Unidades centrais em anéis de grupo sobre os inteiros

Giselle Bertaggia

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

Programa: Matemática

Orientador: Prof. Dr. Raul Antônio Ferraz

Durante o desenvolvimento deste trabalho a autora recebeu auxílio financeiro da CAPES e CNPq

São Paulo, fevereiro de 2014

Unidades centrais em anéis de grupo sobre os inteiros

Esta versão da dissertação contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 14/02/2014. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão Julgadora:

- Prof. Dr. Raul Antonio Ferraz - IME-USP
- Prof. Dr. Francisco César Polcino Milies - IME-USP
- Profª. Drª. Marinês Guerreiro - UFV

"Do rio que tudo arrasta, diz-se que é violento. Mas ninguém chama violentas às margens que o comprimem."(Bertold Brecht)

Agradecimentos

Em primeiro lugar, gostaria de agradecer o Professor Raul, meu orientador, pelos ensinamentos e incentivo, além da paciência em todos os momentos do desenvolvimento desse trabalho.

Agradeço também ao Wagner, pelo companheirismo nos momentos bons e ruins tanto na graduação quanto na pós.

Aos amigos Renato Jeremias, Rodrigo Figueiredo, Robson Figueiredo, Bárbara Sayuri, Patrícia Massae, Renata Marcuz, Rafael Jerônimo e Faber pela constante ajuda nos conteúdos, nos momentos de choro e de alegria. Agradeço também aos amigos Renata Mendes, Valeska Lucena, Wellington e Altino Prazeres pelos anos de graduação, que foram essenciais para a formação obtida.

Ao meu irmão, amigo, confidente, companheiro de todas as horas Leandro Souza, pelos debates, troca de ideias, pelo ombro, pelas conversas, pelos cafés, pelas matérias, pelas risadas e por, principalmente, estar sempre ao meu lado.

Aos amigos que, indiretamente, sempre me ajudaram e me escutaram Ana Anunciato, Fernando Romano, Anderson Bomfim e Rafael Silva.

Ao grande amigo Tiago Montanher, por tudo, pela ajuda no Latex, pelas conversas, por sempre ouvir as lamúrias e histórias a qualquer hora do dia e da noite. À minha amiga Juliana Santos que esteve presente em todas as horas, sempre pronta para me escutar e me aconselhar.

À minha madrasta Ana Crocci e ao meu irmão por nunca me deixarem desistir, principalmente nos momentos mais difíceis.

Aos professores Cristina Barufi, Sérgio Alves, Zara Abud e César Polcino pelas oportunidades oferecidas, que foram de extrema importância para meu crescimento.

Aos funcionários da CPG e da biblioteca, sempre atenciosos procurando resolver os problemas e solicitações.

Aos funcionários da BLK Sistemas Financeiros, em especial, ao meu chefe Paulo César, por entender e me ajudar nas horas difíceis.

Ao meu companheiro Daniel Sant'Ana pelo amor, carinho, companheirismo, compreensão e incentivo que foram essenciais na conclusão desse trabalho.

Ao CNPq e à CAPES, pelo apoio financeiro.

Por fim, *in memoriam*, aos meus pais, por sempre acreditarem em mim.

Resumo

Bertaggia, G. **Unidades Centrais em anéis de grupos sobre os inteiros**. 2014. 100 páginas. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2014.

Sejam G um grupo e $\mathbb{Z}$ o anel dos números inteiros. Consideremos o anel de grupo sobre os inteiros $\mathbb{Z}G$ e seu grupo de unidades $\mathcal{U}(\mathbb{Z}G) = \{u \in \mathbb{Z}G | u \text{ é } \textit{inversível}\}$. Considerando α uma raiz primitiva da unidade sobre $\mathbb{Q}$ e $\mathbb{Z}[\alpha]$ o anel de inteiros ciclotômicos, apresentaremos as unidades de anéis de grupos integrais sobre grupos cíclicos de ordens 7 e 9. Posteriormente, veremos uma generalização, devida à Ferraz, onde se determina um conjunto gerador independente que permite obter as unidades de $\mathbb{Z}C_p$, onde C_p é um grupo cíclico de ordem prima p, considerando θ uma raiz primitiva da unidade de ordem p, tal que $S_\theta = \left\{-1, \theta, 1+\theta, \ldots, 1+\theta+\cdots+\theta^{\frac{p-3}{2}}\right\}$ gera o grupo das unidades de $\mathbb{Z}[\theta]$. Na segunda parte do trabalho, calcularemos as unidades de $\mathbb{Z}A_5$, onde A_5 é o subgrupo alternado do grupo de permutações S_5, utilizando o importante resultado da Teoria de Caracteres $\mathcal{Z}(\mathbb{Q}G) \simeq \mathbb{Q}(\chi_0) \oplus \cdots \oplus \mathbb{Q}(\chi_p)$, onde χ_i, $0 \leqslant i \leqslant p$, são os caracteres irredutíveis complexos não conjugados algebricamente, associados ao grupo em questão, bem como a Teoria Algébrica de Números, em especial, o Teorema de Unidades de Dirichlet.

Palavras-chave: unidades, anéis de grupo, unidades centrais.

Abstract

Bertaggia, G. **Central Units of Integral Group Rings**. 2014. 100 páginas. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2014.

Let $\mathbb{Z}G$ be the integral group ring and $\mathcal{U}(\mathbb{Z}G) = \{u \in \mathbb{Z}G | u \textit{ is invertible}\}$ its unit group, where G is an arbitrary group and $\mathbb{Z}$ is the ring of integers. For a given primitive root of unity α over $\mathbb{Q}$, we denote by $\mathbb{Z}[\alpha]$ the ring of cyclotomic integers. In the first part of this dissertation, we compute the units of integral group rings of cyclic groups of orders 7 and 9. In addition, we study a generalization of this result by Ferraz which establishes an independent generating set that allows us to obtain the units of $\mathbb{Z}C_p$, with C_p a cyclic group of prime order p, by considering a primitive root of unity of order p, θ, such that $S_\theta = \left\{-1, \theta, 1+\theta, \ldots, 1+\theta+\cdots+\theta^{\frac{p-3}{2}}\right\}$ generates the group of units of $\mathbb{Z}[\theta]$. In the final part of this work, we are concerned in computing the units of $\mathbb{Z}A_5$, where A_5 is the subgroup of the alternating group of permutations of S_5. To achieve this purpose, we use the following important result of the theory of characters: $\mathcal{Z}(\mathbb{Q}G) \simeq \mathbb{Q}(\chi_0) \oplus \cdots \oplus \mathbb{Q}(\chi_p)$, where χ_i, $0 \leqslant i \leqslant p$, are the algebraically non-conjugate irreducible complex characters associated with the group concerned. We also use some elements of the Theory of Algebraic Numbers, in particular, the Dirichlet's Unit Theorem.

Keywords: units, group rings, central units.

Sumário

Introdução

Nosso interesse em estudar Anéis de Grupos provém do fato da área ser extremamente rica, no sentido de interligar e utilizar diversas teorias na área de Álgebra, como Teoria de Grupos e Teoria de Anéis, tornando-a repleta de problemas a serem solucionados. Exporemos agora um dos problemas da área, chamado Problema do Isomorfismo, o qual foi uma das inspirações para o estudo das unidades nesta dissertação.

A Teoria de Anéis de Grupos faz uma importante conexão entre a teoria de representações de grupos e a teoria de estruturas algébricas. Assim, podemos nos perguntar se, dado um anel de grupo, conhecendo suas propriedades e estrutura, podemos determinar a estrutura do grupo dado, isto é, dados dois grupos G e H e um anel R, se $RG \simeq RH$, em que condições ocorre $G \simeq H$?

Na literatura, prova-se que se G e H são dois grupos abelianos de mesma ordem finita, então $\mathbb{C}G \simeq \mathbb{C}H$, onde $\mathbb{C}$ denota o corpo dos números complexos, mostrando assim que o Problema do Isomorfismo tem resposta negativa, uma vez que é fácil determinar dois grupos abelianos de mesma ordem não isomorfos.

Estudando os trabalhos da área, temos alguns resultados importantes, como:

- Grupos abelianos finitos são determinados pelo seu anel de grupo sobre o corpo dos números racionais $\mathbb{Q}$ (1950, S. Perlis e C. Walker, [18])
- p-grupos abelianos finitos são determinados sobre seus anéis de grupo sobre qualquer corpo de característica p (1956, W.E. Deskins, [6])
- Se $p \neq 2$ é um inteiro primo e G e H são dois grupos abelianos não isomorfos de ordem p^3, então $\mathbb{Q}G \simeq \mathbb{Q}H$ (1955, S.D. Berman)

D.B. Coleman e D.S. Passman, em [4], conseguiram alguns resultados parciais sobre grupos não comutativos. Assim, acreditou-se que, para grupos específicos, poder-se-ia determinar algum corpo onde a resposta para o Problema do Isomorfismo fosse sempre positiva. Porém,

em 1972, E. Dade publicou um exemplo, em [5], com dois grupos não isomorfos que possuem anéis de grupos isomorfos sobre qualquer corpo K.

A partir daí, conjecturou-se: dados dois grupos finitos G e H, se $\mathbb{Z}G \simeq \mathbb{Z}H$, então $G \simeq H$, onde $\mathbb{Z}$ é o anel dos inteiros. Isso deu-se do fato de que dados dois grupos G e H, se $\mathbb{Z}G \simeq \mathbb{Z}H$, então $RG \simeq RH$, onde R é um anel qualquer com unidade.

Em 1940, em [11], G. Higman havia provado que a conjectura acima é verdadeira no caso de grupos abelianos finitos e também no caso dos 2-grupos que são Hamiltonianos (ou seja, quando todo subgrupo é normal). Também provou-se nos casos dos grupos metabelianos finitos (A. Whitcomb, 1968, [23]); grupos simétricos e grupos alternados; grupos finitos que são grupos de unidades de algum anel; grupos nilpotentes finitos (A. Weiss, 1988, [22]).

Dessa maneira, um estudo mais aprofundado da estrutura de $\mathbb{Z}G$ tornou-se condição *sine qua non* para aqueles que desejassem demonstrar a conjectura e, em especial, dos seus elementos inversíveis (as unidades), pois define-se, assim, o grupo das unidades normalizadas de $\mathbb{Z}G$, denotado por $\mathcal{U}_1(\mathbb{Z}G)$, o qual será mencionado no decorrer desse trabalho. Esse estudo permitiria obter soluções para o problema do isomorfismo, pois sempre que tratamos do fato $\mathbb{Z}G \simeq \mathbb{Z}H$, é possível considerar um isomorfismo normalizado entre $\mathbb{Z}G$ e $\mathbb{Z}H$, o que nos permite estudar um isomorfismo entre G e H, considerando esse como a restrição do isomorfismo normalizado entre esses anéis de grupos.

Essa foi a motivação que nos levou a estudar algumas unidades de alguns anéis de grupos integrais nesse trabalho.

Primeiramente vamos estudar as unidades sobre grupos cíclicos de ordens 7 e 9, calculadas por R.Z. Aleev e G.A Panina em [2], de 1999. Nesse artigo, podemos notar a conexão com a teoria algébrica de números, utilizando as definições e resultados da área.

A partir daí, passamos a nos perguntar se podemos estudar as unidades de anéis de grupos integrais sobre grupos cíclicos de uma maneira mais geral. A resposta vem em um trabalho de Ferraz, [10] de 2009, onde o autor encontrou um grupo de geradores independentes para o grupo das unidades de $\mathbb{Z}C_p$, onde C_p é um grupo cíclico de ordem p e p é um número primo tal que $S = \left\{-1, \theta, 1+\theta, \ldots, 1+\theta+\cdots+\theta^{\frac{p-3}{2}}\right\}$ gera o grupo das unidades de $\mathbb{Z}[\theta]$, onde θ é uma raiz primitiva da unidade de ordem p sobre $\mathbb{Q}$. Posteriormente, Kitani, em [14], estendeu esse resultado para $\mathbb{Z}C_{p^n}$, considerando um conjunto similar que gera $\mathcal{U}\mathbb{Z}[\theta]$. Também, temos, em [20], por Silva, a descrição explícita de um conjunto gerador para o grupo das unidades do anel de grupo integral $\mathbb{Z}C_{2p}$.

Por fim, calculamos as unidades de um anel de grupo integral sobre o grupo alternado A_5, isto é, sobre o subgrupo de permutações pares do grupo simétrico S_5. Essa é uma parte

importante do trabalho, pois, mais uma vez, utilizamos da Teoria Algébrica de Números, mas, além disso, podemos estudar um pouco das teorias de representações e caracteres e notar como as mesmas permitem obter importantes resultados para Teoria de Álgebras de Grupo. Baseamos nosso estudo em [1], porém vale ressaltar que Li e Parmenter o provaram em [15].

Capítulo 1

Preliminares

1.1 Teoria de Grupos

Nessa seção explicitaremos algumas definições e resultados importantes para o desenvolvimento das seções posteriores. Vamos admitir conhecidos os conceitos básicos sobre Teoria de Anéis e de Grupos. Denotaremos por 1 o elemento neutro de um grupo.

Nesse capítulo, os resultados apresentados podem ser encontrados em [16].

Definição 1.1.1. *Sejam H, K subgrupos de um grupo G. Então G é dito* ***produto direto*** *(interno) de H e K e escrito $G = H \times K$ se satisfaz as seguintes condições*

1. $G = HK$
2. $H \cap K = \{1\}$
3. $H \triangleleft G$ *e* $K \triangleleft G$

A definição acima pode ser estendida a uma família arbitrária de subgrupos normais.

Definição 1.1.2. *Seja X um subconjunto não vazio de um grupo G. Definimos o* ***subgrupo gerado por*** *X como intersecção de todos os subgrupos de G contendo X. Esse subgrupo é denotado e descrito por:*

$$\langle X \rangle = \{x_1^{\rho_1} \dots x_k^{\rho_k} : x_i \in X, \rho_i = \pm 1, k \geqslant 1\} \cup \{1\}$$

Se $\langle X \rangle = G$, então dizemos que X é um ***conjunto de geradores de*** *G. Se X é finito, então dizemos que G é um* ***grupo finitamente gerado****.*

Definição 1.1.3. *O* ***centro de um grupo*** G *é o subgrupo*

$$\mathcal{Z}(G) = \{a \in G : ax = xa, \forall x \in G\}$$

Seja a um elemento de um grupo G. Definimos as potências de a por:

$$a^n = \begin{cases} \underbrace{a.a \dots a}_{n \ \ vezes}, n > 0 \\ \underbrace{a^{-1}.a^{-1} \dots a^{-1}}_{|n| \ \ vezes}, n < 0 \\ 1, n = 0 \end{cases}$$

Já que $a^m \cdot a^n = a^{m+n}$, segue que o conjunto $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ é um subgrupo de G, que é chamado de **subgrupo cíclico de** G **gerado por** a.

O menor inteiro positivo n tal que $a^n = 1$ é chamado de ordem de a é denotado por $o(a)$. Se $\langle a \rangle$ infinito, então dizemos que a é um elemento de ordem infinita.

Se existe um elemento a em G tal que $G = \langle a \rangle$, então dizemos que G é um grupo cíclico e a é o gerador de G. Notemos também que $o(a) = |\langle a \rangle|$.

Definição 1.1.4. *Seja G um grupo abeliano. Um elemento g de G é chamado de* ***elemento de torção*** *se tem ordem finita. O subgrupo*

$$T(G) = \{g \in G : o(g) < \infty\}$$

é chamado de ***subgrupo de torção de*** G.

Definição 1.1.5. *Dado um grupo G, o menor inteiro positivo m tal que $g^m = 1$, para todo $g \in G$, é chamado* ***expoente de*** G.

Agora vamos definir a base de um grupo G, definindo primeiramente elementos de G que são multiplicativamente independentes sobre $\mathbb{Z}$.

Definição 1.1.6. *Sejam $a_1, a_2, \dots, a_n$ elementos de um grupo abeliano G. Dizemos que são* ***multiplicativamente independentes sobre*** $\mathbb{Z}$ *se*

$$a_1^{t_1} a_2^{t_2} \dots a_n^{t_n} = 1 \Longrightarrow t_j = 0,$$

para todo $1 \leqslant j \leqslant n$, com $t_j \in \mathbb{Z}$.

Definição 1.1.7. *Seja G um grupo. Um conjunto de elementos multiplicativamente independentes que gera G é chamado uma* ***base de*** *G.*

Definição 1.1.8. *Um grupo abeliano que possui uma base com n elementos é chamado* ***grupo abeliano livre de posto*** *n.*

Teorema 1.1.1. *Seja G um grupo abeliano, finitamente gerado. Então $T(G)$ é finito, $G/T(G)$ é livre de posto finito e*

$$G \simeq T(G) \times \frac{G}{T(G)}$$

Agora, vamos definir os grupos de permutações, já que na última seção desse trabalho, calcularemos as unidades de um anel de grupo, cujo grupo é um subgrupo de um grupo de permutações de 5 elementos.

Definição 1.1.9. *Seja M um conjunto finito. Um função bijetiva de M em si mesmo é chamada uma* ***permutação de*** *M. O conjunto de todas as permutações de M forma um grupo, que é chamado de* ***grupo de permutação*** *ou* ***grupo simétrico*** *e é denotado, usualmente, por S_M. Se $M = \{1, 2 \ldots, n\}$, então S_M é chamado de* ***grupo simétrico de ordem*** *n ou* ***grupo de permutação de ordem*** *n e é denotado por S_n.*

Observemos que a ordem de S_n é $n!$.

Dada uma permutação $\rho \in S_n$ e um inteiro positivo k, com $1 \leqslant k \leqslant n$, dizemos que ρ move k se $\rho(k) \neq k$. Caso contrário, dizemos que ρ fixa k.

Um elemento $\rho \in S_n$ é chamado **ciclo de comprimento** k se existem k inteiros positivos distintos $a_1, a_2, \ldots, a_k$ em M tais que $\rho(a_1) = a_2, \rho(a_2) = a_3, \ldots, \rho(a_{k-1}) = a_k$, $\rho(a_k) = a_1$ e $\rho(a) = a$, para todo outro elemento a em M.

Definição 1.1.10. *Dada uma permutação $\rho \in S_n$, definimos seu* ***sinal*** *por*

$$sgn(\rho) = \prod_{1 \leqslant i \leqslant j \leqslant n} \frac{\rho(i) - \rho(j)}{i - j}$$

Temos que sgn é um homomorfismo sobrejetor de S_n em $\{-1, 1\}$. O kernel de sgn é chamado de grupo alternado de grau n e é denotado por A_n.

Em nosso caso, trabalharemos posteriormente com o grupo alternado A_5.

1.2 Módulos

Nessa seção, nosso intuito é explicitar alguns resultados da Teoria de Módulos, supondo que o leitor conheça alguns conceitos da Teoria de Anéis.

Definição 1.2.1. *Seja R um anel. Um grupo abeliano M (aditivo) é chamado um R-**módulo à esquerda** (ou um módulo à esquerda sobre R) se, para cada elemento $a \in R$ e cada $m \in M$, temos o produto $am \in M$ tal que*

1. $(a+b)m = am + bm$
2. $a(m_1 + m_2) = am_1 + am_2$
3. $a(bm) = (ab)m$
4. $1m = m$,

para todos $a, b \in R$ e $m, m_1, m_2 \in M$

De maneira análoga, definimos um R-**módulo à direita** ou um **módulo à direita sobre** R considerando a multiplicação de elementos de M por elementos de R à direita. Usualmente, chama-se um R-módulo à esquerda apenas de R-**módulo**.

Notemos que se K é um corpo, então um K-módulo nada mais é do que um espaço vetorial sobre K.

Definição 1.2.2. *Seja R um anel comutativo. Um R-módulo A é chamado de R-**algebra** se há uma multiplicação definida em A, tal que, com a adição dada em A e sua multiplicação, A é um anel e tal que a seguinte condição é válida*

$$r(ab) = (ra)b = a(rb),$$

para todos $r \in R$ e $a, b \in A$.

Definição 1.2.3. *Seja M um R-módulo. Um subconjunto não vazio $N \subset M$ é chamado de R-**submódulo** de M se as seguintes condições são verificadas*

1. *para todo $x, y \in N$, temos $x + y \in N$*
2. *para todo $r \in R$ e todo $n \in N$, temos $rn \in N$*

Todo R-módulo M não nulo possui, ao menos, dois submódulos: (0) e o próprio M. Esses dois submódulos são chamados **triviais**. Os demais são chamados **submódulos próprios**. Um módulo que não contém submódulos próprios é chamado **módulo simples**.

Se R é comutativo e M é uma R-álgebra, dizemos que N é uma **R-subálgebra de M** se é tanto um submódulo quanto um subanel de M.

Observemos que se V é um espaço vetorial sobre um corpo K, então K-submódulos de V são precisamente seus subespaços.

Definição 1.2.4. *Um conjunto $S = \{s_i\}_{i\in I}$ de elementos de um R-módulo M é chamado um **conjunto de geradores de** M se $M = RS$, isto é, se todo elemento de M pode ser escrito como uma combinação linear finita de elementos de S com coeficientes em R.*

Definição 1.2.5. *Um conjunto $S = \{s_i\}_{i\in I}$ de elementos de um R-módulo M é chamado **linearmente independente** se, pra toda combinação linear (finita) de elementos de S com coeficientes em R*

$$r_{i_1}s_{i_1} + r_{i_2}s_{i_2} + \cdots + r_{i_t}s_{i_t} = 0$$

implica que $r_{i_1} = r_{i_2} = \cdots = r_{i_t} = 0$

Definição 1.2.6. *Um conjunto $S = \{s_i\}_{i\in I}$ de elementos de um R-módulo M é chamado uma **base de M sobre R** (ou uma R-base) se é um conjunto linearmente independente e também é um conjunto de geradores para M.*

Proposição 1.2.1. *Um conjunto $S = \{s_i\}_{i\in I}$ de elementos de um R-módulo M é uma base se, e somente se, todo elemento $m \in M$ pode ser escrito de maneira única (finita) da seguinte maneira:*

$$m = r_{i_1}s_{i_1} + r_{i_2}s_{i_2} + \cdots + r_{i_t}s_{i_t},$$

com $r_{i_j} \in R$, $s_{i_j} \in S$, onde $1 \leqslant i \leqslant t$.

Definição 1.2.7. *Um R-módulo M é chamado **R-módulo livre** se tem uma base.*

Definição 1.2.8. *Uma família $\{M_i\}_{i\in I}$ de submódulos de um R-módulo M é dita **independente** se, para todo $i \in I$, temos*

$$M_i \cap \left(\sum_{j\neq i} M_j\right) = \{0\}$$

Definição 1.2.9. *Seja $\{M_i\}_{i\in I}$ uma família de submódulos de um R-módulo M. Dizemos que M é uma **soma direta** (interna) de submódulos dessa família e escrevemos $M = \bigoplus_{i\in I} M_i$ se a família é independente, gera M e as seguintes condições são satisfeitas:*

1. *Para todo* $i \in I$, *temos* $M_i \cap \left(\sum_{j \neq i} M_j \right) = \{0\}$

2. $M = \sum_{i \in I} M_i$

   As duas condições acima são equivalentes a

3. *Todo elemento* $m \in M$ *pode ser escrito unicamente como* $m = m_{i_1} + m_{i_2} + \cdots + m_{i_t}$, *com* $m_{i_j} \in M_{i_j}$ *e* $1 \leqslant i \leqslant t$.

Definição 1.2.10. *Um submódulo* N *de um* R*-módulo* M *é dito um* ***somando direto*** *se existe outro submódulo* N' *de* M *tal que* $M = N \oplus N'$. *Um módulo que não contém somando diretos não triviais é chamado* ***indecomponível***.

Definição 1.2.11. *Seja* $\{M_i\}_{i \in I}$ *uma família de* R*-módulos. A* ***soma direta*** *(externa) de módulos dessa família, que é denotada por* $\dot{\bigoplus}_{i \in I} M_i$ *é o conjunto de todos elementos da forma* $\{m_i\}_{i \in I}$, *onde* $m_i \in M_i$ *para todo* $i \in I$ *e* $m_i = 0$, *para quase todo* $i \in I$. *Com a adição e a multiplicação por escalares de* R *definida componente a componente, este conjunto é um* R*-módulo.*

Definição 1.2.12. *Seja* M *um módulo livre sobre um anel comutativo* R *que tem uma base finita. Então, o número de elementos de uma base qualquer de* M *é chamado* ***posto de*** M.

Definição 1.2.13. *Um* R*-módulo é dito* ***semisimples*** *se todo submódulo de* M *é um somando direto.*

Proposição 1.2.2. *Seja* $N \neq 0$ *um submódulo de um módulo semisimples* M. *Então* N *é semisimples e contém um submódulo simples.*

Teorema 1.2.1. *Seja* M *um* R*-módulo. Então as seguintes condições são equivalentes:*

1. M *é semisimples*

2. M *é uma soma direta de submódulos simples*

3. M *é uma soma (não necessariamente direta) de submódulos simples*

Definição 1.2.14. *Um anel* R *é dito* ***anel semisimples*** *se o* R*-módulo* R *à esquerda é semisimples.*

Teorema 1.2.2. *Seja R um anel. Então, as seguintes condições são equivalentes:*

1. *Todo R-módulo é semisimples*
2. *R é um anel semisimples*
3. *R é soma direta de um número finito de ideiais minimais à esquerda*

Definição 1.2.15. *Um elemento e em um anel R é chamado **idempotente** se $e^2 = e$. Os idempotentes diferentes de 0 e 1 são ditos não triviais.*

Teorema 1.2.3. *Seja R um anel. Então R é semisimples se, e somente se, todo ideal L à esquerda de R é da forma $L = Re$, onde $e \in R$ é um idempotente.*

Teorema 1.2.4. *Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de um anel semisimples em soma direta de ideais minimais à esquerda. Então existe uma família $\{e_1, \ldots, e_t\}$ de elementos de R tal que:*

1. *$e_i \neq 0$ é um elemento idempotente, para todo $1 \leqslant i \leqslant t$*
2. *Se $i \neq j$, então $e_i e_j = 0$*
3. *$1 = e_1 + \cdots + e_t$*
4. *e_i não pode ser escrito como $e_i = e_i^{'} + e_i^{''}$, onde $e_i^{'}$ e $e_i^{''}$ são idempotentes tais que $e_i^{'}, e_i^{''} \neq 0$ e $e_i^{'} e_i^{''} = 0$, com $1 \leqslant i \leqslant t$*

Reciprocamente, se existe uma família de idempotentes $\{e_1, \ldots, e_t\}$ satisfazendo as condições acima, então os ideais à esquerda $L_i = Re_i$ são minimais e $R = \oplus_{i=1}^{t} L_i$.

