + \cdots + (-1)^{(\frac{p-3}{2})} g^{(\frac{p-3}{2})\cdot 2^{i-1}} + \\ &+(-1)^{(\frac{p-3}{2})} g^{(\frac{p+3}{2})\cdot 2^{i-1}} + \cdots + g^{(p-2)\cdot 2^{i-1}} - g^{(p-1)\cdot 2^{i-1}}),\end{aligned}$$

$$u_i(a) := (1-\beta_i) + \beta_i a,$$

sendo $\beta_1 = \frac{1-w_1^2 w_2^{-1}}{2}$, $\beta_i = \delta^{i-1}(\beta_1)$, $1 \leq i \leq \frac{p-3}{2}$ e $\delta : \mathbb{Z}C_p \to \mathbb{Z}C_p$ um homomorfismo tal que $\delta(g^i) = g^{2i}$ e que fixa os números inteiros.

Teorema 2.3.1. *Considere o anel de grupo integral $\mathbb{Z}C_{2p}$, onde $C_p = \langle g \rangle, C_2 \cong \langle a \rangle$ e p é um primo ótimo. Se* $\textbf{\textit{ord}}(\rho(w_1)) = 2^{\frac{p-1}{2}} - 1$, *então*

$$\mathcal{U}(\mathbb{Z}C_{2p}) = \langle -1 \rangle \times \langle g, a \rangle \times \left\langle \left\{ w_i : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle \times \left\langle \left\{ u_i(a) : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle.$$

Mais ainda, o conjunto $\left\{w_1, w_2, \ldots, w_{\frac{p-3}{2}}, u_1(a), u_2(a), \ldots, u_{\frac{p-3}{2}}(a)\right\}$ *é multiplicativamente independente.*

Demonstração:

Conforme vimos tem-se que

$$\mathcal{U}(\mathbb{Z}C_p) = \langle -1 \rangle \times \langle g \rangle \times \left\langle \left\{ w_i : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle,$$

Considere o seguinte homomorfismo de anéis $\psi : \mathbb{Z}C_p \to \mathbb{Z}_2(C_p)$ definido de maneira usual e seja $\rho := \psi|_{\mathcal{U}_1^*(\mathbb{Z}C_p)}$. Sabe-se que

$$u \in \mathcal{U}(\mathbb{Z}C_{2p}) \Leftrightarrow u = u_1 \left[\left(\frac{1+u_2}{2} \right) + \left(\frac{1-u_2}{2} \right) a \right],$$

onde $u_1, u_2 \in \mathcal{U}(\mathbb{Z}C_p)$ e $u_2 \in \text{Ker}(\psi|_{\mathcal{U}(\mathbb{Z}C_p)})$.

Sendo p um primo ímpar, do Teorema 1.4.2 tem-se $\mathcal{U}_1(\mathbb{Z}C_p) = \langle g \rangle \times \mathcal{U}_1^*(\mathbb{Z}C_p)$. Entretanto $g \notin \text{Ker}(\psi)$, e como, $\mathcal{U}(\mathbb{Z}C_p) = \pm \mathcal{U}_1(\mathbb{Z}C_p)$, obtém-se que $\text{Ker}(\psi|_{\mathcal{U}(\mathbb{Z}C_p)}) = \langle -1 \rangle \times \langle \text{Ker}(\rho) \rangle$, uma vez que, $-1 \in \text{Ker}(\psi)$. Então, precisamos determinar o núcleo da função ρ.

Do Corolário 2.2.2 tem-se

$$\text{Ker}(\rho) = \left\langle w_1^2 w_2^{-1}, w_2^2 w_3^{-1}, \cdots, w_i^2 w_{i+1}^{-1}, \cdots, w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1} \right\rangle.$$

Defina, para todo $1 \leq i \leq \dfrac{p-3}{2}$, o seguinte elemento $\beta_i := \dfrac{1 - w_i^2 w_{i+1}^{-1}}{2}$ e considere $u_i(a) = (1 - \beta_i) + \beta_1 a$.

Assim

$$u_2 \in \langle -1 \rangle \times \left\langle w_1^2 w_2^{-1}, w_2^2 w_3^{-1}, \cdots, w_i^2 w_{i+1}^{-1}, \cdots, w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1} \right\rangle$$

e, portanto,

$$u_2 = (-1)^n (w_1^2 w_2^{-1})^{\alpha_1} (w_2^2 w_3^{-1})^{\alpha_2} \cdots (w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1})^{\alpha_{\frac{p-3}{2}}}.$$

Do Lema 2.2.7 e do Lema 2.2.8 segue

$$\frac{1+u_2}{2} + \left(\frac{1-u_2}{2} \right) a = \left[\frac{1+(-1)}{2} + \left(\frac{1-(-1)}{2} \right) a \right]^n \left[\frac{1 + w_1^2 w_2^{-1}}{2} + \left(\frac{1 - w_1^2 w_2^{-1}}{2} \right) a \right]^{\alpha_1} \cdots$$

$$\left[\frac{1 + w_{\frac{p-5}{2}}^2 w_{\frac{p-3}{2}}^{-1}}{2} + \left(\frac{1 - w_{\frac{p-5}{2}}^2 w_{\frac{p-3}{2}}^{-1}}{2} \right) a \right]^{\alpha_{\frac{p-5}{2}}} \left[\frac{1 + w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1}}{2} + \left(\frac{1 - w_{\frac{p-1}{2}}^2 w_{\frac{p-1}{2}}^{-1}}{2} \right) a \right]^{\alpha_{\frac{p-3}{2}}},$$

isto é,

$$\frac{1+u_2}{2}+\left(\frac{1-u_2}{2}\right)a=a^n u_1(a)^{\alpha_1}u_2(a)^{\alpha_2}\cdots u_{\frac{p-3}{2}}(a)^{\alpha_{\frac{p-3}{2}}},$$

ou seja,

$$\frac{1+u_2}{2}+\left(\frac{1-u_2}{2}\right)a\in\langle a\rangle\times\left\langle u_1(a),\cdots,u_{\frac{p-3}{2}}(a)\right\rangle.$$

Além disso,

$$u_1\in\mathcal{U}(\mathbb{Z}C_p)=\langle -1\rangle\times\langle g\rangle\times\left\langle\{w_i:1\leq i\leq\frac{p-3}{2}\}\right\rangle,$$

que implica que,

$$\mathcal{U}(\mathbb{Z}C_{2p})=\langle -1\rangle\times\langle g,a\rangle\times\left\langle\{w_i:1\leq i\leq\frac{p-3}{2}\}\right\rangle\times\left\langle u_1(a),u_2(a),\ldots,u_{\frac{p-3}{2}}(a)\right\rangle.$$

Falta verificar que $\{w_1,w_2,\ldots,w_{\frac{p-3}{2}},u_1(a),u_2(a),\ldots,u_{\frac{p-3}{2}}(a)\}$ é um conjunto multiplicativamente independente. Sabe-se que C_{2p} possui 4 subgrupos cíclicos e um único subgrupo cíclico de ordem 2. Assim, do Teorema 1.4.1, tem-se **posto**$(\mathcal{U}_1(\mathbb{Z}C_{2p}))=\frac{1}{2}[2p-2\cdot 4+1+1]=p-3$. Como o conjunto $\{w_1,w_2,\ldots,w_{\frac{p-3}{2}},u_1(a),u_2(a),\ldots,u_{\frac{p-3}{2}}(a)\}$ gera $\mathcal{U}_1(\mathbb{Z}C_{2p})$, segue que tal conjunto é multiplicativamente independente.

■

Vejamos alguns exemplos para ilustrar este Teorema. Para os primos $p=5,7,11,13,19,23$ e 37 os cálculos forma feitos primeiramente no papel e depois usamos tanto o **GAP** quanto o **MAPLE** para conferir as contas. Já para os primos $p=53,59,61$ e 67 os cálculos forma feitos diretamente no **GAP** e no **MAPLE**.

Exemplo 8. *Considere* $C_{10}\cong C_5\times C_2$*, onde* $C_5\cong\langle g\rangle$ *e* $C_2\cong\langle a\rangle$*. Vamos determinar* $\mathcal{U}(\mathbb{Z}C_{10})$

Este exemplo foi feito em [17] por Low. Ferraz em [6] mostrou que:

$$\mathcal{U}_1(\mathbb{Z}C_5)=\langle g\rangle\times\langle v\rangle$$

onde $v=1-g+g^2$. Considere $w=g^4v=-1+g+g^4$.

Considere o seguinte homomorfismo de grupos $\rho:\mathcal{U}_1^*(\mathbb{Z}C_5)\to\mathcal{U}_1^*(\mathbb{Z}_2C_5)$ definido como

$\rho(u) := \psi(u)$, onde $\psi : \mathbb{Z}C_5 \to \mathbb{Z}_2C_5$ define-se da maneira usual. Temos que:

$$\begin{aligned} \rho(w) &= \overline{1} + g + g^4, \\ \rho(w)^2 &= \overline{1} + g^2 + g^3, \\ \rho(w)^3 &= \overline{1}. \end{aligned}$$

Logo $w^3 \in \mathrm{Ker}(\rho)$ e, como 3 é um número primo, então $\mathbf{ord}(\rho(w)) = 3$. Do Corolário 2.2.2 podemos concluir que, $\mathrm{Ker}(\rho) = \langle w^3 \rangle$.

Sendo $w^3 = -7+6g-2g^2-2g^3+6g^4$, considere $\alpha := \dfrac{1-w^3}{2} = 4-3g+g^2+g^3-3g^4$. Definimos $u(a) := (1-\alpha)+\alpha a = (-3+3g-g^2-g^3+3g^4)+(4-3g+g^2+g^3-3g^4)a$

Logo, pelo Teorema 2.3.1

$$\mathcal{U}(\mathbb{Z}C_{10}) = \langle -1 \rangle \times \langle g \rangle \times \langle w \rangle \times \langle u(a) \rangle$$

A condição de que $\mathbf{ord}(\rho(w_1) = 2^{\frac{p-1}{2}} - 1$ é necessária. O exemplo a seguir não satisfaz esta hipótese.

Exemplo 9. *Considere* $C_{74} \cong C_{37} \times C_2$, *onde* $C_{37} \cong \langle g \rangle$ *e* $C_2 \cong \langle a \rangle$. *Nosso objetivo é determinar* $\mathcal{U}(\mathbb{Z}C_{74})$.

Sabemos que

$$\mathcal{U}_1(\mathbb{Z}C_{37}) = \langle g \rangle \times \langle \{u_i : 1 \leq i \leq 17\} \rangle .$$

Seja

$$\begin{aligned} w_1 \ = \ & -1+g-g^2+g^3-g^4+g^5-g^6+g^7-g^8+g^9-g^{10}+g^{11}-g^{12}+g^{13}-g^{14}+g^{15}-g^{16}+ \\ & +g^{17}+g^{20}-g^{21}+g^{22}-g^{23}+g^{24}-g^{25}+g^{26}-g^{27}+g^{28}-g^{29}+g^{30}-g^{31}+g^{32}-g^{33}+ \\ & +g^{34}-g^{35}+g^{36}, \end{aligned}$$

seja $\psi : \mathbb{Z}C_{37} \to \mathbb{Z}_2C_{37}$ determinada de maneira usual, e defina $\rho := \psi|_{\mathcal{U}_1^*(\mathbb{Z}C_{37})}$. Temos que:

$$\begin{aligned}\rho(w_1) &= \overline{1} + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + \\ &\quad + g^{17} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + g^{28} + g^{29} + g^{30} + g^{31} + g^{32} + g^{33} + \\ &\quad + g^{34} + g^{35} + g^{36}.\end{aligned}$$

Do Lema 2.2.4 sabemos que $\rho(w_1)^{262143} = \overline{1}$. Como $262143 = 3^3 \cdot 7 \cdot 19 \cdot 73$ precisamos verificar se $\mathbf{ord}(\rho(w_1) = 262143$. Porém, ao efetuar os cálculos com o auxílio do **GAP**, descobrimos que $\rho(w_1)^{3^2 \cdot 7 \cdot 19 \cdot 73} = \overline{1}$ e, portanto, $\mathbf{ord}(\rho(w_1)) = 3^2 \cdot 7 \cdot 19 \cdot 73 = 87381$, não satisfazendo a nossa hipótese.

Exemplo 10. *Considere $C_{14} \cong C_7 \times C_2$, onde $C_7 \cong \langle g \rangle$ e $C_2 \cong \langle a \rangle$. Queremos determinar $\mathcal{U}(\mathbb{Z}C_{14})$.*

Do Teorema 1.4.3 e lembrando que $\langle g \rangle \times \langle w_1, w_2 \rangle$ também gera $\mathcal{U}_1(\mathbb{Z}C_7)$ tem-se:

$$\mathcal{U}_1(\mathbb{Z}C_7) = \langle g \rangle \times \langle w_1, w_2 \rangle$$

onde $w_1 = 1 - g + g^2 + g^5 - g^6$ e $w_2 = 1 - g^2 + g^3 + g^4 - g^5$.

Sejam $\psi : \mathbb{Z}C_7 \to \mathbb{Z}_2C_7$ e $\rho := \psi|_{\mathcal{U}_1^*(\mathbb{Z}C_7)}$. Observe que:

$$\begin{aligned}\rho(w_1) &= \overline{1} + g + g^2 + g^5 + g^6 \\ \rho(w_1)^4 &= \rho(w_2) \\ \rho(w_1)^7 &= \overline{1}.\end{aligned}$$

Como 7 é um número primo segue que $\mathbf{ord}(\rho(w_1)) = 7$. Sejam:

$$\begin{aligned}\beta_1 &= \frac{1 - w_1^3 w_2^{-1}}{2} = 4 - 3g + 2g^2 - g^3 - g^4 + 2g^5 - 3g^6 \\ \beta_2 &= \frac{1 - w_1 w_2^2}{2} = 4 - g - 3g^2 + 2g^3 + 2g^4 - 3g^5 - g^6\end{aligned}$$

definimos

$$\begin{aligned}
u_1(a) &= (1-\beta_1)+\beta_1 a\\
&= (-3+3g-2g^2+g^3+g^4-2g^5+3g^6)+(4-3g+2g^2-g^3-g^4+2g^5-3g^6)a\\
u_2(a) &= (1-\beta_2)+\beta_2 a\\
&= (-3+g+3g^2-2g^3-2g^4+3g^5+g^6)+(4-g-3g^2+2g^3+2g^4-3g^5-g^6)a
\end{aligned}$$

Do Teorema 2.3.1 obtém-se

$$\mathcal{U}(\mathbb{Z}C_{14})=\langle -1\rangle\times\langle g\rangle\times\langle w_1,w_2\rangle\times\langle u_1(a),u_2(a)\rangle\,.$$

Exemplo 11. *Considere $C_{22}\cong C_{11}\times C_2$, onde $C_{11}\cong\langle g\rangle$ e $C_2\cong\langle a\rangle$. Estamos interessados em descrever $\mathcal{U}(\mathbb{Z}C_{22})$.*

Sabemos que

$$\mathcal{U}_1(\mathbb{Z}C_{11})=\langle g\rangle\times\langle\{w_i:1\leq i\leq 4\}\rangle$$

onde

$$\begin{aligned}
w_1 &= 1-g+g^2-g^3+g^4+g^7-g^8+g^9-g^{10}\\
w_2=\delta(w_1) &= 1-g^2+g^3+g^4-g^5-g^6+g^7+g^8-g^9\\
w_3=\delta^2(w_1) &= 1-g+g^3-g^4+g^5+g^6-g^7+g^8-g^{10}\\
w_4=\delta^3(w_1) &= 1+g-g^2-g^3+g^5+g^6-g^8-g^9+g^{10}\\
w_5=\delta^4(w_1) &= 1+g+g^2-g^4-g^5-g^6-g^7+g^9+g^{10}
\end{aligned}$$

sendo $\delta:\mathbb{Z}C_{11}\to\mathbb{Z}C_{11}$ a função $\delta\left(\sum_{j=0}^{10}a_jg^j\right)=\sum_{j=0}^{10}a_jg^{2j}$.

Considere o seguinte homomorfismo de grupos $\rho:\mathcal{U}_1^*(\mathbb{Z}C_{11})\to\mathcal{U}_1^*(\mathbb{Z}_2C_{11})$ definido como $\rho(u):=\psi(u)$, onde $\psi:\mathbb{Z}C_{11}\to\mathbb{Z}_2C_{11}$ define-se da maneira usual. Temos que:

$$\rho(w_1)=\overline{1}+g+g^2+g^3+g^4+g^7+g^8+g^9+g^{10}.$$

Do Corolário 2.2.1, temos $\rho(w_1)^{2^i}=\rho(w_{i+1}),\ \forall\ 1\leq i\leq 4$ e pelo Lema 2.2.4 obtemos $\rho(w_1)^{31}=\overline{1}$. Como 31 é um número primo, segue que $\mathbf{ord}(\rho(w_1))=31$. Sendo

$w_2^{-1} = 1 + g^3 - g^4 - g^7 + g^8$ então,

$$\beta_1 = \frac{1 - w_1^3 w_2^{-1}}{2} = 4 - 4g + 4g^2 - 4g^3 + 3g^4 - g^5 - g^6 + 3g^7 - 4g^8 + 4g^9 - 4g^{10}$$

e $\beta_i = \delta^{i-1}(\beta_1)$, para todo $1 \leq i \leq 4$. Considere $u_i(a) := (1 - \beta_i) + \beta_i a$, para todo $1 \leq i \leq 4$ e, portanto, pelo Teorema 2.3.1 tem-se

$$\mathcal{U}(\mathbb{Z}C_{22}) = \langle -1 \rangle \times \langle g \rangle \times \langle \{w_i : 1 \leq i \leq 4\} \rangle \times \langle \{u_i(a) : 1 \leq i \leq 4\} \rangle .$$

Exemplo 12. *Considere $C_{26} \cong C_{13} \times C_2$, onde $C_{13} \cong \langle g \rangle$ e $C_2 \cong \langle a \rangle$. Queremos determinar $\mathcal{U}(\mathbb{Z}C_{22})$.*

Como

$$\mathcal{U}_1(\mathbb{Z}C_{13}) = \langle g \rangle \times \langle \{w_i : 1 \leq i \leq 5\} \rangle ,$$

onde $w_1 = -1 + g - g^2 + g^3 - g^4 + g^5 - g^6 + g^7 + g^{10} - g^{11} + g^{12}$ e $w_i = \delta^{i-1}(w_1)$, $\forall\ 2 \leq i \leq 5$, sendo $\delta : \mathbb{Z}C_{13} \to \mathbb{Z}C_{13}$ definida por $\delta\left(\sum_{j=0}^{12} a_j g^j\right) = \sum_{j=0}^{12} a_j g^{2j}$. Considere o seguinte elemento $w_2^{-1} = -1 + g + g^4 - g^5 - g^8 + g^9 + g^{12}$.

Seja o seguinte homomorfismo de anéis $\psi : \mathbb{Z}C_{13} \to \mathbb{Z}_2 C_{13}$ definido da maneira usual e considere $\rho : \mathcal{U}_1^*(\mathbb{Z}C_{13}) \to \mathcal{U}_1^*(\mathbb{Z}_2 C_{13})$ tal que $\rho(u) := \psi(u)$. Então vamos ter que:

$$\rho(w_1) = \overline{1} + g + g^2 + g^3 + g^4 + g^5 + g^8 + g^9 + g^{10} + g^{11} + g^{12}.$$

Do Corolário 2.2.1, segue que $\rho(w_1)^{2^i} = \rho(w_{i+1})$, para todo $1 \leq i \leq 6$ e, do Lema 2.2.4, conclui-se que $\rho(w_1)^{63} = \overline{1}$. Como $63 = 3^2 \cdot 7$, precisamos verificar que $\mathbf{ord}(\rho(w_1)) = 63$. Porém

$$\begin{aligned} \rho(w_1)^{3^2} &= 1 + g + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{12} \neq \overline{1} \\ \rho(w_1)^{3 \cdot 7} &= 1 + g^2 + g^5 + g^6 + g^7 + g^8 + g^{11} \neq \overline{1} \end{aligned}$$

e, portanto, $\mathrm{ord}(\rho(w_1)) = 63$.

Sejam $\beta_1 = \dfrac{1 - w_1^2 w_2^{-1}}{2} = 8 - 7g + 5g^2 - 3g^3 + g^4 + g^9 - 3g^{10} + 5g^{11} - 7g^{12}$ e $\beta_i = \delta^{i-1}(\beta_1)$ e, considere, $u_i(a) := (1 - \beta_i) + \beta_i a$, $\forall\ 1 \leq i \leq 5$. Então pelo Teorema 2.3.1 tem-se

$$\mathcal{U}(\mathbb{Z}C_{26}) = \langle -1 \rangle \times \langle g \rangle \times \langle \{w_i : 1 \leq i \leq 5\} \rangle \times \langle \{u_i(a) : 1 \leq i \leq 5\} \rangle .$$

Exemplo 13. *Considere* $C_{38} \cong C_{19} \times C_2$, *onde* $C_{19} \cong \langle g \rangle$ *e* $C_2 \cong \langle a \rangle$. *Pretende-se determinar* $\mathcal{U}(\mathbb{Z}C_{38})$.

Lembrando que

$$\mathcal{U}_1(\mathbb{Z}C_{19}) = \langle g \rangle \times \langle \{w_i : 1 \leq i \leq 8\} \rangle ,$$

onde $w_1 = 1 - g + g^2 - g^3 + g^4 - g^5 + g^6 - g^7 + g^8 + g^{11} - g^{12} + g^{13} - g^{14} + g^{15} - g^{16} + g^{17} - g^{18}$ e $w_i = \delta^{i-1}(w_1),\ \forall\, 1 \leq i \leq 8$, sendo que $\delta : \mathbb{Z}C_{19} \to \mathbb{Z}C_{19}$ representa a função

$$\delta\left(\sum_{j=0}^{18} a_j g^j\right) = \sum_{j=0}^{18} a_j g^{2j}.$$

Considere o seguinte elemento $w_2^{-1} = 1 + g^3 - g^4 - g^7 + g^8 + g^{11} - g^{12} - g^{15} + g^{16}$. Seja $\psi : \mathbb{Z}C_{19} \to \mathbb{Z}_2C_{19}$ definida de maneira usual e considere $\rho(u) := \psi(u),$ para todo $u \in \mathcal{U}_1^*(\mathbb{Z}C_{19})$. Temos:

$$\rho(w_1) = \overline{1} + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + g^{17} + g^{18}$$

Pelo Corolário 2.2.1, obtemos $\rho(w_1)^{2^i} = \rho(w_i)$ para todo $1 \leq i \leq 9$, e, do Lema 2.2.4, segue que $\rho(w_1)^{511} = \overline{1}$. Como $511 = 7 \cdot 73$, é preciso mostrar que $\mathbf{ord}(\rho(w_1)) = 511$. Sendo

$$\begin{aligned} \rho(w_1)^7 &= 1 + g + g^2 + g^3 + g^4 + g^5 + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} \neq \overline{1} \\ \rho(w_1)^{73} &= 1 + g^2 + g^3 + g^4 + g^5 + g^6 + g^9 + g^{10} + g^{13} + g^{14} + g^{15} + g^{16} + g^{17} \neq \overline{1}, \end{aligned}$$

pode-se concluir que, $\mathbf{ord}(\rho(w_1)) = 511$. Sejam:

$$\beta_1 = \frac{1 - w_1^2 w_2^{-1}}{2} = 8 - 8g + 8g^2 - 8g^3 + 7g^4 - 5g^5 + 3g^6 - g^7 - g^{12} + 3g^{13} - 5g^{14} + 7g^{15} - 8g^{16} + 8g^{17} - 8g^{18}$$

e $\beta_i = \delta^{i-1}(\beta_1)$ e defina $u_i(a) := (1 - \beta_i) + \beta_i a,\ 1 \leq i \leq 8$. Então do Teorema 2.3.1 segue que

$$\mathcal{U}(\mathbb{Z}C_{38}) = \langle -1 \rangle \times \langle g \rangle \times \langle \{w_i : 1 \leq i \leq 8\} \rangle \times \langle \{u_i(a) : 1 \leq i \leq 8\} \rangle .$$

Exemplo 14. *Considere* $C_{46} \cong C_{23} \times C_2$, *onde* $C_{23} \cong \langle g \rangle$ *e* $C_2 \cong \langle a \rangle$. *Queremos descrever* $\mathcal{U}(\mathbb{Z}C_{46})$.