Definição 1.2.16. *Seja R um anel. Uma família de idempotentes $\{e_1, \ldots, e_t\}$ satisfazendo as condições 1, 2 e 3 do Teorema acima é chamada uma **família completa de idempotentes ortogonais**. Um idempotente que satisfaz a condição 4, é chamado **primitivo**.*

1.3 Anéis de Grupos

Agora vamos definir a estrutura algébrica com a qual trabalharemos no decorrer do texto e, em nosso caso, o anel utilizado será o anel dos inteiros $\mathbb{Z}$. Juntamente explicitamos alguns resultados de extrema importância dentro da Teoria de Anéis de Grupos.

Seja G um grupo, não necessariamente finito, e R um anel. Construindo um R-módulo que tem os elementos de G como base, temos a seguinte

Definição 1.3.1. *Seja G um grupo e R um anel. O* ***anel de grupo*** *RG é um conjunto formado pelas somas $\alpha = \sum_{g\in G} a_g g$, onde $a_g \in R$ e $g \in G$, sendo $a_g = 0$, exceto em um número finito de termos.*

Também, se for conveniente, podemos escrever um elemento em RG da seguinte maneira:

$$\alpha = \sum_{g\in G} \alpha(g)g$$

Definição 1.3.2. *Dado um elemento $\alpha = \sum_{g\in G} a_g g$, definimos o* ***suporte de*** *α como o subconjunto de elementos de G que, de fato, aparecem na expressão de α, isto é,*

$$supp(\alpha) = \{g \in G : a_g \neq 0\}$$

Observemos que, da definição, se dois elementos $\alpha = \sum_{g\in G} a_g g$ e $\beta = \sum_{g\in G} b_g g$ em RG são tais que $\alpha = \beta$, então $a_g = b_g$, para todo $g \in G$. Claramente, se $a_g = b_g$, temos $\alpha = \beta$.

Definimos a soma de dois elementos em RG por

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}(a_g + b_g)g.$$

Sendo $\alpha = \sum_{g\in G} a_g g$ e $\beta = \sum_{h\in G} b_h h$, definimos

$$\alpha\beta = \sum_{g,h\in G} a_g b_h gh = \sum_{u\in G} c_u u,$$

onde $c_u = \sum_{gh=u} a_g b_h$.

Dessa maneira, com as operações acima, RG é um anel, com unidade $1 = \sum_{g\in G} u_g g$, onde o coeficiente correspondente ao elemento unidade do grupo é igual a 1 e $u_g = 0$, para qualquer outro elemento $g \in G$.

Definimos o produto de elementos de RG por elementos $\lambda \in R$ como

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

É fácil ver que RG é um R-módulo. Se R é comutativo, então RG é uma álgebra sobre R.

Definição 1.3.3. *O homomorfismo $\varepsilon : RG \longrightarrow R$ dado por*

$$\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$$

é chamado ***função aumento de*** *RG e seu kernel, denotado por $\Delta(G)$, é chamado* ***ideal de aumento de*** *RG.*

Proposição 1.3.1. *O conjunto $\{g-1 : g \in G, g \neq 1\}$ é uma base de $\Delta(G)$. Assim,*

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

onde assumimos que apenas um número finito de coeficientes a_g são não nulos.

Demonstração. Seja $\alpha = \sum_{g\in G} a_g g \in \Delta(G)$. Então

$$\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g = 0$$

Então

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1)$$

Todos elementos da forma $g-1$, com $g \in G$, estão em $\Delta(G)$, então temos que

$$\{g-1 : g \in G, g \neq 1\}$$

é um conjunto de geradores de $\Delta(G)$ sobre R que é linearmente independente. Assim, temos o resultado. □

Teorema 1.3.1. *(Teorema de Mashke) Seja G um grupo. Então o anel de grupo RG é semisimples se, e somente se, as seguintes condições são verificadas:*

1. *R é um anel semisimples*
2. *G é finito*
3. *$|G|$ é invertível em R*

Corolário 1.3.1. *Seja G um grupo finito e seja K um corpo. Então KG é semisimples se, e somente se, $car(K)$ não divide $|G|$.*

Teorema 1.3.2. *Seja G um grupo e seja K um corpo tal que $car(K)$ não divide $|G|$. Então*

1. *KG é uma soma direta de um número finito de ideais bilaterais $\{B_i\}_{1\leqslant i\leqslant r}$, as componentes simples de KG. Cada B_i é um anel simples.*
2. *Qualquer ideal bilateral de KG é soma direta de alguns membros da família $\{B_i\}_{1\leqslant i\leqslant r}$.*
3. *Cada componente simples B_i é isomorfa a um anel de matrizes da forma $M_{n_i}(D_i)$, onde D_i é um anel com divisão contendo uma cópia isomorfa de K em seu centro, e o isomorfismo $KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$é um isomorfismo de K-álgebras*
4. *Em cada anel de matriz $M_{n_i}(D_i)$, o conjunto*

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ x_{n_i} & 0 & \cdots & 0 \end{bmatrix} : x_1, x_2, \ldots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

   é um ideal minimal à esquerda.

   Dado $x \in KG$, consideramos $\Phi(x) = (\alpha_1, \ldots, \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$ e definimos o produto de x por um elemento $m_i \in I_i$ por $xm_i = \alpha_i m_i$. Com essa definição, I_i torna-se um KG-módulo simples

5. *$I_i \not\simeq I_j$ se $i \neq j$.*
6. *Qualquer KG-módulo simples é isomorfo a algum I_i, com $1 \leqslant i \leqslant r$.*

Corolário 1.3.2. *Seja G um grupo finito e seja K um corpo algebricamente fechado tal que $car(K) \nmid |G|$. Então*

$$KG \simeq \bigoplus_{i=1}^{r} M_{n_i}(K)$$

e

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

Definição 1.3.4. *Seja G um grupo finito. Definimos:*

$$\mathcal{U}(\mathbb{Z}G) = \{\alpha \in \mathbb{Z}G | \alpha \text{ é inversível}\}$$

como o ***grupo de unidades de*** $\mathbb{Z}G$.

Definição 1.3.5. *Sejam G e H grupos. Um isomorfismo $\varphi : \mathbb{Z}G \longrightarrow \mathbb{Z}H$ diz-se um* ***isomorfismo normalizado*** *se, para todo $\alpha \in \mathbb{Z}G$ tem-se $\varphi(\alpha) = \varepsilon(\varphi(\alpha))$, ou equivalentemente se, para todo $g \in G$, tem-se $\varepsilon(\varphi(\alpha)) = 1$*

Definição 1.3.6. *Seja G um grupo finito. Definimos:*

$$\mathcal{U}_1(\mathbb{Z}G) = \{\alpha \in \mathcal{U}(\mathbb{Z}G) | \varepsilon(\varphi(\alpha)) = 1\}$$

como ***grupo de unidades normalizadas de*** $\mathbb{Z}G$.

Proposição 1.3.2. *(D. S. Berman) Seja G um grupo finito e seja $\mu = \sum_{i=1}^{n} a_i g_i \in \mathcal{U}(\mathbb{Z}G)$ uma unidade de ordem finita. Se $a_1 \neq 0$, então $\mu = \pm 1$.*

Corolário 1.3.3. *Seja G um grupo finito. Se $\mu = \sum_{i=1}^{n} a_i g_i \in \mathcal{U}(\mathbb{Z}G)$ é central de ordem finita, então $\mu = \pm g_i$, com $g_i \in \mathcal{Z}(G)$.*

Demonstração. Seja $\mu = \sum_{i=1}^{n} a_i g_i$ uma unidade central com ordem m. Suponhamos $a_i \neq 0$, para algum elemento $g_i \in G$. Assim μg_i^{-1} é também uma unidade de ordem finita em $\mathbb{Z}G$. Além disso, o coeficiente de 1 na expressão de μg_i^{-1} é $a_i \neq 0$. Daí, pela proposição 1.3.2, $\mu g_i^{-1} = \pm 1$. Logo, $\mu = \pm g_i$, como queríamos. □

Corolário 1.3.4. *Seja G um grupo finito abeliano. Então toda unidade de ordem finita de $\mathbb{Z}G$ é trivial, isto é, $T(\mathcal{U}(\mathbb{Z}G)) = \{\pm 1\} \times G$ e $T(\mathcal{U}_1(\mathbb{Z}G)) = G$.*

Teorema 1.3.3. *Seja G um grupo abeliano finito e seja H um outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então $G \simeq H$.*

1.4 Anel dos Inteiros Algébricos

O grupo de unidades de $\mathbb{Z}[\theta]$, onde θ é uma raiz primitiva da unidade será de extrema importância no decorrer do presente trabalho. Vamos começar essa seção definindo raiz da unidade:

Definição 1.4.1. *Seja K um corpo e $n \in \mathbb{Z}$, com $n \geqslant 1$. Um elemento ς em K tal que $\varsigma^n = 1$ é chamado* ***raiz n-ésima da unidade*** *ou* ***raiz da unidade de ordem*** *n, isto é, ς é uma raiz n-ésima da unidade em um corpo K quando n for um múltiplo de $o(\varsigma)$, onde $o(\varsigma)$ denota a ordem de ς.*

Seja $W_n(K)$ o conjunto das raízes n-ésimas da unidade em K. Então $W_n(K)$ é um subgrupo de K^* cuja ordem é, no máximo, igual a n, uma vez que $W_n(K)$ consiste das raízes em K do polinômio $x^n - 1$.

Definição 1.4.2. *Diremos que ς é uma* ***raiz primitiva n-ésima da unidade em*** *K se $\varsigma \in W_n(K)$ e $o(\varsigma) = n$.*

Na próxima seção, trabalharemos com anéis de inteiros ciclotômicos do tipo $\mathbb{Z}[\alpha]$, onde α é uma raiz primitiva da unidade. Abaixo faremos uma breve exposição sobre conceitos relacionados que serão utilizados no decorrer do texto.

Uma extensão finita $K \supset \mathbb{Q}$ de um corpo de números racionais é chamado de **corpo de números algébricos**. Todo número $\alpha \in K$ é **algébrico sobre** $\mathbb{Q}$ se satisfaz uma equação da forma

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0,$$

com $a_i \in \mathbb{Q}$, $i = 0, 1, \ldots, n$.

Um elemento $\beta \in K$ é chamado **inteiro algébrico** se satisfaz a equação mônica em $\mathbb{Z}[x]$

$$\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_0 = 0,$$

com $b_i \in \mathbb{Z}$, $i = 0, 1, \ldots, n$.

O conjunto dos inteiros algébricos de K forma um anel denotado por $\mathcal{O}_K$ (ver [8]).

Lema 1.4.1. *O anel $\mathcal{O}_K$ é finitamente gerado e $K = \mathbb{Q}\mathcal{O}_K$*

Teorema 1.4.1. *(Teorema do Elemento Primitivo) Se E é uma extensão finita de um corpo K, de característica 0. Então $E = K(\alpha)$, para algum $\alpha \in E$.*

Demonstração. A demonstração desse teorema pode ser encontrada em [12]. □

Pelo Teorema do Elemento Primitivo 1.4.1, temos $K = \mathbb{Q}(\alpha)$, para algum $\alpha \in K$ e $\alpha \in \mathcal{O}_K$. Então $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$, mas nem sempre ocorre $\mathcal{O}_K \subset \mathbb{Z}[\alpha]$.

Agora, seja $n \geq 1$ e ζ uma raiz primitiva da unidade de ordem n. Então $K = \mathbb{Q}(\zeta)$ é chamado **corpo ciclotômico de ordem** n ou **n-ésimo corpo ciclotômico**. O grau da extensão é $[K : \mathbb{Q}] = \varphi(n)$, onde $\varphi(n)$ denota a função φ de Euler.

Temos alguns fatos que podem ser estudados mais profundamente na literatura específica de Teoria Algébrica de Números:

- Os inteiros do corpo ciclotômico $K = \mathbb{Q}(\zeta)$ são dados por $\mathcal{O}_K = \mathbb{Z}[\zeta]$, isto é, $\mathbb{Z}[\zeta]$ é o anel dos inteiros algébricos no corpo ciclotômico $\mathbb{Q}(\zeta)$ e é chamado **anel dos inteiros ciclotômicos**. O maior subcorpo real de K é $\mathbb{Q}(\zeta + \zeta^{-1}) = E$. O anel dos inteiros algébricos de E é $\mathbb{Z}[\zeta + \zeta^{-1}]$.
- As raízes da unidade contidas em $\mathbb{Q}(\zeta)$ são os elementos do conjunto $\{\pm\zeta^i\}$.

O próximo resultado chama-se Teorema de Unidades de Dirichlet, com o qual podemos determinar o posto do grupo das unidades de um anel de inteiros ciclotômicos, denotado por $\mathcal{U}\mathbb{Z}[\alpha]$, onde α é uma raiz primitiva da unidade. Sua demonstração não é trivial e pode ser encontrada em [8].

Teorema 1.4.2. *(Teorema de Unidades de Dirichlet) Seja $K \supset \mathbb{Q}$ uma extensão finita de grau $n = n_1 + 2n_2$, onde n_1 e $2n_2$ denotam o número de imersões reais e complexas de K, respectivamente. Seja $\mathcal{O}_K$ o anel dos inteiros algébricos de K e $\mathcal{U}(\mathcal{O}_K)$ é seu grupo de unidades. Então $\mathcal{U}(\mathcal{O}_K)$ é um grupo abeliano finitamente gerado. Além disso, $\mathcal{U}(\mathcal{O}_K) = C \times F$, onde C é um grupo cíclico finito e F é livre de torção de posto $p = n_1 + n_2 - 1$.*

Corolário 1.4.1. *Seja $K \supset \mathbb{Q}$ uma extenssão finita. Então $\mathcal{U}(\mathcal{O}_K)$ é finito se, e somente se, $K = \mathbb{Q}$ ou K é da forma $\mathbb{Q}(\sqrt{-d})$, onde d é um inteiro positivo.*

Corolário 1.4.2. *Seja $K = \mathbb{Q}(\zeta)$ um corpo ciclotômico e E um subcorpo. Então $\mathcal{U}(\mathcal{O}_K)$ e $\mathcal{U}(\mathcal{O}_E)$ tem o mesmo posto, isto é,*

$$[\mathcal{U}(\mathcal{O}_E) : \mathcal{U}(\mathcal{O}_K)] < \infty \Longleftrightarrow E = K$$

ou

$$E = \mathbb{Q}(\zeta + \zeta^{-1})$$

De acordo com o Teorema de Unidades de Dirichlet 1.4.2, F pode ser escrito como produto de ρ grupos cíclicos infinitos:

$$F = \langle u_1 \rangle \times \langle u_2 \rangle \times \cdots \times \langle u_p \rangle$$

As unidades $\{u_1, u_2, \ldots, u_p\}$ formam o que chamamos de **sistema fundamental de unidades**.

No caso em que $K = \mathbb{Q}(\zeta)$, onde ζ é raiz primitiva da unidade de ordem n, podemos construir as seguintes unidades:

$$u = \frac{1-\zeta^i}{1-\zeta},$$

onde $mdc(i, n) = 1$

Seja $k \in \mathbb{Z}$ o inverso de i módulo n, isto é, $ik \equiv 1 \mod n$. Então

$$u = \frac{1-\zeta}{1-\zeta^i} = \frac{1-\zeta^{ki}}{1-\zeta^i} = 1 + \zeta + \cdots + \zeta^{i(k-1)} \in \mathbb{Z}[\zeta].$$

Portanto, $u \in \mathcal{U}(\mathcal{O}_K)$.

Essa unidades são ditas **unidades ciclotômicas**.

Teorema 1.4.3. *As unidades ciclotômicas geram um subgrupo de índice finito em $\mathcal{U}(\mathcal{O}_K)$.*

Definição 1.4.3. *Seja A uma $\mathbb{Q}$-álgebra. Um subanel R de A contendo suas unidades é chamado de $\mathcal{Z}$-**ordem**, ou simplesmente, **uma ordem em** A se R é finitamente gerado como um $\mathcal{Z}$-módulo e $\mathbb{Q}R = A$.*

Exemplo: Denotemos por $\mathcal{O}$ o anel dos inteiros algébricos de um corpo de números algébricos K, então $\mathcal{O}$ é uma ordem em K.

Lema 1.4.2. *Sejam $R_1 \subset R_2$ ordens em uma $\mathbb{Q}$-álgebra A. Então, há um inteiro d tal que $dR_2 \subset R_1$. Além disso, o índice dos grupos aditivos $[R_1 : dR_2]$ é finito.*

Lema 1.4.3. *Sejam $R_1 \subset R_2$ duas ordens em uma $\mathbb{Q}$-álgebra A. Então*

1. *O índice dos grupos de unidades multiplicativas $[\mathcal{U}(R_2) : \mathcal{U}(R_1)]$ é finito*
2. *Se $u \in R_1$ é invertível em R_2, então $u^{-1} \in R_1$.*

Capítulo 2

As unidades de anéis de grupo integrais de grupos cíclicos de ordens 7 e 9

2.1 Unidades de anéis de grupo integrais de grupos cíclicos de ordem 7

Nesse capítulo vamos começar a estudar as unidades de alguns anéis de grupos de alguns grupos cíclicos, isto é, vamos determinar $\mathcal{U}(\mathbb{Z}G)$, onde G é um grupo cíclico de ordem 7 ou de ordem 9. Iremos calcular essas unidades através das unidades do anel de inteiros ciclotômicos descrito no capítulo anterior. Posteriormente, iremos explicitar como Ferraz, em [10], encontra um conjunto de geradores para o grupo das unidades de $\mathbb{Z}C_p$, para certos primos p.

Os resultados desse capítulo são baseados no artigo de Aleev e Panina, [2].

Seja α uma raiz primitiva da unidade de ordem 7. Definimos $\eta_1 = \alpha + \alpha^{-1}$ e $\eta_2 = \alpha^2 + \alpha^{-2}$.

Sejam também $\mathbb{Z}[\alpha]$ o anel dos inteiros ciclotômicos de ordem 7, isto é,
$\mathbb{Z}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_6\alpha^6 : a_i \in \mathbb{Z}\}$ e $\mathcal{U}(\mathbb{Z}[\alpha])$ o grupo de unidades de $\mathbb{Z}[\alpha]$.

Considere $C_7 = \langle x \rangle$ um grupo cíclico de ordem 7 e $\mathbb{Z}C_7$ o anel de grupo integral de C_7, ou seja, $\mathbb{Z}C_7 = \left\{\sum_{i=0}^{6} a_i x^i : a_i \in \mathbb{Z}\right\}$.

Denotaremos por $\mathcal{U}(\mathbb{Z}C_7)$ o grupo de unidades de $\mathbb{Z}C_7$ e consideremos os seguintes homomorfismos de anéis:

$$\begin{aligned} \varphi : \mathbb{Z}C_7 &\longrightarrow \mathbb{Z}[\alpha] \\ \sum_{i=0}^{6} a_i x^i &\longmapsto \sum_{i=0}^{6} a_i \alpha^i \end{aligned}$$

e

$$\begin{aligned} \varepsilon : \mathbb{Z}C_7 &\longrightarrow \mathbb{Z} \\ \sum_{i=0}^{6} a_i x^i &\longmapsto \sum_{i=0}^{6} a_i \end{aligned}$$

onde ε é a função aumento definida anteriormente.

Notemos que $1+\alpha+\alpha^2+\cdots+\alpha^6=0$, uma vez que

$$\begin{aligned} &1+\alpha+\alpha^2+\cdots+\alpha^6=\alpha^7+\alpha+\alpha^2+\cdots+\alpha^6 \Rightarrow \\ &\Rightarrow 1+\alpha+\alpha^2+\cdots+\alpha^6=\alpha\left(1+\alpha+\alpha^2+\cdots+\alpha^6\right) \Rightarrow \\ &\Rightarrow \left(1+\alpha+\alpha^2+\cdots+\alpha^6\right)(1-\alpha)=0 \Rightarrow \\ &\Rightarrow 1+\alpha+\alpha^2+\cdots+\alpha^6=0, \end{aligned}$$

uma vez que α é raiz primitiva da unidade de ordem 7. Daí, vem que $\alpha^6=-1-\alpha-\alpha^2-\alpha^3-\alpha^4-\alpha^5$.

Estamos interessados agora em determinar o kernel da função φ. Logo, tomando um elemento v qualquer em $\mathbb{Z}C_7$, temos

$$\varphi(v)=\varphi(a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5+a_6x^6)=a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+\alpha_4\alpha^4+\alpha_5\alpha^5+a_6\alpha^6$$

Se $v\in\ker\varphi$, temos

$$\begin{aligned} &a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_4\alpha^4+a_5\alpha^5+a_6(-1-\alpha-\alpha^2-\alpha^3-\alpha^4-\alpha^5)=0 \Rightarrow \\ &\Rightarrow (a_0-a_6)+(a_1-a_6)\alpha+(a_2-a_6)\alpha^2+\cdots+(a_5-a_6)\alpha^5=0 \Rightarrow \\ &\Rightarrow a_0=a_6, a_1=a_6, \ldots, a_5=a_6 \Rightarrow \\ &\Rightarrow a_0=a_1=a_2=a_3=a_4=a_5=a_6, \end{aligned}$$

pelo fato de que $\{1,\alpha,\alpha^2,\ldots,\alpha^5\}$ é base de $\mathbb{Z}[\alpha]$ (segundo [17], parágrafo 10).

Portanto,

$$\ker\varphi = \left\{ \sum_{i=0}^{6} a_i x^i \quad : \quad a_i = a_6, i = 0, \cdots, 5 \right\}.$$

Chamemos $a_6 = a$. Logo se $b \in \ker\varphi$, então $b = a\sum_{i=0}^{6} x^i$.

Observemos que, para um anel de grupo qualquer sobre os inteiros, $\mathbb{Z}G$, temos

$$\varepsilon(u) = \pm 1, \quad \text{se} \quad u \in \mathcal{U}(\mathbb{Z}G)$$

Lema 2.1.1. *Com a notação estabelecida acima, temos* $\mathcal{U}(\mathbb{Z}[\alpha]) = \langle -1\rangle \times \langle\alpha\rangle \times \langle\eta_1\rangle \times \langle\eta_2\rangle$, *onde* $\eta_1 = \alpha + \alpha^{-1}$ *e* $\eta_2 = \alpha^2 + \alpha^{-2}$.

Demonstração. Para demonstração deste resultado veja [7], página 202. □

Lema 2.1.2. *Seja* $u_1 \in \mathcal{U}(\mathbb{Z}G)$. *Se* $\varphi(u_1) = \eta_1^3$, *então*

$$u_1 = -1 + 2x - x^2 - x^5 + 2x^6$$

e

$$u_1^{-1} = -3 + x + 3x^2 - 2x^3 - 2x^4 + 3x^5 + x^6$$

e se $\varphi(u_1) = \eta_1^k$, *então* $3|k$.

Demonstração. Primeiro vamos demonstrar que não ocorre $\varphi(u) = \eta_1^k$, quando $k = 1$ ou $k = 2$, $\forall u \in \mathcal{U}(\mathbb{Z}C_7)$.

Caso(1): $k = 1$

Temos que $\varphi(u) = \eta_1 = \alpha + \alpha^6$.

Já que

$$u = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 \quad \text{e}$$

$$\varphi(u) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5 + a_6\alpha^6 = \alpha + \alpha^6$$

Temos que $a_1 = 1$ e $a_6 = 1$. Portanto, $u \in x + x^6 + \ker\varphi$. Logo,

$$u = x + x^6 + a\sum_{i=0}^{6} x^i$$

Assim,

$$\pm 1 = \varepsilon(u) = 1 + 1 + 7a = 2 + 7a \Rightarrow 2 + 7a = \pm 1,$$

com $a \in \mathbb{Z}$, o que é uma contradição.

Portanto, $\varphi(u) = \eta_1$ não ocorre, $\forall u \in \mathcal{U}(\mathbb{Z}C_7)$.

Caso(2): $k = 2$
Agora seja $\varphi(u) = \eta_1^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + 2\alpha\alpha^{-1} + \alpha^{-2} = \alpha^2 + 2 + \alpha^5$.
Como $\varphi(u) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5 + a_6\alpha^6$, temos que $a_0 = 2$, $a_2 = 1$ *e* $a_5 = 5$.
Portanto $u \in 2 + x^2 + x^5 + \ker\varphi$. Assim,

$$u = 2 + x^2 + x^5 + a\sum_{i=0}^{6} x_i$$

Novamente,

$$\left.\begin{array}{l} \varepsilon(u) = 2 + 1 + 1 + 7a = 4 + 7a \\ \varepsilon(u) = \pm 1 \end{array}\right\} \Rightarrow 4 + 7a = \pm 1, \quad \text{com } a \in \mathbb{Z}, \text{o que é um absurdo.}$$

Portanto, não ocorre $\varphi(u) = \eta_1^2$, $\forall u \in \mathcal{U}(\mathbb{Z}C_7)$.

Agora vejamos o caso $\varphi(u_1) = \eta_1^3$. Temos:

$$\varphi(u_1) = \eta_1^3 = \quad \alpha^3 + 3\alpha + 3\alpha^{-1} + \alpha^{-3} = \alpha^3 + 3\alpha + 3\alpha^6 + \alpha^4$$

Como

$$\varphi(u_1) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5 + a_6\alpha^6,$$

segue que $a_1 = 3$, $a_3 = 1$, $a_4 = 1$ e $a_6 = 3$. Logo,

$$u_1 \in x + x^3 + x^4 + 3x^6 + \ker\varphi$$

E, portanto,

$$u_1 = x + x^3 + x^4 + 3x^6 + a\sum_{i=0}^{6} x_i$$

Para encontrarmos a calcularemos o aumento de u_1:

$$\left.\begin{array}{l}\varepsilon(u_1) = 1+3+1+3+7a = 8+7a \\ \varepsilon(u_1) = \pm 1\end{array}\right\} \Rightarrow 8+7a = \pm 1$$

Assim, $a = -1$ e obtemos

$$u_1 = -1 + 2x - x^2 - x^5 + 2x^6$$

Um cálculo simples nos mostra que

$$(-1+2x-x^2-x^5+2x^6)(-3+x+3x^2-2x^3-2x^4+3x^5+x^6) = 1$$

Podemos concluir que

$$u_1^{-1} = -3 + x + 3x^2 - 2x^3 - 2x^4 + 3x^5 + x^6$$

Agora vejamos que se $\varphi(u_0) = \eta_1^k$, então $3|k$.

Seja $u_0 \in \mathcal{U}(\mathbb{Z}C_7)$ tal que $\varphi(u_0) = \eta_1^k$.

Suponha que existam $q, r \in \mathbb{Z}$ tais que $k = 3q + r$. Nesse caso, $r \in \{0, 1, 2\}$. Se $r = 1$, temos que

$$\varphi(u_0) = \eta_1^{3q+1} = \eta_1^{3q}\eta_1 = (\eta_1^3)^q\eta_1$$

Sabemos que existe $u_1 \in \mathcal{U}(\mathbb{Z}C_7)$ tal que $\varphi(u_1) = \eta_1^3$. Logo,

$$\varphi(u_0) = \varphi(u_1)^q\eta_1 \quad = \quad \varphi(u_1^q)\eta_1$$

Portanto, $\varphi(u_1^{-q}u_0) = \eta_1$.

Daí, sendo $u_1' = u_1^{-q}u_0 \in \mathcal{U}(\mathbb{Z}C_7)$, temos que $\varphi(u_1') = \eta_1$, o que é uma contradição, pelo caso(1).

Se $r = 2$, temos situação análoga:

$$\varphi(u_0) = \eta_1^{3q}\eta_1^2 = \varphi(u_1)^q\eta_1^2 \Rightarrow$$
$$\Rightarrow \varphi(\underbrace{u_1^{-q}u_0}_{u_1' \in \mathcal{U}(\mathbb{Z}G)}) = \eta_1^2,$$

o que é uma contradição pelo caso (2).

Logo, $r = 0$. Portanto $k = 3q$, ou seja, $3|k$, como queríamos.

□

Lema 2.1.3. *Seja u_2 uma unidade em $\mathbb{Z}C_7$. Se $\varphi(u_2) = \eta_2^3$, então $u_2 = -1+2x^2-x^3-x^4+2x^5$ e $u_2^{-1} = -3+2x+x^2+3x^3+3x^4+x^5-2x^6$. Caso $\varphi(u_2) = \eta_2^n$, então $3|n$.*

Demonstração. Temos que

$$\varphi(u_2) = \eta_2^3 = (\alpha^2+\alpha^{-2})^3 = \alpha+3\alpha^2+3\alpha^5+\alpha^6$$

Portanto,

$$u_2 \in x+3x^2+3x^5+x^6+\ker\varphi$$

Logo,

$$u_2 = x+3x^2+3x^5+x^6+a\sum_{i=0}^{6}x_i$$

Calculando o aumento de u_2, temos

$$\pm 1 = \varepsilon(u_2) = 1+3+3+1+7a = 8+7a, \quad a \in \mathbb{Z}$$

Portanto, $a = -1$ e assim, obtemos

$$u_2 = -1+2x^2-x^3-x^4+2x^5$$

Além disso, um cálculo simples mostra que

$$u_2^{-1} = -3-2x+x^2+3x^3+3x^4+x^5-2x^6$$

Vejamos agora que não ocorre $\varphi(u) = \eta_2^k$, quando $k = 1$ ou $k = 2$, $\forall u \in \mathcal{U}(\mathbb{Z}C_7)$.

Se $k = 1$, temos que

$$\varphi(u) = \eta_2 = \alpha^2+\alpha^{-2} = \alpha^2+\alpha^5$$

Assim, $a_2 = 1$ e $a_5 = 1$. Portanto,

$$u = x^2 + x^5 + a\sum_{i=0}^{6} x_i$$

Temos assim que

$$\left.\begin{array}{l} \pm 1 = \varepsilon(u) = 1 + 1 + 7a = 2 + 7a \\ \varepsilon(u) = \pm 1 \end{array}\right\} \Rightarrow 2 + 7a = \pm 1, \quad \text{com } a \in \mathbb{Z}$$

Portanto, $\varphi(u) = \eta_2$ não ocorre. Se $k = 2$, temos que

$$\varphi(u) = \eta_2^2 = (\alpha^2 + \alpha^{-2})^2 = 2 + \alpha^3 + \alpha^4$$

Logo,

$$u = 2 + x^3 + x^4 + a\sum_{i=0}^{6} x_i$$

Calculando o aumento de u, chegamos a uma contradição novamente:

$$\left.\begin{array}{l} \varepsilon(u) = 2 + 1 + 1 + 7a = 2 + 7a \\ \varepsilon(u) = \pm 1 \end{array}\right\} \Rightarrow 4 + 7a = \pm 1, \quad \text{com } a \in \mathbb{Z}$$

Portanto, $\varphi(u) = \eta_2^2$ não ocorre.

Agora seja $u_0 \in \mathcal{U}(\mathbb{Z}C_7)$ tal que $\varphi(u_0) = \eta_2^n$. Vejamos que $3|n$. Escrevendo $n = 3q + r$, para algum $q \in \mathbb{Z}$, temos que $r \in \{0, 1, 2\}$.

Se $r = 1$, temos

$$\varphi(u_0) = \eta_2^{3q}\eta_2 = (\eta_2^3)^q\eta_2 = (\varphi(u_2))^q\eta_2 = (\varphi(u_2^q))\eta_2$$

Logo,

$$\varphi(u_2^{-q}u_0) = \eta_2$$
$$u_2^{-q}u_0 = u_2^{'} \in \mathcal{U}(\mathbb{Z}C_7)$$

Já que, $u_0, u_2^{-q} \in \mathcal{U}(\mathbb{Z}C_7)$, temos que $u_2' = u_0u_2^{-q} \in \mathcal{U}(\mathbb{Z}C_7)$. Portanto, temos $\varphi(u_2^{'}) = \eta_2$ com $u_2^{'} \in \mathcal{U}(\mathbb{Z}C_7)$, o que é uma contradição pelo que foi visto acima. Logo, $r \neq 1$.Se $r = 2$,

$\varphi(u_0) = \eta_2^{3q}\eta_2^2$. Então se $u_2' = u_1^{-q}u_0 \in \mathcal{U}(\mathbb{Z}G)$, temos

$$\varphi(u_2') = \varphi(u_1^{-q}u_0) = \eta_2^{-3q}\eta_2^{3q}\eta_2^2 = \eta_2^2$$

Portanto, $\varphi(u_2^{'}) = \eta_2^2$ com $u_2^{'} \in \mathcal{U}(\mathbb{Z}C_7)$, o que é um absurdo. Logo, $r \neq 2$. Assim, concluímos que $r = 0$. Portanto, $n = 3q$, ié, $3|n$, como queríamos. □

Lema 2.1.4. *Seja u_3 uma unidade em $\mathbb{Z}C_7$. Se $\varphi(u_3) = \eta_1\eta_2^2$, então $u_3 = -1 + x + x^6$ e $u_3^{-1} = -1 + x - x^3 - x^4 + x^6$. Caso $\varphi(u_3) = \eta_1^r\eta_2^s$ e $3 \nmid s$, $3 \nmid r$, então $r \not\equiv s \pmod 3$.*

Demonstração. Primeiramente vamos mostrar a primeira parte do lema. Temos que

$$\varphi(u_3) = \eta_1\eta_2^2 \;=\; (\alpha + \alpha^{-1})(\alpha^2 + \alpha^{-2})^2 = 2\alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + 2\alpha^6$$

Portanto,

$$u_3 = 2x + x^2 + x^3 + x^4 + x^5 + 2x^6 + a\sum_{i=0}^{6} x_i$$

Logo, calculando o aumento de u_3, encontramos a:

$$\left.\begin{array}{l} \varepsilon(u_3) = 2 + 4 + 2 + 7a = 8 + 7a \\ \varepsilon(u_3) = \pm 1 \end{array}\right\} \Rightarrow a = -1$$

Assim, vem que

$$u_3 = -1 + x + x^6$$

E como $(-1 + x + x^6)(1 + x - x^3 - x^4 + x^6) = 1$, temos que

$$u_3^{-1} = 1 + x - x^3 - x^4 + x^6.$$

Agora vejamos que se $u \in \mathcal{U}(\mathbb{Z}C_7)$, então $\varphi(u) = \eta_1\eta_2$ não ocorre. Temos que

$$\varphi(u) \;=\; \eta_1\eta_2 = (\alpha^1 + \alpha^{-1})(\alpha^2 + \alpha^{-2}) = \alpha + \alpha^3 + \alpha^4 + \alpha^6$$

Portanto

$$u = x + x^3 + x^4 + x^6 + a\sum_{i=0}^{6} x_i$$

Assim,

$$\left.\begin{array}{l}\varepsilon(u) = 1+1+1+1+7a = 2+7a \\ \varepsilon(u) = \pm 1\end{array}\right\} \Rightarrow 4+7a = \pm 1, \quad \text{com } a \in \mathbb{Z}.$$

Portanto, $\varphi(u) = \eta_1\eta_2$ não ocorre. O mesmo acontece quando $\varphi(u) = \eta_1^2\eta_2^2$, $u \in \mathcal{U}(\mathbb{Z}C_7)$:

Temos

$$\varphi(u) = \eta_1^2\eta_2^2 = (\alpha^1+\alpha^{-1})^2(\alpha^2+\alpha^{-2})^2 = 4+\alpha+3\alpha^2+2\alpha^3+2\alpha^4+3\alpha^5+\alpha^6$$

Logo,

$$u = 4+x+3x^2+2x^3+2x^4+3x^5+x^6$$

Calculando o aumento de u, chegamos novamente a uma contradição:

$$\left.\begin{array}{l}\varepsilon(u) = 4+1+3+2+2+3+1 = 16 \\ \varepsilon(u) = \pm 1\end{array}\right\} \Rightarrow 16 = \pm 1,$$

Portanto, $\varphi(u) = \eta_1^2\eta_2^2$ não ocorre. Agora seja $u_0 \in \mathcal{U}(\mathbb{Z}C_7)$.

Considere $\varphi(u_0) = \eta_1^r\eta_2^s$, onde, $3 \nmid r$ e $3 \nmid s$. Como $3 \nmid r$, então podemos escrever $r = 3q+s_1$, para algum $q \in \mathbb{Z}$, onde $s_1 = 1$ ou $s_1 = 2$ e como $3 \nmid s$, então para algum $p \in \mathbb{Z}$, $s = 3p+r_1$, onde $r_1 = 1$ ou $r_1 = 2$.

Suponha por absurdo que $r \equiv s(\mod 3)$. Temos que $r-s = 3(q-p)++(r_1-s_1)$. Como $r \equiv s(\mod 3)$, então $s_1 = r_1$.

Se $s_1 = r_1 = 1$, então $\varphi(u_0) = \eta_1^{3q+1}\eta_2^{3p+1}$. Portanto, $\varphi(u_0u_1^{-q}u_2^{-p}) = \eta_1\eta_2$, o que é uma contradição pelo que foi visto acima.

Analogamente, para $s_1 = r_1 = 2$, temos que $\varphi(u_0u_1^{-q}u_2^{-p}) = \eta_1^2\eta_2^2$ e chegamos mais uma vez a um absurdo. Logo, temos que $r \not\equiv s(\mod 3)$, como queríamos. □

Teorema 2.1.1. *Seja $\mathcal{U}(\mathbb{Z}C_7)$ o grupo de unidades de $\mathbb{Z}C_7$, onde $C_7 = \langle x\rangle$ é um grupo cíclico de ordem 7. Então $\mathcal{U}(\mathbb{Z}C_7) = \langle -1\rangle \times \langle x\rangle \times \langle u_2\rangle \times \langle u_3\rangle$, onde u_2 e u_3 são como nos Lemas 2.1.3 e 2.1.4.*

Demonstração. Seja $u \in \mathcal{U}(\mathbb{Z}C_7)$. Então $\varphi(u) \in \mathcal{U}(\mathbb{Z}[\alpha])$. Pelo Lema 2.1.1,

$$\varphi(u) = (-1)^i\alpha^j\eta_1^k\eta_2^n,$$

com i, j, k, n inteiros apropriados. Logo, $\varphi((-1)^i x^{-j} u) = \eta_1^k \eta_2^n$.

Sendo $k = 3p + r$ e $n = 3t + s$, com $p, t \in \mathbb{Z}$ e $r, s \in \{0, 1, 2\}$ temos

$$\varphi((-1)^i x^{-j} u) \quad = \quad \eta_1^{3p} \eta_1^r \eta_2^{3t} \eta_2^s = (\eta_1^3)^p (\eta_2^3)^q \ \eta_1^r \eta_2^s$$

Então pelos Lemas 2.1.2 e 2.1.3, temos

$$\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u) = \eta_1^r \eta_2^s$$

Se 3|r, então $r = 0$, já que $r = 0$ ou $r = 1$ ou $r = 2$. Assim,

$$\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u) = \eta_2^s$$

Logo, pelo Lema 2.1.3, $3|s$ e, portanto, $s = 0$. Nesse caso, temos $\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u) = = 1$.

Se $3|s$, então, analogamente, $s = r = 0$ e novamente, temos que $\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u) = = 1$.

Se $3 \nmid s$, $3 \nmid r$, pelo lema 2.1.4, $r \not\equiv s(\mod 3)$. Portanto, $r = 1$ e $s = 2$ ou $r = 2$ e $s = 1$. Nesse caso, pelo Lema 2.1.4, temos

$$\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u) = \eta_1 \eta_2^2 = \varphi(u_3)$$

E, portanto,

$$\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u_3^{-1} u) = 1$$

Para $r = 2$ e $s = 1$, temos que

$$\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u) = \eta_1^2 \eta_2 = \eta_1^3 \eta_2^3 \eta_1^{-1} \eta_2^{-2} = \eta_1^3 \eta_2^3 (\eta_1 \eta_2^2) = \varphi(u_1)\varphi(u_2)\varphi(u_3)^{-1}$$

pelos Lemas 2.1.2, 2.1.3 e 2.1.4.

Portanto,

$$\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u u_1^{-1} u_2^{-1} u_3) = 1$$

Temos que φ é injetor sobre o grupo de unidades do anel $\mathbb{Z}C_7$.

Considere o homomorfismo de grupos

$$\varphi \restriction_{\mathcal{U}(\mathbb{Z}C_7))}: \mathcal{U}(\mathbb{Z}C_7) \longrightarrow \mathcal{U}\mathbb{Z}[\alpha]$$

Seja $u \in \ker(\varphi \restriction \mathcal{U}(\mathbb{Z}C_7))$. Portanto $\varphi(u) \in \mathcal{U}(\mathbb{Z}[\alpha])$ e $\varphi(u) = 1$.

Temos,

$$u = 1 + \underbrace{a\sum_{i=0}^{6} x^i}_{\in \ker \varphi}$$

$$\pm 1 = \varepsilon(u) = 1 + 7a \Rightarrow a = 0$$

Portanto, $u = 1$. Assim, $\ker(\varphi \restriction \mathcal{U}(\mathbb{Z}C_7)) = 1$.Concluímos assim que φ é injetora sobre $\mathcal{U}(\mathbb{Z}C_7)$.

Agora podemos encontrar u em cada caso:

Para $r = s = 0$:

$$\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u) = 1 \Rightarrow \varphi(u) = \varphi((-1)^i x^j u_1^p u_2^t)$$

Portanto, temos que $u = (-1)^i x^j u_1^p u_2^t$. Para $r = 1$ e $s = 2$:

$$\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u_3^{-1} u) = 1 \Rightarrow \varphi(u) = \varphi((-1)^i x^j u_1^p u_2^t u_3)$$

Logo, $u = (-1)^i x^j u_1^p u_2^t u_3$. Para $r = 2$ e $s = 1$:

$$\varphi((-1)^i x^{-j} u_1^{-p} u_2^{-t} u_1^{-1} u_2^{-1} u_3 u) = 1 \Rightarrow \varphi(u) = \varphi((-1)^i x^j u_1^{p+1} u_2^{t+1} u_3^{-1})$$

Portanto, temos que $u = (-1)^i x^j u_1^{p+1} u_2^{t+1} u_3^{-1}$. Como $\eta_1^3 = (\eta_1\eta_2^2)^3(\eta_2^3)^{-2}$, então $\varphi(u_1) = \varphi(u_3)^3\varphi(u_2)^{-2}$. Assim, $\varphi(u_1) = \varphi(u_3^3 u_2^{-2})$. Logo, $u_1 = u_3 u_2^{-2}$. Portanto temos que

$$\langle u_1, u_2, u_3 \rangle = \langle u_2, u_3 \rangle$$

Assim, segue o resultado.

□

Antes de começarmos a próxima seção, vamos relembrar dois conceitos que serão utilizados

na mesma. Os resultados abaixo podem ser encontrados em [12].

Relembrando o que definimos anteriormente, dizemos que z é uma **raiz n-ésima da unidade** quando $z^n = 1$, ou seja, quando z for uma das raízes do polinômio $X^n - 1$. Uma raiz n-ésima da unidade ω é dita **primitiva** quando os números ω^k, com $0 \leqslant k \leqslant n-1$, forem todos distintos. Em particular, $\cos\dfrac{2\pi}{n}$ é uma raiz primitiva n-ésima da unidade e temos que $\cos\dfrac{2k\pi}{n}$ é uma raiz primitiva n-ésima da unidade se, e somente se, $mdc(k,n) = 1$.

Seja ω uma raiz primitiva da unidade de ordem m. É fácil ver que ω é um gerador para o grupo cíclico $R = \{1, \omega, \omega^2, \ldots, \omega^{m-1}\}$ e ω^j é uma raiz primitiva da unidade de ordem m se, e somente se, j e m são relativamente primos. Seja P_m o conjunto das raízes primitivas da unidade de ordem m. O **polinômio ciclotômico** ϕ_m é definido por

$$\phi_m(X) = \prod_{\epsilon \in P_m} (X - \epsilon)$$

Proposição 2.1.1. *Temos que o itens abaixo se verificam, nas condições:*

1. $\phi_1(X) = X - 1$
2. *Se p é primo, então* $\phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$
3. $X^n - 1 = \displaystyle\prod_{d|n} \phi_d(X)$
4. $\phi_n(X) = \displaystyle\prod_{\substack{1 \leqslant k \leq n \\ mdc(k,n)=1}} (X - \omega^k)$

Teorema 2.1.2. *Para todo $m \geqslant 1$, o polinômio ciclotômico ϕ_m é irredutível sobre $\mathbb{Q}$.*

Definição 2.1.1. *Seja K uma extensão de $\mathbb{Q}$. Seja β tal que $\{\beta_1, \beta_2, \ldots, \beta_n\}$ seja uma base para $\mathbb{Q}(\beta)$. Então a norma de β é $N(\beta) = \det(a_{ij})$, onde $\beta\omega_i = \displaystyle\sum_{j=1}^{n} a_{ij}\omega_j$, onde $\omega_i = \beta^i$, com $i = 1, 2, \ldots, n$.*

2.2 Unidades de anéis de grupo integrais de grupos cíclicos de ordem 9

Já que $(x^9-1)=\prod_{d|9}\phi_d(x)=\phi_1(x)\phi_3(x)\phi_9(x)$ e $\phi_1(x)=x-1$ e $\phi_3(x)=x^2+x+1$, temos $\phi_9(x)=\dfrac{x^9-1}{x^3-1}=x^6+x^3+1$, que é o polinômio ciclotômico de ordem 9.

Seja α é uma raiz primitiva da unidade de ordem 9 e consideremos $\lambda=\alpha+\alpha^8$ e $\mu=\alpha^4+\alpha^5$.

Sejam $K=\mathbb{Q}(\alpha)$, onde $\mathbb{Q}$ denota o corpo dos números racionais, $P=\langle 1-\alpha^i : 1,\ldots,8\rangle$ o subgrupo do grupo multiplicativo de K, $\mathbb{Z}[\alpha]$, anel dos inteiros ciclotômicos de ordem 9, $\mathcal{U}(\mathbb{Z}[\alpha])$ o grupo de unidades de $\mathbb{Z}[\alpha]$ e $C=P\cap\mathcal{U}(\mathbb{Z}[\alpha])$, subgrupo do grupo das unidades ciclotômicas.

Lema 2.2.1. *$\mathcal{U}(\mathbb{Z}[\alpha])=C$, isto é, qualquer unidade do anel $\mathbb{Z}[\alpha]$ é uma unidade ciclotômica.*

Demonstração. Para esse resultado veja [2]. □

Teorema 2.2.1. *O grupo de unidades do anel dos inteiros ciclotômicos de grau 9 é $\mathcal{U}(\mathbb{Z}[\alpha])=\langle -1\rangle\times\langle\alpha\rangle\times\langle\lambda\rangle\times\langle\mu\rangle$.*

Demonstração. Temos, para $0\leqslant j\leqslant 8$,

$$1-\alpha^{9-j}=1-\alpha^9\alpha^{-j}=1-\alpha^{-j}=(-\alpha^{-j})(1-\alpha^j)$$

e

$$(1-\alpha)(1-\alpha^2)(1-\alpha^4)=(-\alpha^2)(1-\alpha^3),$$

já que α é raiz do polinômio ciclotômico $\phi_9(x)=x^6+x^3+1$. Temos então:

$$\begin{aligned}
(1-\alpha^3) &= (-\alpha^{-2})(1-\alpha)(1-\alpha^2)(1-\alpha^4)\\
(1-\alpha^5) &= (-\alpha^{-4})(1-\alpha^4)\\
(1-\alpha^6) &= (-\alpha^{-3})(-\alpha^{-2})(1-\alpha)(1-\alpha^2)(1-\alpha^4)\\
(1-\alpha^7) &= (-\alpha^{-2})(1-\alpha^2)\\
(1-\alpha^8) &= (-\alpha^{-1})(1-\alpha)
\end{aligned}$$

Portanto,

$$u\in C=\mathcal{U}(\mathbb{Z}[\alpha])\Rightarrow u=(-\alpha^j)(1-\alpha)^n(1-\alpha^2)^p(1-\alpha^4)^r,$$

para j, n, p, r inteiros apropriados.

Seja N a norma da extensão K sobre $\mathbb{Q}$. Temos que $N(1-\alpha^j) = 3$ para $j = 1$, $j = 2$ e $j = 4$ e $N(-\alpha) = 1$. De fato,

Temos $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$, já que $\phi_1(x) = x^6 + x^3 + 1$. Portanto uma base de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-espaço vetorial é $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$ (ver [3]).