Sabemos pelo Teorema 1.4.3 e do fato de $\langle g\rangle \times \langle\{w_i : 1 \leq i \leq 10\}\rangle$ gerar $\mathcal{U}_1(\mathbb{Z}C_{23})$ que

$$\mathcal{U}_1(\mathbb{Z}C_{23}) = \langle g\rangle \times \langle\{w_i : 1 \leq i \leq 10\}\rangle\,,$$

onde

$$w_1 = 1-g+g^2-g^3+g^4-g^5+g^6-g^7+g^8-g^9+g^{10}+g13-g^{14}+g^{15}-g^{16}+g^{17}-g^{18}++g^{19}-g^{20}+g^{21}-g^{22}$$

e $w_i = \delta^{i-1}(w_1)$, para todo $1 \leq i \leq 11$, sendo a função $\delta : \mathbb{Z}C_{23} \to \mathbb{Z}C_{23}$ dada por $\delta\left(\sum_{j=0}^{22} a_j g^j\right) = \sum_{j=0}^{22} a_j g^{2j}$. Sejam $\psi : \mathbb{Z}C_{23} \to \mathbb{Z}_2C_{23}$ e $\rho := \psi|_{U_1^*(\mathbb{Z}C_{23})}$. Observe que:

$$\rho(w_1) = \overline{1}+g+g^2+g^3+g^4+g^5+g^6+g^7+g^8+g^9+g^{10}+g^{13}+g^{14}+g^{15}+g^{16}+g^{17}+g^{18}+g^{19}+g^{20}+g^{21}+g^{22}.$$

Do Corolário 2.2.1, tem-se $\rho(w_1)^{2^i} = \rho(w_{i+1}),\ \forall\ 1 \leq i \leq 10$ e, pelo Lema 2.2.4, obtém-se $\rho(w_1)^{2047} = \overline{1}$. Como $2047 = 23 \cdot 89$, e

$$\begin{aligned}
\rho(w_1)^{23} &= \overline{1} + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} \neq \overline{1} \\
\rho(w_1)^{89} &= \overline{1} + g^3 + g^4 + g^5 + g^9 + g^{11} + g^{12} + g^{14} + g^{18} + g^{19} + g^{20} \neq \overline{1},
\end{aligned}$$

então $\mathbf{ord}(\rho(w_1)) = 2047$.

Considere $w_2^{-1} = 1+g-g^3-g^4-g^5+g^7+g^8+g^9-g^{11}-g^{12}+g^{14}+g^{15}+g^{16}-g^{18}-g^{19}-g^{20}+g^{22}$, e sejam

$$\begin{aligned}
\beta_1 &= \frac{1 - w_1^2 w_2^{-1}}{2} \\
&= 12 - 11g + 10g^2 - 9g^3 + 7g^4 - 6g^5 + 5g^6 - 4g^7 + 4g^8 - 3g^9 + 2g^{10} - g^{11} - g^{12} + 2g^{13} + \\
&\quad -3g^{14} + 4g^{15} - 4g^{16} + 5g^{17} - 6g^{18} + 7g^{19} - 9g^{20} + 10g^{21} - 11g^{22},
\end{aligned}$$

$\beta_i = \delta^{i-1}(\beta_1)$, e defina $u_i(a) = (1 + \alpha_i) + \alpha_i a$, para todo $1 \leq i \leq 10$. Do Teorema 2.3.1 segue que

$$\mathcal{U}(\mathbb{Z}C_{46}) = \langle -1\rangle \times \langle g\rangle \times \langle\{w_i : 1 \leq i \leq 10\}\rangle \times \langle\{u_j(a) : 1 \leq j \leq 10\}\rangle$$

Exemplo 15. *Considere* $C_{58} \cong C_{29} \times C_2$, *onde* $C_{29} \cong \langle g\rangle$ *e* $C_2 \cong \langle a\rangle$. *Nosso intuito é descrever* $\mathcal{U}(\mathbb{Z}C_{58})$.

Como

$$\mathcal{U}_1(\mathbb{Z}C_{29}) = \langle g \rangle \times \langle \{w_i : 1 \leq i \leq 13\} \rangle,$$

onde

$$\begin{aligned} w_1 &= -1 + g - g^2 + g^3 - g^4 + g^5 - g^6 + g^7 + g^{11} - g^8 + g^9 - g^{10} - g^{12} + g^{13} + g^{16} - g^{17} - g^{21} + \\ &\quad + g^{18} - g^{19} + g^{20} + g^{24} + g^{22} - g^{23} - g^{25} + g^{26} - g^{27} + g^{28} \end{aligned}$$

e $w_i = \delta^{i-1}(w_1)$, para todo $1 \leq i \leq 14$, e a função $\delta : \mathbb{Z}C_{29} \to \mathbb{Z}C_{29}$ é definida por $\delta\left(\sum_{j=0}^{28} a_j g^j\right) = \sum_{j=0}^{28} a_j g^{2j}$.

Seja a função $\psi : \mathbb{Z}C_{29} \to \mathbb{Z}_2C_{29}$ definida da maneira usual e considere $\rho := \psi|_{\mathcal{U}_1^*(\mathbb{Z}C_{29})}$. Temos que:

$$\begin{aligned} \rho(w_1) &= \overline{1} + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{16} \\ &\quad + g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + g^{28} \end{aligned}$$

Do Corolário 2.2.1 obtém-se $\rho(w_1)^{2^i} = \rho(w_{i+1})$, $\forall\, 1 \leq i \leq 13$ e ,pelo Lema 2.2.4, $\rho(w_1)^{16383} = \overline{1}$. Temos que $16383 = 3 \cdot 43 \cdot 127$, e como:

$$\begin{aligned} \rho(w_1)^{3\cdot 43} &= \overline{1} + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + \\ &\quad + g^{17} + g^{18} + g^{19} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + g^{28} \neq \overline{1} \\ \rho(w_1)^{3\cdot 127} &= \overline{1} + g^2 + g^4 + g^5 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + \\ &\quad + g^{19} + g^{20} + g^{21} + g^{24} + g^{25} + g^{27} \neq \overline{1} \\ \rho(w_1)^{43\cdot 127} &= \overline{1} + g + g^4 + g^5 + g^6 + g^7 + g^9 + g^{13} + g^{16} + g^{20} + g^{22} + g^{23} + g^{24} + g^{25} + g^{28} \neq \overline{1}, \end{aligned}$$

segue que $\mathbf{ord}(\rho(w_1)) = 16383$. Sejam:

$$\begin{aligned} \beta_1 &= \frac{1 - w_1^2 w_2^{-1}}{2} \\ &= 16 - 15g + 13g^2 - 11g^3 + 9g^4 - 8g^5 + 8g^6 - 8g^7 + 8g^8 - 7g^9 + 5g^{10} - 3g^{11} + g^{12} + g^{17} + \\ &\quad - 3g^{18} + 5g^{19} - 7g^{20} + 8g^{21} - 8g^{22} + 8g^{23} - 8g^{24} + 9g^{25} - 11g^{26} + 13g^{27} - 15g^{28}, \end{aligned}$$

$\beta_i = \delta i - 1(\beta_1)$ e defina $u_i(a) := (1-\beta_i) + \beta_i a,\ 1 \le i \le 13$. Então do Teorema 2.3.1

$$\mathcal{U}(\mathbb{Z}C_{38}) = \langle -1 \rangle \times \langle g \rangle \times \langle \{w_i\ :\ 1 \le i \le 13\} \rangle \times \langle \{u_i(a)\ :\ 1 \le i \le 13\} \rangle .$$

Exemplo 16. *Considere* $C_{106} \cong C_{53} \times C_2$, *onde* $C_{53} \cong \langle g \rangle$ *e* $C_2 \cong \langle a \rangle$. *Nosso intuito é descrever* $\mathcal{U}(\mathbb{Z}C_{106})$.

Como

$$\mathcal{U}_1(\mathbb{Z}C_{53}) = \langle g \rangle \times \langle \{w_i : 1 \le i \le 13\} \rangle ,$$

onde

$$\begin{aligned} w_1 \quad = \quad & -1 + g - g^2 + g^3 - g^4 + g^5 - g^6 + g^7 - g^8 + g^9 - g^{10} + g^{11} - g^{12} + g^{13} - g^{14} + g^{15} - g^{16} + \\ & + g^{17} - g^{18} + g^{19} - g^{20} + g^{21} - g^{22} + g^{23} - g^{24} + g^{25} + g^{28} - g^{29} + g^{30} - g^{31} + g^{32} - g^{33} + \\ & + g^{34} - g^{35} + g^{36} - g^{37} + g^{38} - g^{39} + g^{40} - g^{41} + g^{42} - g^{43} + g^{44} - g^{45} + g^{46} - g^{47} + g^{48} + \\ & - g^{49} + g^{50} - g^{51} + g^{52} \end{aligned}$$

e $w_i = \delta^{i-1}(w_1)$, para todo $1 \le i \le 14$ e sendo a função $\delta : \mathbb{Z}C_{53} \to \mathbb{Z}C_{53}$ definida por $\delta\left(\sum_{j=0}^{52} a_j g^j\right) = \sum_{j=0}^{52} a_j g^{2j}$. Seja a função $\psi : \mathbb{Z}C_{53} \to \mathbb{Z}_2 C_{53}$ definida da maneira usual e considere $\rho := \psi|_{\mathcal{U}_1^*(\mathbb{Z}C_{53})}$. Temos que:

$$\begin{aligned} \rho(w_1) \quad = \quad & \overline{1} + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + \\ & + g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{28} + g^{29} + g^{30} + g^{31} + g^{32} + g^{33} + \\ & + g^{34} + g^{35} + g^{36} + g^{37} + g^{38} + g^{39} + g^{40} + g^{41} + g^{42} + g^{43} + g^{44} + g^{45} + g^{46} + g^{47} + g^{48} + \\ & + g^{49} + g^{50} + g^{51} + g^{52} \end{aligned}$$

Do Corolário 2.2.1 obtém-se $\rho(w_1)^{2^i} = \rho(w_{i+1}),\ \forall\, 1 \le i \le 26$ e, pelo Lema 2.2.4, $\rho(w_1)^{67108863} = \overline{1}$.

Temos que $67108863 = 3 \cdot 2731 \cdot 8191$, e como:

$$
\begin{aligned}
\rho(w_1)^{3\cdot 2731} &= \overline{1} + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{13} + g^{14} + g^{15} + g^{16} + \\
&\quad + g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + g^{28} + g^{29} + \\
&\quad + g^{30} + g^{31} + g^{32} + g^{33} + g^{34} + g^{35} + g^{36} + g^{37} + g^{38} + g^{39} + g^{40} + g^{43} + g^{45} + \\
&\quad + g^{44} + g^{46} + g^{47} + g^{48} + g^{49} + g^{50} + g^{51} + g^{52} \neq \overline{1} \\
\rho(w_1)^{3\cdot 8191} &= \overline{1} + g^2 + g^4 + g^6 + g^8 + g^{10} + g^{12} + g^{13} + g^{16} + g^{17} + g^{36} + g^{37} + g^{40} + g^{41} + \\
&\quad + g^{43} + g^{45} + g^{47} + g^{49} + g^{51} \neq \overline{1} \\
\rho(w_1)^{2731\cdot 8191} &= \overline{1} + g^2 + g^3 + g^5 + g^8 + g^{12} + g^{14} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{26} + \\
&\quad + g^{27} + g^{32} + g^{30} + g^{31} + g^{35} + g^{33} + g^{34} + g^{39} + g^{41} + g^{45} + g^{48} + g^{50} + g^{51},
\end{aligned}
$$

segue que $\mathbf{ord}(\rho(w_1)) = 67108863$. Sejam:

$$
\begin{aligned}
\beta_1 &= \frac{1 - w_1^2 w_2^{-1}}{2} \\
&= 28 - 27g + 25g^2 - 23g^3 + 21g^4 - 20g^5 + 20g^6 - 20g^7 + 20g^8 - 19g^9 + 17g^{10} - 15g^{11} + \\
&\quad + 13g^{12} - 12g^{13} + 12g^{14} - 12g^{15} + 12g^{16} - 11g^{17} + 9g^{18} - 7g^{19} + 5g^{20} - 4g^{21} + 4g^{22} + \\
&\quad - 4g^{23} + 4g^{24} - 3g^{25} + g^{26} + g^{27} - 3g^{28} + 4g^{29} - 4g^{30} + 4g^{31} - 4g^{32} + 5g^{33} - 7g^{34} + \\
&\quad + 9g^{35} - 11g^{36} + 12g^{37} - 12g^{38} + 12g^{39} - 12g^{40} + 13g^{41} - 15g^{42} + 17g^{43} - 19g^{44} + \\
&\quad + 20g^{45} - 20g^{46} + 20g^{47} - 20g^{48} + 21g^{49} - 23g^{50} + 25g^{51} - 27g^{52}
\end{aligned}
$$

$\beta_i = \delta i - 1(\beta_1)$ e defina $u_i(a) := (1 - \beta_i) + \beta_i a$, $\forall\ 1 \leq i \leq 13$. Então do Teorema 2.3.1

$$\mathcal{U}(\mathbb{Z}C_{106}) = \langle -1 \rangle \times \langle g \rangle \times \langle \{w_i \ : \ 1 \leq i \leq 25\} \rangle \times \langle \{u_i(a) \ : \ 1 \leq i \leq 26\} \rangle .$$

Exemplo 17. *Considere* $C_{118} \cong C_{59} \times C_2$, *onde* $C_{59} \cong \langle g \rangle$ *e* $C_2 \cong \langle a \rangle$. *Nosso trabalho é descrever* $\mathcal{U}(\mathbb{Z}C_{118})$.

Como

$$\mathcal{U}_1(\mathbb{Z}C_{59}) = \langle g \rangle \times \langle \{w_i : 1 \leq i \leq 28\} \rangle ,$$

onde

$$\begin{aligned} w_1 &= 1-g+g^2-g^3+g^4-g^5+g^6-g^7+g^8-g^9+g^{10}-g^{11}+g^{12}-g^{13}+g^{14}-g^{15}+g^{16}+\\ &\quad -g^{17}+g^{18}-g^{19}+g^{20}-g^{21}+g^{22}-g^{23}+g^{24}-g^{25}+g^{26}-g^{27}+g^{28}+g^{31}-g^{32}+g^{33}+\\ &\quad -g^{34}+g^{35}-g^{36}+g^{37}-g^{38}+g^{39}-g^{40}+g^{41}-g^{42}+g^{43}-g^{44}+g^{45}-g^{46}+g^{47}-g^{48}+\\ &\quad +g^{49}-g^{50}+g^{51}-g^{52}+g^{53}-g^{54}+g^{55}-g^{56}+g^{57}-g^{58}, \end{aligned}$$

$w_i = \delta^{i-1}(z_1)$, para todo $1 \leq i \leq 29$, e a função $\delta : \mathbb{Z}C_{59} \to \mathbb{Z}C_{59}$ que leva g em g^2 e fixa os números inteiros. Seja a função $\psi : \mathbb{Z}C_{59} \to \mathbb{Z}_2C_{59}$ definida da maneira usual e considere $\rho := \psi|_{\mathcal{U}_1^*(\mathbb{Z}C_{59})}$. Temos que:

$$\begin{aligned} \rho(w_1) &= \overline{1}+g+g^2+g^3+g^4+g^5+g^6+g^7+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{14}+g^{15}+g^{16}+\\ &\quad +g^{17}+g^{18}+g^{19}+g^{20}+g^{21}+g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27}+g^{28}+g^{31}+g^{32}+g^{33}+\\ &\quad +g^{34}+g^{35}+g^{36}+g^{37}+g^{38}+g^{39}+g^{40}+g^{41}+g^{42}+g^{43}+g^{44}+g^{45}+g^{46}+g^{47}+g^{48}+\\ &\quad +g^{49}+g^{50}+g^{51}+g^{52}+g^{53}+g^{54}+g^{55}+g^{56}+g^{57}+g^{58} \end{aligned}$$

Do Corolário 2.2.1 tem-se $\rho(w_1)^{2^i} = \rho(w_{i+1})$, $\forall\ 1 \leq i \leq 29$ e, pelo Lema 2.2.4, $\rho(w_1)^{536870911} = \overline{1}$. Temos que $536870911 = 233 \cdot 1103 \cdot 2089$ e como:

$$\begin{aligned} \rho(w_1)^{233\cdot 1103} &= \overline{1}+g^2+g^3+g^4+g^5+g^6+g^9+g^{10}+g^{11}+g^{12}+g^{14}+g^{19}+g^{24}+g^{25}+g^{27}+\\ &\quad +g^{28}+g^{29}+g^{30}+g^{31}+g^{32}+g^{34}+g^{35}+g^{40}+g^{45}+g^{47}+g^{48}+g^{49}+g^{50}+\\ &\quad +g^{53}+g^{54}+g^{55}+g^{56}+g^{57} \neq \overline{1},\\ \rho(w_1)^{233\cdot 2089} &= \overline{1}+g^2+g^4+g^5+g^7+g^9+g^{17}+g^{20}+g^{21}+g^{22}+g^{24}+g^{26}+g^{33}+g^{35}+g^{37}+\\ &\quad +g^{38}+g^{39}+g^{42}+g^{50}+g^{52}+g^{54}+g^{55}+g^{57} \neq \overline{1},\\ \rho(w_1)^{1103\cdot 2089} &= \overline{1}+g+g^2+g^3+g^5+g^7+g^8+g^{12}+g^{15}+g^{18}+g^{20}+g^{21}+g^{23}+g^{24}+g^{35}+\\ &\quad +g^{36}+g^{38}+g^{39}+g^{41}+g^{44}+g^{47}+g^{51}+g^{52}+g^{54}+g^{56}+g^{57}+g^{58} \neq \overline{1}, \end{aligned}$$

segue que $\mathbf{ord}(\rho(w_1)) = 536870911$. Sejam:

$$\begin{aligned}
\beta_1 &= \frac{1 - w_1^2 w_2^{-1}}{2} \\
&= 28 - 28g + 28g^2 - 28g^3 + 27g^4 - 25g^5 + 23g^6 - 21g^7 + 20g^8 - 20g^9 + 20g^{10} - 20g^{11} + \\
&\quad +19g^{12} - 17g^{13} + 15g^{14} - 13g^{15} + 12g^{16} - 12g^{17} + 12g^{18} - 12g^{19} + 11g^{20} - 9g^{21} + 7g^{22} + \\
&\quad -5g^{23} + 4g^{24} - 4g^{25} + 4g^{26} - 4g^{27} + 3g^{28} - g^{29} - g^{30} + 3g^{31} - 4g^{32} + 4g^{33} - 4g^{34} + 4g^{35} + \\
&\quad -5g^{36} + 7g^{37} - 9g^{38} + 11g^{39} - 12g^{40} + 12g^{41} - 12g^{42} + 12g^{43} - 13g^{44} + 15g^{45} - 17g^{46} + \\
&\quad +19g^{47} - 20g^{48} + 20g^{49} - 20g^{50} + 20g^{51} - 21g^{52} + 23g^{53} - 25g^{54} + 27g^{55} - 28g^{56} + 28g^{57} + \\
&\quad -28g^{58},
\end{aligned}$$

$\beta_i = \delta i - 1(\beta_1)$ e defina $u_i(a) := (1 - \beta_i) + \beta_i a,\ 1 \leq i \leq 28$. Então do Teorema 2.3.1

$$\mathcal{U}(\mathbb{Z}C_{118}) = \langle -1 \rangle \times \langle g \rangle \times \langle \{w_i \ : \ 1 \leq i \leq 28\} \rangle \times \langle \{u_i(a) \ : \ 1 \leq i \leq 28\} \rangle .$$

Exemplo 18. *Considere* $C_{122} \cong C_{61} \times C_2,$ *onde* $C_{61} \cong \langle g \rangle$ *e* $C_2 \cong \langle a \rangle$. *Nossa intenção é descrever* $\mathcal{U}(\mathbb{Z}C_{122})$.

Como

$$\mathcal{U}_1(\mathbb{Z}C_{61}) = \langle g \rangle \times \langle \{w_i : 1 \leq i \leq 29\} \rangle ,$$

onde

$$\begin{aligned}
w_1 &= -1 + g - g^2 + g^3 - g^4 + g^5 - g^6 + g^7 - g^8 + g^9 - g^{10} + g^{11} - g^{12} + g^{13} - g^{14} + g^{15} - g^{16} + \\
&\quad +g^{17} - g^{18} + g^{19} - g^{20} + g^{21} - g^{22} + g^{23} - g^{24} + g^{25} - g^{26} + g^{27} - g^{28} + g^{29} + g^{32} - g^{33} + \\
&\quad +g^{34} - g^{35} + g^{36} - g^{37} + g^{38} - g^{39} + g^{40} - g^{41} + g^{42} - g^{43} + g^{44} - g^{45} + g^{46} - g^{47} + g^{48} + \\
&\quad -g^{49} + g^{50} - g^{51} - g^{53} + g^{54} - g^{55} + g^{56} - g^{57} + g^{58} - g^{59} + g^{60},
\end{aligned}$$

$w_i = \delta^{i-1}(w_1)$, para todo $1 \leq i \leq 30$, e isomorfismo de anéis $\delta : \mathbb{Z}C_{61} \to \mathbb{Z}C_{61}$ tal que $\delta(g) = g^2$.

Seja a função $\psi : \mathbb{Z}C_{61} \to \mathbb{Z}_2C_{61}$ definida da maneira usual e considere $\rho := \psi|_{\mathcal{U}_1^*(\mathbb{Z}C_{61})}$. Temos que:

$$\begin{aligned}\rho(w_1) &= \overline{1} + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + \\ &+ g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + g^{28} + g^{29} + g^{32} + \\ &+ g^{33} + g^{34} + g^{35} + g^{36} + g^{37} + g^{38} + g^{39} + g^{40} + g^{41} + g^{42} + g^{43} + g^{44} + g^{45} + g^{46} + \\ &+ g^{47} + g^{48} + g^{49} + g^{50} + g^{51} + g^{52} + g^{53} + g^{54} + g^{55} + g^{56} + g^{57} + g^{58} + g^{59} + g^{60}.\end{aligned}$$

Do Corolário 2.2.1 temos $\rho(w_1)^{2^i} = \rho(w_{i+1}),\ \forall\ 1 \leq i \leq 30$ e, do Lema 2.2.4, $\rho(w_1)^{1073741823} = \overline{1}$. Como $1073741823 = 3^2 \cdot 7 \cdot 31 \cdot 11 \cdot 151 \cdot 331$, e

$$\begin{aligned}\rho(w_1)^{3 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331} &= \overline{1} + g^2 + g^6 + g^7 + g^8 + g^{10} + g^{11} + g^{17} + g^{18} + g^{21} + g^{23} + g^{24} + g^{26} + \\ &+ g^{28} + g^{29} + g^{30} + g^{31} + g^{32} + g^{33} + g^{35} g^{37} + g^{38} + g^{40} + g^{43} + g^{44} + g^{50} + \\ &+ g^{51} + g^{53} + g^{54} + g^{55} + g^{59} \neq \overline{1}, \\ \rho(w_1)^{3^2 \cdot 11 \cdot 31 \cdot 151 \cdot 331} &= \overline{1} + g + g^2 + g^3 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{11} + g^{13} + g^{15} + g^{16} + g^{18} + \\ &+ g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{27} + g^{28} + g^{33} + g^{34} + g^{37} + g^{38} + g^{39} + \\ &+ g^{40} + g^{41} + g^{43} + g^{45} + g^{46} + g^{48} + g^{50} + g^{52} + g^{53} + g^{54} + g^{55} + g^{56} + \\ &+ g^{58} + g^{59} + g^{60} \neq \overline{1},\end{aligned}$$

$$\begin{aligned}\rho(w_1)^{3^2 \cdot 7 \cdot 31 \cdot 151 \cdot 331} &= \overline{1} + g + g^6 + g^8 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{17} + g^{18} + g^{21} + g^{23} + \\ &+ g^{27} + g^{29} + g^{32} + g^{34} + g^{38} + g^{40} + g^{43} + g^{44} + g^{46} + g^{47} + g^{48} + g^{49} + \\ &+ g^{50} + g^{51} + g^{53} + g^{55} + g^{60} \neq \overline{1}, \\ \rho(w_1)^{3^2 \cdot 7 \cdot 11 \cdot 151 \cdot 331} &= \overline{1} + g + g^4 + g^5 + g^6 + g^9 + g^{11} + g^{13} + g^{14} + g^{17} + g^{21} + g^{23} + g^{29} + g^{32} + \\ &+ g^{38} + g^{40} + g^{44} + g^{47} + g^{48} + g^{50} + g^{52} + g^{55} + g^{56} + g^{57} + g^{60} \neq \overline{1}, \\ \rho(w_1)^{3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 331} &= \overline{1} + g^3 + g^5 + g^6 + g^8 + g^9 + g^{14} + g^{15} + g^{18} + g^{19} + g^{23} + g^{26} + g^{27} + g^{28} + \\ &+ g^{29} + g^{32} + g^{33} + g^{34} + g^{35} + g^{38} + g^{42} + g^{43} + g^{46} + g^{47} + g^{52} + g^{53} + \\ &+ g^{55} + g^{56} + g^{58} \neq \overline{1}, \\ \rho(w_1)^{3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151} &= \overline{1} + g + g^3 + g^4 + g^6 + g^7 + g^9 + g^{10} + g^{11} + g^{13} + g^{15} + g^{22} + g^{23} + g^{24} + \\ &+ g^{27} + g^{29} + g^{32} + g^{34} + g^{37} + g^{38} + g^{39} + g^{46} + g^{48} + g^{50} + g^{51} + g^{52} + \\ &+ g^{54} + g^{55} + g^{57} + g^{58} + g^{60} \neq \overline{1},\end{aligned}$$

segue que $\mathbf{ord}(\rho(w_1)) = 1073741823$. Sejam:

$$\begin{aligned}
\beta_1 &= \frac{1 - w_1^2 w_2^{-1}}{2} \\
&= 32 - 31g + 29g^2 - 27g^3 + 25g^4 - 24g^5 + 24g^6 - 24g^7 + 24g^8 - 23g^9 + 21g^{10} - 19g^{11} + 17g^{12} + \\
&\quad -16g^{13} + 16g^{14} - 16g^{15} + 16g^{16} - 15g^{17} + 13g^{18} - 11g^{19} + 9g^{20} - 8g^{21} + 8g^{22} - 8g^{23} + 8g^{24} + \\
&\quad -7g^{25} + 5g^{26} - 3g^{27} + g^{28} + g^{33} - 3g^{34} + 5g^{35} - 7g^{36} + 8g^{37} - 8g^{38} + 8g^{39} - 8g^{40} + 9g^{41} + \\
&\quad -11g^{42} + 13g^{43} - 15g^{44} + 16g^{45} - 16g^{46} + 16g^{47} - 16g^{48} + 17g^{49} - 19g^{50} + 21g^{51} + 24g^{53} + \\
&\quad -23g^{52} - 24g^{54} - 24g^{56} + 24g^{55} + 25g^{57} - 27g^{58} + 29g^{59} - 31g^{60},
\end{aligned}$$

$\beta_i = \delta i - 1(\beta_1)$ e defina $u_i(a) := (1 - \beta_i) + \beta_i a,\ 1 \leq i \leq 29$. Então do Teorema 2.3.1

$$\mathcal{U}(\mathbb{Z}C_{122}) = \langle -1 \rangle \times \langle g \rangle \times \langle \{w_i \ : \ 1 \leq i \leq 29\} \rangle \times \langle \{u_i(a) \ : \ 1 \leq i \leq 29\} \rangle .$$

Exemplo 19. *Considere* $C_{134} \cong C_{67} \times C_2$, *onde* $C_{67} \cong \langle g \rangle$ *e* $C_2 \cong \langle a \rangle$. *Nosso intuito é descrever* $\mathcal{U}(\mathbb{Z}C_{134})$.

Como

$$\mathcal{U}_1(\mathbb{Z}C_{67}) = \langle g \rangle \times \langle \{w_i : 1 \leq i \leq 32\} \rangle ,$$

onde

$$\begin{aligned}
w_1 &= 1 - g + g^2 - g^3 + g^4 - g^5 + g^6 - g^7 + g^8 - g^9 + g^{10} - g^{11} + g^{12} - g^{13} + g^{14} - g^{15} + g^{16} + \\
&\quad -g^{17} + g^{18} - g^{19} + g^{20} - g^{21} + g^{22} - g^{23} + g^{24} - g^{25} + g^{26} - g^{27} + g^{28} - g^{29} + g^{30} - g^{31} + \\
&\quad +g^{32} + g^{35} - g^{36} + g^{37} - g^{38} + g^{39} - g^{40} + g^{41} - g^{42} + g^{43} - g^{44} + g^{45} - g^{46} + g^{47} - g^{48} + \\
&\quad +g^{49} - g^{50} + g^{51} - g^{52} + g^{53} - g^{54} + g^{55} - g^{56} + g^{57} - g^{58} + g^{59} - g^{60} + g^{61} - g^{62} + g^{63} + \\
&\quad -g^{64} + g^{65} - g^{66},
\end{aligned}$$

$w_i = \delta^{i-1}(w_1)$, para todo $1 \leq i \leq 30$, e o isomorfismo $\delta : \mathbb{Z}C_{61} \to \mathbb{Z}C_{61}$ que leva g em g^2 e fixa os elementos de $\mathbb{Z}$. Seja a função $\psi : \mathbb{Z}C_{67} \to \mathbb{Z}_2C_{67}$ definida da maneira usual e considere

$\rho := \psi|_{\mathcal{U}_1^*(\mathbb{Z}C_{67})}$. Temos que:

$$\begin{aligned}\rho(w_1) &= \overline{1} + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + \\ &\quad + g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + g^{28} + g^{29} + g^{30} + \\ &\quad + g^{31} + g^{32} + g^{35} + g^{36} + g^{37} + g^{38} + g^{39} + g^{40} + g^{41} + g^{42} + g^{43} + g^{44} + g^{45} + g^{46} + \\ &\quad + g^{47} + g^{48} + g^{49} + g^{50} + g^{51} + g^{52} + g^{53} + g^{54} + g^{55} + g^{56} + g^{57} + g^{58} + g^{59} + g^{60} + g^{61} + \\ &\quad + g^{62} + g^{63} + g^{64} + g^{65} + g^{66}.\end{aligned}$$

Do Corolário 2.2.1 obtém-se $\rho(w_1)^{2^i} = \rho(w_{i+1})$, $\forall\ 1 \leq i \leq 33$ e, do Lema 2.2.4, $\rho(w_1)^{8589934591} = \overline{1}$. Temos que $8589934591 = 7 \cdot 23 \cdot 89 \cdot 599479$. Como

$$\begin{aligned}\rho(w_1)^{7\cdot 23\cdot 89} &= \overline{1} + g + g^3 + g^4 + g^5 + g^7 + g^8 + g^{10} + g^{11} + g^{12} + g^{13} + g^{15} + g^{16} + g^{20} + \\ &\quad + g^{21} + g^{23} + g^{24} + g^{27} + g^{29} + g^{31} + g^{32} + g^{35} + g^{36} + g^{38} + g^{40} + g^{43} + g^{44} + \\ &\quad + g^{46} + g^{47} + g^{51} + g^{52} + g^{54} + g^{55} + g^{56} + g^{57} + g^{59} + g^{60} + g^{62} + g^{63} + \\ &\quad + g^{64} + g^{66} \neq \overline{1}, \\ \rho(w_1)^{7\cdot 23\cdot 599479} &= \overline{1} + g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{18} + g^{22} + \\ &\quad + g^{24} + g^{25} + g^{26} + g^{28} + g^{29} + g^{30} + g^{31} + g^{32} + g^{35} + g^{36} + g^{37} + g^{38} + g^{39} + \\ &\quad + g^{41} + g^{42} + g^{43} + g^{45} + g^{49} + g^{50} + g^{53} + g^{54} + g^{55} + g^{57} + g^{58} + g^{59} + g^{60} + \\ &\quad + g^{63} + g^{65} + g^{66} \neq \overline{1}, \\ \rho(w_1)^{7\cdot 89\cdot 599479} &= \overline{1} + g^3 + g^4 + g^6 + g^{12} + g^{13} + g^{14} + g^{17} + g^{18} + g^{20} + g^{21} + g^{23} + g^{24} + g^{25} + \\ &\quad + g^{26} + g^{27} + g^{40} + g^{41} + g^{42} + g^{43} + g^{44} + g^{46} + g^{47} + g^{49} + g^{50} + g^{53} + \\ &\quad + g^{54} + g^{55} + g^{61} + g^{63} + g^{64} \neq \overline{1}, \\ \rho(w_1)^{23\cdot 89\cdot 599479} &= \overline{1} + g^2 + g^6 + g^{10} + g^{13} + g^{16} + g^{17} + g^{18} + g^{19} + g^{23} + g^{28} + g^{30} + g^{37} + \\ &\quad + g^{39} + g^{44} + g^{48} + g^{49} + g^{50} + g^{51} + g^{54} + g^{57} + g^{61} + g^{65} \neq \overline{1},\end{aligned}$$

concluímos que $\mathbf{ord}(\rho(w_1)) = 8589934591$. Sejam:
$\beta_1 = \dfrac{1 - w_1^2 w_2^{-1}}{2} = 32 - 32g + 32g^2 - 32g^3 + 31g^4 - 29g^5 + 27g^6 - 25g^7 + 24g^8 - 24g^9 + 24g^{10} + -24g^{11} + 23g^{12} - 21g^{13} + 19g^{14} - 17g^{15} + 16g^{16} - 16g^{17} + 16g^{18} - 16g^{19} + 15g^{20} - 13g^{21} + 11g^{22} + -9g^{23} + 8g^{24} - 8g^{25} + 8g^{26} - 8g^{27} + 7g^{28} - 5g^{29} + 3g^{30} - g^{31} - g^{36} + 3g^{37} - 5g^{38} + 7g^{39} - 8g^{40} + 8g^{41} + -8g^{42} + 8g^{43} - 9g^{44} + 11g^{45} - 13g^{46} + 15g^{47} - 16g^{48} + 16g^{49} - 16g^{50} + 16g^{51} - 17g^{52} + 19g^{53} - 21g^{54} + +23g^{55} - 24g^{56} + 24g^{57} - 24g^{58} + 24g^{59} - 25g^{60} + 27g^{61} - 29g^{62} + 31g^{63} - 32g^{64} + 32g^{65} - 32g^{66}$,

$\beta_i = \delta i - 1(\beta_1)$ e defina $u_i(a) := (1 - \beta_i) + \beta_i a \; \forall \; 1 \leq i \leq 32$. Então do Teorema 2.3.1

$$\mathcal{U}(\mathbb{Z}C_{134}) = \langle -1 \rangle \times \langle g \rangle \times \langle \{ w_i \; : \; 1 \leq i \leq 32 \} \rangle \times \langle \{ u_i(a) \; : \; 1 \leq i \leq 32 \} \rangle \, .$$

Capítulo 3

Unidades de $\mathbb{Z}(C_{2p} \times C_2)$

3.1 Introdução

Queremos agora estender as ideias do Capítulo anterior. Considere o seguinte anel de grupo integral $\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}})$, onde $C_p \cong \langle g \rangle$ e cada $C_2 \cong \langle a_i \rangle$, $1 \leq i \leq n$. Utilizando que $\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}}) \cong \mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}})C_2$ todo elemento α de $\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}})$ pode ser escrito como $\alpha = x + ya_n$, onde $x, y \in \mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}})$.

Logo $u \in \mathcal{U}(\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}}))$, se e somente se, existe $v \neq 0 \in \mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}})$ tal que $uv = 1 = vu$. Como $u, v \in \mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}})$ existem $x, y, z, t \in \mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}})$ de forma que $u = x + ya_n$ e $v = z + ta_n$, e obtemos:

$$\begin{cases} xz + yt = 1 \\ xt + yz = 0 \end{cases}$$

Somando e subtraindo estas equações temos

$$\begin{cases} (x + y)(z + t) = 1 \\ (x - y)(z - t) = 1 \end{cases}$$

isto é, $x + y, x - y \in \mathcal{U}(\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}}))$.

Portanto existem $u_1, u_2 \in \mathcal{U}(\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}}))$ tais que $u_1 = x + y$ e $u_2 = x - y$. Desta maneira:

$x = \dfrac{u_1+u_2}{2}$ e $y = \dfrac{u_1-u_2}{2}$, ou ainda, $x = u_1\left(\dfrac{1+u_1^{-1}u_2}{2}\right)$ e $y = u_1\left(\dfrac{1-u_1^{-1}u_2}{2}\right)$, com $u_1, u_2 \in U(\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}}))$.

Como $x, y \in \mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}})$ então $\dfrac{1 \pm u_1^{-1}u_2}{2} \in \mathbb{Z}(C_p \times \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}})$. Sendo assim: $1 \pm u_1^{-1}u_2 \equiv 0 \pmod{\langle 2\rangle}$, ou seja, $u_1^{-1}u_2 \equiv 1 \pmod{\langle 2\rangle}$.

Assim

$$u \in \mathcal{U}(\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}})) \Rightarrow u = u_1\left[\left(\frac{1+u_2}{2}\right) + \left(\frac{1-u_2}{2}\right)a\right]$$

onde $u_1, u_2 \in \mathcal{U}(\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}}))$ e $u_2 \equiv 1 \pmod{\langle 2\rangle}$.

Considere o homomorfismo de anéis $\phi : \mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}}) \to \mathbb{Z}_2(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}})$ e defina $\Phi := \phi|_A$, onde A representa o conjunto $\mathcal{U}(\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}}))$. Para encontrarmos as unidades de $\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}})$ devemos conhecer as unidades de $\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n-1 \text{ vezes}})$ e determinar o núcleo da função Φ.

Defina:

$$u_j(a_{i_1} \cdots a_{i_k}) := (1-\beta_j) + \beta_j a_{i_1} \cdots a_{i_k},$$

onde $\beta_1 = \dfrac{1 - w_1^2 w_2^{-1}}{2}$, $\beta_j = \delta_{\beta_1}^{j-1}$, para todo $i_t \in \{1, 2, \cdots, n\}$ e $2 \leq j \leq \dfrac{p-3}{2}$.

Lema 3.1.1. *Os elementos $u_j(a_{i_1} \cdots a_{i_k})$ definidos acima são unidades de $\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{n \text{ vezes}})$ e seus inversos são dados por $u_j(a_{i_1} \cdots a_{i_k})^{-1} := (1-2\beta_j)^{-1}[(1-\beta_j) - \beta_j a_{i_1} \cdots a_{i_k}]$*

Demonstração:

De fato,

$$u_j(a_{i_1} \cdots a_{i_k}) u_j(a_{i_1} \cdots a_{i_k})^{-1} = (1-2\beta_j)^{-1}[(1-\beta_j) + \beta_j a_{i_1} \cdots a_{i_k}][(1-\beta_j) - \beta_j a_{i_1} \cdots a_{i_k}],$$

ou seja,

$$u_j(a_{i_1} \cdots a_{i_k}) u_j(a_{i_1} \cdots a_{i_k})^{-1} = (1-2\beta_j)^{-1}[(1-\beta_j)^2 - (\beta_j a_{i_1} \cdots a_{i_k})^2],$$

isto é,

$$u_j(a_{i_1} \cdots a_{i_k}) u_j(a_{i_1} \cdots a_{i_k})^{-1} = (1-2\beta_j)^{-1}[(1-2\beta_j+\beta_j^2) - \beta_j^2],$$

de onde,

$$u_j(a_{i_1} \cdots a_{i_k}) u_j(a_{i_1} \cdots a_{i_k})^{-1} = 1.$$

$\blacksquare$

Em seguida descreveremos algumas unidades que estão sempre no núcleo do homomorfismo Φ.

Lema 3.1.2. *Considere $u_j(a_{i_1} \cdots a_{i_k})$ definido anteriormente. Então $u_j(a_{i_1} \cdots a_{i_k})^2$ são elementos do núcleo de Φ.*

Demonstração:

Observe que:

$$\Phi(u_j(a_{i_1} \cdots a_{i_k}))^2 = [(\overline{1} + \phi(\beta_j)) + \phi(\beta_j) a_{i_1} \cdots a_{i_k})]^2,$$

isto é,

$$\Phi(u_j(a_{i_1} \cdots a_{i_k}))^2 = (\overline{1} + \phi(\beta_j))^2 + \phi(\beta_j)^2 (a_{i_1} \cdots a_{i_k}))^2,$$

ou seja,

$$\Phi(u_j(a_{i_1} \cdots a_{i_k}))^2 = \overline{1} + \phi(\beta_j)^2 + \phi(\beta_j)^2 = \overline{1}.$$

$\blacksquare$

Para facilitar a descrição do grupo das unidades, trocamos as unidades encontradas pelas unidades que definimos no início deste Capítulo. O resultado a seguir possibilita esta troca.

Lema 3.1.3. *Seja $\gamma_j(a_{i_1} \cdots a_{i_k}) := \dfrac{1 - u_j(a_{i_1} \cdots a_{i_k})^2}{2}$, $1 \leq j \leq \frac{p-3}{2}$, e defina $v_j(a_{i_1} \cdots a_{i_k}) := (1 - \gamma_j(a_{i_1} \cdots a_{i_k})) + \gamma_j(a_{i_1} \cdots a_{i_k}) a_n$. Então*

$$v_j(a_{i_1} \cdots a_{i_k}) = u_j(a_{i_1} \cdots a_{i_k}) u_j(a_n) u_j(a_{i_1} \cdots a_{i_k} a_n)^{-1}$$

Demonstração:

Temos que

$$\gamma_j(a_{i_1} \cdots a_{i_k}) = \frac{1 - u_j(a_{i_1} \cdots a_{i_k})^2}{2} = \frac{1 - [(1 - \beta_j) + \beta_j a_{i_1} \cdots a_{i_k}]^2}{2}],$$

ou seja,

$$\gamma_j(a_{i_1} \cdots a_{i_k}) = \frac{1 - [(1 - 2\beta_j + \beta_j^2) + 2(1 - \beta_j)\beta_j a_{i_1} \cdots a_{i_k} + \beta_j^2}{2},$$

isto é,

$$\gamma_j(a_{i_1} \cdots a_{i_k}) = \frac{2\beta_j - 2\beta_j^2 - 2(1 - \beta_j)\beta_j a_{i_1} \cdots a_{i_k}}{2},$$

ou ainda,

$$\gamma_j(a_{i_1} \cdots a_{i_k}) = (1 - \beta_j)\alpha_j - (1 - \beta_j)\beta_j a_{i_1} \cdots a_{i_k}.$$

Por outro lado,

$$u_j(a_{i_1}\cdots a_{i_k})u_j(a_n)=[(1-\beta_j)+\beta_j a_{i_1}\cdots a_{i_k}][(1-\beta_j)+\beta_j a_n],$$

de onde,

$$u_j(a_{i_1}\cdots a_{i_k})u_j(a_n)=(1-\beta_j)^2+(1-\beta_j)\beta_j a_{i_1}\cdots a_{i_k}+(1-\beta_j)\beta_j a_n+\beta_j^2 a_{i_1}\cdots a_{i_k}a_n,$$

isto é,

$$u_j(a_{i_1}\cdots a_{i_k})u_j(a_n)=[(1-2\beta_j)+\beta_j^2]+(1-\beta_j)\beta_j a_{i_1}\cdots a_{i_k}+(1-\beta_j)\beta_j a_n+\beta_j^2 a_{i_1}\cdots a_{i_k}a_n.$$

Assim
$u_j(a_{i_1}\cdots a_{i_k})u_j(a_n)u_j(a_{i_1}\cdots a_{i_k}a_n)^{-1} = (1-2\beta_j)^{-1}[(1-2\beta_j)+\beta_j^2+(1-\beta_j)\beta_j a_{i_1}\cdots a_{i_k}+$
$+(1-\beta_j)\beta_j a_n+\beta_j^2 a_{i_1}\cdots a_{i_k}a_n][(1-\beta_j)-\beta_j a_{i_1}\cdots a_{i_k}a_n],$
ou seja,
$u_j(a_{i_1}\cdots a_{i_k})u_j(a_n)u_j(a_{i_1}\cdots a_{i_k}a_n)^{-1} = (1-2\beta_j)^{-1}[(1-2\beta_j)(1-\beta_j)+(1-\beta_j)\beta_j^2+$
$+(1-\beta_j)^2\beta_j a_{i_1}\cdots a_{i_k}+(1-\beta_j)^2\beta_j a_n+(1-\beta_j)\beta_j^2 a_{i_1}\cdots a_{i_k}a_n-(1-2\beta_j)\beta_j a_{i_1}\cdots a_{i_k}a_n+$
$-\beta_j^3 a_{i_1}\cdots a_{i_k}a_n-(1-\beta_j)\beta_j^2 a_n-(1-\beta_j)\beta_j^2 a_{i_1}\cdots a_{i_k}-\beta_j^3],$
isto é,
$u_j(a_{i_1}\cdots a_{i_k})u_j(a_n)u_j(a_{i_1}\cdots a_{i_k}a_n)^{-1}=(1-2\beta_j)^{-1}\{(1-2\beta_j)(1-\beta_j)+(1-2\beta_j)\beta_j^2+[(1-2\beta_j)+$
$-(1-2\beta_j)\beta_j]\beta_j a_{i_1}\cdots a_{i_k}+[(1-2\beta_j)-(1-2\beta_j)\beta_j]\beta_j a_n-[(1-2\beta_j)-(1-2\beta_j)\beta_j]\beta_j a_{i_1}\cdots a_{i_k}a_n\},$
de onde,
$u_j(a_{i_1}\cdots a_{i_k})u_j(a_n)u_j(a_{i_1}\cdots a_{i_k}a_n)^{-1} = [(1-\beta_j)+\beta_j^2]+(1-\beta_j)\beta_j a_{i_1}\cdots a_{i_k}+(1-\beta_j)\beta_j a_n+$
$-(1-\beta_j)\beta_j a_{i_1}\cdots a_{i_k}a_n,$
ou ainda,
$u_j(a_{i_1}\cdots a_{i_k})u_j(a_n)u_j(a_{i_1}\cdots a_{i_k}a_n)^{-1} = 1-[(1-\beta_j)\beta_j-(1-\beta_j)\beta_j a_{i_1}\cdots a_{i_k}]+[(1-\beta_j)\beta_j+$
$-(1-\beta_j)\beta_j a_{i_1}\cdots a_{i_k}]a_n$
e, portanto,

$$u_j(a_{i_1}\cdots a_{i_k})u_j(a_n)u_j(a_{i_1}\cdots a_{i_k}a_n)^{-1}=1-\gamma_j(a_{i_1}\cdots a_{i_k})+\gamma_j(a_{i_1}\cdots a_{i_k})a_n=v_j(a_{i_1}\cdots a_{i_k}).$$

■

Para demonstrar o Teorema principal deste Capítulo, precisamos determinar os inversos, e saber como multiplicar elementos de determinadas forma. Os resultados abaixo nos auxiliam nisto.

Lema 3.1.4. *Sejam* $\langle a_1 \rangle, \langle a_2 \rangle, \cdots, \langle a_k \rangle$ *tais que* $C_2 \cong \langle a_i \rangle$. *Seja* $b, b_i \in 2\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{k\ vezes})$. *Então*

$$\frac{1+b_1b_2\cdots b_n}{2} + \frac{1-b_1b_2\cdots b_n}{2}a_1\cdots a_k = \left[\frac{1+b_1}{2} + \frac{1-b_1}{2}a_1\cdots a_k\right]\cdots\left[\frac{1+b_n}{2} + \frac{1-b_n}{2}a_1\cdots a_k\right],$$

$n \geq 2 \in \mathbb{N}$. *Em particular, tem-se que*

$$\left[\frac{1+b}{2} + \frac{1-b}{2}a_1\cdots a_k\right]^n = \frac{1+b^n}{2} + \frac{1-b^n}{2}a_1\cdots a_k$$

Demonstração:

Façamos a prova por indução sobre n.

Para $n = 2$, temos que

$$\left[\frac{1+b_1}{2} + \frac{1-b_1}{2}a_1\cdots a_k\right]\left[\frac{1+b_2}{2} + \frac{1-b_2}{2}a_1\cdots a_k\right] = \frac{(1+b_1+b_2+b_1b_2)+(1-b_1-b_2+b_1b_2)}{4} +$$

$$+\frac{(1+b_1-b_2-b_1b_2)+(1-b_1+b_2-b_1b_2)}{4}a_1\cdots a_k,$$

ou seja,

$$\left[\frac{1+b_1}{2} + \frac{1-b_1}{2}a_1\cdots a_k\right]\left[\frac{1+b_2}{2} + \frac{1-b_2}{2}a_1\cdots a_k\right] = \frac{2+2b_1b_2}{4} + \frac{2-2b_1b_2}{4}a_1\cdots a_k,$$

isto é,

$$\left[\frac{1+b_1}{2} + \frac{1-b_1}{2}a_1\cdots a_k\right]\left[\frac{1+b_2}{2} + \frac{1-b_2}{2}a_1\cdots a_k\right] = \frac{1+b_1b_2}{2} + \frac{1-b_1b_2}{2}a_1\cdots a_k.$$

Suponhamos que a igualdade vale para $n = t$, o que significa que

$$\frac{1+b_1b_2\cdots b_t}{2} + \frac{1-b_1b_2\cdots b_t}{2}a_1\cdots a_k = \left[\frac{1+b_1}{2} + \frac{1-b_1}{2}a_1\cdots a_k\right]\cdots\left[\frac{1+b_t}{2} + \frac{1-b_t}{2}a_1\cdots a_k\right]$$

e vamos mostrar que a fórmula se verifica para $n = t+1$. Pela hipótese indutiva, tem-se

$$\left[\frac{1+b_1}{2} + \frac{1-b_1}{2}a_1\cdots a_k\right]\cdots\left[\frac{1+b_t}{2} + \frac{1-b_t}{2}a_1\cdots a_k\right]\left[\frac{1+b_{t+1}}{2} + \frac{1-b_{t+1}}{2}a_1\cdots a_k\right] =$$

$$= \left[\frac{1+b_1b_2\cdots b_t}{2} + \frac{1-b_1b_2\cdots b_t}{2}a_1\cdots a_k\right]\left[\frac{1+b_{t+1}}{2} + \frac{1-b_{t+1}}{2}a_1\cdots a_k\right],$$

e, como provamos que vale para $n = 2$, segue que

$$\frac{1+b_1b_2\cdots b_tb_{t+1}}{2} + \frac{1-b_1b_2\cdots b_tb_{t+1}}{2}a_1\cdots a_k.$$

Tomando $b_1 = \cdots = b_n = b$, do que acabamos de mostrar, obtemos o caso particular.