Fazendo

$$(1-\alpha)\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j, \quad \omega_i = \alpha^i; i = 0, 1, 2, 3, 4, 5.$$

Então $N(1-\alpha) = det(a_{ij})$.Temos ainda

$$\begin{aligned}
(1-\alpha)1 &= 1 + (-1)\alpha + 0\alpha^2 + 0\alpha^3 + 0\alpha^4 + 0\alpha^5 \\
(1-\alpha)\alpha &= 0\cdot 1 + \alpha + (-1)\alpha^2 + 0\alpha^3 + 0\alpha^4 + 0\alpha^5 \\
(1-\alpha)\alpha^2 &= 0\cdot 1 + 0\alpha + 1\alpha^2 + (-1)\alpha^3 + 0\alpha^4 + 0\alpha^5 \\
(1-\alpha)\alpha^3 &= 0\cdot 1 + 0\alpha + 0\alpha^2 + 1\alpha^3 + (-1)\alpha^4 + 0\alpha^5 \\
(1-\alpha)\alpha^4 &= 0\cdot 1 + 0\alpha + 0\alpha^2 + 0\alpha^3 + 1\alpha^4 + (-1)\alpha^5 \\
(1-\alpha)\alpha^5 &= 1\cdot 1 + 0\alpha + 0\alpha^2 + 1\alpha^3 + 0\alpha^4 + 1\alpha^5
\end{aligned}$$

Portanto,

$$N(1-\alpha) = \begin{vmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{vmatrix} = 3$$

Analogamente,

$$\begin{aligned}
(1-\alpha^2)1 &= 1 - \alpha^2 \\
(1-\alpha^2)\alpha &= \alpha - \alpha^3 \\
&\vdots \\
(1-\alpha^2)\alpha^4 &= 1 + \alpha^3 + \alpha^4 \\
(1-\alpha^2)\alpha^5 &= \alpha + \alpha^4 + \alpha^5
\end{aligned}$$

Logo,

$$N(1-\alpha^2) = \begin{vmatrix} 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{vmatrix} = 3$$

e

$$\begin{aligned} (1-\alpha^4)1 &= 1-\alpha^4 \\ (1-\alpha^4)\alpha &= \alpha-\alpha^5 \\ (1-\alpha^4)\alpha^2 &= \alpha^2-\alpha^6 = \alpha^2+\alpha^3+1 \\ (1-\alpha^4)\alpha^3 &= \alpha^3+-\alpha^7 = \alpha^3+\alpha^4+\alpha \\ (1-\alpha^4)\alpha^4 &= \alpha^4-1\alpha^8 = \alpha^4+\alpha^5+\alpha^2 \\ (1-\alpha^4)\alpha^5 &= \alpha^5-1 \end{aligned}$$

Assim,

$$N(1-\alpha^4) = \begin{vmatrix} 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 1 \end{vmatrix} = 3$$

Temos também

$$N(-\alpha) = \begin{vmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{vmatrix} = 1$$

Portanto,

$$\begin{aligned} N(u) &= N((-\alpha)^j)N((1-\alpha)^n)N((1-\alpha^2)^p)N((1-\alpha^4)^r) = \\ &= (N(-\alpha)^j)(N(1-\alpha))^n(N(1-\alpha^2))^p(N(1-\alpha^4))^r = \\ &= 1^j 3^n 3^p 3^r \end{aligned}$$

Mas $N(u) = 1$. Portanto, $n + p + r = 0$. Deste modo,

$$(1-\alpha)^n = (1-\alpha)^{-p-r} = (1-\alpha)^{-p}(1-\alpha)^{-r}$$

Logo,

$$u = (-\alpha)^{-j}\left(\frac{1-\alpha^2}{1-\alpha}\right)^p\left(\frac{1-\alpha^4}{1-\alpha}\right)^r$$

Como

$$\left(\frac{1-\alpha^2}{1-\alpha}\right) = (1+\alpha) \quad \text{e} \quad \left(\frac{1-\alpha^4}{1-\alpha}\right) = (1+\alpha)(1+\alpha^2)$$

e

$$\lambda = \alpha + \alpha^8 = \alpha^8(1+\alpha^2) = \alpha^{-1}(1+\alpha^2)$$
$$\mu = \alpha^4 + \alpha^5 = \alpha^4(1+\alpha)$$

Portanto, segue que

$$\mathcal{U}(\mathbb{Z}[\alpha]) = \langle -1\rangle \times \langle \alpha\rangle \times \langle \lambda\rangle \times \langle \mu\rangle$$

□

A partir de agora, consideremos $C_9 = \langle x\rangle$ um grupo cíclico de ordem 9. Sejam os seguintes homomorfismos de anéis:

$$\begin{aligned} \varphi: \quad \mathbb{Z}C_9 &\longrightarrow \mathbb{Z}[\alpha] \\ \sum_{i=0}^{8} a_i x^i &\longmapsto \sum_{i=0}^{8} a_i \alpha^i, \end{aligned}$$

$$\begin{aligned} \tau: \quad \mathbb{Z}C_9 &\longrightarrow \mathbb{Z}[\alpha^3] \\ \sum_{i=0}^{8} a_i x^i &\longmapsto \sum_{i=0}^{8} a_i \alpha^{3i} \end{aligned}$$

$$\begin{array}{rccc} \varepsilon: & \mathbb{Z}C_9 & \longrightarrow & \mathbb{Z} \\ & \displaystyle\sum_{i=0}^{8} a_i x^i & \mapsto & \displaystyle\sum_{i=0}^{8} a_i \end{array}$$

Lema 2.2.2. *(1)* $\ker\varphi = \left\{ \displaystyle\sum_{i=0}^{2} c_i x^i (1 + x^3 + x^6) : c_0, c_1, c_2 \in \mathbb{Z} \right\}$

(2) $\mathcal{U}(\mathbb{Z}[\alpha^3]) = \{\pm 1, \pm\alpha^3, \pm(1+\alpha^3)\}$

Demonstração. É fácil ver que

$$c_0(1 + x^3 + x^6) + c_1 x(1 + x^3 + x^6) + c_2 x^2(1 + x^3 + x^6) \in \ker\varphi.$$

Agora seja $a \in \ker\varphi$. Então $a = a_0 + a_1 x + a_2 x^2 + \cdots + a_8 x^8$ e $\varphi(a) = 0$. Logo, $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_8\alpha^8 = 0$. Já que $\phi_9(x) = 1 + x^3 + x^6$, então $1 + \alpha^3 + \alpha^6 = 0$. Portanto,

$$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5 + a_6(-\alpha^3 - 1) + a_7\alpha^7 + a_8\alpha^8 = 0$$

e $a_0 = a_6 = a_3$. Chamando $a_0 = c_0$, temos

$$\begin{aligned} c_0 + a_1\alpha + a_2\alpha^2 + c_0\alpha^3 + a_4\alpha^4 + a_5\alpha^5 + c_0\alpha^6 + a_7\alpha^7 + a_8\alpha^8 &= 0 \Rightarrow \\ \Rightarrow \alpha(a_1 + a_2\alpha + a_4\alpha^3 + a_5\alpha^4 + a_7\alpha^6 + a_8\alpha^7) &= 0 \end{aligned}$$

Como $\alpha \neq 0$, temos $a_1 = a_4 = a_7$. Assim, chamando $a_1 = c_1$

$$\begin{aligned} c_1 + a_2\alpha + c_1\alpha^3 + a_5\alpha^4 + c_1\alpha^6 + a_8\alpha^7 &= 0 \Rightarrow \\ \Rightarrow \alpha(a_2 + a_5\alpha^3 + a_8\alpha^6) &= 0, \end{aligned}$$

o que implica $a_2 = a_5 = a_8$. Chamando $a_2 = c_2$, temos,

$$\varphi(a) = c_0 + c_1\alpha + c_2\alpha^2 + c_0\alpha^3 + c_1\alpha^4 + c_2\alpha^5 + c_0\alpha^6 + c_1\alpha^7 + c_2\alpha^8$$

Portanto,

$$\begin{aligned} a &= c_0(1+x^3+x^6)+c_1(x+x^4+x^7)+c_2(x^2+x^5+x^8) \\ &= c_0(1+x^3+x^6)+c_1x(1+x^3+x^6)+c_2x^2(1+x^3+x^6) \\ &= (c_0+c_1x+c_2x^2)(1+x^3+x^6)=\sum_{i=0}^{2}c_ix^i(1+x^3+x^6) \end{aligned}$$

Logo,

$$\ker\varphi=\left\{\sum_{i=0}^{2}c_ix^i(1+x^3+x^6):\quad c_0,c_1c_2\quad\in\mathbb{Z}\right\}$$

Para demonstração de *(2)*, veja [3], capítulo 2, parágrafo 7. □

Lema 2.2.3. *Seja $u_1\in\mathbb{Z}C_9$. Então,*

(a) Se $\varphi(u_1)=\lambda^3$, então $u_1=-1+2(x+x^8)-(x^2+x^7)-(x^4+x^5)$ e $u_1^{-1}=5+(x+x^8)-5(x^2+x^7)-3(x^3+x^6)+4(x^4+x^5)$.

(b) Se $\varphi(u_1)=\lambda^k$, então $3|k$.

Demonstração. (a) Temos que

$$\varphi(u_1)=\lambda^3=(\alpha+\alpha^8)^3=3\alpha+\alpha^3+\alpha^6+3\alpha^8$$

Portanto,

$$u_1\in 3\alpha+\alpha^3+\alpha^6+3\alpha^8+\ker\varphi$$

Então,

$$\begin{aligned} u_1 &= 3x+x^3+x^6+3x^8+c_0(1+x^3+x^6)+c_1(x+x^4+x^7)+ \quad (2.1)\\ &+ c_2(x^2+x^5+x^8) \quad (2.2)\end{aligned}$$

Portanto,

$$\left.\begin{array}{l}\varepsilon(u_1)=3+1+1+3+3c_0+3c_1+3c_2=8+3(c_0+c_1+c_2)\\ \varepsilon(u_1)=\pm1, \text{já que } u_1\in\mathcal{U}(\mathbb{Z}C_9)\end{array}\right\}\Rightarrow c_0+c_1+c_2=-3$$

Agora vamos calcular $\tau(u_1)$.

$$\begin{aligned}\tau(u_1) &= 3\alpha^3+\alpha^9+\alpha^{18}+3\alpha^{24}+c_0(1+\alpha^9+\alpha^{18})+c_1(\alpha^3+\alpha^{12}+\alpha^{21})+\\ &\quad +c_2(\alpha^6+\alpha^{15}+\alpha^{24})=\\ &= 3\alpha^3+1+1+3\alpha^6+c_0(1+1+1)+c_1(3\alpha^3)+c_2(3\alpha^6)=\\ &= (2+3c_0)+(3c_1+3)\alpha^3+(3c_2+3)\alpha^6\end{aligned}$$

Temos que $\alpha^6=-\alpha^3-1$ e, portanto,

$$\begin{aligned}\tau(u_1) &= 2+3c_0+(3c_1+3)\alpha^3+(3c_2+3)(-\alpha^3-1)=\\ &= 3c_0-3c_2-1+\alpha^3(3c_1-3c_2)\end{aligned}$$

Mas $\tau(u_1)\in\mathcal{U}(\mathbb{Z}[\alpha^3])=\{\pm1,\pm\alpha^3,\pm(1+\alpha^3)\}$. Assim, analisando caso a caso, temos que a única possibilidade é $3c_0-3c_2-1+\alpha^3(3c_1-3c_2)=-1$ e daí segue que $c_0=c_1=c_2$. Como $c_0+c_1+c_2=-3$, temos $c_0=c_1=c_2=-1$.

Portanto,

$$u_1=-1+2(x+x^8)-(x^2+x^7)-(x^4+x^5)$$

e, um cálculo simples mostra que

$$u_1^{-1}=5+(x+x^8)-5(x^2+x^7)-3(x^3+x^6)+4(x^4+x^5).$$

(b) Agora se $\varphi(u)=\lambda=\alpha+\alpha^8$, para qualquer u em $\mathcal{U}(\mathbb{Z}C_9)$, temos que $u\in x+x^8+\ker\varphi$ e, portanto, $u=x+x^8+c_0(1+x^3+x^6)+c_1(x+x^4++x^7)+c_2(x^2+x^5+x^8)$.

Portanto, temos $\varepsilon(u)=1+1+3(c_0+c_1+c_2)$. Logo, $3(c_0+c_1+c_2)=\pm1-2$. Assim, $c_0+c_1+c_2=-1$. Logo,

$$\begin{aligned}\tau(u) &= \alpha^3+\alpha^{24}+c_0(1+\alpha^9+\alpha^{18})+c_1(\alpha^3+\alpha^{12}+\alpha^{21})+c_2(\alpha^6+\alpha^{15}+\alpha^{24})=\\ &= \alpha^3+(-\alpha^3-1)+3c_0+3c_1\alpha^3+3c_2(-\alpha^3-1)=\\ &= (-1+3c_0-3c_2)+3(c_1+c_2)\alpha^3\end{aligned}$$

E, nesse caso, já vimos que $c_0=c_1=c_2$. Portanto, $3c_0=-1$, que é um absurdo, pois $c_0\in\mathbb{Z}$. Deste modo, $\varphi(u)=\lambda$ não ocorre, qualquer que seja $u\in\mathcal{U}(\mathbb{Z}C_9)$.

Vejamos agora o caso em que $\varphi(u)=\lambda^2$, para $u\in\mathcal{U}(\mathbb{Z}C_9)$ qualquer. Temos que $\varphi(u)=$

$\alpha^2 + 2 + \alpha^7$ e assim,

$$u = 2 + x^2 + x^7 + c_0(1 + x^3 + x^6) + c_1(x + x^4 + x^7) + c_2(x^2 + x^5 + x^8)$$

Logo,

$$\varepsilon(u) = 2 + 1 + 1 + 3(c_0 + c_1 + c_2) = 4 + 3(c_0 + c_1 + c_2) \Rightarrow$$
$$\Rightarrow c_0 + c_1 + c_2 = -1$$

e temos também

$$\begin{aligned} \tau(u) &= 2 + \alpha^6 + \alpha^{21} + 3c_0 + 3c_1\alpha^3 + 3c_2\alpha^6 = \\ &= (1 + 3c_0 - 3c_2) + 3(c_1 - c_2)\alpha^3 \end{aligned}$$

Como $\tau(u) \in \mathcal{U}(\mathbb{Z}[\alpha^3]) = \{\pm 1, \pm\alpha^3, \pm(1 + \alpha^3)\}$, segue

$$3c_0 - 3c_2 + 1 = 1 \quad e \quad 3c_1 - 3c_2 = 0$$

e, portanto,

$$c_0 = c_1 = c_2 = -\frac{1}{3}$$

Assim, $\varphi(u) = \lambda^2$ não ocorre, qualquer que seja $u \in \mathcal{U}(\mathbb{Z}C_9)$. Agora seja $u_0 \in \mathcal{U}(\mathbb{Z}C_9)$ tal que $\varphi(u_0) = \lambda^k$. Dividindo k por 3, temos $k = 3q + r$, com $q \in \mathbb{Z}, 0 \leqslant r < 3$. Temos que $\varphi(u_0) = \lambda^{3q}\lambda^r = (\lambda^3)^q\lambda^r = \varphi(u_1)^q\lambda^r$. Assim, $\varphi(u_0)\varphi(u_1)^{-q} = = \lambda^r \Rightarrow \varphi(u_0u_1^{-q}) = \lambda^r$. Chamando $u_1' = u_0u_1^{-q} \in \mathcal{U}(\mathbb{Z}C_9)$, temos que $\varphi(u_1') = \lambda^r$. Como $\varphi(u_1') = \lambda$ e $\varphi(u_1') = \lambda^2$ não ocorrem, temos que $r = 0$. Logo, $k = 3q$, ou seja, $3|k$.

□

Lema 2.2.4. *Seja* $u_2 \in \mathcal{U}(\mathbb{Z}C_9)$

(a) Se $\varphi(u_2) = \mu^3$, *então* $u_2 = -1 - (x + x^8) - (x^2 + x^7) + 2(x^4 + x^5)$ *e* $u_2^{-1} = 5 - 5(x + x^8) + 4(x^2 + x^7) - 3(x^3 + x^6) + (x^4 + x^5)$.

(b) Se $\varphi(u_2) = \mu^n$, *então* $3|n$.

Demonstração. (a) Temos que $\varphi(u_2) = \mu^3 = (\alpha^4 + \alpha^5)^3 = -1 + 3\alpha^4 + 3\alpha^5$. Então,

$$u_2 = -1 + 3x^4 + 3x^5 + c_0(1 + x^3 + x^6) + c_1(x + x^4 + x^7) + c_2(x^2 + x^5 + x^8).$$

Portanto,

$$\left.\begin{array}{l}\varepsilon(u_2) = -1+3+3+3(c_0+c_1+c_2) = 5+3(c_0+c_1+c_2)\\ \varepsilon(u_2) = \pm 1\end{array}\right\} \Rightarrow c_0+c_1+c_2 = -2$$

Agora vamos calcular $\tau(u_2)$. Lembramos que τ é o homomorfismo de anéis que leva $\mathbb{Z}C_9$ em $\mathbb{Z}[\alpha^3]$ dado por

$$\tau(\sum_{i=0}^{8} a_i x^i) = \sum_{i=0}^{8} a_i \alpha^{3i}$$

Assim,

$$\begin{array}{rcl}\tau(u_2) & = & -1+3\alpha^{12}+3\alpha^{15}+3c_0+3c_1\alpha^3+3c_2\alpha^6 = \\ & = & (-4+3c_0-3c_2)+(3c_1-3c_2)\alpha^3\end{array}$$

mas, pelo Lema 2.2.2, $\tau(u_2) \in \mathcal{U}(\mathbb{Z}[\alpha^3]) = \{\pm 1, \pm\alpha^3, \pm(1+\alpha^3)\}$. Assim, temos que a única possibilidade é $3c_0-3c_2-4+\alpha^3(3c_1-3c_2) = -1$ e assim, $c_1 = c_2$. Como $c_0+c_1+c_2 = -2$, temos $c_0 = 0$ e $c_1 = c_2 = -1$. Com isso temos,

$$u_2 = -1-(x+x^8)-(x^2+x^7)+2(x^4+x^5),$$

como queríamos. Além disso, um cálculo rotineiro mostra que

$$u_2^{-1} = 5-5(x+x^8)+4(x^2+x^7)-3(x^3+x^6)+(x^4+x^5).$$

(b) Agora suponha que $\varphi(u) = \mu = \alpha^4+\alpha^5$, para algum $u \in \mathcal{U}(\mathbb{Z}C_9)$. Então,

$$u = x^4+x^5+c_0(1+x^3+x^6)+c_1(x+x^4+x^7)+c_2(x^2+x^5+x^8).$$

Assim,

$$\varepsilon(u) = 2+3(c_0+c_1+c_2) = \pm 1$$

Concluímos que

$$c_0+c_1+c_2 = -1$$

Temos também que

$$\begin{aligned}\tau(u) &= \alpha^3+\alpha^6+3c_0+c_1\alpha^3+3c_2\alpha^6\\ &= \alpha^3+(-\alpha^3-1)+3c_0+3c_1\alpha^3+3c_2(-\alpha^3-1)\\ &= (-1+3c_0-3c_2)+3(c_1-c_2)\alpha^3\end{aligned}$$

Pelo Lema 2.2.2, temos

$$-1+3c_0+-3c_2+\alpha^3(3c_1-3c_2)=-1$$

e daí $c_0=c_1=c_2$. Como $c_0+c_1+c_2=-1$, temos $3c_0=-1$, com $c_0\in\mathbb{Z}$, o que é um absurdo. Deste modo, $\varphi(u)=\mu$ não ocorre, qualquer que seja $u\in\mathcal{U}(\mathbb{Z}C_9)$. Suponha agora que $\varphi(u)=\mu^2=2+\alpha+\alpha^8$, para algum $u\in\mathcal{U}(\mathbb{Z}C_9)$. Temos que

$$u=2+x+x^8+c_0(1+x^3+x^6)+c_1(x+x^4+x^7)+c_2(x^2+x^5+x^8).$$

Portanto,

$$\varepsilon(u)=4+3(c_0+c_1+c_2)\ \Rightarrow c_0+c_1+c_2=-1$$

e também

$$\begin{aligned}\tau(u) &= 2+\alpha^3+\alpha^6+3c_0+3c_1\alpha^3+3c_2\alpha^6\\ &= (1+3c_0-3c_2)+3(c_1-c_2)\alpha^3.\end{aligned}$$

Já vimos que nesse caso $c_0=c_1=c_2$ e como $c_0+c_1+c_2=-1$, chegamos a uma contradição.

Assim $\varphi(u)=\mu^2$ não ocorre, para $u\in\mathcal{U}(\mathbb{Z}C_9)$. Agora seja $u_0\in\mathcal{U}(\mathbb{Z}C_9)$ tal que $\varphi(u_0)=\mu^n$. Dividindo n por 3, temos $n=3q+r$, com $q\in\mathbb{Z}, 0\leqslant r<3$. Temos

$$\varphi(u_0)=\mu^n=(\lambda^3)^q\lambda^r\Rightarrow\varphi(u_0)=\varphi(u_2)^q\mu^r=\varphi(u_2^q)\mu^r.$$

Portanto, $\varphi(u_0u_2^{-q})=\mu^r$. Chamando $u_2'=u_0u_2^{-q}\in\mathcal{U}(\mathbb{Z}C_9)$, temos que $\varphi(u_2')=\mu^r$.

Como $r=1$ e $r=2$ não ocorre, então $r=0$ e daí $3|n$, como queríamos.

□

Lema 2.2.5. *Seja* $u_3\in\mathcal{U}(\mathbb{Z}C_9)$

(a) Se $\varphi(u_3)=\lambda\mu^2$, *então* $u_3=1+(x+x^8)-(x^3+x^6)-(x^4+x^5)$ *e* $u_3^{-1}=-1+(x+x^8)-$

$(x^2 + x^7)$

(b) Se $\varphi(u_3) = \lambda^r \mu^s$, *e* $3 \nmid n$, $3 \nmid s$, *então* $r \not\equiv s (mod 3)$

Demonstração. (a) Se

$$\varphi(u_3) = \lambda\mu^2 = (\alpha + \alpha^8)(\alpha^4 + \alpha^5)^2 = 2 + 2\alpha + \alpha^2 + \alpha^7 + 2\alpha^8,$$

então

$$u_3 = 2 + 2x + x^2 + x^7 + 2x^8 + c_0(1 + x^3 + x^6) + c_1(x + x^4 + x^7) + c_2(x^2 + x^5 + x^8)$$

Temos

$$\left.\begin{array}{l} \varepsilon(u_3) = 8 + 3(c_0 + c_1 + c_2) = \\ \varepsilon(u_2) = \pm 1 \end{array}\right\} \Rightarrow c_0 + c_1 + c_2 = -3$$

Temos também

$$\begin{aligned} \tau(u_3) &= 2 + 2\alpha^3 + \alpha^6 + \alpha^{21} + \alpha^{24} + 3c_0 + 3c_1\alpha^3 + 3c_2\alpha^6 \\ &= (-1 + 3c_0 - 3c_1) + (3c_1 - 3c_2)\alpha^3 \end{aligned}$$

Anteriormente, vimos que, nesse caso, $3c_0 - 3c_2 - 1 + \alpha^3(3c_1 - 3c_2) = -1$ e daí vem que $c_0 = c_1 = c_2$. Como $c_0 + c_1 + c_2 = -3$, temos $c_0 = c_1 = c_2 = -1$. Portanto,

$$u_3 = 1 + (x + x^8) - (x^3 + x^6) - (x^4 + x^5),$$

como queríamos. Além disso, $u_3^{-1} = -1 + (x + x^8) - (x^2 + x^7)$.

(b) Vejamos agora o que acontece se $u \in \mathbb{Z}C_9$ é tal que $\varphi(u) = \lambda\mu$, para algum $u \in \mathcal{U}(\mathbb{Z}C_9)$. Temos

$$\varphi(u) = (\alpha + \alpha^8)(\alpha^4 + \alpha^5) = \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6.$$

Então,

$$u = x^3 + x^4 + x^5 + x^6 + c_0(1 + x^3 + x^6) + c_1(x + x^4 + x^7) + c_2(x^2 + x^5 + x^8).$$

Portanto,

$$\varepsilon(u) = 4 + 3(c_0 + c_1 + c_2) = \pm 1$$

Concluímos que

$$c_0 + c_1 + c_2 = -1$$

E temos também

$$\begin{aligned}\tau(u) &= \alpha^6+\alpha^{12}+\alpha^{15}+\alpha^{18}+3c_0+c_1\alpha^3+3c_2\alpha^6 = \\ &= (-1+3c_0-3c_2)+(-1+3c_1-3c_2)\alpha^3\end{aligned}$$

Temos assim

$$\begin{aligned}-1+3c_0+-3c_2+\alpha^3(-1+3c_1-3c_2) &= \pm 1 \\ \text{e}\quad -1+3c_0+-3c_2+\alpha^3(-1+3c_1-3c_2) &= \pm\alpha^3\end{aligned}$$

não ocorrem. Também não ocorre $-1+3c_0-3c_2+\alpha^3(-1+3c_1-3c_2) = 1+\alpha^3$. Assim, concluímos que

$$-1+3c_0+-3c_2+\alpha^3(-1+3c_1-3c_2) = -1-\alpha^3,$$

implicando que $c_0 = c_1 = c_2$. Como $c_0+c_1+c_2 = -1$, temos $3c_0 = -1$, com $c_0 \in \mathbb{Z}$, o que é um absurdo. Deste modo,$\varphi(u) = \lambda\mu$ não ocorre para nenhum $u \in \mathcal{U}(\mathbb{Z}C_9)$. Seja agora

$$\varphi(u) = \lambda^2\mu^2 = (2+\alpha^2+\alpha^7)(2+\alpha^8+\alpha^{10}) = 4+3\alpha+2\alpha^2++\alpha^3+\alpha^6+2\alpha^7+3\alpha^8,$$

para algum $u \in \mathcal{U}(\mathbb{Z}C_9)$. Temos que

$$u = 4+3x+2x^2+x^3+x^6+2x^73x^8+c_0(1+x^3+x^6)+c_1(x+x^4+x^7)+c_2(x^2+x^5+x^8)$$

e assim,

$$\varepsilon(u) = 16+3(c_0+c_1+c_2)$$

Logo,

$$c_0+c_1+c_2 = -5$$

Temos também

$$\begin{aligned}\tau(u) &= 4+3\alpha^3+2(-\alpha^3-1)+1+1+2\alpha^3+3(-\alpha^3-1)3c_0+3c_1\alpha^3-3c_2-3c_2\alpha^3 = \\ &= (1+3c_0-3c_2)+3(c_1-c_2)\alpha^3\end{aligned}$$

Nesse caso, $c_0 = c_1 = c_2$. Como $c_0+c_1+c_2 = -5$, chegamos a uma contradição. Logo, $\nexists u \in \mathcal{U}(\mathbb{Z}C_9)$ tal que $\varphi(u) = \lambda^2\mu^2$.

Agora suponha $\varphi(u_0) = \lambda^r\mu^s$, com $3 \nmid r$, $3 \nmid s$ e $u_0 \in \mathcal{U}(\mathbb{Z}\langle x\rangle)$ e que $r \equiv s(\mod 3)$.

$$3 \nmid r \Rightarrow r = 3q+r_1, \text{com } r_1 \in \{1,2\}$$

$$3 \nmid s \Rightarrow s = 3q + s_1, \text{com } s_1 \in \{1, 2\}$$

Como $r \equiv s(\mod 3)$ e $r - s = 3(q - p) + (r_1 - s_1)$, então $r_1 = s_1$.

Assim,

$$r_1 = 1 = s_1 \Rightarrow \varphi(u_0) = (\lambda^3)^q \lambda (\mu^3)^p \mu \Rightarrow$$
$$\Rightarrow \varphi(u_0 u_1^{-q} u_2^{-p}) = \lambda\mu, \quad \text{com} \quad u_0 u_1^{-q} u_2^{-p} \in \mathcal{U}(\mathbb{Z}C_9).$$

e

$$r_1 = 2 = s_1 \Rightarrow \varphi(u_0 u_1^{-q} u_2^{-p}) = \lambda^2\mu^2, \quad \text{onde} \quad u_0 u_1^{-q} u_2^{-p} \in \mathcal{U}(\mathbb{Z}G).$$

Nesses dois casos, chegamos a contradições. Logo, $r \not\equiv s(\mod 3)$.

□

Teorema 2.2.2. *Seja $\mathcal{U}(\mathbb{Z}C_9)$ o grupo de unidades de um anel de grupo integral de um grupo cíclico de ordem 9 $C_9 = \langle x \rangle$. Então $\mathcal{U}(\mathbb{Z}C_9) = \langle -1 \rangle \times \langle x \rangle \times \langle u_2 \rangle \times \langle u_3 \rangle$, onde u_2 e u_3 são como nos Lemas 2.2.4 e 2.2.5.*

Demonstração. Seja $u \in \mathcal{U}(\mathbb{Z}C_9)$. Temos $\varphi(u) \in \mathcal{U}(\mathbb{Z}[\alpha])$. Pelo Teorema 2.2.1, temos que $\mathcal{U}(\mathbb{Z}[\alpha]) = \langle -1 \rangle \times \langle \alpha \rangle \times \langle \lambda \rangle \times \langle \mu \rangle$.