■

Lema 3.1.5. *Sejam* $\langle a_1\rangle, \langle a_2\rangle, \cdots, \langle a_k\rangle$ *tais que* $C_2 \cong \langle a_i\rangle$. *Seja* b *uma unidade de* $\mathbb{Z}(C_p \times \underbrace{C_2 \times \ldots \times C_2}_{k\ \ vezes})$. *Tem-se*

$$\left[\frac{1+b}{2} + \frac{1-b}{2}a_1\cdots a_k\right]^{-1} = \frac{1+b^{-1}}{2} + \frac{1-b^{-1}}{2}a_1\cdots a_k.$$

Demonstração:

Como

$$\left[\frac{1+b}{2} + \frac{1-b}{2}a_1\cdots a_k\right]\left[\frac{1+b^{-1}}{2} + \frac{1-b^{-1}}{2}a_1\cdots a_k\right] = \frac{(1+b+b^{-1}+1)+(1-b-b^{-1}+1)}{4} +$$

$$+ \frac{(1-b+b^{-1}-1)-(1+b-b^{-1}-1)}{4}a_1\cdots a_k,$$

ou seja,

$$\left[\frac{1+b}{2} + \frac{1-b}{2}a_1\cdots a_k\right]\left[\frac{1+b^{-1}}{2} + \frac{1-b^{-1}}{2}a_1\cdots a_k\right] = 1$$

Portanto,

$$\left[\frac{1+b}{2} + \frac{1-b}{2}a_1\cdots a_k\right]^{-1} = \frac{1+b^{-1}}{2} + \frac{1-b^{-1}}{2}a_1\cdots a_k$$

■

O próximo resultado ilustra o que ocorre quando multiplicamos a imagem da Φ aplicada aos elementos $u_i(a_{i_1}\cdots a_{i_k})$.

Lema 3.1.6. *Para todo* $n \in \mathbb{N}$, *tem-se*
$\Phi(u_{j_1}(a_{i_1}\cdots a_{i_k}))\cdots\Phi(u_{j_m}(a_{i1}\cdots a_{i_k})) = \overline{1}+(\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_m}))+(\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_m}))a_{i_1}\cdots a_{i_k}$,
onde $1 \le j_m \le \frac{p-3}{2}$, *para todo* $1 \le m \le n$.

Demonstração:

Façamos tal demonstração por indução sobre n. Se $n = 2$ temos que

$$\Phi(u_{j_1}(a_{i1} \cdots a_{i_k}))\Phi(u_{j_2}(a_{i1} \cdots a_{i_k})) = [(\overline{1}+\phi(\beta_{j_1}))+\phi(\beta_{j_1})a_{i1} \cdots a_{i_k}][(\overline{1}+\phi(\beta_{j_2}))+\phi(\beta_{j_2})a_{i1} \cdots a_{i_k}],$$

de onde,

$$\begin{aligned}\Phi(u_{j_1}(a_{i1} \cdots a_{i_k}))\Phi(u_{j_2}(a_{i_1} \cdots a_{i_k})) &= (\overline{1} + \phi(\beta_{j_1}) + \phi(\beta_{j_2}) + \phi(\beta_{j_1})\phi(\beta_{j_2})) + [(1 + \phi(\beta_{j_1}))\phi(\beta_{j_2}) + \\ &\quad +(1 + \phi(\beta_{j_2}))\phi(\beta_{j_1})]a_{i1} \cdots a_{i_k} + \phi(\beta_{j_1})\phi(\beta_{j_2}),\end{aligned}$$

ou ainda,

$$\Phi(u_{j_1}(a_{i1} \cdots a_{i_k}))\Phi(u_{j_2}(a_{i_1} \cdots a_{i_k})) = (\overline{1} + \phi(\beta_{j_1}) + \phi(\beta_{j_2})) + (\phi(\beta_{j_1}) + \phi(\beta_{j_2}))a_{i_1} \cdots a_{i_k}.$$

Vamos supor que para $n = t$ tem-se que

$$\Phi(u_{j_1}(a_{i_1} \cdots a_{i_k})) \cdots \Phi(u_{j_t}(a_{i1} \cdots a_{i_k})) = (\overline{1}+\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t}))+(\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t}))a_{i_1} \cdots a_{i_k}$$

e vamos mostrar que

$$\begin{aligned}\Phi(u_{j_1}(a_{i1} \cdots a_{i_k})) \cdots \Phi(u_{j_{t+1}}(a_{i1} \cdots a_{i_k})) &= (\overline{1} + \phi(\beta_{j_1}) + \cdots + \phi(\beta_{j_{t+1}})) + \\ &\quad + (\phi(\beta_{j_1}) + \cdots + \phi(\beta_{j_{t+1}}))a_{i_1} \cdots a_{i_k}.\end{aligned}$$

Pela hipótese indutiva, tem-se

$$\begin{aligned}\Phi(u_{j_1}(a_{i1} \cdots a_{i_k})) \cdots \Phi(u_{j_{t+1}}(a_{i1} \cdots a_{i_k})) &= [(\overline{1} + \phi(\beta_{j_1}) + \cdots + \phi(\beta_{j_t})) + (\phi(\beta_{j_1}) + \cdots + \\ &\quad +\phi(\beta_{j_t}))a_{i_1} \cdots a_{i_k}][(\overline{1} + \phi(\beta_{j_{t+1}})) + \phi(\beta_{j_{t+1}})a_{i_1} \cdots a_{i_k}],\end{aligned}$$

de onde,

$$\begin{aligned}\Phi(u_{j_1}(a_{i1} \cdots a_{i_k})) \cdots \Phi(u_{j_{t+1}}(a_{i1} \cdots a_{i_k})) &= (\overline{1} + \phi(\beta_{j_1}) + \cdots + \phi(\beta_{j_m}))(\overline{1} + \phi(\beta_{j_{t+1}})) + \\ &\quad +(\phi(\beta_{j_1}) + \cdots + \phi(\beta_{j_t}))(\overline{1} + \phi(\beta_{j_{t+1}}))a_{i_1} \cdots a_{i_k} + \\ &\quad +(\overline{1} + \phi(\beta_{j_1}) + \cdots + \phi(\beta_{j_t}))\phi(\beta_{j_{m+1}})a_{i_1} \cdots a_{i_k} + \\ &\quad +(\phi(\beta_{j_1}) + \cdots + \phi(\beta_{j_t}))\phi(\beta_{j_{t+1}}),\end{aligned}$$

logo,

$$\begin{aligned}\Phi(u_{j_1}(a_{i1}\cdots a_{i_k}))\cdots\Phi(u_{j_{m+1}}(a_{i1}\cdots a_{i_k})) &= (\overline{1}+\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t}))+\\ &+(\overline{1}+\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t}))\phi(\beta_{j_{t+1}})\\ &+(\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t}))a_{i_1}\cdots a_{i_k}+\\ &+(\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t}))\phi(\beta_{j_{t+1}})a_{i_1}\cdots a_{i_k}+\\ &+(\overline{1}+\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t}))\phi(\beta_{j_{t+1}})a_{i_1}\cdots a_{i_k}+\\ &+(\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t}))\phi(\beta_{j_{t+1}})\end{aligned}$$

e, portanto,

$$\begin{aligned}\Phi(u_{j_1}(a_{i1}\cdots a_{i_k}))\cdots\Phi(u_{j_{t+1}}(a_{i1}\cdots a_{i_k})) &= (\overline{1}+\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t})+\phi(\beta_{j_{t+1}}))+\\ &+(\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_t})+\phi(\beta_{j_{t+1}}))a_{i_1}\cdots a_{i_k}.\end{aligned}$$

■

Portanto, se $\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_m}) \notin 2\mathbb{Z}(C_p\times\underbrace{C_2\times\ldots\times C_2}_{n\text{ vezes}}))$, para todo $1\leq j_m\leq\frac{p-3}{2}$ e, para todo $1\leq m\leq n$ o resultado acima garante que $\left\langle\{w_1^2w_2^{-1},w_2^2w_3^{-1},\cdots,w_{\frac{p-3}{2}}^2w_{\frac{p-1}{2}}^{-1},u_{j_i}(a_k)^2:1\leq i\leq\frac{p-3}{2}\text{ e }1\leq i\leq n\}\right\rangle$ é um cadidato ao núcleo do homomorfismo de grupo Φ.

Porém, se $\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_m})\in 2\mathbb{Z}(C_p\times\underbrace{C_2\times\ldots\times C_2}_{n\text{ vezes}}))$, para algum $1\leq j_m\leq\frac{p-3}{2}$ e $1\leq m\leq n$ então do Lema 3.1.6 tem-se $u_{j_1}\cdots u_{j_m}\in\mathrm{Ker}(\Phi)$.

Considere o conjunto

$$\{w_1^2w_2^{-1},w_2^2w_3^{-1},\cdots,w_{\frac{p-3}{2}}^2w_{\frac{p-1}{2}}^{-1},u_j(a_k)^2,u_{j_1}\cdot\cdots\cdot u_{j_m}:1\leq i\leq\frac{p-3}{2}\text{ e }1\leq i\leq n\},$$

onde $u_{j_1}\cdot\cdots\cdot u_{j_m}$ é tal que $\phi(\beta_{j_1})+\cdots+\phi(\beta_{j_m})\in 2\mathbb{Z}(C_p\times\underbrace{C_2\times\ldots\times C_2}_{n\text{ vezes}}))$. Este conjunto é um possível gerador para o núcleo de Φ.

Assim determinar o núcleo do nosso homomorfimo de grupos Φ é um pouco complicado, o que torna difícil generalizar o Teorema 2.3.1 do Capítulo 2.

3.2 Construindo as unidades

Para excluir o caso em que existe um elemento da forma $u_{j_1} \cdot \dots \cdot u_{j_m}$ no núcleo e caracterizar o núcleo da função Φ inicialmente iremos nos restringir ao caso $\mathbb{Z}(C_{2p} \times C_2)$ e, além disso, vamos supor que o conjunto $\{\phi(\beta_1), \cdots, \phi(\beta_{\frac{p-3}{2}})\}$ é linearmente independente.

Lema 3.2.1. *Seja p um primo ótimo e considere que $\boldsymbol{ord}(\Phi(w_1)) = 2^{\frac{p-1}{2}} - 1$. Se o conjunto $\{\phi(\beta_1), \cdots, \phi(\beta_{\frac{p-3}{2}})\}$ é linearmente independente, então*

$$Ker(\Phi) = \langle -1 \rangle \times \left\langle \left\{ w_i^2 w_{i+1}^{-1} : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle \times \left\langle \left\{ u_j(a_1)^2 : 1 \leq j \leq \frac{p-3}{2} \right\} \right\rangle.$$

Demonstração:

Pelo Lema 3.1.2, $\left\langle \{u_j(a_1)^2 : 1 \leq j \leq \frac{p-3}{2}\} \right\rangle \subseteq$ Ker(Φ) e, pelos resultados do Capítulo 2, temos

$$\langle -1 \rangle \times \left\langle \{ w_i^2 w_{i+1}^{-1} : 1 \leq i \leq \frac{p-3}{2} \} \right\rangle \subseteq \text{Ker}(\Phi).$$

Assim

$$\langle -1 \rangle \times \left\langle \{ w_i^2 w_{i+1}^{-1} : 1 \leq i \leq \frac{p-3}{2} \} \right\rangle \times \left\langle \{ u_j(a_1)^2 : 1 \leq j \leq \frac{p-3}{2} \} \right\rangle \subseteq \text{Ker}(\Phi).$$

Por outro lado, seja $x \in$ Ker(Φ), como $x \in \mathcal{U}(\mathbb{Z}C_{2p})$, então

$$x = (-1)^n g^m a_1^t w_1^{r_1} \cdots w_{\frac{p-3}{2}}^{r_{\frac{p-3}{2}}} u_1(a_1)^{s_1} \cdots u_{\frac{p-3}{2}}(a_1)^{s_{\frac{p-3}{2}}}$$

tal que $\Phi(x) = \overline{1}$. Entretanto,

$$\Phi(x) = g^m \Phi(w_1^{r_1} \cdots w_{\frac{p-3}{2}}^{r_{\frac{p-3}{2}}}) \Phi(u_1(a_1))^{s_1} \cdots \Phi(u_{\frac{p-3}{2}}(a_1))^{s_{\frac{p-3}{2}}} = \overline{1}.$$

Logo

$$\Phi(x)^2 = g^{2m} \Phi\left(w_1^{r_1} \cdots w_{\frac{p-3}{2}}^{r_{\frac{p-3}{2}}} \right) = \overline{1}.$$

Sendo $\Phi\left(w_1^{r_1} \cdots w_{\frac{p-3}{2}}^{r_{\frac{p-3}{2}}} \right)$ uma unidade simétrica normalizada então g^{2m} tem de ser simétrica também. Portanto, $2m \equiv 0 \pmod p$ e, sendo assim, $m \equiv 0 \pmod p$.

Assim,

$$\Phi(x)^2 = \Phi\left(w_1^{r_1} \cdots w_{\frac{p-3}{2}}^{r_{\frac{p-3}{2}}} \right) = \overline{1}$$

ou seja,

$$w_1^{r_1}\cdots w_{\frac{p-3}{2}}^{r_{\frac{p-3}{2}}} \in \langle -1\rangle \times \left\langle n_1,\cdots,n_{\frac{p-3}{2}}\right\rangle.$$

Desta forma,

$$\Phi(x)=a_1^t\Phi(u_1(a_1))^{s_1}\cdots\Phi(u_{\frac{p-3}{2}}(a_1))^{s_{\frac{p-3}{2}}}=\overline{1}.$$

Sendo $u_j(a_1)$ unidades simétricas, então $\Phi\left(u_1(a_1)^{s_1}\cdots u_{\frac{p-3}{2}}(a_1)^{s_{\frac{p-3}{2}}}\right)$ também é simétrica e, portanto, a_1^t deve ser simétrica, de onde, obtem-se $t\equiv 0 \pmod 2$. Logo, $\Phi(x)=\Phi(u_1(a_1))^{s_1}\cdots\Phi(u_{\frac{p-3}{2}}(a_1))^{s_{\frac{p-3}{2}}}=\overline{1}$. Do Lema 3.1.2 e da nossa hipótese segue que $s_j=2t_j$, para todo $1\leq j\leq \frac{p-3}{2}$, de onde conclui-se que,

$$x\in\langle -1\rangle\times\left\langle w_1^2w_2^{-1},\cdots,w_{\frac{p-3}{2}}^2w_{\frac{p-1}{2}}^{-1}\right\rangle\times\left\langle \{u_j(a_1)^2:1\leq j\leq \frac{p-3}{2}\}\right\rangle.$$

Portanto,

$$\mathrm{Ker}(\phi):=\langle -1\rangle\times\left\langle\left\{w_iw_{i+1}^{-1}:1\leq i\leq\frac{p-3}{2}\right\}\right\rangle\times\left\langle\left\{u_j(a_1)^2:1\leq j\leq\frac{p-3}{2}\right\}\right\rangle.$$

■

Lembre-se

$$\begin{aligned}
w_i &= (-1)^{(\frac{p-3}{2})}(1-g^{2^{i-1}}+g^{22^{i-1}}+\cdots+(-1)^{(\frac{p-3}{2})}g^{(\frac{p-3}{2})2^{i-1}}+\\
&\quad +(-1)^{(\frac{p-3}{2})}g^{(\frac{p+3}{2})2^{i-1}}+\cdots+g^{(p-2)2^{i-1}}-g^{(p-1)2^{i-1}}),\\
\beta_1 &= \frac{1-w_1^2w_2^{-1}}{2},\\
\beta_i &= \delta(\beta_1)\\
u_j(a_{i_1}a_{i_2}) &= (1-\beta_j)+\beta_ja_{i_1}a_{i_2},\\
\gamma_j(a_1) &= \frac{1-u_j(a_1)^2}{2},
\end{aligned}$$

com δ é o isomorfismo definido em $\mathbb{Z}C_p$ que leva g em g^2 e fixa os inteiros.

Teorema 3.2.1. *Considere o anel de grupo integral $\mathbb{Z}(C_p\times C_2\times C_2)$. Sejam $\langle a_1\rangle$, $\langle a_2\rangle$ tais que $C_2\cong\langle a_i\rangle$. Se p é um primo ótimo, **ord**$(\Phi(w_1))=2^{\frac{p-1}{2}}-1$ e $\{\phi(\beta_1),\cdots,\phi(\beta_{\frac{p-3}{2}})\}$ é um conjunto linearmente independente, então,*
$\mathcal{U}(\mathbb{Z}(C_{2p}\times C_2))=\langle -1\rangle\times\langle g,a_1,a_2\rangle\times\left\langle w_1,\cdots,w_{\frac{p-3}{2}}\right\rangle\times\left\langle\left\{u_j(a_1),u_j(a_2),u_j(a_1a_2):1\leq j\leq\frac{p-3}{2}\right\}\right\rangle.$

Mais ainda, o conjunto $\left\{w_j,u_j(a_1),u_j(a_2),u_j(a_1a_2):1\leq j\leq\frac{p-3}{2}\right\}$ é multiplicativamente inde-

pendente.

Demonstração:

Sabemos que $u \in \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2)) \Leftrightarrow u = u_1\left[\frac{1+u_2}{2} + \left(\frac{1-u_2}{2}\right)a_2\right]$, onde $u_1, u_2 \in \mathcal{U}(\mathbb{Z}(C_{2p}))$ e $u_2 \in$ Ker(Φ).

Do Teorema 2.3.1

$$u_1 \in \langle -1\rangle \times \langle g, a_1\rangle \times \left\langle w_1, w_2, \ldots, w_{\frac{p-3}{2}}\right\rangle \times \left\langle \{u_j(a_1) : 1 \leq j \leq \frac{p-3}{2}\}\right\rangle.$$

Do Lema 3.2.1 tem-se

$$u_2 \in \langle -1\rangle \times \left\langle w_1^2 w_2^{-1}, \cdots, w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1}\right\rangle \times \left\langle \{u_j(a_1)^2 : 1 \leq j \leq \frac{p-3}{2}\}\right\rangle$$

e, portanto,

$$u_2 = (-1)^m (w_1^2 w_2^{-1})^{r_1} \cdots (w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1})^{r_{\frac{p-3}{2}}} u_1(a_1)^{2s_1} \cdots u_{\frac{p-3}{2}}^{2s_{\frac{p-3}{2}}}.$$

Dos Lemas 3.1.4 e 3.1.5 obtém-se

$$\frac{1+u_2}{2} + \left(\frac{1-u_2}{2}\right)a_2 = \left[\frac{1+(-1)}{2} + \left(\frac{1-(-1)}{2}\right)a_2\right]^m \left[\frac{1+u_1(a_1)^2}{2} + \left(\frac{1-u_1(a_1)^2}{2}\right)a_2\right]^{s_1}$$

$$\left[\frac{1+u_2(a_1)^2}{2} + \left(\frac{1-u_2(a_1)^2}{2}\right)a_2\right]^{s_2} \cdots \left[\frac{1+u_{\frac{p-3}{2}}(a_1)^2}{2} + \left(\frac{1-u_{\frac{p-3}{2}}(a_1)^2}{2}\right)a_2\right]^{s_{\frac{p-3}{2}}}.$$

do Lema 3.1.3, segue que

$$\frac{1+u_2}{2} + \left(\frac{1-u_2}{2}\right)a_2 = a_2^m[u_1(a_1)u_1(a_2)u_1(a_1a_2)^{-1}]^{s_1} \cdots [u_{\frac{p-3}{2}}(a_1)u_{\frac{p-3}{2}}(a_2)u_{\frac{p-3}{2}}(a_1a_2)^{-1}]^{s_{\frac{p-3}{2}}},$$

logo,

$$\frac{1+u_2}{2} + \left(\frac{1-u_2}{2}\right)a_2 \in \langle a_2\rangle \times \left\langle \{u_j(a_1), u_j(a_2), u_j(a_1a_2) : 1 \leq j \leq \frac{p-3}{2}\}\right\rangle.$$

Além disso, $u_1 \in \mathcal{U}(\mathbb{Z}C_{2p}) = \langle -1\rangle \times \langle g, a_1\rangle \times \left\langle w_1, w_2, \cdots, w_{\frac{p-3}{2}}\right\rangle \times \left\langle \left\{u_j(a_1) : 1 \leq j \leq \frac{p-3}{2}\right\}\right\rangle$ e sendo assim obtemos o resultado.

Falta verificar que $\{w_i, u_i(a_1), u_i(a_2), u_i(a_1a_2)\}$ é um conjunto multiplicativamente independente. Sabe-se que $C_{2p} \times C_2$ possui 8 subgrupos cíclicos e 2 subgrupos cíclico de ordem 2. Assim, do Teorema 1.4.1, tem-se rank$(\mathcal{U}_1(\mathbb{Z}C_{2p})) = \frac{1}{2}[4p - 2.8 + 3 + 1] = 2p - 6 = 2(p-3)$. Como o conjunto $\{w_j, u_j(a_1), u_j(a_2), \ldots, u_j(a_1a_2) : 1 \leq i \leq \frac{p-3}{2}\}$ gera $\mathcal{U}_1(\mathbb{Z}C_{2p})$, segue que tal conjunto é multiplicativamente independente.

■

Observe que $\{\phi(\beta_1), \cdots, \phi(\beta_{\frac{p-3}{2}})\}$ é um conjunto linearmente independente é equivalente a mostrar que o posto da matriz cujas as entradas correspondem aos coeficientes de $\phi(\beta_i)$ é igual a $\dfrac{p-3}{2}$. Tais escalonamentos foram feitos por nós e conferidos no **GAP**.

Na próxima seção mostraremos através de escalonamento que está condição é satisfeita para os primos $7, 11, 13$ e 19.

3.3 Exemplos

Vejamos alguns exemplos da aplicabilidade do Teorema 3.2.1.

Exemplo 20. *Considere o anel de grupo integral* $\mathbb{Z}(C_{10} \times C_2)$*, onde* $\langle a_1 \rangle$ *e* $\langle a_2 \rangle$ *são tais que* $C_2 \cong \langle a_i \rangle$ *e* $C_5 \cong \langle g \rangle$. *Queremos determinar* $\mathcal{U}(\mathbb{Z}(C_{10} \times C_2))$.

Pelo Teorema 2.3.1,

$$\mathcal{U}(\mathbb{Z}C_{10}) = \langle -1 \rangle \times \langle g, a_1 \rangle \times \langle w_1 \rangle \times \langle u(a_1) \rangle,$$

onde $w_1 = -1 + g + g^4$, $\beta = 4 - 3g + g^2 + g^3 - 3g^4$ e $u(a_1) = (1 - \beta) + \beta a_1$. Como $\phi(\beta) = g + g^2 + g^3 + g^4 \neq \overline{0}$, do Teorema 3.2.1,

$$\mathcal{U}(\mathbb{Z}(C_{10} \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2 \rangle \times \langle w \rangle \times \langle \{u(a_1), u(a_2), u(a_1a_2)\} \rangle.$$

Exemplo 21. *Considere o anel de grupo integral* $\mathbb{Z}(C_{14} \times C_2)$*, com* $\langle a_1 \rangle$ *e* $\langle a_2 \rangle$ *são tais que* $C_2 \cong \langle a_i \rangle$ *e* $C_7 \cong \langle g \rangle$. *Queremos encontrar* $\mathcal{U}(\mathbb{Z}(C_{14} \times C_2))$.

Pelo Teorema 2.3.1 tem-se que

$$\mathcal{U}(\mathbb{Z}C_{14}) = \langle -1 \rangle \times \langle g, a_1 \rangle \times \langle w_1, w_2 \rangle \times \langle u_1(a_1), u_2(a_1) \rangle,$$

onde

$$\begin{aligned} w_1 &= 1 - g + g^2 + g^5 - g^6, \\ w_2 &= \delta(w_1), \\ \beta_1 &= 4 - 3g + 2g^2 - g^3 - g^4 + 2g^5 - 3g^6, \\ \beta_2 &= \delta(\beta_1) = 4 - g - 3g^2 + 2g^3 + 2g^4 - 3g^5 - g^6, \\ u(a_1) &= (1 - \beta_i) + \beta_i a_1, \end{aligned}$$

$i = 1, 2$. Sabemos que $\phi(\beta_1) = g + g^3 + g^4 + g^6$ e $\phi(\beta_2) = g + g^2 + g^5 + g^6$.

Considere:

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Escalonando a matriz acima obtemos:

$$A \sim \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

que possui posto 2. Segue do Teorema 3.2.1

$$\mathcal{U}(\mathbb{Z}(C_{14} \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2 \rangle \times \langle w_1, w_2 \rangle \times \langle u_1(a_1), u_1(a_2), u_2(a_1)u_2(a_2), u_1(a_1a_2), u_2(a_1a_2) \rangle .$$

Exemplo 22. *Considere o anel de grupo integral $\mathbb{Z}(C_{22} \times C_2)$, sendo $\langle a_1 \rangle$ e $\langle a_2 \rangle$ são tais que $C_2 \cong \langle a_i \rangle$ e $C_{11} \cong \langle g \rangle$. Queremos descrever $\mathcal{U}(\mathbb{Z}(C_{22} \times C_2))$.*

Do Teorema 2.3.1

$$\mathcal{U}(\mathbb{Z}C_{22}) = \langle -1 \rangle \times \langle g, a_1 \rangle \times \langle \{w_i : 1 \leq i \leq 4\} \rangle \times \langle \{u_i(a_1) : 1 \leq i \leq 4\} \rangle ,$$

onde

$$\begin{aligned}
w_1 &= 1 - g + g^2 - g^3 + g^4 + g^7 - g^8 + g^9 - g^{10}, \\
w_i &= \delta^{i-1}(w_1), \\
\beta_1 &= 4 - 4g + 4g^2 - 4g^3 + 3g^4 - g^5 - g^6 + 3g^7 - 4g^8 + 4g^9 - 4g^{10}, \\
\beta_i &= \delta^{i-1}(\beta_1), \\
u_i(a_1) &= (1 - \beta_i) + \beta_i a_1,
\end{aligned}$$

$i = 1, 2$. Considere

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Esta matriz é formada pelos coeficientes de $\phi(\beta_j)$. Observe que, quando retiramos a primeira coluna da matriz A, obtemos uma matriz B tal que $a_{ij} = a_{i(p-j)}$. Vamos escalonar esta nova matriz

$$B = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix},$$

logo,

$$B \sim \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix},$$

que tem posto 4. Logo, do Teorema 3.2.1

$$\mathcal{U}(\mathbb{Z}(C_{22} \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2 \rangle \times \langle \{w_i : 1 \leq i \leq 4\} \rangle \times \langle \{u_j(a_1), u_j(a_2), u_j(a_1 a_2) : 1 \leq j \leq 4\} \rangle .$$

Exemplo 23. *Considere o anel de grupo integral* $\mathbb{Z}(C_{26} \times C_2)$, *onde* $\langle a_1 \rangle$ *e* $\langle a_2 \rangle$ *são tais que* $C_2 \cong \langle a_i \rangle$ *e* $C_{13} \cong \langle g \rangle$. *Queremos determinar* $\mathcal{U}(\mathbb{Z}(C_{26} \times C_2))$.

Do Teorema 2.3.1 obtemos

$$\mathcal{U}(\mathbb{Z}C_{26}) = \langle -1 \rangle \times \langle g, a_1 \rangle \times \langle \{w_i : 1 \leq i \leq 5\} \rangle \times \langle \{u_i(a) : 1 \leq i \leq 5\} \rangle ,$$

onde

$$\begin{array}{rcl} w_1 & = & -1 + g - g^2 + g^3 - g^4 + g^5 + g^8 - g^9 + g^{10} - g^{11} + g^{12}, \\ w_i & = & \delta^{i-1}(w_1), \\ \beta_1 & = & 8 - 7g + 5g^2 - 3g^3 + g^4 + g^9 - 3g^{10} + 5g^{11} - 7g^{12}, \\ \beta_i & = & \delta^{i-1}(\beta_1), \\ u_i(a_1) & = & (1 - \beta_i) + \beta_i a_1, \end{array}$$

$1 \leq i \leq 5$. Considere

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Observe que a matriz A quando excluímos a primeira coluna se transforma numa matriz B tal que $a_{ij} = a_{i(p-j)}$. Considerando as 6 primeiras colunas da matriz B, obtemos a seguinte matriz

$$C = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix},$$

logo, escalonando tal matriz tem-se

$$C \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

ou ainda,

$$C \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix},$$

de onde

$$C \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix},$$

que possui posto 5. Logo, segue do Teorema 3.2.1

$$\mathcal{U}(\mathbb{Z}(C_{26} \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2 \rangle \times \langle \{w_i : 1 \leq i \leq 5\} \rangle \times \langle \{u_j(a_1), u_j(a_2), u_j(a_1 a_2) : 1 \leq j \leq 5\} \rangle .$$

Exemplo 24. *Considere o anel de grupo integral* $\mathbb{Z}(C_{38} \times C_2)$, *sendo* $\langle a_1 \rangle$ *e* $\langle a_2 \rangle$ *tais que* $C_2 \cong \langle a_i \rangle$ *e* $C_{19} \cong \langle g \rangle$. *Queremos descrever* $\mathcal{U}(\mathbb{Z}(C_{38} \times C_2))$.

Do Teorema 2.3.1 obtemos

$$\mathcal{U}(\mathbb{Z}C_{38}) = \langle -1 \rangle \times \langle g, a_1 \rangle \times \langle \{w_i : 1 \leq i \leq 8\} \rangle \times \langle \{u_i(a) : 1 \leq i \leq 8\} \rangle ,$$

onde

$$
\begin{aligned}
w_1 &= 1 - g + g^2 - g^3 + g^4 - g^5 + g^6 - g^7 + g^8 + g^{11} - g^{12} + g^{13} - g^{14} + g^{15} - g^{16} + g^{17} - g^{18},\\
w_i &= \delta^{i-1}(w_1),\\
\beta_1 &= 8 - 8g + 8g^2 - 8g^3 + 7g^4 - 5g^5 + 3g^6 - g^7 - g^{12} + 3g^{13} - 5g^{14} + 7g^{15} - 8g^{16} + 8g^{17} - 8g^{18},\\
\beta_i &= \delta^{i-1}(\beta_1),\\
u_i(a_1) &= (1 - \beta_i) + \beta_i a_1,
\end{aligned}
$$

$1 \leq i \leq 8$. Considere

$$
A = \begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1\\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1\\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1\\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0\\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0\\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1
\end{pmatrix}.
$$

Observe que a matriz A quando excluímos a primeira coluna se transforma numa matriz B tal que $a_{ij} = a_{i(p-j)}$. Considerando as primeiras 9 colunas desta matriz encontramos

$$
C = \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1\\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1\\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1\\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0\\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0\\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1\\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0
\end{pmatrix},
$$

logo, escalonado a matriz C tem-se,

$$C \sim \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix},$$

sendo assim,

$$C \sim \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix},$$

e, desta maneira,

$$C \sim \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

e, portanto,

$$C \sim \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix},$$

que possui posto 8. Assim pelo Teorema 3.2.1

$$\mathcal{U}(\mathbb{Z}(C_{38} \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2 \rangle \times \langle \{w_i : 1 \leq i \leq 8\} \rangle \times \langle \{u_j(a_1), u_j(a_2), u_j(a_1a_2) : 1 \leq j \leq 8\} \rangle .$$

Conforme o primo aumenta, as contas vão ficando maiores. Verificamos com o auxílio do **GAP**, que para os primos $23, 29, 53, 59, 61$ e 67 também temos que os postos das respectivas matrizes serão $\dfrac{p-3}{2}$.

Capítulo 4

Unidades de $\mathbb{Z}(C_{2p} \times C_2 \times C_2)$ e unidades centais de $\mathbb{Z}(C_p \times Q_8)$

Neste Capítulo vamos estudar o caso em que $n = 3$, ou seja, vamos descrever as unidades do anel de grupo $\mathbb{Z}(C_{2p} \times C_2 \times C_2)$, onde $C_p \cong \langle g \rangle$, e $\langle a_i \rangle$ são tais que $C_2 \cong \langle a_i \rangle$, $1 \leq i \leq 3$. Além disso, iremos também exibir um conjunto gerador das unidades centrais de $\mathbb{Z}(C_p \times Q_8)$.

4.1 Unidades de $\mathbb{Z}(C_{2p} \times C_2 \times C_2)$

Conforme vimos no Capítulo anterior, tem-se

$$u \in \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2 \times C_2 \times C_2)) \Longleftrightarrow u = u_1 \left[\left(\frac{1+u_2}{2} \right) + \left(\frac{1-u_2}{2} \right) a \right],$$

onde $u_1, u_2 \in \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2))$ e $u_2 \equiv 1 \pmod{\langle 2 \rangle}$, ou equivalentemente, $u_2 \in \mathrm{Ker}(\Phi)$, com $\Phi : \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2)) \to \mathcal{U}(\mathbb{Z}_2(C_{2p} \times C_2))$.

Portanto, para determinarmos as unidades de $\mathbb{Z}(C_{2p} \times C_2 \times C_2)$, basta caracterizarmos o núcleo da função Φ.

Tome $u \in \mathrm{Ker}(\Phi)$, então $u \in \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2))$ é tal que $\Phi(u) = \overline{1}$. Do Teorema 3.2.1

$$\begin{aligned} u \;\; = \;\; & (-1)^n g^m a_1^{\epsilon_1} a_2^{\epsilon_2} w_1^{k_1} w_2^{k_2} \cdots w_{\frac{p-3}{2}}^{k_{\frac{p-3}{2}}} u_1(a_1)^{r_1} \cdots u_{\frac{p-3}{2}}(a_1)^{r_{\frac{p-3}{2}}} u_1(a_2)^{s_1} \cdots u_{\frac{p-3}{2}}(a_2)^{s_{\frac{p-3}{2}}} \\ & u_1(a_1a_2)^{t_1} \cdots u_{\frac{p-3}{2}}(a_1a_2)^{t_{\frac{p-3}{2}}}. \end{aligned}$$

Como $g^m, a_i^{\epsilon_i} \notin \mathrm{Ker}(\Phi)$ se $1 \leq m \leq p-1$ e $\epsilon_i = 1$, para todo $i \in \{1,2\}$, tem-se que

$$u = (-1)^n w_1^{k_1} w_2^{k_2} \cdots w_{\frac{p-3}{2}}^{k_{\frac{p-3}{2}}} u_1^{r_1}(a_1) \cdots u_{\frac{p-3}{2}}^{r_{\frac{p-3}{2}}}(a_1) u_1^{s_1}(a_2) \cdots u_{\frac{p-3}{2}}^{s_{\frac{p-3}{2}}}(a_2) u_1^{t_1}(a_1a_2) \cdots u_{\frac{p-3}{2}}^{t_{\frac{p-3}{2}}}(a_1a_2).$$

Assim

$$\begin{aligned}\Phi(u) &= \Phi(w_1^{k_1} w_2^{k_2} \cdots w_{\frac{p-3}{2}}^{k_{\frac{p-3}{2}}})\Phi(u_1(a_1))^{r_1} \cdots \Phi(u_{\frac{p-3}{2}}(a_1))^{r_{\frac{p-3}{2}}} \Phi(u_1(a_2))^{s_1} \cdots \Phi(u_{\frac{p-3}{2}}(a_2))^{s_{\frac{p-3}{2}}} \\ &\quad \Phi(u_1(a_1a_2))^{t_1} \cdots \Phi(u_{\frac{p-3}{2}}(a_1a_2))^{t_{\frac{p-3}{2}}} \\ &= \overline{1}.\end{aligned}$$

Lembrando que $\Phi(w_1)^{2^{i-1}} = \Phi(w_i)$ e que $u_j(a_1)^2, u_j(a_2)^2, u_j(a_1a_2)^2 \in \mathrm{Ker}(\Phi)$, para todo $1 \leq i \leq \frac{p-3}{2}$, obtém-se $\Phi(u)^2 = \Phi(w_1)^{2\alpha} = \overline{1}$, onde $\alpha = 2 \cdot (k_1 + 2k_2 + \cdots + 2^{\frac{p-5}{2}} k_{\frac{p-3}{2}})$. Supondo que $\mathrm{ord}(\Phi(w_1)) = 2^{\frac{p-1}{2}} - 1$, então $2\alpha = (2^{\frac{p-1}{2}} - 1)\beta$. Sendo $2^{\frac{p-1}{2}} - 1$ um número ímpar então $\beta = 2q$ e, portanto, $\alpha = (2^{\frac{p-1}{2}} - 1)q$.

Pode-se concluir que

$$w_1^{k_1} w_2^{k_2} \cdots w_{\frac{p-3}{2}}^{k_{\frac{p-3}{2}}} \in \langle -1 \rangle \times \left\langle w_1^2 w_2^{-1}, \cdots, w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1} \right\rangle.$$

Sendo assim
$\Phi(u_1(a_1))^{r_1} \cdots \Phi(u_{\frac{p-3}{2}}(a_1))^{r_{\frac{p-3}{2}}} \Phi(u_1(a_2))^{s_1} \cdots \Phi(u_{\frac{p-3}{2}}(a_2))^{s_{\frac{p-3}{2}}} \Phi(u_1(a_1a_2))^{t_1} \cdots \Phi(u_{\frac{p-3}{2}}(a_1a_2)))^{t_{\frac{p-3}{2}}}$
$= \Phi(u) = \overline{1}$.

Porém, $\Phi(u_j(h))^2 = \overline{1}$, com $h \in \{a_1, a_2, a_1a_2\}$, para todo $1 \leq j \leq \frac{p-3}{2}$, então pode-se reduzir a equação anterior à seguinte igualdade

$$\Phi(u_{i_1}(a_1)) \cdots \Phi(u_{i_n}(a_1))\Phi(u_{j_1}(a_2)) \cdots \Phi(u_{j_m}(a_2))\Phi(u_{l_1}(a_1a_2)) \cdots \Phi(u_{l_q}(a_1a_2)) = \overline{1}.$$

Do Lema 3.1.6 tem-se
$\{\overline{1} + \phi(\beta_{i_1}) \cdots \phi(\beta_{i_n}) + [\phi(\beta_{i_1}) \cdots \phi(\beta_{i_n})]a_1\}\{\overline{1} + \phi(\beta_{j_1}) \cdots \phi(\beta_{j_m}) + [\phi(\beta_{j_1}) \cdots \phi(\beta_{j_m})]a_2\}$
$\{\overline{1} + \phi(\beta_{l_1}) \cdots \phi(\beta_{l_q}) + (\phi(\beta_{l_1}) \cdots \phi(\beta_{l_q})]a_1a_2\} = \overline{1}$

Sejam

$$\begin{aligned}
\alpha_1 &= \phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n}),\\
\alpha_2 &= \phi(\beta_{j_1}) + \cdots + \phi(\beta_{j_m}),\\
\alpha_3 &= \phi(\beta_{l_1}) + \cdots + \phi(\beta_{l_q}).
\end{aligned}$$

Observe que $\alpha_i \in \mathrm{Im}(\phi) \subseteq \mathbb{Z}_2 C_p$. Assim:

$$\Phi(u) = (\overline{1} + \alpha_1 + \alpha_1 a_1)(\overline{1} + \alpha_2 + \alpha_2 a_2)(\overline{1} + \alpha_3 + \alpha_3 a_1 a_2) = \overline{1},$$

ou seja,
$\Phi(u) = [(\overline{1} + \alpha_1)(\overline{1} + \alpha_2)(\overline{1} + \alpha_3) + \alpha_1\alpha_2\alpha_3] + [\alpha_1(\overline{1} + \alpha_2)(\overline{1} + \alpha_3) + (\overline{1} + \alpha_1)\alpha_2\alpha_3]a_1 +$
$+[(\overline{1} + \alpha_1)\alpha_2(\overline{1} + \alpha_3) + \alpha_1(\overline{1} + \alpha_2)\alpha_3]a_2 + [\alpha_1)\alpha_2(\overline{1} + \alpha_3) + (\overline{1} + \alpha_1)(\overline{1} + \alpha_2)\alpha_3]a_1a_2 = \overline{1}$,
isto é,
$\Phi(u) = [(\overline{1} + \alpha_1 + \alpha_2 + \alpha_3) + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3] + [\alpha_1 + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3]a_1 +$
$+[\alpha_2 + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3]a_2 + [\alpha_3 + \alpha_1)\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3]a_1a_2 = \overline{1}$
e, portanto,

$$\begin{cases}
\overline{1} + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \overline{1}\\
\alpha_1 + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \overline{0}\\
\alpha_2 + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \overline{0}\\
\alpha_3 + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \overline{0}
\end{cases}$$

de onde se conclui que $\alpha_1 = \alpha_2 = \alpha_3$ e, desta maneira, $\alpha_1^2 = \alpha_1$. Assim, $\Phi(u) = \overline{1}$ se reduz a equação $(\overline{1} + \alpha_1 + \alpha_1^2) + (\alpha_1 + \alpha_1^2)a_1 + (\alpha_1 + \alpha_1^2)a_2 + (\alpha_1 + \alpha_1^2)a_1a_2 = \overline{1}$.

Levando em conta que $w_i^2 w_{i+1}^{-1} \in \mathrm{Ker}(\Phi)$, então

$$w_i^2 w_{i+1}^{-1} = a_0 + \sum_{i=1}^{p-1} a_i g^i,$$

com a_0 ímpar e $a_i = a_{p-i}$ par, para todo $1 \leq i \leq \frac{p-1}{2}$. Observe que:

$$\epsilon\left(\sum_{i=1}^{p-1} a_i g^i\right) = 2\sum_{i=1}^{\frac{p-1}{2}} a_i,$$

o que nos leva a concluir,

$$\epsilon\left(\sum_{i=1}^{p-1} a_i g^i\right) \equiv 0 \pmod{4}.$$

Como $1 - w_i^2 w_{i+1}^{-1}$ tem aumento trivial, então $(1 - a_0) - 2\sum_{i=1}^{\frac{p-1}{2}} a_i = 0$, ou seja, $(1 - a_0) \equiv 0 \pmod{4}$. Então existe $q \in \mathbb{Z}$ tal que $1 - a_0 = 4q$, assim, $\dfrac{1 - a_0}{2} = 2q$. Logo $\dfrac{1 - a_0}{2} \equiv 0 \pmod{2}$. Portanto,

$$\phi(\beta_j) = \sum_{i=1}^{p-1} b_i g^i$$

com $b_i = b_{p-i} \in \mathbb{Z}_2$.

O próximo resultado determina a existência do elemento idempotente não trivial α em $\mathrm{Im}(\phi)$.

Lema 4.1.1. *Seja p um primo ótimo. Se* $\boldsymbol{ord}(\Phi(w_1)) = 2^{\frac{p-1}{2}} - 1$, *existe no máximo um idempotente não trivial $\alpha \in Im(\Phi)$.*

Demonstração:

Sabemos que $u \in \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2 \times C_2)) \Leftrightarrow u = u_1\left[\dfrac{1 + u_2}{2} + \left(\dfrac{1 - u_2}{2}\right) a_2\right]$, onde $u_1, u_2 \in \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2))$ e $u_2 \in \mathrm{Ker}(\Phi)$, com $\Phi : \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2)) \to \mathcal{U}(\mathbb{Z}_2(C_{2p} \times C_2))$. Do Teorema 3.2.1, segue

$$u_1 \in \langle -1 \rangle \times \langle g, a_1 \rangle \times \left\langle \{w_i : 1 \leq i \leq \frac{p-3}{2}\} \right\rangle \times \left\langle \{u_j(a_1), u_j(a_2), u_j(a_1a_2) : 1 \leq j \leq \frac{p-3}{2}\} \right\rangle.$$

Como $u_2 \in \mathrm{Ker}(\Phi)$, então,

$$\begin{aligned} u_2 \quad = \quad & (-1)^n (w_1^2 w_2^{-1})^{r_1} \cdots (w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1} w_{\frac{p-1}{2}}^{-1})^{r_{\frac{p-3}{2}}} (u_1(a_1)^{2s_1} \cdots u_{\frac{p-3}{2}}(a_1)^{2s_{\frac{p-3}{2}}} u_1(a_2)^{2t_1} \cdots u_{\frac{p-3}{2}}(a_2)^{2t_{\frac{p-3}{2}}} \\ & u_1(a_1a_2)^{2m_1} \cdots u_{\frac{p-3}{2}}(a_1a_2)^{2m_{\frac{p-3}{2}}}. \end{aligned}$$

Da análise feita anteriormente, $\Phi(u) = \overline{1}$ se reduz a equação

$$(\overline{1} + \alpha + \alpha^2) + (\alpha + \alpha^2)a_1 + (\alpha + \alpha^2)a_2 + (\alpha + \alpha^2)a_1a_2 = \overline{1},$$

onde $\alpha = \phi(\beta_{i_1}) + \cdots \phi(\beta_{i_n})$.

Sabendo que $\alpha = \phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n})$, então vimos que $\alpha = \displaystyle\sum_{i=1}^{p-1} a_i g^i$, onde $a_i \in \mathbb{Z}_2$ e $a_i = a_{p-i}$ e, sendo assim, $\alpha^2 = \displaystyle\sum_{i=1}^{p-1} a_i^2 g^{k_i}$.

Para todo $1 \leq i \leq \frac{p-1}{2}$, considere $k_i \in \mathbb{Z}$ tal que $k_i \equiv 2i \pmod p$. Do fato que $\alpha^2 = \alpha$, tem-se $a_k = a_i^2$, $1 \leq i \leq p-1$.

Caso 1. Se $\overline{2}$ gera $\mathcal{U}(\mathbb{Z}_p)$

Neste caso, se $i \neq 0$, então i será uma potência de 2. Se $i \equiv 2^n \pmod p$, então $a_i = a_{2^n} = a_{2^{n-1}} = \cdots = a_2 = a_1 = \overline{1}$, isto é, $a_i = \overline{1}$, $1 \leq i \leq p-1$, de onde, $\alpha = \overline{1} + \widehat{g}$.

Caso 2. Se $\overline{2}$ gera $\mathcal{U}(\mathbb{Z}_p)^2$ e $-\overline{1} \notin \mathcal{U}(\mathbb{Z}_p)^2$

Neste caso, como $-\overline{1} \notin \mathcal{U}(\mathbb{Z}_p)^2$ para $i \neq 0$, tem-se que, ou $i \in \mathcal{U}(\mathbb{Z}_p)^2$, ou $p - i \in \mathcal{U}(\mathbb{Z}_p)^2$ e, portanto, ou i é uma potência de 2, ou $p-i$ é uma potência de 2. Assim, ou $a_i = \overline{1}$, ou $a_{p-i} = \overline{1}$. Como ambos são iguais, tem-se que $a_i = \overline{1}$, $1 \leq i \leq p-1$ e, desta forma, $\alpha = \overline{1} + \widehat{g}$.

$\blacksquare$

Primeiramente estudaremos o caso em que este idempotene não trivial não existe.

Lema 4.1.2. *Seja p um primo ótimo e **ord**$(\Phi(w_1)) = 2^{\frac{p-1}{2}} - 1$. Se não existe $\alpha \in Im(\Phi)$, idempotente não trivial, então*

$$Ker(\Phi) = \langle -1 \rangle \times \left\langle \left\{ w_i^2 w_{i+1}^{-1} : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle \times \left\langle \left\{ u_j(a_1)^2, u_j(a_2)^2, u_j(a_1a_2)^2 : 1 \leq j \leq \frac{p-3}{2} \right\} \right\rangle.$$

Demonstração:

Segue do Corolário 2.2.2 que $\langle -1 \rangle \times \left\langle \left\{ w_i^2 w_{i+1}^{-1} : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle \subseteq \mathrm{Ker}(\Phi)$. Seja $S = \langle -1 \rangle \times \left\langle \left\{ w_i^2 w_{i+1}^{-1} : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle \times \left\langle \left\{ u_j^2(a_1), u_j^2(a_2), u_j^2(a_1a_2) : 1 \leq j \leq \frac{p-3}{2} \right\} \right\rangle$, onde $u_j(h) = (1 - \beta_j) + \beta_j h$ com $h \in \{a_1, a_2, a_1a_2\}$.