Portanto,

$$\varphi(u) = (-1)^i \alpha^j \lambda^k \mu^n$$

Logo,

$$\varphi((-1)^i x^{-j} u) = \lambda^k \mu^n$$

Dividindo k e n por 3, temos

$$k = 3q + r, \text{com} \quad r \in \{0, 1, 2\}$$

$$n = 3t + s, \text{com} \quad s \in \{0, 1, 2\}$$

Então, $\varphi((-1)^i x^{-j} u) = (\lambda^3)^p (\lambda)^r (\mu^3)^t \mu^s$. Sendo $u_2 = -1 - (x + x^8) - -(x^2 + x^7) + 2(x^4 + x^5)$, pelo Lema 2.2.4 temos que $\varphi(u_2) = \mu^3$ e sendo

$$u_1 = -1 + 2(x + x^8) - (x^2 + x^7) - (x^4 + x^5),$$

pelo Lema 2.2.3, $\varphi(u_1) = \lambda^3$. Logo,

$$\varphi((-1)^i x^{-j} u) = (\lambda^3)^p (\lambda)^r (\mu^3)^t \mu^s = \varphi(u_1)^p \lambda^r \varphi(u_2)^t \mu^s$$

e, assim

$$\varphi((-1)^i x^{-j} u u_1^{-p} u_2^{-t}) = \lambda^r \mu^s$$

Se $3|r$, então $r = 0$ (já que $r \in \{0,1,2\}$) e $\varphi((-1)^i x^{-j} u u_1^{-p} u_2^{-t}) = \mu^s$. Então pelo Lema 2.2.4, $3|s$ e portanto $s = 0$ (já que $r \in \{0,1,2\}$). Nesse caso, $\varphi((-1)^i x^{-j} u u_1^{-p} u_2^{-t}) = 1$

Se $3|s$, temos que $s = 0$ e portanto $3|r$(pelo Lema 2.2.3). Daí, $r = 0$. Se $3 \nmid r$,$3 \nmid s$ pelo Lema 2.2.5 $r \not\equiv s(\mod 3)$. Assim, $r = 1$ e $s = 2$ ou $r = 2$ e $s = 1$. Se $r = 1$ e $s = 2$, temos $\varphi((-1)^i x^{-j} u u_1^{-p} u_2^{-t} u_3^{-1}) = \lambda\mu^2$. Pelo Lema 2.2.5, temos $\varphi(u_3) = \lambda\mu^2$. Portanto, $\varphi((-1)^i x^{-j} u u_1^{-p} u_2^{-t} u_3^{-1}) = 1$

Se $r = 2$ e $s = 1$, temos $\varphi((-1)^i x^{-j} u u_1^{-p} u_2^{-t}) = \lambda^2\mu = \lambda^3\mu^3\lambda^{-1}\mu^{-2}$. Pelos Lemas 2.2.3, 2.2.4, 2.2.5, temos $\varphi(u_1) = \lambda^3$, $\varphi(u_2) = \mu^3$ e $\varphi(u_3) = \lambda\mu^2$.

Assim, $\varphi((-1)^i x^j u u_1^{-p} u_2^{-t}) = \varphi(u_1)\varphi(u_2)\varphi(u_3)^{-1}$. Logo, $\varphi((-1)^i x^j u u_1^{-p} u_2^{-t} u_1^{-p} u_2^{-1} u_3) = 1$.

Para $r = s = 0$, temos

$$\begin{aligned} \varphi(u)\varphi((-1)^i x^j u_1^{-p} u_2^{-t} &= 1 \\ \therefore \varphi(u)(-1)^i\varphi(x^j)\varphi(u_1^{-p})\varphi(u_2^{-t}) &= 1 \end{aligned}$$

Isto é, $\varphi(u) = \varphi((-1)^i x^j u_1^p u_2^t)$.

Como φ é injetor em $\mathcal{U}(\mathbb{Z}C_9)$ segue que $\mu = (-1)^i x^j u_1^p u_2^t$

Para $r = 1, s = 2$, temos

$$\varphi(u) = \varphi((-1)^i x^j u_1^p u_2^t u_3)$$

Portanto, $\mu = (-1)^i x^j u_1^p u_2^t u_3$.

Para $r = 2, s = 1$, temos

$$\varphi(u) = \varphi((-1)^i x^j u_1^{p+1} u_2^{t+1} u_3^{-1})$$

Então, $\mu = (-1)^i x^j u_1^{p+1} u_2^{t+1} u_3^{-1}$.

Desse modo, $\mathcal{U}(\mathbb{Z}C_9) = \langle -1\rangle \times \langle x\rangle \times \langle u_1, u_2, u_3\rangle$. Como $\lambda^3 = (\lambda\mu^2)^3(\mu^3)^{-2}$, então

$$\varphi(u_1) = \varphi(u_3)^3\varphi(u_2)^{-2}$$

Logo, $\varphi(u_1) = \varphi(u_3u_2)^{-2}$. Como φ é injetor em $\mathcal{U}(\mathbb{Z}C_9)$, então $u_1 = u_3u_2^{-2}$

Dessa maneira, temos

$$\langle u_1, u_2, u_3 \rangle = \langle u_2, u_3 \rangle$$

Assim,

$$\mathcal{U}(\mathbb{Z}C_9) = \langle -1 \rangle \times \langle\ x \rangle \times \langle u_2, u_3 \rangle$$

Logo, segue o resultado.

□

Capítulo 3

Unidades de $\mathcal{U}(\mathbb{Z}C_p)$

Sejam G um grupo finito, $\mathbb{Z}$ o anel dos inteiros, $\mathbb{Z}G$ o anel de grupo de G sobre $\mathbb{Z}$ e $\mathcal{U}(\mathbb{Z}G)$ o grupo de unidades de $\mathbb{Z}G$. Seja $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ o centro de $\mathcal{U}(\mathbb{Z}G)$, o qual é um grupo abeliano finitamente gerado ([16], capítulo 8). Logo, $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ deve ser da forma $T \times A$, onde T é o grupo de torção de G e A é um subgrupo livre abeliano de $\mathcal{U}(\mathbb{Z}G)$. Em [16], corolário 7.1.3, temos que $T = \pm\mathcal{Z}(G)$, lembrando o seguinte resultado, que vimos no começo desse trabalho:

Proposição 3.0.1. *Seja $\gamma = \sum_{g\in G}\gamma(g)g$ uma unidade de ordem finita em um anel de grupo integral $\mathbb{Z}G$ de um grupo finito G e assuma que $\gamma(1) \neq 0$. Então, $\gamma = \gamma(1) = \pm 1$.*

Temos que A não é unicamente determinado e para determinar A é suficiente encontrar uma $\mathbb{Z}$-base S para um $\mathbb{Z}$-módulo livre A. Nesse caso, dizemos que S é um subconjunto multiplicativamente independente de A.

No capítulo 1 dessa dissertação, vimos que Aleev e Panina determinaram esse grupo S para anéis de grupo sobre grupos cíclicos de ordens 7 e 9.

Sejam p um primo, C_p um grupo cíclico de ordem p e $\mathcal{U}(\mathbb{Z}C_p)$ o grupo de unidades do anel de grupo integral de C_p. Nesse parte do trabalho, mostraremos como Ferraz, em [10], determina um subconjunto multiplicativamente independente S de $\mathcal{U}(\mathbb{Z}C_p)$ que gera um complemento para $\pm C_p$ em $\mathcal{U}(\mathbb{Z}C_p)$.

Se p é um número primo, temos que o conjunto

$$\{1+\theta, 1+\theta+\theta^2, \ldots, 1+\theta+\cdots+\theta^{\frac{p-3}{2}}\}$$

é um conjunto multiplicativamente independente (ver [21]), onde θ é uma raiz primitiva da unidade de ordem p.

De acordo com [21], para primos p tais que $p \leqslant 67$, temos que $S_\theta = \{-1, \theta, 1+\theta, 1+\theta+\theta^2, \ldots, 1+\theta+\cdots+\theta^{\frac{p-3}{2}}\}$ gera $\mathcal{U}(\mathbb{Z}[\theta])$.

No que segue, vamos considerar apenas primos tais que S_θ gera $\mathcal{U}(\mathbb{Z}[\theta])$. Para esses primos, que denotaremos por p, encontraremos um conjunto multiplicativamente independente S, tal que $A = \langle S \rangle$ é um complemento para $\pm C_p$ em $\mathcal{U}(\mathbb{Z}C_p)$.

Então, sejam p como mencionado acima e θ uma raiz primitiva p-ésima da unidade. Para $i \geqslant 1$, definimos $\mu_i = 1+\theta+\cdots+\theta^{i-1} \in \mathbb{Z}[\theta]$.

Notemos, primeiramente, que $1+\theta+\cdots+\theta^{p-1} = 0$, pois

$$
\begin{aligned}
&1+\theta+\cdots+\theta^{p-1} = \theta^p+\theta+\cdots+\theta^{p-1} \Rightarrow \\
&\Rightarrow 1+\theta+\cdots+\theta^{p-1} = \theta(\theta^{p-1}+1+\cdots+\theta^{p-2}) \Rightarrow \\
&\Rightarrow 1+\theta+\cdots+\theta^{p-1} = \theta(1+\theta+\cdots+\theta^{p-1}) \Rightarrow \\
&\Rightarrow (1+\theta+\cdots+\theta^{p-1})(1-\theta) = 0 \Rightarrow \\
&\Rightarrow 1+\theta+\cdots+\theta^{p-1} = 0,
\end{aligned}
$$

uma vez que θ é raiz p-ésima primitiva da unidade.

Assim, temos que, se $a_i \in \mathbb{Z}$, $0 \leqslant i \leqslant p-1$:

$$
\begin{aligned}
&a_0+a_1\theta+\cdots+a_{p-1}\theta^{p-1} = 0 \Rightarrow \\
&\Rightarrow a_0+a_1\theta+\cdots+a_{p-1}\theta^{p-1} = 1+\theta+\cdots+\theta^{p-1} \Rightarrow \\
&\Rightarrow (a_0-1)+(a_1-1)\theta+\cdots+(a_{p-1}-1)\theta^{p-1} = 0 \Rightarrow \\
&\Rightarrow (a_0-1)+(a_1-1)\theta+\cdots+(a_{p-1}-1)\theta^{p-1} = 1+\theta+\cdots+\theta^{p-1} \Rightarrow \\
&\Rightarrow (a_0-2)+(a_1-2)\theta+\cdots+(a_{p-1}-2)\theta^{p-1} = 0 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\Rightarrow (a_0-a_{p-1})+(a_1-a_{p-1})\theta+\cdots+(a_{p-1}-a_{p-1})\theta^{p-1} = 0 \Rightarrow \\
&\Rightarrow (a_0-a_{p-1})+(a_1-a_{p-1})\theta+\cdots+(a_{p-2}-a_{p-1})\theta^{p-2} = 0
\end{aligned}
$$

Como $\{1, \theta, \theta^2, \ldots, \theta^{p-2}\}$ é base de $\mathbb{Z}[\theta]$, temos que

$$a_0 = a_{p-1}, a_1 = a_{p-1}, \ldots, a_{p-2} = a_{p-1}$$

Logo, $a_0 = a_1 = \cdots = a_{p-1}$.

Se $1 \leqslant i \leqslant p-1$, temos que $\mu_i \in \mathcal{U}(\mathbb{Z}[\theta])$. De fato, se $ij \equiv 1 \mod p$, temos que

$$\begin{aligned}&\mu_i.(1+\theta^i+\theta^{2i}+\cdots+\theta^{i(j-1)}) = (1+\theta+\cdots+\theta^{i-1})(1+\theta^i+\theta^{2i}+\cdots+\theta^{i(j-1)}) = \\ &= (1+\theta^i+\theta^{2i}+\cdots+\theta^{i(j-1)}) + (\theta+\theta^{i+1}+\theta^{2i+1}+\cdots+\theta^{i(j-1)+1}) + \cdots + \\ &+(\theta^{i-1}+\theta^{2i-1}+\cdots+\theta ij-1) = \frac{1-\theta^{ij}}{1-\theta}\end{aligned}$$

Como $ij \equiv 1 \mod p$, então $p|(ij-1)$ e, portanto $ij = kp+1$, para algum $k \in \mathbb{Z}$. Logo, segue que

$$\mu_i.(1+\theta^i+\theta^{2i}+\cdots+\theta^{i(j-1)}) = \frac{1-\theta.\theta^{kp}}{1-\theta} = \frac{1-\theta.(\theta^p)^k}{1-\theta} = \frac{1-\theta}{1-\theta} = 1,$$

uma vez que $\theta^p = 1$.

Logo, segue que $\mu_i \in \mathcal{U}(\mathbb{Z}[\theta])$ quando $1 \leqslant i \leqslant p-1$.

Agora consideremos θ como acima e o ideal $\langle 1-\theta \rangle$ de $\mathbb{Z}[\theta]$. Assim, temos que

$$\mathbb{Z}[\theta]/\langle 1-\theta \rangle \simeq \mathbb{Z}_p$$

De fato, definindo $\Psi : \mathbb{Z}[\theta] \longrightarrow \mathbb{Z}_p$ por

$$\Psi(a_0+a_1\theta+\cdots+a_{p-1}\theta^{p-1}) = \overline{a_0+a_1+\cdots+a_{p-1}},$$

temos que Ψ é um epimorfismo de anéis e $\ker\Psi = \langle 1-\theta \rangle$. Portanto, pelo Teorema do Homomorfismo, $\mathbb{Z}[\theta]/\langle 1-\theta \rangle \simeq \mathbb{Z}_p$.

Vejamos que Ψ é, de fato, um epimorfismo de anéis e que $\ker\Psi = \langle 1-\theta \rangle$:

Sejam $x = a_0+a_1\theta+\cdots+a_{p-1}\theta^{p-1}$ e $y = b_0+b_1\theta+\cdots+b_{p-1}\theta^{p-1}$. Se $x = y$, então temos

$$\begin{aligned}&a_0+a_1\theta+\cdots+a_{p-1}\theta^{p-1} = b_0+b_1\theta+\cdots+b_{p-1}\theta^{p-1} \Rightarrow \\ &\Rightarrow (a_0-b_0)+(a_1-b_1)\theta+\cdots+(a_{p-1}-b_{p-1})\theta^{p-1} = 0 \Rightarrow \\ &\Rightarrow a_0-b_0 = a_1-b_1 = \cdots = a_{p-1}-b_{p-1},\end{aligned}$$

pelo que vimos acima.

Então, chamemos $a_0 - b_0 = a_1 - b_1 = \cdots = a_{p-1} - b_{p-1} = a$, com $a \in \mathbb{Z}$. Temos então que $a_0 = a + b_0, a_1 = a + b_1, \ldots, a_{p-1} = a + b_{p-1}$. Logo,

$$\begin{aligned}\Psi(x) &= \overline{a_0 + a_1 + \cdots + b_{p-1}} = \overline{a + b_0 + a + b_1 + \cdots + a + b_{p-1}} = \\ &= \overline{pa + b_0 + b_1 + \cdots + b_{p-1}} = \overline{pa} + \overline{b_0 + b_1 + \cdots + b_{p-1}} = \\ &= \overline{pa} + \Psi(y) = \overline{0} + \Psi(y) = \Psi(y)\end{aligned}$$

Portanto $x = y \Rightarrow \Psi(x) = \Psi(y)$.

Agora, como

$$\begin{aligned}&\Psi(x+y) = \Psi((a_0 + b_0) + (a_1 + b_1)\theta + \cdots + (a_{p-1} + b_{p-1})\theta^{p-1}) = \\ &= \overline{(a_0 + b_0) + (a_1 + b_1) + \cdots + (a_{p-1} + b_{p-1})} = \\ &= \overline{a_0 + a_1 + \cdots + a_{p-1}} + \overline{b_0 + b_1 + \cdots + b_{p-1}} = \Psi(x) + \Psi(y)\end{aligned}$$

e

$$\begin{aligned}&\Psi(xy) = \overline{a_0b_0 + a_1b_{p-1} + a_2b_{p-2} + \cdots + a_{p-1}b_1 + a_0b_1 + a_1b_0} + \\ &+\overline{a_2b_{p-1} + \cdots + a_{p-1}b_2 + a_0b_{p-1} + a_1b_{p-2} + \cdots + a_{p-1}b_0} = \\ &= \overline{a_0(b_0 + b_1 + \cdots + b_{p-1} + \cdots + a_{p-1})(b_0 + b_1 + \cdots + b_{p-1})} = \\ &= \overline{(a_0 + a_1 + \cdots + a_{p-1})(b_0 + b_1 + \cdots + b_{p-1})} = \\ &= \overline{(a_0 + a_1 + \cdots + a_{p-1})} \cdot \overline{(b_0 + b_1 + \cdots + b_{p-1})} = \Psi(x)\Psi(y)\end{aligned}$$

Temos que Ψ é um homomorfismo de anéis.

Vejamos agora que Ψ é sobrejetora.

Seja $\overline{a} \in \mathbb{Z}_p$. Tomando $x = a\theta \in \mathbb{Z}[\theta]$, temos que $\Psi(x) = \Psi(a\theta) = \overline{a}$. Logo, $\Psi(\mathbb{Z}[\theta]) = \mathbb{Z}_p$, isto é, Ψ é sobrejetora e, portanto, é um epismorfismo.

Para vermos que $\ker \Psi = \langle 1 - \theta \rangle$ basta notar que

$$a_0 + a_1\theta + a_2\theta^2 + + \cdots + a_{p-1}\theta^{p-1} = t(\theta)(1-\theta) + (a_0 + a_1 + \cdots + a_{p-1}),$$

onde

$$t(\theta) = a_{p-1}\theta^{p-2} + (a_{p-1} + a_{p-2})\theta^{p-3} + \cdots + (a_{p-1} + a_{p-2} + \cdots + a_2)\theta + (a_1 + \cdots + a_{p-1})$$

Assim, se $x \in \ker \Psi$, sendo x como descrito acima, temos que

$$\overline{a_0 + a_1 + \cdots + a_{p-1}} = \overline{0}$$

Isto é, $a_0 + a_1 + \cdots + a_{p-1} = kp$, para algum $k \in \mathbb{Z}$.

Já que

$$1 + \theta + \theta^2 + \cdots + \theta^{p-1} = \theta^p + \theta + \theta^2 + \cdots + \theta^{p-1} = \theta(1 + \theta + \theta^2 + + \cdots + \theta^{p-1}),$$

então segue que

$(1 + \theta + \theta^2 + \cdots + \theta^{p-1})(1 - \theta) = 0$ e, portanto, $1 + \theta + \theta^2 + \cdots + \theta^{p-1} = 0$ ou $\theta = 1$.

Uma vez que θ é raiz primitiva p-ésima da unidade, temos que $\theta \neq 1$. Logo,

$$1 + \theta + \theta^2 + \cdots + \theta^{p-1} = 0$$

Dessa maneira, podemos escrever $-1 - \theta - \theta^2 - \cdots - \theta^{p-1} = 0$ e daí

$$(1 - \theta) + (1 - \theta^2) + \cdots + (1 - \theta^{p-1}) = p$$

Como

$$(1 - \theta^l) = (1 - \theta)(\theta^{l-1} + \theta^{l-2} + + \cdots + \theta + 1),$$

temos que p é um múltiplo de $(1 - \theta)$ e, assim, $x \in \langle 1 - \theta \rangle$.

Assim, temos que $\ker \Psi \subset \langle 1 - \theta \rangle$.

Seja agora $q \in \langle 1 - \theta \rangle$. Então $q(\theta) = g(\theta)(1 - \theta)$ e temos

$$\Psi(q(\theta)) = \Psi(q(\theta))\Psi(1 - \theta) = \Psi(q(\theta)).\overline{0} = \overline{0}$$

Concluímos então que $\ker \Psi = \langle 1 - \theta \rangle$, como queríamos.

Temos que Ψ é um epimorfismo completamente determinado pela igualdade $\Psi(\theta) = \overline{1}$.

Consideremos agora $\psi = \Psi \restriction \mathcal{U}(\mathbb{Z}[\theta])$, isto é, ψ é a restrição de Ψ ao subgrupo das unidades de $\mathbb{Z}[\theta]$.

Nosso objetivo agora é encontrar um conjunto de geradores para $\ker\psi$, que denotaremos por $\mathcal{U}_\psi$.

Primeiramente, notemos que $\psi(\mu_i) = \overline{i}$ (de fato, $\psi(\mu_i) = \psi(1+\theta+\cdots++\theta^{i-1}) = \overline{1+1+\cdots+1} = \overline{i}$). Seja $\overline{i} \in \mathbb{Z}_p$ e tomemos $\mu_i = 1+\theta+\cdots+\theta^{i-1}$, com θ como mencionado acima. Temos assim $\psi(\mu_i) = \overline{i}$. Portanto, ψ é sobrejetora. Agora, como $\psi(1) = \psi(\theta) = \overline{1}$, temos que 1 e θ pertencem a $\mathcal{U}_\psi$.

Observemos agora que $\mu_i = \mu_j$ quando $i \equiv j \mod p$ e $\mu_k = 0$ se $p|k$. De fato, se $i \equiv j \mod p$ e $\mu_k = 0$, então $p|(i-j)$ e, portanto, $i = kp + j$. Daí vem que

$$\begin{aligned}\mu_i &= 1+\theta+\cdots+\theta^{i-2}+\theta^{i-1} = 1+\theta+\cdots+\theta^{(kp+j)-2}+\theta^{(kp+j)-1} = \\ &= 1+\theta+\cdots+\theta^{kp}\theta^{j-2}+\theta^{kp}\theta^{j-1} = 1+\theta+\cdots+\theta^{j-2}+\theta^{j-1} = \mu_j,\end{aligned}$$

uma vez que $\theta^p = 1$.

E se $p|k$, temos $k = ap$, para algum $a \in \mathbb{Z}$. Dessa maneira

$$\begin{aligned}\mu_k &= 1+\theta+\cdots+\theta^{k-1} = 1+\theta+\cdots+\theta^{ap-1} = 1+\theta+\cdots+(\theta^a)^p\theta^{-1} = \\ &= 1+\theta+\cdots+\theta^{p-1} = 0\end{aligned}$$

Agora, caso $1 \leqslant k \leqslant p$, escrevendo $1+\theta+\cdots+\theta^{k-1}+\theta^k+\cdots+\theta^{p-1} = 0$, segue que $1+\theta+\cdots+\theta^{k-1} = -(\theta^k+\cdots+\theta^{p-1}) = -\theta^k(1+\theta+\cdots+\theta^{(p-k)-1})$. Portanto, $\mu_k = -\theta^k\mu_{p-k}$.

E se $k+s = mp$, isto é, se $k+s$ é um múltiplo de p, temos $p|(k+s)$ e, portanto $\mu_{k+s} = 0$. Daí,

$$\begin{aligned}&0 = \mu_{k+s} = 1+\theta+\theta^2+\cdots+\theta^{k-1}+\theta^k+\theta^{k+1}+\cdots+\theta^{k+s-1} \Rightarrow \\ &1+\theta+\theta^2+\cdots+\theta^{k-1} = -(\theta^k+\theta^{k+1}+\cdots+\theta^{k+s-1}) \Rightarrow \\ &\mu_k = -\theta^k(1+\theta+\theta^2+\cdots+\theta^{s-1}) \Rightarrow \\ &\mu_k = -\theta^k\mu_s\end{aligned}$$

Agora, utilizando a notação acima, vamos demonstrar que o conjunto gerado por $1, \theta, \mu_t, \mu_{t^2}, \ldots, \mu_{t^{\frac{p-3}{2}}}$ gera $\mathcal{U}(\mathbb{Z}[\theta])$, onde t é gerador de $\mathcal{U}(\mathbb{Z}[\theta])$.

Teorema 3.0.3. *Seja $p \geqslant 5$ um primo como considerado acima e $t \in \mathbb{Z}$ tal que $\overline{t}$ gera o grupo $\mathcal{U}(\mathbb{Z}_p)$. Então $S_1 = \left\langle -1, \theta, \mu_t, \mu_{t^2}, \ldots, \mu_{t^{\frac{p-3}{2}}} \right\rangle = \mathcal{U}(\mathbb{Z}[\theta])$.*

Demonstração. Primeiramente vamos mostrar que $S_1 \subseteq \mathcal{U}(\mathbb{Z}[\theta])$.

Sabemos que $\mathcal{U}(\mathbb{Z}[\theta]) = \left\langle -1, \theta, \mu_2, \ldots, \mu_{\frac{p-1}{2}} \right\rangle$. Então $-1, \theta \in \mathcal{U}(\mathbb{Z}[\theta])$.

Consideremos $1 \leqslant j \leqslant \dfrac{p-3}{2}$. Como $\mathcal{U}(\mathbb{Z}[\theta]) = \langle \bar{t} \rangle$, então $\bar{t}^j \in \mathcal{U}(\mathbb{Z}_p)$. Assim, $\bar{t}^j = \bar{i}$, para algum i, $1 \leqslant i \leqslant p-1$, isto é, $t^j \equiv i \mod p$, com $1 \leqslant i \leqslant p-1$.

Pelo que vimos anteriormente, $\mu_{t^j} = \mu_i$. Temos que $\mu_i, 1 \leqslant i \leqslant p-1 \Rightarrow \mu_i \in \mathcal{U}(\mathbb{Z}[\theta])$. Portanto, $\mu_{t^j} \in \mathcal{U}(\mathbb{Z}[\theta])$, com $1 \leqslant j \leqslant \frac{p-3}{2}$. Assim, $S_1 \subseteq \mathcal{U}(\mathbb{Z}[\theta])$.

Agora mostremos que $\mathcal{U}(\mathbb{Z}[\theta]) \subseteq S_1$.

Seja $\mu_i = 1 + \theta + \cdots + \theta^{i-1} \in \mathcal{U}(\mathbb{Z}[\theta])$. Logo, $1 \leqslant i \leqslant p-1$.

Uma vez que $\mathcal{U}(\mathbb{Z}_p) = \left\{\bar{1}, \bar{2}, \ldots, \overline{p-1}\right\}$ é cíclico, $t^{p-1} \equiv 1 \mod p$, pelo Pequeno Teorema de Fermat e $1 \leqslant i \leqslant p-1$, então $\bar{i} = \bar{t}^j$, para algum $1 \leqslant j \leqslant p-1$. Logo, $i \equiv t^j \mod p$, com $1 \leqslant j \leqslant p-1$ e, portanto, $\mu_i = \mu_{t^j}$.

Se $1 \leqslant j \leqslant \dfrac{p-3}{2} = \dfrac{p-1}{2} - 1$, então $\mu_i \in S_1$.

Agora vamos analisar $\dfrac{p-1}{2} \leq j \leq p-1$.

Seja $s = j - \dfrac{p-1}{2}$. Temos que

$$i \equiv t^j \equiv t^s t^{\frac{p-1}{2}} \mod p$$

Como $t^{p-1} \equiv 1 \mod p$, temos $t^{\frac{p-1}{2}} t^{\frac{p-1}{2}} \equiv 1 \mod p$. Portanto, $p|(t^{\frac{p-1}{2}})^2 - 1$.

Daí, $p|(t^{\frac{p-1}{2}} - 1)(t^{\frac{p-1}{2}} + 1)$. Como p é primo, temos que $p|(t^{\frac{p-1}{2}} - 1)$ ou $p|(t^{\frac{p-1}{2}} + 1)$.

Se $p|(t^{\frac{p-1}{2}} - 1)$, então $t^{\frac{p-1}{2}} \equiv 1 \mod p$. Mas $|\mathcal{U}(\mathbb{Z}_p)| = p-1$. Então, caso $t^{\frac{p-1}{2}} \equiv 1 \mod p$, teríamos $|\mathcal{U}(\mathbb{Z}_p)| = \dfrac{p-1}{2}$, o que é uma contradição.

Concluímos então que $t^{\frac{p-1}{2}} \equiv -1 \mod p$. Portanto, $i \equiv t^s t^{\frac{p-1}{2}} \equiv -t^s \mod p$. Assim, $p|(i + t^s)$ e, portanto, $\mu_i = \theta^i \mu_{t^s}$.

Como $s = j - \dfrac{p-1}{2}$, então $0 < s < \dfrac{p-1}{2} = \dfrac{p-3}{2} - 1$, isto é, $1 \leqslant s \leqslant \dfrac{p-3}{2}$. Portanto, $\mu_i = \theta^i \mu_{t^s}$ com $1 \leqslant s \leqslant \dfrac{p-3}{2}$ é tal que $\mu_i \in S_1$.

Agora, se $j = \dfrac{p-1}{2}$, temos que $i \equiv t^j \equiv t^{\frac{p-1}{2}} \equiv -1 \equiv (p-1) \mod p$. Logo,

$$\mu_i = \mu_{p-1} = 1 + \theta + \cdots + \theta^{p-2} = -\theta^{p-1} \in S_1$$

Caso $j = p-1$, então $i \equiv t^j \equiv t^{p-1} \equiv 1 \mod p$. Daí

$$\mu_i = \mu_1 = 1 \in S_1$$

Portanto, $\mathcal{U}(\mathbb{Z}[\theta]) \subseteq S_1$. Concluímos $\mathcal{U}(\mathbb{Z}[\theta]) = S_1$, como queríamos.

□

Proposição 3.0.2. *Sejam t e S_1 como no Teorema 3.0.3.*
Seja $S_2 = \left\langle -1, \theta, \mu_t, \mu_t^{-2}\mu_{t^2}, \ldots, \mu^{-\frac{p-3}{2}}\mu_{t^{\frac{p-3}{2}}} \right\rangle$ subgrupo de $\mathcal{U}(\mathbb{Z}[\theta])$. Então $S_1 = S_2$.

Demonstração. É fácil ver que $S_2 \subset S_1$. Agora vejamos que $S_1 \subset S_2$.
Para cada μ_{t^i}, com $2 \leqslant i \leqslant \dfrac{p-3}{2}$, temos $\mu_{t^i} = \mu_t^i \mu_t^{-i} \mu_{t^i} = \mu_t^i(\mu_t^{-i}\mu_{t^i})$. Já que μ_t e $\mu_t^{-i}\mu_{t^i}$ estão em S_2, então $\mu_{t^i} \in S_2$. Como -1 e θ pertencem também à S_2, então concluímos que $S_1 \subset S_2$, como queríamos.

□

Consideremos agora o seguinte subconjunto de $\mathcal{U}(\mathbb{Z}[\theta])$:

$\mathcal{U} = \{\theta, -\mu^{\frac{p-1}{2}t}, \mu_t^{-2}\mu_{t^2}, \ldots, \mu_t^{-\frac{p-3}{2}}\mu_{t^{\frac{p-3}{2}}}\}$.

Lembrando que $\psi(\mu_i) = \overline{i}$, com $1 \leqslant i \leqslant p-1$, temos

$$\psi(\mu_t^{-i}\mu_{t^i}) = \psi(\mu_t)^{-i}\psi(\mu_{t^i}) = \overline{t}^{-i}\overline{t^i} = \overline{t^{-i}t^i} = \overline{1}$$

Como $\psi(-\mu^{\frac{p-1}{2}}) = -\overline{t}^{\frac{p-1}{2}} = -(\overline{-1}) = \overline{1}$ (uma vez que $t^{\frac{p-1}{2}} \equiv -1 \mod p$) e $\psi(\theta) = \overline{1}$, concluímos que $\langle \mathcal{U} \rangle \subset \ker \psi$.

Teorema 3.0.4. *Com as definições acima, temos $\langle \mathcal{U} \rangle = \mathcal{U}_\psi$.*

Demonstração. Vimos acima que $\langle \mathcal{U} \rangle \subset \ker \psi = \mathcal{U}_\psi$. Então basta mostrar a inclusão contrária.

Pelo Teorema 3.0.3 e pela Proposição 3.0.2, temos que $S_1 = \mathcal{U}(\mathbb{Z}[\theta])$ e $S_1 = S_2$, respectivamente. Logo, $\mathcal{U}(\mathbb{Z}[\theta]) = S_2$.

Seja $\nu \in \mathcal{U}(\mathbb{Z}[\theta])$. Então, $\nu = -1^{\alpha}\theta^{k_0}\mu_t^{k_1}v_2^{k_2}\ldots v_{\frac{p-3}{2}}^{k_{\frac{p-3}{2}}}$, onde $0 \leqslant \alpha \leqslant 1$, $0 \leqslant k_0 \leqslant p-1$, $k_i \in \mathbb{Z}$ e $v_i = \mu_t^{-i}\mu_{t^i}$, com $1 \leqslant i \leqslant \dfrac{p-3}{2}$.

Vimos anteriormente que θ e v_i, com $1 \leqslant i \leqslant \dfrac{p-3}{2}$, pertencem a $\mathcal{U}_\psi = \ker\psi$. Logo, $\psi(\nu) = \overline{1} \Longleftrightarrow \psi(-1^{\alpha}\mu_t^{k_1}) = \overline{1}$. Temos

$$\psi(-1^{\alpha}\mu_t^{k_1}) = \overline{1} \Longleftrightarrow \psi(-1)^{\alpha}\psi(\mu)^{k_1} = \overline{1} \Longleftrightarrow -1^{\alpha}\overline{t}^{k_1} = \overline{1}$$

Portanto, $\overline{t}^{k_1} = \overline{-1}$ e $\alpha = 1$ ou $\overline{t}^{k_1} = \overline{1}$ e $\alpha = 0$.

No caso de $\overline{t}^{k_1} = \overline{-1}$ e $\alpha = 1$, temos que $t^{k_1} \equiv -1 \mod p \equiv (p-1) \mod p$. Vimos anteriormente que $t^{\frac{p-1}{2}} \equiv -1 \mod p \equiv (p-1) \mod p$, logo, $\overline{t}^{k_1} = \overline{-1} = \overline{t}^{\frac{p-1}{2}}$. Como $\overline{t}^{\frac{p-1}{2}} \in \mathcal{U}(\mathbb{Z}_p)$, então existe $\overline{t}^{-\frac{p-1}{2}}$ em $\mathcal{U}(\mathbb{Z}_p)$ tal que $\overline{t}^{\frac{p-1}{2}}\overline{t}^{-\frac{p-1}{2}} = \overline{1}$. Como $\overline{t}^{k_1} = \overline{-1} = \overline{t}^{\frac{p-1}{2}}$, temos que $\overline{t}^{k_1}\overline{t}^{-\frac{p-1}{2}} = \overline{1}$. Dessa maneira, $\overline{t}^{k_1-\frac{p-1}{2}} = \overline{1} = \overline{t}^{p-1}$. Assim, segue que $p-1$ divide $k_1 - \dfrac{p-1}{2}$. Logo, $k_1 = q(p-1) + \dfrac{p-1}{2}$, com $q \in \mathbb{Z}$.

Daí vem que

$$\begin{aligned} -\mu_t^{k_1} &= -\mu_t^{q(p-1)+\frac{p-1}{2}} = -\mu_t^{q(\frac{p-1}{2}+\frac{p-1}{2})+\frac{p-1}{2}} = -\mu_t^{2q(\frac{p-1}{2})+\frac{p-1}{2}} \\ &= -\mu_t^{\frac{p-1}{2}(2q+1)} = (\mu_t^{\frac{p-1}{2}})^{2q+1} \end{aligned}$$

Então, $\mu_t^{k_1} \in \mathcal{U}$ e, portanto, nesse caso, $\nu \in \langle\mathcal{U}\rangle$.

No caso de $\overline{t}^{k_1} = \overline{1}$ e $\alpha = 0$, temos, analogamente, que

$$\overline{t}^{k_1} = \overline{1} \Longrightarrow (p-1)|k_1,$$

uma vez que $t^{p-1} \equiv 1 \mod p$, pelo Pequeno Teorema de Fermat.

Assim, temos que $k_1 = m(p-1)$, com $m \in \mathbb{Z}$. Segue que

$$\mu_t^{k_1} = \mu_t^{m(p-1)} = \mu^{m(\frac{p-1}{2}+\frac{p-1}{2})} = (\mu_t^{\frac{p-1}{2}})^{2m}$$

Portanto, $\nu \in \langle\mathcal{U}\rangle$. Logo, temos que $\ker\psi \subset \langle\mathcal{U}\rangle$ e, dessa maneira, $\ker\psi = \mathcal{U}_\psi = \langle\mathcal{U}\rangle$. □

Por exemplo, seja θ uma raiz primitiva da unidade de ordem $p = 11$. Temos que $\mathcal{U} =$

$\{\theta, -(1+\theta)^5, (1+\theta)^{-2}(1+\theta+\theta^2+\theta^3), (1+\theta)^{-3}(1+\theta+\cdots+\theta^7), (1+\theta)^{-4}(1+\theta+\cdots+\theta^4)\}$ é um conjunto de geradores de $\mathcal{U}_\psi$.

Agora vamos encontrar outro conjunto de geradores para $\mathcal{U}_\psi$.

Já vimos que $t^{\frac{p-1}{2}} \equiv p-1 \mod p$, então temos que $\mu_{t^{\frac{p-1}{2}}} = \mu_{p-1} = 1+\theta+\theta^2+\cdots+\theta^{p-2} = -\theta^{p-1}$. Multiplicando ambos os membros por θ, temos que $\theta\mu_{t^{\frac{p-1}{2}}} = -1$. Assim, segue que $-\mu_t^{-\frac{p-1}{2}} = \theta\mu_{t^{\frac{p-1}{2}}}\mu_t^{-\frac{p-1}{2}}$.

Vamos alterar um pouco o conjunto $\mathcal{U}$ a fim de obter um novo conjunto que gera o mesmo subgrupo gerado por $\mathcal{U}$.

Primeiramente, ao invés de considerarmos o elemento $-\mu_t^{\frac{p-1}{2}}$, vamos considerar o seu inverso $-\mu_t^{-\frac{p-1}{2}}$. Já que $\theta \in \mathcal{U}$ e $-\mu_t^{-\frac{p-1}{2}} = \theta\mu_{t^{\frac{p-1}{2}}}\mu_t^{-\frac{p-1}{2}}$, consideremos $\mu_{t^{\frac{p-1}{2}}}\mu_t^{-\frac{p-1}{2}}$ ao invés do elemento $-\mu_t^{-\frac{p-1}{2}}$. Assim, obtemos o conjunto

$$\mathcal{U}' = \{\theta, \mu_t^{-2}\mu_{t^2}, \ldots, \mu_{t^{\frac{p-3}{2}}}\mu_t^{-\frac{p-3}{2}}, \mu_{t^{\frac{p-1}{2}}}\mu_t^{-\frac{p-1}{2}}\}.$$

Agora dado um inteiro q e um inteiro s relativamente primos, introduzimos a seguinte notação

$$\omega_{q,s} = \sum_{j=0}^{q-1} \theta^{js} = 1 + \theta^s + \theta^{2s} + \cdots + \theta^{(q-1)s}.$$

Observemos que se q é positivo, então $\mu_q = \omega_{q,1}$

Proposição 3.0.3. *Sejam q e s inteiros positivos relativamente primos e seja também $\omega_{q,s} = \sum_{j=0}^{q-1} \theta^{js} = 1 + \theta^s + \theta^{2s} + \cdots + \theta^{(q-1)s}$. Então*

$$\mu_{q^s} = \prod_{j=0}^{s-1} \omega_{q,q^j} = \omega_{q,1}\omega_{q,q}\ldots\omega_{q,q^{s-1}}.$$

Demonstração. Provaremos utilizando indução em s. Se $s = 0$, então $\mu_q = 1+\theta+\theta^2+\cdots+\theta^{q-1}$

e $\omega_{q,1} = \sum_{j=0}^{q-1} \theta^j = 1 + \theta + \theta^2 + + \cdots + \theta^{q-1}$. Logo, $\mu_q = \omega_{q,1}$

Suponhamos agora que o resultado vale para $s = n-1$. Vamos provar o resultado para $s = n$. Assim, devemos mostrar que $\mu_{q^n} = \mu_{q^{n-1}}\omega_{q,q^{n-1}}$.

Temos

$$\begin{aligned}
\mu_{q^{n-1}}\omega_{q,q^{n-1}} &= (1+\theta+\cdots+\theta^{q^{n-1}-1})(1+\theta^{q^{n-1}}+\cdots+\theta^{(q-1)q^{n-1}}) = \\
&= (1+\theta+\theta^2+\cdots+\theta^{q^{n-1}-1}) + \\
&+ (1+\theta+\theta^2+\cdots+\theta^{q^{n-1}-1})\theta^{q^{n-1}} + \\
&+ (1+\theta+\theta^2+\cdots+\theta^{q^{n-1}-1})\theta^{q^{n-2}} + \\
&+ (1+\theta+\theta^2+\cdots+\theta^{q^{n-1}-1})\theta^{(q-1)q^{n-1}} = \\
&= (1+\theta+\theta^2+\cdots+\theta^{q^{n-1}-1}) + \\
&+ (\theta^{q^{n-1}}+\cdots+\theta^{2q^{n-1}-1}) + \\
&+ (\theta^{2q^{n-1}}+\cdots+\theta^{3q^{n-1}-1}) + \cdots + \\
&+ (\theta^{(q-1)q^{n-1}}+\cdots+\theta^{qq^{n-1}-1} = \\
&= 1+\theta+\cdots+\theta^{q^{n-1}} = \mu_{q^n},
\end{aligned}$$

como queríamos. □

Suponhamos agora que t fixado tal que $\mathcal{U}(\mathbb{Z}_p = \langle \bar{t} \rangle)$ e seja h_i a unidade $h_i = \omega_{t,1}^{-1}\omega_{t,t^i}$.

Teorema 3.0.5. *Com a notação acima, o conjunto* $\mathcal{U}_0 = \{\theta, h_1, h_2, \ldots, h_{\frac{p-3}{2}}\}$ *gera* $\mathcal{U}_\psi$. *Além disso, os grupos gerados por* $\mathcal{U}$ *e* $\mathcal{U}_0$ *são iguais.*

Demonstração. Como vimos no Teorema 3.0.4, $\langle \mathcal{U} \rangle = \mathcal{U}_\psi$, então basta provar a última afirmação.

Pela Proposição 3.0.3, temos

$$\mu_{t^i} = \prod_{j=0}^{i-1} \omega_{t,t^j} = \omega_{t,1}\omega_{t,t}\ldots\omega_{t,t^{i-1}},$$

onde $mdc(i,p) = 1$.

Como $mdc(t,1) = 1$, temos, ainda pela Proposição 3.0.3 que

$$\omega_{t,1} = 1 + \theta + \cdots + \theta^{t-1} = \mu_t$$

Portanto,

$$\mu_{t^i}\mu_t^{-1} = (\omega_{t,1}\omega_{t,t}\ldots\omega_{t,t^{i-1}})(\omega_{t,1})^{-1} = \omega_{t,t}\ldots\omega_{t,t^{i-1}}$$

Agora, multiplicando ambos os lados da igualdade obtida acima por μ_t^{-i+1}, temos:

$$\begin{aligned}
\mu_{t^i}\mu_t^{-1}(\mu_t^{-i+1}) &= (\mu_t^{-i+1})(\omega_{t,t}\ldots\omega_{t,t^{i-1}}) = \underbrace{(\mu_t^{-1}\ldots\mu_t^{-1})}_{i-1 vezes}(\omega_{t,t}\ldots\omega_{t,t^{i-1}}) = \\
&= (\mu_t^{-1}\omega_{t,t})(\mu_t^{-1}\omega_{t,t^2})\ldots(\mu_t^{-1}\omega_{t,t^{i-1}}) = \\
&= (\omega_{t,1}^{-1}\omega_{t,t})(\omega_{t,1}^{-1}\omega_{t,t^2})\ldots(\omega_{t,1}^{-1}\omega_{t,t^{i-1}}) = \\
&= h_1h_2\ldots h_{i-1},
\end{aligned}$$

para todo i.

Para $2 \leqslant i \leqslant \dfrac{p-1}{2}$, temos $\langle\mathcal{U}'\rangle \subset \langle\mathcal{U}_0\rangle$.

Mas $\langle\mathcal{U}'\rangle = \langle\mathcal{U}\rangle$. Logo, $\langle\mathcal{U}\rangle \subset \langle\mathcal{U}_0\rangle$.

Agora temos que

$$\omega_{t,t^i} = \mu_t^{i+1}\mu_{t^i}^{-1}.$$

De fato,

$$\mu_t^{i+1} = \underbrace{(\omega_{t,1}\omega_{t,t}\ldots\omega_{t,t^{i-1}})}_{\mu_{t^i}}(\omega_{t,t^i})$$

Portanto, $\mu_{t^{i+1}} = \mu_{t^i}\omega_{t,t^i}$. Logo, $\omega_{t,t^i} = \mu_{t^{i+1}}\mu_{t^i}^{-1}$. Assim, segue que

$$h_i = \omega_{t,1}^{-1}\omega_{t,t^i} = \omega_{t,1}^{-1}\mu_t^{i+1}\mu_{t^i}^{-1} = \mu_t^{-1}\mu_{t^i}^{-1}\mu_t^{i+1} = \mu_t^{-(i+1)}\mu_t^i\mu_{t^i}^{-1}\mu_{t^{i+1}} = (\mu_t^{-(i+1)}\mu_{t^{i+1}})(\mu_t^{-i}\mu_{t^i})$$

Logo, para $2 \leqslant i \leqslant \dfrac{p-3}{2}$, temos que $h_i \in \mathcal{U}'$.

Agora, para $i = 1$, temos

$$h_1 = \omega_{t,1}^{-1}\omega_{t,t} = \mu_t^{-1}\omega_{t,t} = \mu_t^{-1} = \mu_t^{-1}\mu_t^{-1}\mu_{t^2} = \mu_t^{-2}\mu_{t^2},$$

que está em $\mathcal{U}'$.

Logo, $\langle \mathcal{U}_0 \rangle \subset \langle \mathcal{U}' \rangle = \langle \mathcal{U} \rangle$.

Portanto, $\langle \mathcal{U}_0 \rangle = \langle \mathcal{U} \rangle$, como queríamos. □

Introduziremos agora o conjunto de unidades normalizadas de $\mathbb{Z}C_p$.

Anteriormente, definimos a função aumento ε. Em nosso caso, onde o anel considerado é $\mathbb{Z}$, $\varepsilon : \mathbb{Z}G \longrightarrow \mathbb{Z}$, definida por

$$\varepsilon\left(\sum_{x\in G} \alpha_x x\right) = \sum_{x\in G} \alpha_x$$

Agora, vamos tomar as unidades em $\mathbb{Z}G$, cujo aumento é 1. Este conjunto, que é subgrupo de $\mathcal{U}(\mathbb{Z}G)$ é chamado de subgrupo de unidades normalizadas é dado por

$$V = \{u \in \mathcal{U}(\mathbb{Z}G) : \varepsilon(u) = 1\}$$

Proposição 3.0.4. *Com as notações acima, temos, para todo grupo G, $\mathcal{U}(\mathbb{Z}G) = \langle -1 \rangle \times V$.*

Demonstração. Vamos mostrar que:

1. $\mathcal{U}(\mathbb{Z}G) = SV$, onde $S = \langle -1 \rangle$
2. $\langle -1 \rangle \cap V = \{1\}$
3. $\langle -1 \rangle \triangleleft \mathcal{U}(\mathbb{Z}G)$ e $V \triangleleft \mathcal{U}(\mathbb{Z}G)$

Para provarmos 1, primeiramente consideremos $x \in SV$. Então $x = sv$, onde $s \in S$ e $v \in V$. Como $s \in \mathcal{U}(\mathbb{Z}G)$, então $sv \in \mathcal{U}(\mathbb{Z}G)$. Logo, $x \in \mathcal{U}(\mathbb{Z}G)$. Assim, $SV \subset \mathcal{U}(\mathbb{Z}G)$.

Agora seja $x \in \mathcal{U}(\mathbb{Z}G)$. Então existe $x^{-1} \in \mathbb{Z}G$ tal que $xx^{-1} = x^{-1}x = 1$. Seja $y = \varepsilon(x) \in \mathcal{U}(\mathbb{Z})$. Logo, existe $y^{-1} \in \mathbb{Z}$ tal que $yy^{-1} = y^{-1}y = 1$.

Consideremos agora o elemento $k = y^{-1}x \in \mathcal{U}(\mathbb{Z}G)$. Temos que

$$\varepsilon(k) = \varepsilon(y^{-1}x) = \varepsilon(y)^{-1}\varepsilon(x) = y^{-1}y = 1$$

E $k = y^{-1}x \Rightarrow x = yk$, com $y \in \mathcal{U}(\mathbb{Z}) = S$ e $k \in V$.

Portanto, $\mathcal{U}(\mathbb{Z}G) \subset SV$, como queríamos. Agora seja $x \in S \cap V$. Então, $x = 1$ ou $x = -1$, com $x \in V$. Como $\varepsilon(1) = 1$ e $\varepsilon(-1) = -1$, temos que $x = 1$. Logo, $S \cap V \subset \{1\}$.

Agora, é óbvio que $\{1\} \subset S \cap V$, uma vez que $\varepsilon(1) = 1$ e $1 \in S$. Assim, provamos 2. Para demonstrarmos 3, observamos que S e V são subgrupos de $\mathcal{U}(\mathbb{Z}G)$. Primeiramente, vamos mostrar que $V \triangleleft \mathcal{U}(\mathbb{Z}G)$.

Seja $u \in \mathcal{U}(\mathbb{Z}G)$ e seja $x \in uVu^{-1}$. Portanto, $x = uwu^{-1}$, onde $w \in V$. Logo, $w \in \mathcal{U}(\mathbb{Z}G)$ e assim, $x \in \mathcal{U}(\mathbb{Z}G)$. Ainda,

$$\varepsilon(x) = \varepsilon(u)\varepsilon(w)\varepsilon(u^{-1}) = \varepsilon(uu^{-1}) = \varepsilon(1) = 1$$

Segue que $x \in V$ e, portanto, $uVu^{-1} \subset V$, para todo $u \in \mathcal{U}(\mathbb{Z}G)$.

Agora seja $x \in uSu^{-1}$, com $u \in \mathcal{U}(\mathbb{Z}G)$. Logo, $x = uhu^{-1}$, com $h \in S$. Se $h = 1$, temos que $x = uu^{-1} = 1$. Caso $h = -1$, $x = -1$. Nos dois casos, $x \in S$. Segue que $uSu^{-1} \subset V$, para todo $u \in \mathcal{U}(\mathbb{Z}G)$ e assim concluímos a demonstração. □

Em particular, quando $G = C_p = \langle g \rangle$, um grupo cíclico de ordem p, gerado por g, é suficiente determinar um subconjunto V tal que $V = \langle S, g \rangle$. Nesse caso, usaremos a notação $\mathcal{U}_1(\mathbb{Z}C_p)$ para denotar o subgrupo de unidades normalizadas.

Teorema 3.0.6. *Se p é um primo, então os grupos $\mathcal{U}_\psi$ e $\mathcal{U}_1(\mathbb{Z}C_p)$ são isomorfos, via isomorfismo τ*

$$\tau(a_0 + a_1\theta + \cdots + a_{p-1}\theta^{p-1}) = a_0 + a_1 g + \cdots + a_{p-1}g^{p-1} - k\hat{g},$$

onde $k = \dfrac{a_0 + a_1 + \cdots + a_{p-1} - 1}{p}$ *e* $\hat{g} = 1 + g + \cdots + g^{p-1}$

Demonstração. Sejam $x = a_0 + a_1\theta + \cdots + a_{p-1}\theta^{p-1}$ e $x = b_0 + b_1\theta + \cdots + b_{p-1}\theta^{p-1}$, $x, y \in \mathcal{U}_\psi$.

Temos

$$\begin{aligned} x = y &\Rightarrow a_0 + a_1\theta + \cdots + a_{p-1}\theta^{p-1} = b_0 + b_1\theta + \cdots + b_{p-1}\theta^{p-1} \Rightarrow \\ &\Rightarrow (a_0 - b_0) + (a_1 - b_1)\theta + \cdots + (a_{p-1} - b_{p-1})\theta^{p-1} = 0 \end{aligned}$$

Como $1 + \theta + \theta^2 + \cdots + \theta^{p-1} = 0$, então $1 + \theta + \theta^2 + \cdots + \theta^{p-2} = -\theta^{p-1}$.

Portanto,

$$\begin{aligned} & (a_0 - b_0) + (a_1 - b_1)\theta + \cdots + (a_{p-1} - b_{p-1})(1 + \theta + \theta^2 + \cdots + \theta^{p-2}) = 0 \Rightarrow \\ \Rightarrow \quad & [(a_0 - b_0) - (a_{p-1} - b_{p-1})] + [(a_2 - b_2) - (a_{p-1} - b_{p-1})]\,\theta + \cdots + \\ & + [(a_{p-2} - b_{p-2}) - (a_{p-1} - b_{p-1})]\,\theta^{p-2} = 0 \end{aligned}$$

Como $\{1, \theta, \ldots, \theta^{p-2}\}$ é base de $\mathbb{Z}[\theta]$, temos que $a_i - b_i = a_{p-1} - b_{p-1}$, para todo $i \in \{0, \ldots, p-2\}$.