Do Lema 3.1.2, segue $\left\{ u_j^2(a_1), u_j^2(a_2), u_j^2(a_1a_2) : 1 \leq j \leq \frac{p-3}{2} \right\} \subseteq \mathrm{Ker}(\Phi)$ e, portanto, $S \subseteq \mathrm{Ker}(\Phi)$.

Tome $u \in \mathrm{Ker}(\Phi)$. Como $u \in \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2 \times C_2))$ e da observação anterior, tem-se

$$u = (-1)^n w_1^{k_1} w_2^{k_2} \cdots w_{\frac{p-3}{2}}^{k_{\frac{p-3}{2}}} u_1^{r_1}(a_1) \cdots u_{\frac{p-3}{2}}^{r_{\frac{p-3}{2}}}(a_1) u_1^{s_1}(a_2) \cdots u_{\frac{p-3}{2}}^{s_{\frac{p-3}{2}}}(a_2) u_1^{t_1}(a_1a_2) \cdots u_{\frac{p-3}{2}}^{t_{\frac{p-3}{2}}}(a_1a_2),$$

com

$$w_1^{k_1} w_2^{k_2} \cdots w_{\frac{p-3}{2}}^{k_{\frac{p-3}{2}}} \in \langle -1 \rangle \times \left\langle \left\{ w_i^2 w_{i+1}^{-1} : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle$$

e

$$\Phi(u_{i_1}(a_1)) \cdots \Phi(u_{i_n}(a_1)) \Phi(u_{i_1}(a_2)) \cdots \Phi(u_{i_n}(a_2)) \Phi(u_{i_1}(a_1a_2)) \cdots \Phi(u_{i_n}(a_1a_2))) = \overline{1}.$$

Considere $\alpha = \phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n})$. Então tem-se

$$\Phi(u) = (\overline{1} + \alpha + \alpha^2) + (\alpha + \alpha^2)a_1 + (\alpha + \alpha^2)a_2 + (\alpha + \alpha^2)a_1a_2 = \overline{1}.$$

Como não existe $\alpha \in \mathrm{Im}(\Phi)$ idempotente não trivial obtemos

$$u = (-1)^n(w_1^2w_2^{-1})^{n_1}\cdots(w^2_{\frac{p-3}{2}}w^{-1}_{\frac{p-1}{2}})^{n_{\frac{p-3}{2}}}u_1(a_1)^{2m_1}\cdots u_{\frac{p-3}{2}}(a_1)^{2m_{\frac{p-3}{2}}}\cdots u_1(a_2)^{2q_1}\cdots u_{\frac{p-3}{2}}(a_2)^{2q_{\frac{p-3}{2}}}$$

ou seja,

$$u \in \langle -1\rangle \times \left\langle w_1^2w_2^{-1}, \cdots, w_i^2w_{i+1}^{-1}, \cdots, w^2_{\frac{p-3}{2}}w^{-1}_{\frac{p-1}{2}}\right\rangle \times \left\langle \{u_j(a_1)^2, u_j(a_2)^2, u_j(a_1a_2)^2 : 1 \leq j \leq \frac{p-3}{2}\}\right\rangle.$$

Conclui-se que

$$\mathrm{Ker}(\Phi) = \langle -1\rangle \left\langle \left\{ w_i^2w_{i+1}^{-1} : 1 \leq i \leq \frac{p-3}{2}\right\}\right\rangle \times \left\langle \left\{ u_j(a_1)^2, u_j(a_2)^2, u_j(a_1a_2)^2 : 1 \leq j \leq \frac{p-3}{2}\right\}\right\rangle.$$

■

Como conseguimos descrever o núcleo da função Φ, podemos descrever as unidades de $\mathbb{Z}(C_{2p} \times C_2 \times C_2)$. Lembre-se que

$$\begin{aligned}
w_i &:= g^{(\frac{p-1}{2})\cdot 2^{i-1}}v_i = (-1)^{(\frac{p-3}{2})}(1 - g^{2^{i-1}} + g^{2\cdot 2^{i-1}} + \cdots + (-1)^{(\frac{p-3}{2})}g^{(\frac{p-3}{2})\cdot 2^{i-1}} + \\
&\quad +(-1)^{(\frac{p-3}{2})}g^{(\frac{p+3}{2})\cdot 2^{i-1}} + \cdots + g^{(p-2)\cdot 2^{i-1}} - g^{(p-1)\cdot 2^{i-1}}),\\
\beta_1 &= \frac{1 - w_1^2w_2^{-1}}{2},\\
\beta_i &= \delta^{i-1}(\beta_1),\\
u_i(h) &= (1-\beta_j) + \beta_i h,
\end{aligned}$$

$1 \leq i \leq \frac{p-3}{2}$, com $h \in \{a_1, a_2, a_3, a_1a_2, a_1a_3, a_2a_3, a_1a_2a_3\}$. Além disso, δ representa o isomorfismo de $\mathbb{Z}C_p$ que leva g e, g^2 e fixa os elementos de $\mathbb{Z}$.

Teorema 4.1.1. *Considere o anel de grupo $\mathbb{Z}(C_{2p} \times C_2 \times C_2)$, onde p é um primo ótimo, **ord**$(\rho(w_1)) = 2^{\frac{p-1}{2}} - 1$, $\{\phi(\beta_1), \cdots, \phi(\beta_{\frac{p-3}{2}})\}$ é um conjunto linearmente independente e que não exista $\alpha \in Im(\phi)$ idempotente não trivial. Então*

$$\mathcal{U}(\mathbb{Z}(C_{2p} \times C_2 \times C_2)) = \langle -1\rangle \times \langle g, a_1, a_2, a_3\rangle \times \left\langle \{w_i : 1 \leq i \leq \frac{p-3}{2}\}\right\rangle \times \langle S\rangle$$

onde

$$S=\left\{u_j(a_1),u_j(a_2),u_j(a_3),u_j(a_1a_2),u_j(a_1a_3),u_j(a_2a_3),u_j(a_1a_2a_3):1\leq j\leq\frac{p-3}{2}\right\}.$$

Demonstração:

Sabemos que $u\in\mathcal{U}(\mathbb{Z}(C_{2p}\times C_2\times C_2))\Leftrightarrow u=u_1\left[\frac{1+u_2}{2}+\frac{1-u_2}{2}a_2\right]$, onde $u_1,u_2\in\mathcal{U}(\mathbb{Z}(C_{2p}\times C_2))$ e $u_2\in$ Ker(Φ) com $\Phi:\mathcal{U}(\mathbb{Z}(C_{2p}\times C_2))\to\mathcal{U}(\mathbb{Z}_2(C_{2p}\times C_2))$. Do Teorema 3.2.1

$$u_1\in\langle -1\rangle\times\langle g,a_1\rangle\times\left\langle\{w_i:1\leq i\leq\frac{p-3}{2}\}\right\rangle\times\left\langle\{u_j(a_1),u_j(a_2),u_j(a_1a_2):1\leq j\leq\frac{p-3}{2}\}\right\rangle.$$

Como $u_2\in$ Ker(Φ), então

$$\begin{aligned}u_2 \;=\;& (-1)^n(w_1^2w_2^{-1})^{r_1}\cdots(w^2_{\frac{p-3}{2}}w^{-1}_{\frac{p-1}{2}w^{-1}_{\frac{p-1}{2}}})^{r_{\frac{p-3}{2}}}(u_1(a_1)^{2s_1}\cdots u_{\frac{p-3}{2}}(a_1)^{2s_{\frac{p-3}{2}}}u_1(a_2)^{2t_1}\cdots u_{\frac{p-3}{2}}(a_2)^{2t_{\frac{p-3}{2}}}\\ & u_1(a_1a_2)^{2m_1}\cdots u_{\frac{p-3}{2}}(a_1a_2)^{2m_{\frac{p-3}{2}}},\end{aligned}$$

e, do Lema 3.1.4, e do Lema 3.1.5, obtém-se

$$\frac{1+u_2}{2}+\left(\frac{1-u_2}{2}\right)a_3=\left[\frac{1+(-1)}{2}+\frac{1-(1)}{2}a_3\right]^n\left[\frac{1+w_1^2w_2^{-1}}{2}+\frac{1-w_1^2w_2^{-1}}{2}a_3\right]^{r_1}\cdots$$

$$\left[\frac{1+w^2_{\frac{p-3}{2}}w^{-1}_{\frac{p-1}{2}}}{2}+\frac{1-w^2_{\frac{p-3}{2}}w^{-1}_{\frac{p-1}{2}}}{2}a_3\right]^{r_{\frac{p-3}{2}}}\left[\frac{1+u_1(a_1)^2}{2}+\frac{1-u_1(a_1)^2}{2}a_3\right]^{s_1}\cdots$$

$$\left[\frac{1+u_{\frac{p-3}{2}}(a_1)^2}{2}+\frac{1-u_{\frac{p-3}{2}}(a_1)^2}{2}a_3\right]^{s_{\frac{p-3}{2}}}\left[\frac{1+u_1(a_2)^2}{2}+\frac{1-u_1(a_2)^2}{2}a_3\right]^{t_1}\cdots$$

$$\left[\frac{1+u_{\frac{p-3}{2}}(a_2)^2}{2}+\frac{1-u_{\frac{p-3}{2}}(a_2)^2}{2}a_3\right]^{t_{\frac{p-3}{2}}}\left[\frac{1+u_1(a_1a_2)^2}{2}+\frac{1-u_1(a_1a_2)^2}{2}a_3\right]^{m_1}\cdots$$

$$\left[\frac{1+u_{\frac{p-3}{2}}(a_1a_2)^2}{2}+\frac{1-u_{\frac{p-3}{2}}(a_1a_2)^2}{2}a_3\right]^{m_{\frac{p-3}{2}}}$$

Para todo $1 \leq j \leq \frac{p-3}{2}$, sejam

$$\begin{aligned}
\lambda_j(a_1) &= \frac{1-u_j(a_1)^2}{2}, \\
\lambda_j(a_2) &= \frac{1-u_j(a_2)^2}{2}, \\
\lambda_j(a_1a_2) &= \frac{1-u_j(a_1a_2)^2}{2},
\end{aligned}$$

e sejam

$$\begin{aligned}
v_j(a_1a_3) &= (1-\lambda_j(a_1)) + \lambda_j(a_1)a_3, \\
v_j(a_2a_3) &= (1-\lambda_j(a_2)) + \lambda_j(a_2)a_3, \\
v_j(a_1a_2a_3) &= (1-\lambda_j(a_1a_2)) + \lambda_j(a_1a_2)a_3.
\end{aligned}$$

Do Lema 3.1.3, segue

$$\begin{aligned}
v_j(a_1a_3) &= u_j(a_1)u_j(a_3)u_j(a_1a_3)^{-1}, \\
v_j(a_2a_3) &= u_j(a_2)u_j(a_3)u_j(a_2a_3)^{-1} \\
v_j(a_1a_2a_3) &= u_j(a_1a_2)u_j(a_3)u_j(a_1a_2a_3)^{-1}.
\end{aligned}$$

Desta forma,

$$\left(\frac{1+u_2}{2}\right) + \left(\frac{1-u_2}{2}\right)a_3 = a_3^n u_1(a_3)^{r_1}\cdots u_{\frac{p-3}{2}}(a_3)^{r_{\frac{p-3}{2}}}(u_1(a_1)u_1(a_3)u_1(a_1a_3)^{-1})^{s_1}\cdots (u_{\frac{p-3}{2}}(a_1)u_{\frac{p-3}{2}}(a_3)u_{\frac{p-3}{2}}(a_1a_3)^{-1})^{s_{\frac{p-3}{2}}}(u_1(a_2)u_1(a_3)u_1(a_2a_3)^{-1})^{t_1}\cdots(u_{\frac{p-3}{2}}(a_2)u_{\frac{p-3}{2}}(a_3)u_{\frac{p-3}{2}}(a_2a_3)^{-1})^{t_{\frac{p-3}{2}}} (u_1(a_1a_2)u_1(a_3)u_1(a_1a_2a_3)^{-1})^{m_1}\cdots(u_{\frac{p-3}{2}}(a_1a_2)u_{\frac{p-3}{2}}(a_3)u_{\frac{p-3}{2}}(a_1a_2a_3)^{-1})^{m_{\frac{p-3}{2}}}.$$

Assim, provamos que

$$\mathcal{U}(\mathbb{Z}(C_{2p} \times C_2 \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2, a_3 \rangle \times \left\langle \left\{ w_i : 1 \leq i \leq \frac{p-3}{2} \right\} \right\rangle \times \langle S \rangle .$$

■

Façamos um exemplo para ilustrar este resultado.

Exemplo 25. *Considere cada grupo cíclico C_2 é gerado por a_i e $C_p \cong \langle g \rangle$. Descreveremos as unidades do anel de grupo $\mathbb{Z}(C_{22} \times C_2 \times C_2)$.*

Do Teorema 3.2.1

$\mathcal{U}(\mathbb{Z}(C_{11}\times C_2\times C_2)) = \langle -1\rangle \times \langle g, a_1, a_2\rangle \times \langle w_1, \cdots, w_4\rangle \times \langle \{u_j(a_i), u_j(a_1a_2) : 1 \leq j \leq 4 \text{ e } 1 \leq i \leq 2\}\rangle$.

Tem-se que

$$\begin{aligned}
\phi(\beta_1) &= g^4 + g^5 + g^6 + g^7, \\
\phi(\beta_1)^2 &= g + g^3 + g^8 + g^{10} \neq \phi(\beta_1), \\
\phi(\beta_2) &= g + g^3 + g^8 + g^{10}, \\
\phi(\beta_2)^2 &= g^2 + g^5 + g^6 + g^9 \neq \phi(\beta_2), \\
\phi(\beta_3) &= g^2 + g^5 + g^6 + g^9, \\
\phi(\beta_3)^2 &= g + g^4 + g^7 + g^{10} \neq \phi(\beta_3), \\
\phi(\beta_4) &= g + g^4 + g^7 + g^{10}, \\
\phi(\beta_4)^2 &= g^2 + g^3 + g^8 + g^9 \neq \phi(\beta_4)
\end{aligned}$$

além disso,

$$\begin{aligned}
\phi(\beta_1) + \phi(\beta_2) &= g + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^{10}, \\
(\phi(\beta_1) + \phi(\beta_2))^2 &= g + g^2 + g^3 + g^5 + g^6 + g^8 + g^9 + g^{10} \neq \phi(\beta_1) + \phi(\beta_2), \\
\phi(\beta_1) + \phi(\beta_3) &= g^2 + g^4 + g^7 + g^9, \\
(\phi(\beta_1) + \phi(\beta_3))^2 &= g^3 + g^4 + g^7 + g^8 \neq \phi(\beta_1) + \phi(\beta_3), \\
\phi(\beta_1) + \phi(\beta_4) &= g + g^5 + g^6 + g^{10}, \\
(\phi(\beta_1) + \phi(\beta_4))^2 &= g + g^2 + g^9 + g^{10} \neq \phi(\beta_1) + \phi(\beta_4), \\
\phi(\beta_2) + \phi(\beta_3) &= g + g^2 + g^3 + g^5 + g^6 + g^8 + g^9 + g^{10}, \\
(\phi(\beta_2) + \phi(\beta_3))^2 &= g + g^2 + g^4 + g^5 + g^6 + g^7 + g^9 + g^{10} \neq \phi(\beta_2) + \phi(\beta_3), \\
\phi(\beta_2) + \phi(\beta_4) &= g^3 + g^4 + g^7 + g^8, \\
(\phi(\beta_2) + \phi(\beta_4))^2 &= g^3 + g^5 + g^6 + g^8 \neq \phi(\beta_2) + \phi(\beta_4), \\
\phi(\beta_3) + \phi(\beta_4) &= g + g^2 + g^4 + g^5 + g^6 + g^7 + g^9 + g^{10}, \\
(\phi(\beta_3) + \phi(\beta_4))^2 &= g + g^2 + g^3 + g^4 + g^7 + g^8 + g^9 + g^{10} \neq \phi(\beta_3) + \phi(\beta_4),
\end{aligned}$$

e também,

$$\begin{aligned}
\phi(\beta_1)+\phi(\beta_2)+\phi(\beta_3) &= g+g^2+g^3+g^4+g^7+g^8+g^9+g^{10},\\
(\phi(\beta_1)+\phi(\beta_2)+\phi(\beta_3))^2 &= g^2+g^3+g^4+g^5+g^6+g^7+g^8+g^9 \neq \phi(\beta_1)+\phi(\beta_2)+\phi(\beta_3),\\
\phi(\beta_1)+\phi(\beta_2)+\phi(\beta_4) &= g^3+g^5+g^6+g^8,\\
(\phi(\beta_1)+\phi(\beta_2)+\phi(\beta_4))^2 &= g+g^5+g^6+g^{10} \neq \phi(\beta_1)+\phi(\beta_2)+\phi(\beta_4),\\
\phi(\beta_1)+\phi(\beta_3)+\phi(\beta_4) &= g+g^2+g^9+g^{10},\\
(\phi(\beta_1)+\phi(\beta_3)+\phi(\beta_4))^2 &= g^2+g^4+g^7+g^9 \neq \phi(\beta_1)+\phi(\beta_3)+\phi(\beta_4),\\
\phi(\beta_2)+\phi(\beta_3)+\phi(\beta_4) &= g^2+g^3+g^4+g^5+g^6+g^7+g^8+g^9,\\
(\phi(\beta_2)+\phi(\beta_3)+\phi(\beta_4))^2 &= g+g^3+g^4+g^5+g^6+g^7+g^8+g^{10} \neq \phi(\beta_2)+\phi(\beta_3)+\phi(\beta_4),
\end{aligned}$$

e ainda,

$$\begin{aligned}
\phi(\beta_1)+\phi(\beta_2)+\phi(\beta_3)+\phi(\beta_4) &= g+g^3+g^8+g^{10},\\
(\phi(\beta_1)+\phi(\beta_2)+\phi(\beta_3)+\phi(\beta_4))^2 &= g^4+g^5+g^6+g^7 \neq \phi(\beta_1)+\phi(\beta_2)+\phi(\beta_3)+\phi(\beta_4).
\end{aligned}$$

Portanto não existe um idempotente não trivial $\alpha \in \mathrm{Im}(\Phi)$. Logo, pelo Teorema 4.1.1

$$\mathcal{U}(\mathbb{Z}(C_{22} \times C_2 \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2, a_3 \rangle \times \langle w_1, w_2 \rangle \times \langle S \rangle\,,$$

onde $S = \{u_1(a_1), u_1(a_2), u_1(a_3), u_2(a_1), u_2(a_2), u_2(a_3), u_1(a_1a_2), u_1(a_1a_3), u_1(a_2a_3), u_2(a_1a_2), u_2(a_1a_3),$ $u_2(a_2a_3), u_1(a_1a_2a_3), u_2(a_1a_2a_3)\}$.

Vamos ver o que acontece com o núcleo do homomorfismo Φ se existe um idempotente não trivial $\alpha \in \mathrm{Im}(\Phi)$.

Lema 4.1.3. *Seja p um primo ótimo. Se $\boldsymbol{ord}(\Phi(w_1)) = 2^{\frac{p-1}{2}} - 1$, e se existe um idempotente não trivial $\alpha \in Im(\Phi)$, então*

$$Ker(\Phi) = \langle -1 \rangle \times \left\langle \left\{ w_i^2 w_{i+1}^{-1} : 1 \le i \le \frac{p-3}{2} \right\} \right\rangle \times \langle S \rangle\,,$$

onde
$S := \left\{ u_j(a_1)^2, u_j(a_2)^2, u_j(a_1a_2)^2, v : 1 \le j \le \dfrac{p-3}{2} \right\} \setminus \{u_{i_1}(a_1a_2)\}$ *é um conjunto multiplicativamente independente com $v = u_{i_1}(a_1) \cdots u_{i_n}(a_1) u_{i_1}(a_2) \cdots u_{i_n}(a_2) u_{i_1}(a_1a_2) \cdots u_{i_n}(a_1a_2)$ sendo que*

os índices i_k são determinados por α.

Demonstração:

Do Corolário 2.2.2 segue que $\langle -1 \rangle \times \left\{ w_i^2 w_{i+1}^{-1} : 1 \leq i \leq \dfrac{p-3}{2} \right\} \subseteq \mathrm{Ker}(\Phi)$. Seja $N = \langle -1 \rangle \times \left\{ w_i^2 w_{i+1}^{-1} : 1 \leq i \leq \dfrac{p-3}{2} \right\} \times \left\{ u_j^2(a_1), u_j^2(a_2), u_j^2(a_1a_2) : 1 \leq j \leq \dfrac{p-3}{2} \right\}$, onde $u_j(h) = (1-\beta_j) + \beta_j h$ com $h \in \{a_1, a_2, a_1a_2\}$.

Do Lema 3.1.2 $\left\{ u_j^2(a_1), u_j^2(a_2), u_j^2(a_1a_2) : 1 \leq j \leq \dfrac{p-3}{2} \right\} \subseteq \mathrm{Ker}(\Phi)$ e, portanto, $N \subseteq \mathrm{Ker}(\Phi)$.

Tome $u \in \mathrm{Ker}(\Phi)$. Como $u \in \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2))$, então, do Teorema e das considerações feitas, segue que

$$\begin{aligned} u &= (-1)^n w_1^{k_1} w_2^{k_2} \cdots w_{\frac{p-3}{2}}^{k_{\frac{p-3}{2}}} u_1^{r_1}(a_1) u_2^{r_2}(a_1) \cdots u_{\frac{p-3}{2}}^{r_{\frac{p-3}{2}}}(a_1) u_1^{s_1}(a_2) u_2^{s_2}(a_2) \cdots u_{\frac{p-3}{2}}^{s_{\frac{p-3}{2}}}(a_2) u_1^{t_1}(a_1a_2) \\ &\quad u_2^{t_2}(a_1a_2) \cdots u_{\frac{p-3}{2}}^{t_{\frac{p-3}{2}}}(a_1a_2), \end{aligned}$$

onde

$$\begin{aligned} \Phi(u) &= \Phi(u_{i_1}(a_1))\Phi(u_{i_2}(a_1)) \cdots \Phi(u_{i_n}(a_1))\Phi(u_{i_1}(a_2))\Phi(u_{i_2}(a_2)) \cdots \Phi(u_{i_n}(a_2))\Phi(u_{i_1}(a_1a_2)) \\ &\quad \Phi(u_{i_2}(a_1a_2)) \cdots \Phi(u_{i_n}(a_1a_2))) \\ &= \overline{1}. \end{aligned}$$

Do Lema 3.1.6, obtemos

$$\begin{aligned} \Phi(u) &= [(\overline{1} + \phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n})) + (\phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n}))a_1][(\overline{1} + \phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n})) + \\ &\quad +(\phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n}))a_2][(\overline{1} + \phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n})) + (\phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n}))a_1a_2] \\ &= \overline{1}. \end{aligned}$$

Considere $\alpha = \phi(\beta_{i_1}) + \cdots + \phi(\beta_{i_n})$. Assim

$$\Phi(w) = (\overline{1} + \alpha_1 + \alpha_1 a_1)(\overline{1} + \alpha_2 + \alpha_2 a_2)(\overline{1} + \alpha_3 + \alpha_3 a_1 a_2) = \overline{1},$$

ou seja,

$$\Phi(u) = (\overline{1} + \alpha + \alpha^2) + (\alpha + \alpha^2)a_1 + (\alpha + \alpha^2)a_2 + (\alpha + \alpha^2)a_1a_2) = \overline{1}.$$

Da hipótese, segue

$$\Phi(u_{i_1}(a_1)\cdots u_{i_n}(a_1)u_{i_1}(a_2)\cdots u_{i_n}(a_2)u_{i_1}(a_1a_2)\cdots u_{i_n}(a_1a_2)) = \overline{1}.$$

Logo,

$$\begin{aligned} u &= (-1)^n(w_1^2w_2^{-1})^{d_1}\cdots(w^2_{\frac{p-3}{2}}w^{-1}_{\frac{p-1}{2}})^{d_{\frac{p-1}{2}}}u_1(a_1)^{2e_1}\cdots u_{\frac{p-3}{2}}(a_1)^{2e_{\frac{p-3}{2}}}\cdots u_1(a_2)^{2f_1}\cdots u_{\frac{p-3}{2}}(a_2)^{2f_{\frac{p-3}{2}}} \\ & \quad (u_{i_1}(a_1)\cdots u_{i_n}(a_1)u_{i_1}(a_2)\cdots u_{i_n}(a_2)u_{i_1}(a_1a_2)\cdots u_{i_n}(a_1a_2))^t, \end{aligned}$$

ou seja,
$u \in \langle -1\rangle \times \left\langle w_1^2w_2^{-1},\cdots,w_i^2w_{i+1}^{-1},\cdots,w^2_{\frac{p-3}{2}}w^{-1}_{\frac{p-1}{2}}\right\rangle \times \left\langle \{u_j(a_1)^2, u_j(a_2)^2, u_j(a_1a_2)^2, v : 1 \leq j \leq \dfrac{p-3}{2}\}\right\rangle.$

Como
$[u_{i_1}(a_1)\cdots u_{i_n}(a_1)u_{i_1}(a_2)\cdots u_{i_n}(a_2)u_{i_1}(a_1a_2)\cdots u_{i_n}(a_1a_2)]^2(u_{i_1})^2(u_{i_2}(a_1))^{-2}\cdots(u_{i_n}(a_1))^{-2}$
$(u_{i_1}(a_2))^{-2}\cdots(u_{i_n}(a_2))^{-2}(u_{i_2}(a_1a_2))^{-2}\cdots(u_{i_n}(a_1a_2))^{-2} = u_{i_1}(a_1a_2)$
então, para que nosso conjunto seja multiplicativamente independente, devemos retirar o elemento $u_{i_1}(a_1a_2)^2$ do núcleo. Portanto,

$$\mathrm{Ker}(\Phi) = \langle -1\rangle \times \left\langle \left\{ w_i^2w_{i+1}^{-1} : 1 \leq i \leq \frac{p-3}{2}\right\}\right\rangle \times \langle S\rangle$$

■

Tendo conhecimento do núcleo do homomorfismo Φ, é fácil descrever o conjunto das unidades do anel de grupo $\mathbb{Z}(C_{2p} \times C_2 \times C_2)$. Lembre-se que

$$\begin{aligned} w_j &:= g^{(\frac{p-1}{2})\cdot 2^{j-1}}v_i = (-1)^{(\frac{p-3}{2})}(1 - g^{2^{j-1}} + g^{2\cdot 2^{j-1}} + \cdots + (-1)^{(\frac{p-3}{2})}g^{(\frac{p-3}{2})\cdot 2^{j-1}} + \\ & \quad +(-1)^{(\frac{p-3}{2})}g^{(\frac{p+3}{2})\cdot 2^{j-1}} + \cdots + g^{(p-2)}, \\ \beta_1 &= \frac{1 - w_1^2w_2^{-1}}{2}, \\ \beta_j &= \delta^{j-1}(\beta_1), \\ u_j(h) &= (1-\beta_j) + \beta_j h, \end{aligned}$$

$1 \leq j \leq \frac{p-3}{2}$, com $h \in \{a_1, a_2, a_3, a_1a_2, a_1a_3, a_2a_3, a_1a_2a_3\}$ e além disso δ representa o isomorfismo em $\mathbb{Z}C_p$ que leva g em g^2 e fixa os números inteiros.