Temos que

$$\begin{aligned} \tau(x) &= a_0 + a_1 g + \cdots + a_{p-1} g^{p-1} - k\hat{g} = \\ &= a_0 + a_1 g + \cdots + a_{p-1} g^{p-1} - \hat{g}\left(\frac{a_0 + a_1 + \cdots + a_{p-1} - 1}{p}\right) \end{aligned}$$

$$\begin{aligned} \tau(y) &= b_0 + b_1 g + \cdots + b_{p-1} g^{p-1} - k\hat{g} = \\ &= a_0 + a_1 g + \cdots + a_{p-1} g^{p-1} - \hat{g}\left(\frac{b_0 + b_1 + \cdots + b_{p-1} - 1}{p}\right) \end{aligned}$$

Logo,

$$\begin{aligned} & \tau(x) - \tau(y) = \left[(a_0 - b_0) + (a_1 - b_1)g + \cdots + (a_{p-1} - b_{p-1})g^{p-1}\right] - \\ & -\hat{g}\left[\frac{(a_0 - b_0) + (a_1 - b_1) + \cdots + (a_{p-1} - b_{p-1})}{p}\right] \end{aligned}$$

Para cada $i \in \{0, 1, \ldots, p-2\}$, chamemos $a_i - b_i = a_{p-1} - b_{p-1} = t$.

Assim,

$$\begin{aligned}\tau(x)-\tau(y) &= \left(t+tg+\cdots+tg^{p-1}\right)-\hat{g}\left(\frac{\overbrace{(t+t+\cdots+t)}^{p\ vezes}}{p}\right)= \\ &= \left(t+tg+\cdots+tg^{p-1}\right)-\hat{g}t = t(1+g+\cdots+g^{p-1})-t\hat{g}=t\hat{g}-t\hat{g}=0\end{aligned}$$

Logo, $\tau(x)=\tau(y)$ e, portanto, τ está bem definida.

É fácil ver que τ é homomorfismo de anéis. Então vamos provar agora a injetividade de τ;

Sejam $x,y\in\mathcal{U}_\psi$, como acima. Chamemos

$$k_1=\left(\frac{a_0+a_1+\cdots+a_{p-1}-1}{p}\right)$$

e

$$k_2=\left(\frac{b_0+b_1+\cdots+b_{p-1}-1}{p}\right).$$

$$\begin{aligned}&\tau(x)=\tau(y)\Rightarrow a_0+a_1g+\cdots+a_{p-1}g^{p-1}-k_1\hat{g}=b_0+b_1g+\cdots+b_{p-1}g^{p-1}-k_2\hat{g}\Rightarrow \\ &\Rightarrow (a_0-b_0)+(a_1-b_1)g+\cdots+(a_{p-1}-b_{p-1})g^{p-1}-k_1\hat{g}+k_2\hat{g}=0\Rightarrow \\ &\Rightarrow (a_0-b_0)+\cdots+(a_{p-1}-b_{p-1})g^{p-1}-\left[\frac{(a_0-b_0)+\cdots+(a_{p-1}-b_{p-1})}{p}\right]\hat{g}=0\end{aligned}$$

Como $x,y\in\mathcal{U}_\psi=\ker\psi$, temos que

$$\overline{a_0+a_1+\cdots+a_{p-1}}=\overline{b_0+b_1+\cdots+b_{p-1}}=\overline{1}$$

Daí $\overline{(a_0-b_0)+(a_1-b_1)+\cdots+(a_{p-1}-b_{p-1})}=\overline{0}$. Portanto,

$$p|\left[(a_0-b_0)+(a_1-b_1)+\cdots+(a_{p-1}-b_{p-1})\right]$$

Assim, $(a_0 - b_0) + (a_1 - b_1) + \cdots + (a_{p-1} - b_{p-1}) = qp$, para algum q inteiro. Logo, vem que

$$\begin{aligned}
&\tau(x) - \tau(y) = (a_0 - b_0) + \cdots + (a_{p-1} - b_{p-1})g^{p-1} - q\hat{g} = 0 \Rightarrow \\
&\Rightarrow (a_0 - b_0) + \cdots + (a_{p-1} - b_{p-1})g^{p-1} - q(1 + g + \cdots + g^{p-1} = 0 \Rightarrow \\
&\Rightarrow (a_0 - b_0 - q) + \cdots + (a_{p-1} - b_{p-1} - q)g^{p-1} = 0
\end{aligned}$$

Como $\{1, g, g^2, \ldots, g^{p-1}\}$ é uma base de $\mathbb{Z}G$,temos que $a_i - b_i - q = 0$, para $i = 0, 1, \ldots, p-1$. Assim, segue que

$$\begin{aligned}
x - y &= (a_0 - b_0) + (a_1 + b_1)\theta + \cdots + (a_{p-1} - b_{p-1})\theta^{p-1} = q + q\theta + \cdots + q\theta^{p-1} = \\
&= q(\underbrace{1 + \theta + \cdots + \theta^{p-1}}_{=0}) = 0
\end{aligned}$$

Portanto, $x = y$, provando que τ é injetora. Agora vamos mostrar que τ é sobrejetora. Tomemos $y \in V$. Então $y \in \mathcal{U}(\mathbb{Z}G)$ e $\varepsilon(y) = 1$, isto é, $y = \sum_{i=0}^{p-1} a_i g^i$, com $y = \sum_{i=0}^{p-1} a_i = 1$.

Seja $x = \sum_{i=0}^{p-1} a_i \theta^i$. Vamos mostrar que $x \in \mathcal{U}(\mathbb{Z}[\theta])$. Já que $y \in \mathcal{U}(\mathbb{Z}G)$, então existe $y^{-1} \in \mathbb{Z}G$ tal que $yy^{-1} = y^{-1}y = 1$ e $y^{-1} = \sum_{i=0}^{p-1} b_i g^i$. Seja agora $x^{-1} = \sum_{i=0}^{p-1} b_i \theta^i$. Temos que

$$\begin{aligned}
xx^{-1} &= \left(\sum_{i=0}^{p-1} a_i\theta^i\right)\left(\sum_{i=0}^{p-1} b_i\theta^i\right) = a_0b_0 + a_0b_1\theta + a_0b_2\theta^2 + \cdots + a_0b_{p-1}\theta^{p-1} + \\
&+ a_1b_{p-1} + a_1b_0\theta + a_1b_1\theta^2 + \cdots + a_1b_{p-2}\theta^{p-1} + \cdots + \\
&+ a_{p-1}b_1 + a_{p-1}b_2\theta + a_{p-1}b_3\theta^2 + \cdots + a_{p-1}b_0\theta^{p-1} = \\
&= (a_0b_0 + a_1b_{p-1} + \cdots + a_{p-1}b_1) + (a_0b_1 + a_1b_0 + \cdots + a_{p-1}b_2)\theta + \\
&+ (a_0b_2 + a_1b_1 + \cdots + a_{p-1}b_3)\theta^2 + \cdots + (a_0b_{p-1} + a_1b_{p-2} + \cdots + a_{p-1}b_0)\theta^{p-1}
\end{aligned}$$

Uma vez que $yy^{-1} = y^{-1}y = 1$, temos que $\left(\sum_{i=0}^{p-1} a_i g^i\right)\left(\sum_{i=0}^{p-1} b_i g^i\right) = 1$.

Portanto,

$$(a_0b_0 + a_1b_{p-1} + \cdots + a_{p-1}b_1) + (a_0b_1 + a_1b_0 + \cdots + a_{p-1}b_2)g + \\ +(a_0b_2 + a_1b_1 + \cdots + a_{p-1}b_3)g^2 + \cdots + (a_0b_{p-1} + a_1b_{p-2} + \cdots + a_{p-1}b_0)g^{p-1} = 1$$

Logo, $(a_0b_0 + a_1b_{p-1} + \cdots + a_{p-1}b_1) = 1$, $(a_0b_2 + a_1b_1 + \cdots + a_{p-1}b_3) = 0, \ldots,$ $(a_0b_{p-1} + a_1b_{p-2} + \cdots + a_{p-1}b_0) = 0$.

Assim, segue que $xx^{-1} = x^{-1}x = 1$ e, portanto, $x \in \mathcal{U}(\mathbb{Z}G)$, como queríamos. Temos também que $\psi(x) = \overline{a_0 + a_1 + \cdots + a_{p-1}} = \overline{1}$. Dessa maneira, $x \in \mathcal{U}_\psi = \ker\psi$. Segue que

$$\begin{aligned}
\tau(x) &= \tau(a_0 + a_1\theta + \cdots + a_{p-1}\theta^{p-1}) = a_0 + a_1g + \cdots + a_{p-1}g^{p-1} - k\hat{g} = \\
&= a_0 + a_1g + \cdots + a_{p-1}g^{p-1} - \left(\frac{\overbrace{(a_0 + \cdots + a_{p-1})}^{=1} - 1}{p} \right) \hat{g} = \\
&= a_0 + a_1g + \cdots + a_{p-1}g^{p-1} = y
\end{aligned}$$

Portanto, τ é sobrejetora e assim, concluímos que τ é um isomorfismo. □

A fim de demonstrar o próximo resultado, enunciaremos o resultado a seguir:

Proposição 3.0.5. *Sejam $C_p = \langle g \rangle$ um grupo cíclico de ordem p, onde p é um primo ímpar e θ é uma raiz primitiva de unidade de ordem p. Então a aplicação*

$$\begin{aligned}
\gamma_1 : \mathbb{Z}C_p &\longrightarrow \mathbb{Z}[\theta] \times \mathbb{Z} \\
\sum_{i=0}^{p-1} \alpha_i g^i &\longmapsto \left(\sum_{i=0}^{p-1} \alpha_i \theta^i, \sum_{i=0}^{p-1} \alpha_i \right)
\end{aligned}$$

induz um isomorfismo de $\mathbb{Z}C_p$ com o subanel A de $\mathbb{Z}[\theta] \times \mathbb{Z}$ dado por $A = \{(x, y) | \Psi(x) = \rho(y)\}$, onde $\Psi : \mathbb{Z}[\theta] \longrightarrow \mathbb{Z}_p$ é o homomorfismo definido por $\Psi(\theta) = \overline{1}$ e $\rho : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ é o homomorfismo natural.

Demonstração. Ver [14], página 21. □

Agora suponhamos que t é uma raiz primitiva módulo p, isto é, $\overline{t}$ gera $\mathcal{U}(\mathbb{Z}_p)$.

Seja r o menor inteiro positivo tal que $tr \equiv 1 \mod p$ e $k = \dfrac{rt-1}{p}$. Para cada i, $1 \leqslant i \leqslant \dfrac{p-3}{2}$, definimos

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

Com essa notação, temos o seguinte

Teorema 3.0.7. *O conjunto* $W = \left\{u_1, u_2, \ldots, u_{\frac{p-3}{2}}\right\}$ *é um subconjunto multiplicativamente independente de* $\mathcal{U}_1(\mathbb{Z}C_p)$ *tal que* $\mathcal{U}_1(\mathbb{Z}C_p) = \langle g \rangle \times \langle W \rangle$.

Demonstração. Primeiramente, notemos que, como $tr \equiv 1 \mod p$, então $p|(tr-1)$. Logo, segue que $\mu_{tr-1} = 0$, isto é, $1+\theta+\cdots+\theta^{tr-2} = 0$. Notemos ainda que $\omega_{t,1}^{-1} = 1+\theta^t+\cdots+\omega^{t(r-1)}$, uma vez que

$$\begin{aligned}
\omega_{t,1}\omega_{t,1}^{-1} &= \left(1 + \theta + \cdots + \theta^{t-1}\right)\left(1 + \theta^t + \cdots + \omega^{t(r-1)}\right) = \\
&= 1 + \theta^t + \theta^{2t} + \cdots + \theta^{t(r-1)} + \\
&\quad +\theta + \theta^{t+1} + \theta^{t+2} + \cdots + \theta^{t(r-1)+1} + \cdots + \\
&\quad +\theta^{t-1} + \theta^{2t-1} + \theta^{3t-1} + \cdots + \theta^{tr-1}
\end{aligned}$$

Logo,

$$\begin{aligned}
\omega_{t,1}\omega_{t,1}^{-1} &= \left(1 + \theta + \theta^2 + \cdots + \theta^{t-1} + \theta^t + \cdots + \theta^{2t} + \cdots + \theta^{tr-2}\right) + \theta^{tr-1} = \\
&= 0 + \theta^{tr-1} = \theta^{pq} = (\theta^p)^q = 1,
\end{aligned}$$

uma vez que $p|(tr-1)$ e então $tr - 1 = qp$, para algum inteiro q.

Definimos anteriormente $h_i = \omega_{t,1}^{-1}\omega_{t,t^i}$ e vimos que $\langle \mathcal{U}_0 \rangle = \mathcal{U}_\psi$, onde $\mathcal{U}_0 = \left\{\theta, h_1, h_2, \ldots, h_{\frac{p-3}{2}}\right\}$.

Logo, $h_i \in \mathcal{U}_\psi$, quando $1 \leqslant i \leqslant \dfrac{p-3}{2}$.

Pela proposição 3.0.5, temos que $\mathcal{U}(\mathbb{Z}C_p) \simeq \mathcal{U}(A)$. Consideremos agora uma função que é a restrição de γ_1, restrita ao subgrupo $\mathcal{U}_1(\mathbb{Z}C_p)$, onde $G = C_p$. Assim, temos que γ_2 é a inversa de τ, definida acima, isto é, $\gamma_2 : \mathcal{U}_\psi \longrightarrow \mathcal{U}_1(\mathbb{Z}C_p)$, completamente determinada por $\gamma_2(g) = \theta$.

Temos assim

$$\begin{aligned}
\gamma_2(u_i) &= \gamma_2\left(\left(1+g^t+\cdots+g^{t(r-1)}\right)\left(1+g^{t^i}+\cdots+g^{t^i(t-1)}\right)-k\hat{g}\right)= \\
&= \gamma_2\left(1+g^t+\cdots+g^{t(r-1)}\right)\gamma_2\left(1+g^{t^i}+\cdots+g^{t^i(t-1)}\right)-\gamma_2\left(k\hat{g}\right)= \\
&= \left(1+\theta^t+\cdots+\theta^{t(r-1)}\right)\left(1+\theta^{t^i}+\cdots+\theta^{t^i(t-1)}\right)-k(\overbrace{1+\theta+\cdots+\theta^{p-1}}^{=0})= \\
&= \omega_{t,1}^{-1}\omega_{t,t^i}=h_i
\end{aligned}$$

Assim,$\gamma_2(u_i)=h_i \Rightarrow u_i=\tau(h_i)$.Vimos que

$$\mathcal{U}_\psi = \langle \mathcal{U} \rangle$$

e

$$\langle \mathcal{U} \rangle = \langle \mathcal{U}_0 \rangle ,$$

logo $\langle \mathcal{U}_0 \rangle = \mathcal{U}_\psi$. Assim, segue que $\tau\left(\langle \mathcal{U}_0 \rangle\right) = \tau\left(\mathcal{U}_\psi\right) = \mathcal{U}_1(\mathbb{Z}C_p)$.

Por outro lado,

$$\tau\left(\langle \mathcal{U}_0 \rangle\right) = \tau\left(\left\langle \theta, h_1, \ldots, h_{\frac{p-3}{2}} \right\rangle\right) = \left(\left\langle \tau(\theta), \tau(h_1), \ldots, \tau(h_{\frac{p-3}{2}}) \right\rangle\right) = \langle g, W \rangle .$$

□

Considerando agora um grupo G e $h \in G$ um elemento de ordem n, suponhamos que k, $3 \leqslant k \leqslant n-2$ é um inteiro ímpar, com $mdc(k,n)=1$.

Seja $\alpha_k(h) = 1 - h + h^2 - \cdots - h^{k-2} + h^{k-1} = \sum_{j=0}^{k-1}(-1)^j h^j$

Agora considere k' o menor inteiro positivo que é o inverso de k módulo n, isto é, $kk' \equiv 1 \mod n$.

Temos que

$$\beta = \sum_{j=0}^{k'-1}(-1)^j h^{jk}$$

é o inverso de α_k, se k' é ímpar e

$$\gamma = h \sum_{j=0}^{n-(k^{'}+1)} (-1)^j h^{jk},$$

se $k^{'}$ é par.

De fato, temos, se $k^{'}$ é ímpar

$$\begin{aligned}
\alpha_k.\beta &= (1-h+h^2-\cdots-h^{k-2}+h^{k-1})(1-h^k+h^{2k}+\cdots-h^{(k^{'}-2)k}+h^{(k^{'}-1)k}) = \\
&= 1-h^k+h^{2k}-h^{3k}+\cdots-h^{(k^{'}-2)k}+h^{(k^{'}-1)k}- \\
&- h+h^{k+1}-h^{2k+1}+h^{3k+1}-\cdots+h^{(k^{'}-2)k+1}-h^{(k^{'}-1)k+1}+ \\
&+ h^2-h^{k+2}+h^{2k+2}-h^{3k+2}+\cdots-h^{(k^{'}-2)k+2}+h^{(k^{'}-1)k+2}-\cdots- \\
&- h^{k-2}+h^{2k-2}-h^{3k-2}+h^{4k-2}-\cdots+h^{(k^{'}-2)k+(k-2)}-h^{(k^{'}-1)k+(k-2)}+ \\
&+ h^{k-1}-h^{2k-1}+h^{3k-1}-h^{4k-1}+\cdots-h^{(k^{'}-2)k+(k-1)}+h^{(k^{'}-1)k+(k-1)} = \\
&= 1-h+h^2-\cdots-h^{k-2}+h^{k-1}-h^k+h^{k+1}-h^{k-2}+\cdots+ \\
&+ h^{2k-2}-h^{2k-1}+h^{2k}-h^{2k+1}+\cdots+h^{(k^{'}-1)k}-h^{(k^{'}-1)k+1}+\cdots- \\
&- h^{(k^{'}-1)k+(k-2)}+\underbrace{h^{kk^{'}-1}}_{=1}
\end{aligned}$$

Temos que $h^{kk^{'}-1}=1$, pois $kk^{'} \equiv 1 \mod n$ e, portanto, $kk^{'}-1=sn$, para algum s inteiro. Como k e $k^{'}$ são ímpares, temos que $kk^{'}-1$ é par. Logo, sn é par. Já que n é ímpar, temos que s é par.

Nessa soma, temos $kk^{'}$ elementos. Podemos escrevê-la em $s+1$ linhas, da seguinte maneira:

$$\begin{aligned}
\alpha_k.\beta &= (1-h+h^2-h^3+\cdots-h^{k-2}+h^{k-1}-h^k+\cdots+h^{n-1})- \\
&- (h^n-h^{n+1}+h^{n+2}-h^{n+3}+\cdots-h^{2n-1})+ \\
&+ (h^{2n}-h^{2n+1}+h^{2n+2}+\cdots-h^{3n-1})-\cdots- \\
&- (h^{(sn-1)n}+\cdots-h^{sn-1})+ \\
&+ h^{sn}= \\
&= (1-h+h^2-h^3+\cdots-h^{k-2}+h^{k-1}-h^k+\cdots+h^{n-1})- \\
&- (1-h+h^2-h^3+\cdots-h^{k-2}+h^{k-1}-h^k+\cdots+h^{n-1})+ \\
&+ (1-h+h^2-h^3+\cdots-h^{k-2}+h^{k-1}-h^k+\cdots+h^{n-1})- \\
&- \cdots- \\
&- (1-h+h^2-h^3+\cdots-h^{k-2}+h^{k-1}-h^k+\cdots+h^{n-1})+ \\
&+ \underbrace{h^{sn}}_{=1}= \\
&= 1
\end{aligned}$$

Como s é par, $s+1$ é ímpar. Assim, cancelando as s primeiras linhas, segue que $\alpha_k.\beta = 1$. Agora consideremos o caso onde $k^{'}$ é par. O produto

$$\alpha_k.\gamma = h(1-h+h^2-\cdots-h^{k-2}+h^{k-1})(1-h^k+h^{2k}-\cdots-h^{(n-(k^{'}+1)-1)k}+h^{(n-(k^{'}+1))k})$$

tem $k.(n-k^{'})$ elementos.

$$\begin{aligned}
\alpha_k.\gamma &= h(1-h+h^2-\cdots-h^{k-2}+h^{k-1})(1-h^k+h^{2k}-\cdots-h^{(n-(k^{'}+1)-1)k}+h^{(n-(k^{'}+1))k})= \\
&= h(1-h^k+h^{2k}-\cdots-h^{(n-(k^{'}+1)-1)k}+h^{(n-(k^{'}+1))k}- \\
&- h+h^{k+1}-h^{2k+1}+\cdots+h^{(n-(k^{'}+1)-1)k+1}-h^{(n-(k^{'}+1))k+1}+ \\
&+ \cdots+ \\
&+ h^{k-1}-h^{2k-1}+\cdots+h^{k(n-k^{'})-1})
\end{aligned}$$

Temos que $k(n-k^{'}) = kn-kk^{'} \equiv -kk^{'} \equiv -1 \mod n \equiv (n-1) \mod n$. Assim, $n|[k(n-k^{'})+1]$ e, portanto $k(n-k^{'}) = qn-1$, para algum $q \in \mathbb{Z}$. E como $k(n-k^{'})$ e n são ímpares, temos que $(qn-1)$ é ímpar e assim q é par. Assim, podemos escrever o produto acima em q linhas:

$$\begin{aligned}
\alpha_k.\gamma &= h(1-h+h^2-\cdots-h^{k-2}+h^{k-1})(1-h^k+h^{2k}-\cdots-h^{(n-(k'+1)-1)k}+h^{(n-(k'+1))k}= \\
&= h[(1-h+\cdots+h^{k-1}-h^k+\cdots+h^{n-1})- \\
&= (h^n+h^{n-1}-\cdots-h^{2n-1})+ \\
&+ \cdots- \\
&- (h^{(q-2)n}+\cdots+h^{(q-1)n-1})- \\
&- (h^{(q-1)n}+h^{(q-1)n+1}-\cdots+h^{qn-2})]
\end{aligned}$$

As primeiras $(q-2)$ linhas são canceladas, uma vez que $(q-2)$ é par. E nas linhas $(q-1)$ e q todos os elementos são cancelados, exceto $h^{(q-1)n-1}$.

Portanto,

$$\alpha_k.\gamma = h.h^{(q-1)n-1} = h^{(q-1)n} = 1$$

Assim, podemos enunciar o seguinte

Teorema 3.0.8. *Se $\langle\overline{2}\rangle = \mathcal{U}(\mathbb{Z}_p)$, então o conjunto das unidades alternadas $\mathcal{C} = \{\alpha_3, \alpha_4, \ldots, \alpha_{p-2}\}$ é multiplicativativamente independente e tal que*

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

onde $\mathcal{U}_1$ é o subgrupo de unidades normalizadas de $\mathbb{Z}C_p$.

Demonstração. Como $\langle\overline{2}\rangle = \mathcal{U}(\mathbb{Z}_p) = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ e r é o menor inteiro positivo tal que $2r \equiv 1 \mod p$, então $p|(2r-1)$ e, portanto, $r = \dfrac{lp+1}{2}$, onde l é um inteiro.

Assim, para $l = 1$, temos que $r = \dfrac{p+1}{2}$ e $k = \dfrac{2r-1}{p} = 1$.

Daí, para cada $1 \leqslant i \leqslant \dfrac{p-3}{2}$, u_i é da forma

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

Agora, coloquemos

$\eta_i = u_i$, se $2^i \equiv k \mod p$, com k ímpar e $\eta_i = u_i g^{p-k}$, se $2^i \equiv k \mod p$, com k par, onde $2 \leqslant k \leqslant p-3$.

Segue que $\left\langle g, \eta_1, \ldots, \eta_{\frac{p-3}{2}} \right\rangle = \langle g, W \rangle$. Anteriormente, vimos que $\mathcal{U}_1 = \langle g, W \rangle$, onde $\mathcal{U}_1$ é o grupo de unidades normalizadas de $\mathbb{Z}C_p$. Logo, vem que

$$\left\langle g, \eta_1, \ldots, \eta_{\frac{p-3}{2}} \right\rangle = \mathcal{U}_1$$

Temos que $2^{p-1} \equiv 1 \mod p$, pelo Pequeno Teorema de Fermat. Logo,

$$2^{\frac{p-1}{2}} 2^{\frac{p-1}{2}} \equiv 1 \mod p \Rightarrow (2^{\frac{p-1}{2}})^2 \equiv 1 \mod p \Rightarrow p \left| \left((2^{\frac{p-1}{2}})^2 - 1\right)\right.$$

Então ou $p \left| \left(2^{\frac{p-1}{2}} - 1\right)\right.$ ou $p \left| \left(2^{\frac{p-1}{2}} + 1\right)\right.$.

Se $p \left| \left(2^{\frac{p-1}{2}} - 1\right)\right.$, então $2^{\frac{p-1}{2}} \equiv 1 \mod p$, o que é um absurdo, já que a ordem de $\mathcal{U}(\mathbb{Z}_p)$ é $(p-1)$.

Assim, $2^{\frac{p-1}{2}} \equiv -1 \mod p \equiv (p-1) \mod p$.

Suponhamos que $2^i \equiv -1 \mod p$, com $1 \leqslant i \leqslant \dfrac{p-1}{2} - 1$. Logo,

$$2^{\frac{p-1}{2}} 2^i \equiv 1 \mod p$$

e

$$\frac{p-1}{2} \leqslant \frac{p-1}{2} + i \leqslant \frac{p-1}{2} + \frac{p-1}{2} - 1 = p - 1 - 1 = p - 2$$

Mas não ocorre $2^b \equiv 1 \mod p$, com $\dfrac{p-1}{2} \leqslant b \leqslant (p-2)$.

Assim, $2^{\frac{p-1}{2}} \not\equiv -1 \mod p$ e $2^{\frac{p-1}{2}} \equiv 1 \mod p$ não ocorre pelo mesmo motivo.