Teorema 4.1.2. *Considere o anel de grupo $\mathbb{Z}(C_{2p} \times C_2 \times C_2)$, onde p é um primo ótimo,*

ord$(\rho(z_1)) = 2^{\frac{p-1}{2}}-1, \{\phi(\beta_1),\cdots,\phi(\beta_{\frac{p-3}{2}})\}$ *é um conjunto linearmente independente e existe um idempotente não trivial* $\alpha\in Im(\phi)$. *Então*

$$\mathcal{U}(\mathbb{Z}(C_{2p}\times C_2\times C_2)) = \langle -1\rangle \times \langle g,a_1,a_2,a_3\rangle \times \left\langle \left\{ w_i : 1\le i\le \frac{p-3}{2}\right\}\right\rangle \times \langle S\rangle\,,$$

onde
$S = \left\{u_j(a_1),u_j(a_2),u_j(a_3),u_j(a_1a_2),u_j(a_1a_3),u_j(a_2a_3),u_j(a_1a_2a_3),v : 1\le j\le \frac{p-3}{2}\right\} \setminus \{u_{i_1}(a_1a_2)\}$,

$$\begin{aligned} v &= (1-\gamma)+\gamma a_3,\\ \gamma &= u_{i_1}(a_1)\cdots u_{i_n}(a_1)u_{i_1}(a_2)\cdots u_{i_n}(a_2)u_{i_1}(a_1a_2)\cdots u_{i_n}(a_1a_2). \end{aligned}$$

Demonstração:

Sabemos que

$$u\in\mathcal{U}(\mathbb{Z}(C_{2p}\times C_2\times C_2)) \Leftrightarrow u = u_1\left[\frac{1+u_2}{2}+\left(\frac{1-u_2}{2}\right)a_2\right],\ \text{onde } u_1,u_2\in\mathcal{U}(\mathbb{Z}(C_{2p}\times C_2)),$$

com $u_2\in$ Ker(Φ) e $\Phi:\mathcal{U}(\mathbb{Z}(C_{2p}\times C_2))\to\mathcal{U}(\mathbb{Z}_2(C_{2p}\times C_2))$.

Do Teorema 3.2.1, segue

$$u_1\in\langle -1\rangle\times\langle g,a_1,a_2\rangle\times\left\langle \{w_i : 1\le i\le \frac{p-3}{2}\}\right\rangle \times \left\langle \{u_j(a_1),u_j(a_2),u_j(a_1a_2) : 1\le j\le\frac{p-3}{2}\}\right\rangle.$$

Como $u_2\in$ Ker(Φ), então

$$\begin{aligned} u_2 \;=\;& (-1)^n(w_1^2w_2^{-1})^{r_1}\cdots(w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1})^{r_{\frac{p-3}{2}}}(u_1(a_1)^{2s_1}\cdots u_{\frac{p-3}{2}}(a_1)^{2s_{\frac{p-3}{2}}}u_1(a_2)^{2t_1}\cdots u_{\frac{p-3}{2}}(a_2)^{2t_{\frac{p-3}{2}}}\\ & u_1(a_1a_2)^{2m_1}\cdots u_{\frac{p-3}{2}}(a_1a_2)^{2m_{\frac{p-3}{2}}}(u_{i_1}(a_2)\cdots u_{i_n}(a_2)u_{i_1}(a_1a_2)\cdots u_{i_n}(a_1a_2))^d. \end{aligned}$$

Do Lema 3.1.4 e do Lema 3.1.5, obtém-se

$$\begin{aligned} \frac{1+u_2}{2}+\left(\frac{1-u_2}{2}\right)a_3 \;=\;& \left[\frac{1+(-1)}{2}+\left(\frac{1-(-1)}{2}\right)a_3\right]^n\left[\frac{1+w_1^2w_2^{-1}}{2}+\left(\frac{1-w_1^2w_2^{-1}}{2}\right)a_3\right]^{r_1}\cdots\\ & \left[\frac{1+w_{\frac{p-3}{2}}^2w_{\frac{p-1}{2}}^{-1}}{2}+\left(\frac{1-w_{\frac{p-3}{2}}^2w_{\frac{p-1}{2}}^{-1}}{2}\right)a_3\right]^{r_{\frac{p-3}{2}}}\left[\frac{1+u_1(a_1)^2}{2}+\left(\frac{1-u_1(a_1)^2}{2}\right)a_3\right]^{s_1}\cdots \end{aligned}$$

$$\left[\frac{1+u_{\frac{p-3}{2}}(a_1)^2}{2} + \left(\frac{1-u_{\frac{p-3}{2}}(a_1)^2}{2}\right) a_3\right]^{s_{\frac{p-3}{2}}} \left[\frac{1+u_1(a_2)^2}{2} + \left(\frac{1-u_1(a_2)^2}{2}\right) a_3\right]^{t_1} \cdots$$

$$\left[\frac{1+u_{\frac{p-3}{2}}(a_2)^2}{2} + \left(\frac{1-u_{\frac{p-3}{2}}(a_2)^2}{2}\right) a_3\right]^{t_{\frac{p-3}{2}}} \left[\frac{1+u_1(a_1a_2)^2}{2} + \left(\frac{1-u_1(a_1a_2)^2}{2}\right) a_3\right]^{m_1} \cdots$$

$$\left[\frac{1+u_{\frac{p-3}{2}}(a_1a_2)^2}{2} + \left(\frac{1-u_{\frac{p-3}{2}}(a_1a_2)^2}{2}\right) a_3\right]^{m_{\frac{p-3}{2}}}$$

$$\left[\frac{1+u_{i_n}(a_2)u_{i_1}(a_1a_2)\cdots u_{i_n}(a_1a_2)}{2} + \left(\frac{1-u_{i_n}(a_2)u_{i_1}(a_1a_2)\cdots u_{i_n}(a_1a_2)}{2}\right) a_3\right]^{d}$$

Para todo $1 \leq j \leq \frac{p-3}{2}$, defina

$$\begin{aligned}
\lambda_j(a_1) &= \frac{1-u_j(a_1)^2}{2}, \\
\lambda_j(a_2) &= \frac{1-u_j(a_2)^2}{2}, \\
\lambda_j(a_1a_2) &= \frac{1-u_j(a_1a_2)^2}{2}, \\
\gamma &= \frac{1-u_{i_1}(a_1)\cdots u_{i_n}(a_1)u_{i_1}(a_2)\cdots u_{i_n}(a_2)u_{i_1}(a_1a_2)\cdots u_{i_n}(a_1a_2)}{2},
\end{aligned}$$

e sejam

$$\begin{aligned}
v_j(a_1a_3) &= (1-\lambda_j(a_1)) + \lambda_j(a_1)a_3, \\
v_j(a_2a_3) &= (1-\lambda_j(a_2)) + \lambda_j(a_2)a_3, \\
v_j(a_1a_2a_3) &= (1-\lambda_j(a_1a_2)) + \lambda_j(a_1a_2)a_3, \\
v &= (1-\gamma) + \gamma a_3.
\end{aligned}$$

Do Lema 3.1.3, temos

$$\begin{aligned}
v_j(a_1a_3) &= u_j(a_1)u_j(a_3)u_j(a_1a_3)^{-1}, \\
v_j(a_2a_3) &= u_j(a_2)u_j(a_3)u_j(a_2a_3)^{-1} \\
v_j(a_1a_2a_3) &= u_j(a_1a_2)u_j(a_3)u_j(a_1a_2a_3)^{-1}.
\end{aligned}$$

Desta forma,

$$\frac{1+u_2}{2} + \left(\frac{1-u_2}{2}\right) a_3 = a_3^n u_1(a_3)^{r_1} \cdots u_{\frac{p-1}{2}}(a_3)^{r_{\frac{p-3}{2}}} [u_1(a_1)u_1(a_3)u_1(a_1a_3)^{-1}]^{s_1} \cdots [u_{\frac{p-3}{2}}(a_1)u_{\frac{p-3}{2}}(a_3)$$

$u_{\frac{p-3}{2}}(a_1a_3)^{-1}\Big]^{s_{\frac{p-3}{2}}} [u_1(a_2)u_1(a_3)u_1(a_2a_3)^{-1}]^{t_1} \cdots [u_{\frac{p-3}{2}}(a_2)u_{\frac{p-3}{2}}(a_3)u_{\frac{p-3}{2}}(a_2a_3)^{-1}\Big]^{t_{\frac{p-3}{2}}} [u_1(a_1a_2)u_1(a_3)$

$u_1(a_1a_2a_3)^{-1}]^{m_1} \cdots [u_{\frac{p-3}{2}}(a_1a_2)u_{\frac{p-3}{2}}(a_3)u_{\frac{p-3}{2}}(a_1a_2a_3)^{-1}\Big]^{m_{\frac{p-3}{2}}} v^d$

e, portanto,

$$\frac{1+u_2}{2} + \left(\frac{1-u_2}{2}\right) a_3 \in \langle a_3 \rangle \times \left\langle \{u_j(a_i), u_j(a_ia_k), u_j(a_1a_2a_3), v : 1 \leq j \leq \frac{p-3}{2} \text{ e } 1 \leq i, k \leq 3\} \right\rangle.$$

Assim, provamos que:

$$\mathcal{U}(\mathbb{Z}(C_{2p} \times C_2 \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2, a_3 \rangle \times \left\langle \left\{ w_j : 1 \leq j \leq \frac{p-3}{2} \right\} \right\rangle \times \langle S \rangle .$$

■

Vamos ilustrar este Teorema com um exemplo.

Exemplo 26. *Considere cada grupo cíclico C_2 é gerado por a_i. Descreveremos as unidades do anel de grupo $\mathbb{Z}(C_{26} \times C_2 \times C_2)$.*

Do Teorema 3.2.1,

$\mathcal{U}(\mathbb{Z}(C_{13} \times C_2 \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2 \rangle \times \langle w_1, w_2, \ldots, w_5 \rangle \times \langle \{u_j(a_1), u_j(a_2), u_j(a_1a_2) : 1 \leq j \leq 5\} \rangle$.

Considere $\alpha = \beta_1 + \beta_3 + \beta_5$. Como $\phi(\alpha) = \overline{1} + \widehat{g}$, então $\phi(\alpha)^2 = \phi(\alpha)$, segue do Teorema 4.1.2,

$$\mathcal{U}(\mathbb{Z}(C_{13} \times C_2 \times C_2)) = \langle -1 \rangle \times \langle g, a_1, a_2, a_3 \rangle \times \langle z_1, \cdots, z_5 \rangle \times \langle S \rangle ,$$

onde

$S = \{u_j(a_1), u_j(a_2), u_j(a_3), u_j(a_1a_2), u_j(a_1a_3), u_j(a_2a_3), u_k(a_1a_2a_3), v : 1 \leq j \leq 5, \text{ e } 2 \leq k \leq 5\}$ e

$$v = u_1(a_1)u_3(a_1)u_5(a_1)u_1(a_2)u_3(a_2)u_5(a_2)u_1(a_1a_2)u_3(a_1a_2)u_5(a_1a_3).$$

4.2 Unidades centrais de $\mathbb{Z}(C_p \times Q_8)$

Considere o seguinte grupo não abeliano $Q_8 := \langle a, b : a^2 = b^2, a^4 = 1, bab^{-1} = a^{-1} \rangle$. Nosso intuito agora será descrever as unidades centrais do anel de grupo $\mathbb{Z}(C_p \times Q_8) \cong (\mathbb{Z}C_p)Q_8$.

Primeiramente iremos determinar o centro deste anel. As classes de conjugação de Q_8 são $C_1 = \{1\}$, $C_a = \{a, a^3\}$, $C_{a^2} = \{a^2\}$, $C_b = \{b, a^2b\}$ e $C_{ab} = \{ab, a^3b\}$ e as somas de classe de conjugação são $\gamma_1 = \widehat{C_1} = 1$, $\gamma_a = \widehat{C_a} = a + a^3$, $\gamma_{a^2} = \widehat{C_{a^2}} = a^2$, $\gamma_b = \widehat{C_b} = b + a^2b$ e $\gamma_{ab} = \widehat{C_{ab}} = ab + a^3b$. Do Teorema 1.3.1, o conjunto $\{\gamma_1, \gamma_a, \gamma_{a^2}, \gamma_b, \gamma_{ab}\}$ forma uma base para $\mathcal{Z}((\mathbb{Z}C_p)Q_8)$ sobre $\mathbb{Z}(C_p)$. Desta maneira, qualquer elemento do centro de $(\mathbb{Z}C_p)Q_8$ se escreve como $\alpha_0 + \alpha_1(a + a^3) + \alpha_2(b + a^2b) + \alpha_3(ab + a^3b) + \alpha_4 a^2$, com $\alpha_i \in \mathbb{Z}C_p$, $1 \leq i \leq 4$.

Seja $\mathbb{H}(\mathbb{Z}C_p)$ o anel dos quatérnios com coeficientes em $\mathbb{Z}C_p$ e considere $f : (\mathbb{Z}C_p)Q_8 \to \mathbb{H}(\mathbb{Z}C_p)$ definida por $f(a) = i$ e $f(b) = j$ sendo f $\mathbb{Z}C_p-$ linear. Tal função é um homomorfimo de anéis. Iremos focar nossa atenção no homomorfismo de grupos $F := f|_{\mathcal{Z}(\mathcal{U}((\mathbb{Z}C_p)Q_8))}$. Repare que $\mathrm{Im}(F) \subseteq \mathcal{U}(\mathbb{Z}C_p)$.

De fato, seja u uma unidade central de $\mathbb{Z}(C_p \times Q_8)$. Então

$$u = \alpha_0 + \alpha_1(a + a^3) + \alpha_2(b + a^2b) + \alpha_3(ab + a^3b) + \alpha_4 a^2,$$

onde $\alpha_i \in \mathbb{Z}C_p$, $1 \leq i \leq 4$. Como F é um homomorfismo de grupos, então $F(u)$ é uma unidade central de $\mathbb{H}(\mathbb{Z}C_p)$, ou seja, é uma unidade de $\mathbb{Z}C_p$.

Para toda unidade central u de $(\mathbb{Z}C_p)Q_8$, temos que

$$F(u) = \alpha_0 + \alpha_1(i + i^3) + \alpha_2(j + i^2j) + \alpha_3(ij + i^3j) + \alpha_4 i^2,$$

ou ainda,

$$F(u) = \alpha_0 + \alpha_1(i - i) + \alpha_2(j - j) + \alpha_3(k + -ij) - \alpha_4,$$

ou seja,

$$F(u) = \alpha_0 + \alpha_3(k - k) - \alpha_4 = \alpha_0 - \alpha_4 \in \mathcal{U}(\mathbb{Z}C_p).$$

Podemos enfim caracterizar as unidades centrais do anel de grupo $(\mathbb{Z}C_p)Q_8$.

Teorema 4.2.1. $\mathcal{Z}(\mathcal{U}((\mathbb{Z}C_p)Q_8)) = \mathcal{U}(\mathbb{Z}C_p) \times Ker(F)$.

Demonstração:

Seja $u \in \mathcal{Z}(\mathcal{U}((\mathbb{Z}C_p)Q_8))$. Então podemos escrever $u = F(u)[F(u)^{-1}u]$. Sabemos que

$$F(u) = \alpha_0 - \alpha_4 \in \mathcal{U}(\mathbb{Z}C_p),$$

falta mostrar que $F(u)^{-1}u$ pertence ao núcleo de F.

Como $F(u) \in \mathcal{U}(\mathbb{Z}C_p)$, em particular, $F(u)$ é uma unidade central de $\mathbb{Z}(C_p \times Q_8)$ e, portanto,

$$F(u)^{-1}u = \beta_0 + \beta_1(a + a^3) + \beta_2(b + a^2b) + \beta_3(ab + a^3b) + \beta_4 a^2,$$

onde $\beta_i = F(u)^{-1}\alpha_i$, para todo $1 \leq i \leq 4$, é uma unidade central de $(\mathbb{Z}C_p)Q_8$. Repare que $\beta_0 - \beta_4 = F(u)^{-1}\alpha_0 - F(u)^{-1}\alpha_4 = F(u)^{-1}(\alpha_0 - \alpha_4) = F(u)^{-1}F(u) = 1$ e, sendo assim, $\beta_0 = 1 + \beta_4$. Desta forma,

$$F(u)^{-1}u = 1 + \beta_4 + \beta_1(a + a^3) + \beta_2(b + a^2b) + \beta_3(ab + a^3b) + \beta_4 a^2.$$

Logo

$$F(F(u)^{-1}u) = 1 + \beta_4 - \beta_4 = 1,$$

de onde concluímos que, $F(u)^{-1}u \in \mathrm{Ker}(F)$.

Falta verificar que $\mathcal{U}(\mathbb{Z}C_p) \cap \mathrm{Ker}(F) = \{1\}$. Seja $w \in \mathrm{Ker}(F)$. Então

$$w = \alpha_0 + \alpha_1(a + a^3) + \alpha_2(b + a^2b) + \alpha_3(ab + a^3b) + \alpha_4 a^2,$$

tal que $F(w) = \alpha_0 - \alpha_4 = 1$, ou seja, $\alpha_0 = 1 + \alpha_4$ e, desta maneira,

$$w = 1 + \alpha_4 + \alpha_1(a + a^3) + \alpha_2(b + a^2b) + \alpha_3(ab + a^3b) + \alpha_4 a^2.$$

Como $w \in \mathcal{U}(\mathbb{Z}C_p)$, devemos ter $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0$, de onde, $w = 1$. Portanto,

$$\mathcal{Z}(\mathcal{U}((\mathbb{Z}C_p)Q_8)) = \mathcal{U}(\mathbb{Z}C_p) \times \mathrm{Ker}(F).$$

■

Assim, para caracterizar as unidades centrais do anel de grupo $(\mathbb{Z}C_p)Q_8$, devemos determinar o núcleo de F. Como queremos utilizar os resultados obtidos na seção anterior vamos construir um novo homomorfismo de grupos.

Sejam $\langle a_i \rangle$ tais que $C_2 \cong \langle a_i \rangle$, $i = 1, 2$. Considere o homomorfismo de anéis $\lambda : Q_8 \to C_2 \times C_2$ definido por $\lambda(a) = a_1$ e $\lambda(b) = a_2$.

Sejam Λ a extensão linear sobre $\mathbb{Z}C_p$ de λ, $\psi := \Lambda|_{\mathcal{Z}(\mathcal{U}((\mathbb{Z}C_p)Q_8))}$ e $\Psi := \psi|_{\mathrm{Ker}(F)}$. Temos que $\mathrm{Im}(\Psi) \subseteq \mathrm{Ker}(\Phi)$.

De fato, seja $x \in \mathrm{Ker}(F)$. Então

$$x = 1 + \alpha_0 + \alpha_1(a + a^3) + \alpha_2(b + a^2b) + \alpha_3(ab + a^3b) + \alpha_0,$$

com $\alpha_i \in \mathbb{Z}C_p$ e $x \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}(C_p \times Q_8)))$. Então

$$\Psi(x) = 1 + 2\alpha_0 + 2\alpha_1 a_1 + 2\alpha_2 a_2 + 2\alpha_3 a_1 a_2.$$

Observe que

$$(1 + 2\alpha_0) + 2\alpha_1 a_1 + 2\alpha_2 a_2 + 2\alpha_3 a_1 a_2 \in \mathbb{Z}(C_{2p} \times C_2)$$

e $\Phi(\Psi(x)) = \overline{1}$. Logo $\mathrm{Im}(\Psi) \subseteq \mathrm{Ker}(\Phi)$.

O próximo resultado mostra que a função Ψ é um isomorfismo de grupos.

Lema 4.2.1. *Ker*$(F) \cong$ *Ker*(Φ)

Demonstração:

Como Ψ é um homomorfismo de grupos, resta mostrar que Ψ é uma bijeção. Para isso, primeiramente iremos mostrar que Ψ é injetora, isto é, $\mathrm{Ker}(\Psi) = \{1\}$. Seja $w \in \mathrm{Ker}(\Psi)$. Então $\Psi(w) = 1$, ou seja, $(1 + 2\alpha_0) + 2\alpha_1 a_1 + 2\alpha_2 a_2 + 2\alpha_3 a_1 a_2 = 1$ e, portanto, $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0$, de onde, $w = 1$. Logo, $\mathrm{Ker}(\Psi) = \{1\}$, ou seja, Ψ é injetora.

Vejamos que Ψ é sobrejetora. Seja $y \in \mathrm{Ker}(\Phi)$, então $y \in \mathcal{U}(\mathbb{Z}(C_{2p} \times C_2))$ tal que $\Phi(y) = \overline{1}$. Então $y = 1 + 2\alpha$, onde $\alpha \in \mathbb{Z}(C_{2p} \times C_2)$, ou seja, $\alpha = y_0 + y_1 a_1 + y_2 a_2 + y_3 a_1 a_2$ e, sendo assim, $y = 1+2(y_0+y_1a_1+y_2a_2+y_3a_1a_2)$. Considere $x = 1+y_0+y_1(a+a^3)+y_2(b+a^2b)+y_3(ab+a^3b)+y_0a^2$.

Falta verificarmos que $x \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}(C_p \times Q_8)))$. Como y é uma unidade de $\mathbb{Z}(C_p \times C_2 \times C_2)$ então existe $z = (1 + 2\beta_0) + 2\beta_1 a_1 + 2\beta_2 a_2 + 2\beta_3 a_1 a_2 \neq 0$ tal que $yz = zy = 1$. Assim,

$$\begin{aligned} y \cdot z \;&=\; (1 + 2\alpha_0)(1 + 2\beta_0) + 2(1 + \alpha_0)\beta_1 a_1 + 2(1 + 2\alpha_0)\beta_2 a_2 + 2(1 + 2\alpha_0)\beta_3 a_1 a_2 + 2(1 + 2\beta_0)\alpha_1 a_1 + \\ &\quad +4\alpha_1\beta_1 + 4\alpha_1\beta_2 a_1 a_2 + 4\alpha_1\beta_3 a_2 + 2(1 + 2\beta_0)\alpha_2 a_2 + 4\alpha_2\beta_1 a_1 a_2 + 4\alpha_2\beta_2 + 4\alpha_2\beta_3 a_1 + \\ &\quad +2(1 + 2\beta_0)\alpha_3 a_1 a_2 + 4\alpha_3\beta_1 a_2 + 4\alpha 3\beta_2 a_1 + 4\alpha_3\beta_3 \\ &=\; 1, \end{aligned}$$

ou seja,

$y{\cdot}z = (1{+}2\alpha_0{+}2\beta_0{+}4\alpha_0\beta_0{+}4\alpha_1\beta_1{+}4\alpha_2\beta_2{+}4\alpha_3\beta_3){+}(2\beta_1{+}2\alpha_1{+}4\alpha_0\beta_1{+}4\alpha 1\beta_0{+}4\alpha_2\beta_3{+}4\alpha 3\beta_2)a_1{+}$ ${+}(2\alpha_2{+}2\beta_2{+}2\alpha_0\beta_2{+}4\alpha_1\beta_3{+}4\alpha_2\beta_0{+}4\alpha_3\beta_1)a_2{+}(2\alpha_3{+}2\beta_3{+}4\alpha_0\beta_3{+}4\alpha_1\beta_2{+}4\alpha_2\beta_1{+}2\alpha_3\beta_0)a_1a_2 = 1,$

isto é,

$[2(\alpha_0 + \beta_0) + 4(\alpha_0\beta_0 + \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3)] + [2(\alpha_1 + \beta_1) + 4(\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 + \alpha_3\beta_2)]a_1 +$
$+[2(\alpha_2+\beta_2)+4(\alpha_0\beta_2+\alpha_1\beta_3+\alpha_2\beta_0+\alpha_3\beta_1)]a_2+[2(\alpha_3+\beta_3)+4(\alpha_0\beta_3+\alpha_1\beta_2+\alpha_2\beta_1+\alpha_3\beta_0)]a_1a_2 = 0.$

Assim

$$\begin{cases} \alpha_0 + \beta_0 + 2(\alpha_0\beta_0 + \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3) = 0 \\ \alpha_1 + \beta_1 + 2(\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 + \alpha_3\beta_2) = 0 \\ \alpha_2 + \beta_2 + 2(\alpha_0\beta_2 + \alpha_1\beta_3 + \alpha_2\beta_0 + \alpha_3\beta_1) = 0 \\ \alpha_3 + \beta_3 + 2(\alpha_0\beta_3 + \alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_3\beta_0) = 0 \end{cases}$$

Vejamos que o inverso de $v = 1 + \alpha_0 + \alpha_1(a + a^3) + \alpha_2(b + a^2b) + \alpha_3(ab + a^3b) + \alpha_0a^2$ é $w = 1 + \beta_0 + \beta_1(a + a^3) + \beta_2(b + a^2b) + \beta_3(ab + a^3b) + \beta_0$.

De fato,

$v \cdot w = (1 + \alpha_0)(1 + \beta_0) + (1 + \alpha_0)\beta_1(a + a^3) + (1 + \alpha_0)\beta_2(b + a^2b) +$
$+(1+\alpha_0)\beta_3(ab+a^3b)+(1+\alpha_0)\beta_0a^2+\alpha_1(1+\beta_0)(a+a^3)+\alpha_1\beta_1(a+a^3)(a+a^3)+\alpha_1\beta_2(a+a^3)(b+a^2b)+$
$+\alpha_1\beta_3(a + a^3)(ab + a^3b) + \alpha_1\beta_0(a + a^3)a^2 + \alpha_2(1 + \beta_0)(b + a^2b) + \alpha_2\beta_1(b + a^2b)(a + a^3) +$
$+\alpha_2\beta_2(b + a^2b)(b + a^2b) + \alpha_2\beta_3(b + a^2b)(ab + a^3b) + \alpha_2\beta_0(b + a^2b)a^2 + \alpha_3(1 + \beta_0)(ab + a^3b) +$
$+\alpha_3\beta_1(ab + a^3b)(a + a^3) + \alpha_3\beta_2(ab + a^3b)(b + a^2b) + \alpha_3\beta_3(ab + a^3b)(ab + a^3b) + \alpha_3\beta_0(ab + a^3b)a^2 +$
$+\alpha_0(1 + \beta_0)a^2 + \alpha_0\beta_1a^2(a + a^3) + \alpha_0\beta_2a^2(b + a^2b) + \alpha_0\beta_3a^2(ab + a^3b) + \alpha_0\beta_0,$

ou seja,

$v \cdot w = (1 + \alpha_0 + \beta_0 + 2\alpha_0\beta_0 + 2\alpha_1\beta_1 + 2\alpha_3\beta_3) + (\alpha_1 + \beta_1 + 2\alpha_0\beta_1 + 2\alpha_1\beta_0 + 2\alpha_2\beta_3 + 2\alpha_3\beta_2)(a +$
$+a^3) + (\alpha_2 + \beta_2 + 2\alpha_0\beta_2 + 2\alpha_1\beta_3 + 2\alpha_2\beta_0 + 2\alpha_3\beta_1)(b + a^2b) + (\alpha_3 + \beta_3 + 2\alpha_0\beta_3 + 2\alpha_1\beta_2 +$
$+2\alpha_2\beta_1 + 2\alpha_3\beta_0)(ab + a^3b) + (\alpha_0 + \beta_0 + 2\alpha_0\beta_0 + 2\alpha_1\beta_1 + 2\alpha_2\beta_2 + 2\alpha_3\beta_3)a^2.$

Das condições anteriores, tem-se que $v \cdot w = 1$. Portanto, w é o inverso de v.

Como $x \in \text{Ker}(F)$ é tal que $\Psi(x) = 1 + 2y_0 + 2y_1a_1 + 2y_2a_2 + 2y_3a_1a_2 = y$, segue que Ψ é sobrejetora. Concluímos que Ψ é uma bijeção. Logo Ψ é um isomorfismo.

■

O próximo resultado caracteriza o grupo das unidades centrais de $\mathbb{Z}(C_p \times Q_8)$ com base nos núcleos da seção anterior.

Teorema 4.2.2. *Considere o anel de grupo $\mathbb{Z}(C_p \times Q_8)$. Seja p um primo ótimo tal que **ord**$(\Phi(w_1)) = 2^{\frac{p-1}{2}} - 1$ e o conjunto $\{\phi(\beta_1), \cdots, \phi(\beta_{\frac{p-1}{2}})\}$ é linearmente independente. Então*

$$\mathcal{Z}(\mathcal{U}(\mathbb{Z}(C_p \times Q_8))) = \langle -1 \rangle \times \mathcal{U}_1(\mathbb{Z}C_p) \times \mathcal{U}_1(H) \times \langle a^2 \rangle,$$

com $\mathcal{U}_1(H) := \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}(C_p \times C_2 \times C_2))) \bigcap Ker(F)$.

Demonstração:

Do Teorema 4.2.1, tem-se que $\mathcal{Z}(\mathcal{U}(\mathbb{Z}(C_p \times Q_8))) \cong \mathcal{U}(\mathbb{Z}C_p) \times \mathrm{Ker}(G)$. Do Lema 4.2.1, obtém-se $\mathrm{Ker}(F) \cong \mathrm{Ker}(\Phi)$.

No entanto, $\mathrm{Ker}(\Phi) = \langle -1 \rangle \times \mathcal{U}_1(\mathbb{Z}(C_{2p} \times C_2) \bigcap \mathrm{Ker}(\Phi)$. Além disso,$-a^2 = 1 + (-1) + (-1)a^2$, logo, $\Psi(-a^2) = -1$, então

$$\mathrm{Ker}(F) = \left\langle -a^2 \right\rangle \times \mathcal{Z}(\mathcal{U}_1(\mathbb{Z}(C_{2p} \times C_2))) \bigcap \mathrm{Ker}(F)$$

e, portanto, segue o resultado.

■

Vejamos alguns exemplos que ilustram o Teorema acima.

Exemplo 27. *Considere o anel de grupo* $\mathbb{Z}(C_5 \times Q_8)$*, onde* $C_5 = \langle g \rangle$*. Pretende-se descrever as unidades centrais normalizadas deste anel de grupo.*

Considere $\langle a_i \rangle$ tais que $C_2 \cong \langle a_i \rangle$. Para encontrar as unidades de $\mathbb{Z}(C_5 \times Q_8)$, devemos determinar o núcleo da função $\Phi : \mathcal{U}(\mathbb{Z}(C_{10} \times C_2)) \to \mathcal{U}(\mathbb{Z}_2(C_{10} \times C_2))$. Sejam $w_1 = -1 + g + g^4$, $w_2 = -1 + g^2 + g^3$ e $u(a_1) = (1 - \beta) + \beta a_1$ com $\beta = 4 - 3g + g^2 + g^3 - 3g^4$.

Observe que $\phi(\beta) = g + g^2 + g^3 + g^4 = \overline{1} + \widehat{g}$. Logo $\phi(\beta)^2 = \phi(\beta)$ e do Lema 4.1.3tem-se que

$$\mathrm{Ker}(\Phi) = \langle -1 \rangle \times \left\langle w_1^2 w_2^{-1} \right\rangle \times \left\langle u(a_1)^2, u(a_2)^2, u(a_1)u(a_2)u(a_1a_2) \right\rangle.$$

Considere

$$\begin{aligned}
\alpha_1 &= -64 + 52g - 20g^2 - 20g^3 + 52g^4, \\
\alpha_2 &= -96 + 78g - 30g^2 - 30g^3 + 78g^4, \\
\alpha_3 &= -32 + 26g - 10g^2 - 10g^3 + 26g^4.
\end{aligned}$$

Então,

$$\begin{aligned}
w_1^2 w_2^{-1} &= -7 + 6g - 2g^2 - 2g^3 + 6g^4, \\
u(a_1)^2 &= 1 - \alpha_1 + \alpha_1 a_1, \\
u(a_2)^2 &= 1 - \alpha_1 + \alpha_1 a_2, \\
u(a_1)u(a_2)u(a_1 a_2) &= (1 - \alpha_2) + \alpha_3 a_1 + \alpha_3 a_2 + \alpha_3 a_1 a_2.
\end{aligned}$$

Desta forma,

$$\begin{aligned}
\Psi^{-1}(w_1^2 w_2^{-1}) &= 1 - \beta + \beta a^2, \\
\Psi^{-1}(u(a_1)^2) &= (1 - \alpha_3 + \alpha_3(a + a^3) + \alpha_3 a^2, \\
\Psi^{-1}(u(a_2)^2) &= 1 - \alpha_3 + \alpha_3(b + a^2 b) + \alpha_3 a^2, \\
\Psi^{-1}(u(a_1)u(a_2)u(a_1 a_2)) &= 1 - \frac{\alpha_2}{2} + (\frac{\alpha_3}{2})(a + a^3) + (\frac{\alpha_3}{2})(b + a^2 b) + (\frac{\alpha_3}{2})(ab + a^3 b) + (\frac{\alpha_3}{2})a^2.
\end{aligned}$$

Pelo Teorema 4.2.2

$$\mathcal{U}_1(\mathbb{Z}(C_5 \times Q_8)) = \left\langle a^2 \right\rangle \times \langle g, w_1 \rangle \times \langle v_0, v_1, v_2, v_3 \rangle,$$

onde

$$\begin{aligned}
v_0 &= \Psi^{-1}(w_1^2 w_2^{-1}), \\
v_1 &= \Psi^{-1}(u(a_1)^2), \\
v_2 &= \Psi^{-1}(u(a_2)^2), \\
v_3 &= \Psi^{-1}(u(a_1)u(a_2)u(a_1 a_2)).
\end{aligned}$$

Exemplo 28. *Considere o anel de grupo $\mathbb{Z}(C_7 \times Q_8)$, onde $C_7 \cong \langle g \rangle$. Pretende-se determinar as unidades centrais normalizadas deste anel de grupo.*

Sejam $\langle a_1 \rangle$ e $\langle a_2 \rangle$ tais que $C_2 \cong \langle a_i \rangle$. Para encontrar as unidades de $\mathbb{Z}(C_7 \times Q_8)$, devemos determinar o núcleo da função $\Phi : \mathcal{U}(\mathbb{Z}(C_{14} \times C_2)) \to \mathcal{U}(\mathbb{Z}_2(C_{14} \times C_2))$. Seja $w_1 = 1 - g + g^2 + g^5 - g^6, u_i(a_1) = (1 - \beta_i) + \beta_i a_1,\ i = 1, 2$ e $\beta_1 = 4 - 3g + 2g^2 - g^3 - g^4 + 2g^5 - 3g^6$.

Observe que

$$\begin{aligned}
\phi(\beta_1) &= g + g^3 + g^4 + g^6, \\
\phi(\beta_1)^2 &= g + g^2 + g^5 + g^6 \neq \phi(\beta_1), \\
\phi(\beta_2) &= g + g^2 + g^5 + g^6, \\
\phi(\beta_2)^2 &= g^2 + g^3 + g^4 + g^5 \neq \phi(\beta_2), \\
\phi(\beta_1) + \phi(\beta_2) &= g^2 + g^3 + g^4 + g^5, \\
\phi(\beta_1)^2 + \phi(\beta_2)^2 &= g + g^3 + g^4 + g^6 \neq \phi(\beta_1) + \phi(\beta_2).
\end{aligned}$$

Logo não exist um idempotente não trivial $\alpha \in \mathrm{Im}(\phi)$. Então, do Lema 4.1.2,
$\mathrm{Ker}(\Phi) = \langle -1 \rangle \times \left\langle w_1^2 w_2^{-1}, w_2^2 w_3^{-1} \right\rangle \times \left\langle u_1(a_1)^2, u_2(a_1)^2, u_1(a_2)^2, u_2(a_2)^2, u_1(a_1a_2)^2, u_2(a_1a_2)^2 \right\rangle.$

Sejam

$$\begin{aligned}
\alpha_1 &= -80 + 72g - 50g^2 + 18g^3 + 18g^4 - 50g^5 + 72g^6, \\
\alpha_2 &= -80 + 18g + 72g^2 - 50g^3 - 50g^4 + 72g^5 + 18g^6.
\end{aligned}$$

Então

$$\begin{aligned}
w_1^2 w_2^{-1} &= -7 + 6g - 4g^2 + 2g^3 + 2g^4 - 4g^5 + 6g^6, \\
w_2^2 w_3^{-1} &= -7 + 2g + 6g^2 - 4g^3 - 4g^4 + 6g^5 + 2g^6, \\
u_1(a_1)^2 &= 1 - \alpha_1 + \alpha_1 a_1, \\
u_1(a_2)^2 &= 1 - \alpha_1 + \alpha_1 a_2, \\
u_2(a_1)^2 &= 1 - \alpha_2 + \alpha_2 a_1, \\
u_2(a_2)^2 &= 1 - \alpha_2 + \alpha_2 a_2, \\
u_1(a_1a_2)^2 &= 1 - \alpha_1 + \alpha_1 a_1 a_2, \\
u_2(a_1a_2)^2 &= 1 - \alpha_2 + \alpha_2 a_1 a_2.
\end{aligned}$$

Assim

$$\begin{aligned}
\Psi^{-1}(w_1^2 w_2^{-1}) &= 1 - \beta_1 + \beta_1 a^2, \\
\Psi^{-1}(w_2^2 w_3^{-1}) &= 1 - \beta_2 + \beta_2 a^2, \\
\Psi^{-1}(u_1(a_1)^2) &= 1 + (\frac{\alpha_1}{2}) + (\frac{\alpha_1}{2})(a + a^3) + (\frac{\alpha_1}{2})a^2, \\
\Psi^{-1}(u_1(a_2)^2) &= 1 + (\frac{\alpha_1}{2}) + (\frac{\alpha_1}{2})(b + a^2 b) + (\frac{\alpha_1}{2})a^2, \\
\Psi^{-1}(u_1(a_1 a_2)^2) &= 1 + (\frac{\alpha_1}{2}) + (\frac{\alpha_1}{2})(ab + a^3 b) + (\frac{\alpha_1}{2})a^2, \\
\Psi^{-1}(u_2(a_1)^2) &= 1 + (\frac{\alpha_2}{2}) + (\frac{\alpha_2}{2})(a + a^3) + (\frac{\alpha_2}{2})a^2, \\
\Psi^{-1}(u_2(a_2)^2) &= 1 + (\frac{\alpha_2}{2}) + (\frac{\alpha_2}{2})(b + a^2 b) + (\frac{\alpha_2}{2})a^2, \\
\Psi^{-1}(u_2(a_1 a_2)^2) &= 1 + (\frac{\alpha_2}{2}) + (\frac{\alpha_2}{2})(ab + a^3 b) + (\frac{\alpha_2}{2})a^2.
\end{aligned}$$

Pelo Teorema 4.2.2

$$\mathcal{U}_1(\mathbb{Z}(C_7 \times Q_8)) = \langle a^2 \rangle \times \langle g \rangle \times \langle w_1, w_2 \rangle \times \langle v_0, v_1, v_2, v_3, v_4, v_5, v_6, v_7 \rangle,$$

onde

$$\begin{aligned}
v_0 &= \Psi^{-1}(w_1^2 w_2^{-1}), \\
v_1 &= \Psi^{-1}(w_2^2 w_3^{-1}), \\
v_2 &= \Psi^{-1}(u_1(a_1)^2), \\
v_3 &= \Psi^{-1}(u_1(a_2)^2), \\
v_4 &= \Psi^{-1}(u_1(a_1 a_2)^2), \\
v_5 &= \Psi^{-1}(u_2(a_1)^2), \\
v_6 &= \Psi^{-1}(u_2(a_2)^2), \\
v_7 &= \Psi^{-1}(u_2(a_1 a_1)^2).
\end{aligned}$$

Capítulo 5

Apêndice

Esta parte se reserva aos detalhes dos cálculos dos exemplos apresentados durante o trabalho. Os programas que nós utilizamos foram o **MAPLE** e o **GAP**. Em ambos os programas fizemos os cálculos para determinar o elemento $\beta_1 = \frac{1-w_1^2w_2^{-1}}{2}$. Além disso, com o auxílio do **GAP** foi possível verificar a hipótese da ordem do elemento $\rho(w_1)$ e do conjunto $\{\phi(\beta_1), \cdots, \phi(\beta_{\frac{p-3}{2}})\}$ ser linearmente independente. Abaixo segue os comandos feitos no **GAP** para realizar tais tarefas.

O passo à passo descrito a seguir serve para demonstrar que a ordem de $\rho(w_1) = 2^{\frac{p-1}{2}} - 1$ para o caso $\mathbb{Z}C_{23}$. Aqui u representa $\rho(w_1)$.

$K := GF(2)$

$G :=$ `CyclicGroup`(23)

$KG :=$ `GroupRing`(K, G);

$L :=$ `MinimalGeneratingSet`(G);

$l :=$ `List`$(L, g- > g$^`Embedding`(G, KG);

$g := l[1]$;

$w :=$ `Identity`(KG);

`for` i `in` $[1..22]$ `do`

$w := w + g^i od$;

w;

$D :=$ `DivisorInt`(2047);

$j := ()$;

`for` i `in` D `do`

`if` $u^i =$ `Identity`(KG) `then`

`Add`(j, i)

`fi`;

```
od;
```

O roteiro abaixo exemplifica como foi verificado que o conjunto $\{\phi(\beta_1), \cdots, \phi(\beta_{\frac{p-3}{2}})\}$ é linearmente independente para o exemplo $\mathbb{Z}(C_{38})$. Neste caso os elementos a_i representam os coeficientes de $\phi(\beta_i)$ em relação a base G e m representa a matriz que possui posto $\frac{p-3}{2} = 8$.

```
a1 := Z(2) * [0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0];
a2 := Z(2) * [0,0,0,0,0,1,0,1,1,1,1,1,1,0,1,0,0,0,0];
a3 := Z(2) * [0,1,0,1,0,1,0,0,0,1,1,0,0,0,1,0,1,0,1];
a4 := Z(2) * [0,1,1,0,0,0,1,0,0,1,1,0,0,1,0,0,0,1,1];
a5 := Z(2) * [0,1,1,0,1,0,0,1,0,0,0,0,1,0,0,1,0,1,1];
a6 := Z(2) * [0,0,1,0,1,1,0,0,1,0,0,1,0,0,1,1,0,1,0];
a7 := Z(2) * [0,0,0,1,1,0,0,0,1,1,1,1,0,0,0,1,1,0,0];
a8 := Z(2) * [0,1,0,1,0,0,1,0,1,0,0,1,0,1,0,0,1,0,1];
ConvertToVectorRep(a1,2);
ConvertToVectorRep(a2,2);
ConvertToVectorRep(a3,2);
ConvertToVectorRep(a4,2);
ConvertToVectorRep(a5,2);
ConvertToVectorRep(a6,2);
ConvertToVectorRep(a7,2);
ConvertToVectorRep(a8,2);
m := [a1,a2,a3,a4,a5,a6,a7,a8];
ConvertToMatrixRep(m,GF(2));
RankMat(m);
```

Referências Bibliográficas

[1] R. Z. Aleev, *Higman's Central Unit Theorem, Units of Integral Group Rings and Fibonacci Numbers*, International J. Alg. Comp. 4, (1994), 309-358.

[2] R. Z. Aleev and Z. Panina, *The Units of Cyclic Groups of Orders* 7 *and* 9, Russ. Math. 43, (2000), 80-83.

[3] H. Bass, *The Dirichlet Unit Theorem, Induced Characters and Whitehead Groups of Finite Groups* , Topology 4, (1966), 391-410.

[4] S. D. Berman, *On the Equation $x^n = 1$ in a Integral Group Ring*, Ukrain. Math. Zh. 7, (1995), 253-261.

[5] A. Cayley, *On the Theory of Groups as Depending on the Symbolic Equation $\theta^n = 1$*, Phil. Mag. 7, (1854) 40-47.

[6] R. A. Ferraz, *Units of $\mathbb{Z}C_p$*, Groups, Rings and Group Rings, Contemp. Math. 499, Amer. Math. Soc., Providence, RI, (2009), 107-119.

[7] R. A. Ferraz and J. J. Simón Pinero, *Central Units in Metacyclic Group Rings*, Comm. Algebra 36 (10), (2008), 3708-3722.

[8] A. Garcia e Y. Lequain, *Elementos de Álgebra*, Terceira Edição, IMPA, Rio de Janeiro (2005).

[9] G. Higman *The Units of Group Rings*, Proc. London. Math. Soc. 46, (1940), 231-248.

[10] K. Hoechsmann, *Constructing Units in Commutative Group Rings*, Manuscripta Math. 75, (1992), No. 1, 5-23.

[11] K. Hoechsmann, *Unit Bases in Small Cyclic Group Rings*, Methods in Ring Theory (Levico Terme, 1997), 121-139, Lecture Notes in Pure and Applied Math. 198, Marcel Dekker, New York (1998).

[12] K. Hoechsmann and S. Sehgal, *Units in Regular Abelian p-Group Rings*, J. Number Theory 30, No. 3, (1988), 375-381.

[13] E. Jespers, M. Parmenter and S. Sehgal, *Central Units of Integral Group Rings of Nilpotent Groups*, Proc. Amer. Math. Soc. 124, (1996), 1007-1012.

[14] G. Karpilovsky, *Commutative Group Algebras*, Marcel Dekker, New York, (1983).

[15] G. Karpilovsky, *Units of Group Rings* Longman Scientific & Technical, New York, (1989).

[16] Y. Li and M. M. Parmenter, *Central Units of the Integral Group Ring* $\mathbb{Z}A_5$ Proc. Amer. Math. Soc. 125, (1997), 61-65.

[17] R. M. Low, *On the Units of the Integral Group Ring* $\mathbb{Z}(G \times C_p)$, Journal of Algebra and Its Aplication 7, No. 3, (2008), 393-403.

[18] P. A. Martin, *Introdução à Teoria dos Grupos e à Teoria de Galois*, Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo, São Paulo, (1998).

[19] C. Polcino Milies and S. K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Netherlands, (2002).

[20] C. Polcino Milies and S. K. Sehgal, *Central Units of Integral Group Rings*, Comm. Algebra 27, (1999), 6233-6241.

[21] S. K. Sehgal, *Units in Integral Group Rings*, Longman Scientific & Technical, Essex, (1993).

[GAP] The GAP Group, *GAP - Groups, Algorithms, and Programming, Version 4.4.12*; 2008, (`http://www.gap-system.org`).

[MAPLE] *Maple 13, Windows Version*; 2009.