Observemos que o intuito da mudança no segundo caso é trocar o elemento

$$u_i = (1 + g^2 + \cdots + g^{p-1})(1 + g^k) - \hat{g}$$

por

$$u_i = (1 + g^2 + \cdots + g^{p-1})(1 + g^{p-k}) - \hat{g},$$

quando k é par.

Para k ímpar, $3 \leqslant k \leqslant p-2$, temos:

$$\begin{aligned}
& (1 + g^2 + \cdots + g^{p-1})(1 + g^k) - \hat{g} = \\
= \; & (1 + g^2 + \cdots + g^{p-1}) + (1 + g^2 + \cdots + g^{p-1})g^k - \hat{g} = \\
= \; & (1 + g^2 + \cdots + g^{k-1}) + (g^{k+1} + g^{k+3} + \cdots + g^{p-1}) + (1 + g^2 + \cdots + g^{p-1})g^k - \hat{g} = \\
= \; & (1 + g^2 + \cdots + g^{k-1}) + (g^{k+1} + g^{k+3} + \cdots + g^{p-1}) + (g^k + g^{k+2} + \cdots + g^{p-2}) + \\
+ \; & (1 + g^2 + \cdots + g^{k-1}) - \hat{g} = \\
= \; & 2(1 + g^2 + \cdots + g^{k-1}) + (g^k + g^{k+1} + \cdots + g^{p-1}) - \hat{g} = \\
= \; & 2(1 + g^2 + \cdots + g^{k-1}) + g^k + g^{k+1} + \cdots + g^{p-1} - 1 - g^2 - g^k - g^{k+1} - \cdots - g^{p-1} = \\
= \; & 2(1 + g^2 + \cdots + g^{k-1}) - 1 - g^2 - g^k - g^{k+1} - \cdots - g^{k-1} = \\
= \; & 1 - g + g^2 - g^3 + \cdots - g^{k-2} + g^{k-1} = \alpha_k
\end{aligned}$$

Agora, observemos que $\eta_i = \eta_j \Rightarrow u_i = g^{p-k}u_j \Rightarrow u_i = u_j^{-1} = g^{p-k} \Rightarrow (u_i = u_j^{-1})^p = 1 \Rightarrow u_i^p = u_j^p$, o que é um absurdo.

Assim, concluímos que

$$\left\{\eta_1, \ldots, \eta_{\frac{p-3}{2}}\right\} = \left\{(1 + g^2 + \cdots + g^{p-1})(1 + g^3) - \hat{g}, \ldots, (1 + g^2 + \cdots + g^{p-1})(1 + g^{p-2}) - \hat{g}\right\}$$

E, portanto,

$$\left\{\eta_1, \ldots, \eta_{\frac{p-3}{2}}\right\} = \{\alpha_3, \ldots, \alpha_{p-2}\} = \mathcal{C},$$

o que conclui a demonstração. □

Capítulo 4

Unidades centrais de $\mathbb{Z}A_5$

Nesse capítulo explicitaremos as unidades centrais de $\mathbb{Z}A_5$, onde A_5 denota o subgrupo de permutações pares de S_5. Primeiramente estudaremos um pouco da Teoria de Caracteres e alguns resultados de Teoria de Números.

4.1 Teoria de Caracteres

Definição 4.1.1. *Seja G um grupo, R um anel comutativo e V um R-módulo livre de posto finito. Uma* ***representação de G sobre R, com espaço de representação V****, é um homomorfismo de grupos $T : G \longrightarrow GL(V)$, onde $GL(V)$ denota o grupo de R-automorfismos de V. O posto de V é chamado de grau da representação T e será denotada por $deg(T)$.*

Denotaremos por $T_g : V \longrightarrow V$ o correspondente automorfismo em T, para um elemento $g \in G$. Assim, se $g, h \in G$, temos que $T_{gh} = T_g \circ T_h$ e $T_1 = I$, onde I é a identidade.

Podemos fixar uma R-base em V e definir um isomorfismo ρ de $GL(V)$ em $GL(n, R)$, onde $GL(n, R)$ é o grupo das matrizes invertíveis de ordem n, com coeficientes em R, associando cada automorfismo $T \in GL(V)$ à uma matriz, com respeito a uma base fixada.

Desta forma, temos a seguinte definição:

Definição 4.1.2. *Seja G um grupo e R um anel comutativo. Uma* ***representação matricial de G sobre R de grau n*** *é um homomorfismo de grupos $T : G \longrightarrow GL(n, R)$.*

Logo, se $T : G \longrightarrow GL(n, R)$ é uma representação de G sobre R, como espaço de representação V e consideramos o isomorfismo $\rho : GL(V) \longrightarrow GL(n, R)$, associado a uma base fixada, então $\rho \circ T : G \longrightarrow GL(n, R)$ é uma representação matricial de G. Analogamente, se temos uma representação matricial $T : G \longrightarrow GL(n, R)$, então $\rho^{-1} \circ T : G \longrightarrow GL(V)$ é uma repre-

sentação de G sobre R. Por esse motivo, não distinguiremos representação de representação matricial.

Definição 4.1.3. *Uma representação $T : G \longrightarrow GL(V)$ de um grupo G sobre um corpo K é dita* ***irredutível*** *se V não é nulo e os únicos espaços invariantes de V sob T são os triviais: 0 e V. A representação é chamada redutível se V contém um subespaço não trivial W, que é invariante sob T.*

Agora, dada uma matriz $A = (a_{ij})$ de ordem n, temos que o **traço de** A é dado por $tr(A) = \sum_{i=1}^{n} a_{ii}$. Notemos que se temos duas matrizes A e B, de mesma ordem, então $tr(AB) = tr(BA)$.

Definição 4.1.4. *Seja G um grupo e V um espaço vetorial de dimensão finita sobre um corpo K. Então um* ***caracter χ de G associado à representação*** *T é a função $\chi : G \longrightarrow K$ é dada por $\chi(g) = tr(T_g)$, para todo $g \in G$. O caracter χ é dito* ***caracter irredutível*** *se T é uma representação irredutível. Chamaremos de $Irr(G)$ o conjunto de todos caracteres irredutíveis do grupo G.*

Proposição 4.1.1. *Seja K um corpo algebricamente fechado e G um gripo finito. Então, o número de elementos de $Irr(G)$ é igual ao número de classes de conjugação de G.*

Se χ denota o caracter associado à representação $T : G \longrightarrow GL(V)$, o grau da representação é também chamado de o **grau do caracter** χ, isto é, $deg(\chi) = [V : K]$.

Notemos que se K tem característica zero, então $\chi(1_G) = tr(T_{1_G}) = tr(I) = [V : K] = deg(\chi)$

Definição 4.1.5. *Sejam $x, y \in G$. Dizemos que x é o* ***conjugado*** *a y em G se $y = g^{-1}xg$, para algum $g \in G$. O conjunto de todos os elementos conjugados a x em G é $x^G = \{g^{-1}xg : g \in G\}$ e é chamado de* ***classe de conjugação*** *de x em G.*

Definição 4.1.6. *Se $G = \bigcup_{i=1}^{r} x_i^G$, onde as classes de conjugação $x_1^G, \ldots, x_r^G$ são distintas, então chamamos $x_1, \ldots, x_r$ de* ***representantes das classes de conjugação de*** *G.*

Definição 4.1.7. *Sejam G um grupo, R um anel comutativo e $\{C_i\}_{i \in I}$ o conjunto de classes de conjugação de G que contém apenas um número finito de elementos. Para cada $i \in I$, seja $y_i = \hat{C}_i = \sum_{x \in C_i} x$. Esses elementos são chamados de* ***somas de classe de*** *G* ***sobre*** *R.*

Teorema 4.1.1. *Seja G um grupo e seja R um anel comutativo. Então, o conjunto $\{y_i\}_{i\in I}$ de todas as somas de classe de G sobre R, formam uma base de $\mathcal{Z}(RG)$, o centro de RG sobre R.*

Demonstração. Ver [16], página 151, teorema 3.6.2. □

Definição 4.1.8. *Uma função $\varphi : G \longrightarrow \mathbb{C}$ é chamada uma* ***função de classe*** *se é constante nas classes de conjugação de G, isto é, se $x = g^{-1}yg$, para $x, y, g \in G$ implica que $\varphi(x) = \varphi(y)$*

Proposição 4.1.2. *Toda função de classe $\varphi : G \longrightarrow \mathbb{C}$ pode ser expressa unicamente na forma*

$$\varphi = \sum_{i=1}^{r} a_i\chi_i,$$

onde $a_i \in \mathbb{C}, 1 \leqslant i \leqslant r$. Assim, $\{\chi_1, \chi_2, \ldots \chi_r\}$ é uma base do $\mathbb{C}$-espaço vetorial de todas as funções de classe de G sob $\mathbb{C}$.

Notemos que, pela Proposição acima, uma função de classe que pode ser escrita na forma

$$\varphi = \sum_{i=1}^{r} a_i\chi_i,$$

onde $a_i \in \mathbb{C}$, $1 \leqslant i \leqslant r$, é um caracter se e somente se $\varphi \neq 0$, $a_i \in \mathbb{Z}$, $a_i \geqslant 0$, $1 \leqslant i \leqslant r$. O caractere χ_i, cujo coeficiente correspondente é a_i, com $a_i \neq 0$, é chamado de *constituintes* de φ.

Sabemos que os caracteres são contantes nas classes de conjugação $C_1, \ldots, C_r$ de G. Então, escolhamos elementos $x_i \in C_i$, onde $1 \leqslant i \leqslant r$. Logo, os caracteres $\chi_1, \ldots, \chi_r$ são completamente determinados pelos valores $\chi_i(x_j)$, com $1 \leqslant i, j \leqslant r$. Assim, podemos colocar esses valores numa matriz quadrada, da seguinte forma:

$$\begin{bmatrix} \chi_1(x_1) & \chi_1(x_2) & \cdots & \chi_1(x_r) \\ \chi_2(x_1) & \chi_2(x_2) & \ldots & \chi_2(x_r) \\ \vdots & \vdots & \vdots & \vdots \\ \chi_r(x_1) & \chi_r(x_2) & \cdots & \chi_r(x_r) \end{bmatrix}$$

Definição 4.1.9. *A matriz $(\chi_i(x_j))$ acima é chamada de* ***tábua de caracteres do grupo*** *G.*

Agora, dado um grupo G, denotemos por $\{e_1, e_2, \ldots, e_r\}$ o conjunto de idempotentes centrais primitivos de $\mathbb{C}G$. Temos:

Teorema 4.1.2. *Com as notações acima, temos*

$$e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g$$

Demonstração. Ver [16], página 185, teorema 5.1.11. □

Teorema 4.1.3. *Sejam T uma representação de um grupo G sobre $\mathbb{C}$ de grau n e χ o caracter de G. Então, temos:*

1. *$[T_g]$ é semelhante à matriz*

$$[T_g] \sim \begin{bmatrix} \zeta_1 & 0 & \cdots & 0 \\ 0 & \zeta_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \zeta_n \end{bmatrix}$$

   onde ζ_i é raiz n-ésima da unidade de ordem n.

2. $\chi(g) = \sum_{i=1}^{n} \zeta_i$ *e* $|\chi(g)| \leqslant \chi(1)$

3. $\chi(g^{-1}) = \overline{\chi(g)}$

Demonstração. 1. Temos que $g^{|G|} = 1$. Logo, $T_g^{|G|} = I$. Portanto, T_g é raiz do polinômio $x^{|G|} - 1$, o qual é um múltiplo do pôlinômio minimal de $[T_g]$. Logo, $[T_g]$ é diagonalizável e segue

$$[T_g] \sim \begin{bmatrix} \zeta_1 & 0 & \cdots & 0 \\ 0 & \zeta_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \zeta_n \end{bmatrix}$$

2. Pela demonstração anterior, segue diretamente que $\chi(g) = \sum_{i=1}^{n} \zeta_i$

   Temos ainda

$$|\chi(g)| = |\sum_{i=1}^{n} \zeta_i| \leqslant \sum_{i=1}^{n} |\zeta_i| = n = \chi(1)$$

3. Temos

$$[T_g^{-1}] \sim \begin{bmatrix} \zeta_1^{-1} & 0 & \cdots & 0 \\ 0 & \zeta_2^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \zeta_n^{-1} \end{bmatrix}$$

Logo, $\chi(g^{-1}) = \sum_{i=1}^{n} \zeta_i^{-1}$. Como toda raiz complexa da unidade ζ satisfaz $\zeta^{-1} = \overline{\zeta}$, segue que $\chi(g^{-1}) = \sum_{i=1}^{n} \overline{\zeta_i} = \overline{\chi(g)}$.

□

Agora, seja G um grupo finito. Vamos utilizar as seguintes notações:

- $K_0 = 1, K_1, \ldots, K_r$ são as classes de conjugação de G
- $y_0 = 1, y_1, \ldots, y_r$ são as somas de classe de $K_0 = 1, K_1, \ldots, K_r$, respectivamente
- $x_0 = 1, x_1, \ldots, x_r$ são os representantes das classes $K_0 = 1, K_1, \ldots, K_r$, respectivamente
- $\{\chi_0 = 1_G, \chi_1, \ldots, \chi_r\}$ é um conjunto de caracteres complexos irredutíveis do grupo G, onde 1_G é o caracter principal (o caracter principal é aquele que satisfaz $\chi(g) = 1_G$, para todo $g \in G$) e os graus de $\chi_0 = 1_G, \chi_1, \ldots, \chi_r$ são $deg(\chi_0) = 1, deg(\chi_1), \ldots, deg(\chi_r)$, respectivamente.
- $\{e_0, e_1, \ldots, e_r\}$ é um sistema completo de idempotentes minimais ortogonais tais que para todo $0 \leqslant i \leqslant r$, o idempotente e_i corresponde ao caracter χ_i.

Vamos considerar também, a decomposição de $\mathbb{C}G$ como soma direta de suas componentes simples.

Como vimos anteriormente, temos

$$\mathbb{C}G = \bigoplus_{i=0}^{r} (\mathbb{C}G)e_i \simeq \bigoplus_{i=0}^{r} (M_{n_i}\mathbb{C}),$$

onde $\{e_1, \ldots, e_r\}$ é um conjunto de idempotentes centrais primitivos. Para cada idempotente e_i, temos o correspondente $(0, \ldots, 0, I^{n_i}, 0, \ldots, 0)$, via isomorfismo, onde I^{n_i} denota a matriz identidade do anel $M_{n_i}(\mathbb{C})$, com $i \in \{1, \ldots, r\}$. Se considerarmos T_i como representação da álgebra $\mathbb{C}G$ definida por $T_i\left(\sum_{g\in G} \alpha(g)g\right) = \sum_{g\in G} \alpha(g)T_i(g)$, temos que $T_i(e_i)$ é a função linear definida sobre $I_i \simeq \mathbb{C}^{n_i}$, pela multiplicação pelo elemento identidade. Isto é, é a função identidade sobre a componente simples. Já que $e_ie_j = 0$ se $i \neq j$, segue que $T_i(e_j)$ é nula sobre I_j. Logo, temos que $\chi(e_i) = tr(I^{(i)}) = deg(T_i) = \chi(1)$ e $\chi(e_j) = 0$, se $i \neq j$.

Assim, temos a seguinte

Proposição 4.1.3. *Seja G um grupo finito. Consideremos $\mathbb{C}G = (\mathbb{C}G)e_1 \oplus (\mathbb{C}G)e_2 \oplus \cdots \oplus (\mathbb{C}G)e_r$, onde r é o número de classes de conjugação distintas de G. Considerando as notações acima, temos*

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{j=0}^{r} \overline{\chi_i(x_j)} y_j$$

e

$$y_i = |K_i| \sum_{j=0}^{r} \frac{\chi_j(x_i)}{\chi_j(1)} e_j$$

Ou seja, podemos escrever os idempotentes e_i na base $\mathcal{B} = \{y_1, y_2, \ldots, y_r\}$ e cada elemento da base $\mathcal{B}$, y_i, pode ser escrito na base $\{e_1, e_2, \ldots, e_r\}$.

Demonstração. Temos que $\sum_{g\in G} \overline{\chi_i(g)}g = \sum_{g\in K_1} \overline{\chi_i(g)}g + \cdots + \sum_{g\in K_r} \overline{\chi_i(g)}g$, uma vez que $G = K_1 \bigcup \cdots \bigcup K_r$. Sabemos que χ_i, $1 \leqslant i \leqslant r$, é constante nas classes de conjugação de G. Logo, vem que

$$\sum_{g\in G} \overline{\chi_i(g)}g = \overline{\chi_i(x_1)} \left(\sum_{g\in K_1} g\right) + \cdots + \overline{\chi_i(x_r)} \left(\sum_{g\in K_r} g\right)$$

Como $y_1, \ldots, y_r$ são as somas de classe, segue

$$\sum_{g\in G} \overline{\chi_i(g)}g = \overline{\chi_i(x_1)}y_1 + \cdots + \overline{\chi_i(x_r)}y_r = \sum_{j=1}^{r} \overline{\chi_i(x_j)}y_j$$

Pela Proposição 4.1.2, temos

$$e_i = \frac{1}{|G|}\sum_{g\in G}\chi_i(1)\chi_i(g^{-1})g$$

Logo,

$$e_i = \frac{1}{|G|}\sum_{g\in G}\chi_i(1)\chi_i(g^{-1})g = \frac{\chi_i(1)}{|G|}\sum_{j=0}^{r}\overline{\chi_i(x_j)}y_j$$

Agora, seja $y_i \in \mathcal{B}$. Como y_i está em $\mathbb{C}G = \bigoplus_{i=0}^{r}(\mathbb{C}G)e_i$, podemos escrever $y_i = \sum_{k=1}^{r} x_k e_k$. Daí, vem que

$$\chi_j(y_i) = \sum_{k=0}^{r} x_k\chi_j(e_k) = x_j\chi_j(1)$$

Também temos que

$$\chi_j(y_i) = \chi\left(\sum_{g\in K_i} g\right) = |K_i|\chi_j(x_i)$$

Assim, $x_j = \dfrac{|K_i|\chi_j(x_i)}{\chi_j(1)}$. Portanto, $y_i = |K_i|\sum_{j=0}^{r}\dfrac{\chi_j(x_i)}{\chi_j(1)}e_j$.

Agora, podemos escrever

$$e_i = \frac{\chi_i(1)}{|G|}\sum_{j=0}^{r}\overline{\chi_i(x_j)}y_j = \sum_{j=0}^{r} t_{ij}y_j$$

e

$$y_i = |K_i|\sum_{j=0}^{r}\frac{\chi_j(x_i)}{\chi_j(1)}e_j = \sum_{j=0}^{r} s_{ij}e_j$$

□

Então a matriz $T = (t_{ij})$ é a matriz de transformação da base $\{y_0, \ldots, y_r\}$ para a base $\{e_0, \ldots, e_r\}$. Analogamente, $S = (s_{ij})$ é a matriz de transformação da base $\{e_0, \ldots, e_r\}$ para a base $\{y_0, \ldots, y_r\}$. Também temos a matriz que é chamada de **tábua de caracteres**, conforme

Definição 4.1.9: $X = (\chi_{ij})$, onde $\chi_{ij} = \chi_i(x_j)$, com $i = 0, 1, \ldots, r$. Vamos denotar a matriz diagonal com entradas $d_0, \ldots, d_r$ por $diag(d_0, \ldots, d_r)$. Então, temos que

$$S = diag\left(\frac{1}{deg(\chi_0)}, \ldots, \frac{1}{deg(\chi_r)}\right).X.diag(|K_0|, \ldots, |K_r|)$$

e

$$T = \left(\frac{1}{|G|}\right).X^*.diag(deg(\chi_0), \ldots, deg(\chi_r)),$$

onde X^* é a matriz transporta conjugada de X.

Seja u um elemento qualquer em $\mathbb{C}G$. Escrevendo u nas duas bases, temos $u = \sum_{i=0}^{r} \gamma_i y_i = \sum_{i=0}^{r} \beta_i e_i$. Então temos

$$\begin{bmatrix} \beta_0 \\ \vdots \\ \beta_r \end{bmatrix} = S \begin{bmatrix} \gamma_0 \\ \vdots \\ \gamma_r \end{bmatrix}$$

e

$$\begin{bmatrix} \gamma_0 \\ \vdots \\ \gamma_r \end{bmatrix} = T \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_r \end{bmatrix},$$

para todo $i \in \{1, \ldots, r\}$.

Daí,

$$\beta_i = \sum_{j=0}^{r} s_{ij}\gamma_j = \sum_{j=0}^{r} \frac{|K_j|\chi_i(x_j)\gamma_j}{(\chi_i(1))} = \frac{1}{\chi_i(1)} \sum_{j=0}^{r} \chi_i(y_j)\gamma_j \tag{4.1}$$

e

$$\gamma_i = \sum_{j=0}^{r} t_{ij}\beta_j = \sum_{j=0}^{r} \frac{1}{|G|} \sum_{j=0}^{r} \chi_j(1)\overline{\chi_j(x_i)}\beta_j \tag{4.2}$$

Agora enunciaremos o teorema de Brauer, que nos permitirá encontrar uma extensão que é um corpo de decomposição para o grupo G.

Teorema 4.1.4. *Seja G um grupo finito de expoente m. Então a extensão $\mathbb{Q}(\sqrt[m]{1})$ de $\mathbb{Q}$ é um corpo de decomposição para o grupo G.*

Agora consideremos A o grupo de Galois da extensão $\mathbb{Q}(\sqrt[m]{1})$ sobre o corpo $\mathbb{Q}$. Temos a seguinte

Definição 4.1.10. *Sejam G um grupo de expoente m e A o grupo de Galois da extensão $\mathbb{Q}(\sqrt[m]{1})$. Se $\sigma \in A$, podemos definir para todo $i = 0, 1, \ldots, r$ a aplicação $\chi_i^\sigma : G \longrightarrow \mathbb{C}$, onde $\chi_i^\sigma(x) = \sigma(\chi_i(x))$, para todo $x \in G$. Nesse caso, dizemos que os caracteres χ_i e χ_i^σ são* ***algebricamente conjugados****.*

Notemos que, para todo i, χ_i^σ é um caracter irredutível do grupo G e então $\chi_i^\sigma \in \{\chi_0, \ldots, \chi_r\}$.

Teorema 4.1.5. *Seja $\{\chi_0, \ldots, \chi_p\}$ um conjunto de caracteres irredutíveis complexos não conjugados algebricamente de um grupo G. Para cada $i = 0, 1, \ldots, p$, denotamos por $\mathbb{Q}(\chi_i)$ a menor extensão do corpo $\mathbb{Q}$ que contém a imagem do caracter χ_i. Então o centro da álgebra de grupo $\mathcal{Z}(\mathbb{Q}G)$ é tal que $\mathcal{Z}(\mathbb{Q}G) \simeq \mathbb{Q}(\chi_0) \oplus \cdots \oplus \mathbb{Q}(\chi_p)$.*

Demonstração. [1], Teorema 1. □

Teorema 4.1.6. *O grupo de unidades do centro $\mathcal{Z}(\mathbb{Q}G)$ é isomorfo ao produto direto $\mathcal{U}(\mathbb{Q}(\chi_0)) \oplus \cdots \oplus \mathcal{U}(\mathbb{Q}(\chi_p))$.*

Demonstração. [1], Teorema 2. □

Teorema 4.1.7. *O centro $\mathcal{Z}(\mathbb{Z}G)$ de um anel de grupo $\mathbb{Z}G$ tem apenas unidades triviais se e somente se, os valores de todos caracteres irredutíveis complexos do grupo G são inteiros ou estão no corpo $\mathbb{Q}(\sqrt{-d})$, onde d é um inteiro positivo.*

Demonstração. [1], Teorema 6. □

Vamos ver um exemplo de como aplicar o Teorema 4.1.5, considerando o subgrupo de permutações pares de S_4, o grupo alternado A_4.

Consideremos a tábua de caracteres de A_4 (ver [13], página 181):

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \lambda & \lambda^2 \\ 1 & 1 & \lambda^2 & \lambda \\ 3 & -1 & 0 & 0 \end{bmatrix},$$

onde $\lambda = \frac{-1}{2} + \frac{\sqrt{-3}}{2}$

Sabemos que A_4 tem 4 classes de conjugação. Logo, tem 4 caracteres irredutíveis, isto é, $Irr(A_4) = \{\chi_1 = 1, \chi_2, \chi_3, \chi_4\}$. Seja A o grupo de Galois do corpo $K = \mathbb{Q}(\sqrt[m]{1})$, onde m é o expoente de A_4. Sabemos que $m = 3$ e, portanto, $K = \mathbb{Q}(\sqrt{-3})$. Temos que se $\sigma \in A$, então $\sigma : K \longrightarrow K$ é tal que $\sigma(x) = x$, para todo $x \in \mathbb{Q}$. Podemos observar que $\lambda^2 = \frac{-1}{2} - \frac{\sqrt{-3}}{2}$. O automorfismo que leva um elemento da forma $a + b\sqrt{-3}$ em $a - b\sqrt{-3}$, para $a, b \in \mathbb{Q}$, pertence a A, uma vez que fixa os racionais e é um automorfismo de $\mathbb{Q}(\sqrt{-3})$ em $\mathbb{Q}(\sqrt{-3})$. Além disso, por esse automorfismo, temos que λ e λ^2 são algebricamente conjugados, uma vez que $\lambda^2 = \frac{-1}{2} - \frac{\sqrt{-3}}{2}$. Então, temos 2 caracteres algebricamente conjugados e são únicos, uma vez que os demais tem elementos racionais não comuns. Assim, pelo Teorema 4.1.5, temos que $\mathcal{Z}(\mathbb{Q}A_4) \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\lambda) = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\sqrt{-3})$.

Agora, considerando o grupo alternado A_5, subgrupo das permutações pares de S_5, temos que sua tábua de caracteres, segundo [13], página 221, é

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & -1 & 0 & \omega & \omega' \\ 3 & -1 & 0 & \omega' & \omega \\ 4 & 0 & 1 & -1 & -1 \\ 5 & 1 & -1 & 0 & 0 \end{bmatrix},$$

onde $\omega = \frac{1+\sqrt{5}}{2}$ e $\omega' = \frac{1-\sqrt{5}}{2}$

Sabemos que A_5 tem 5 classes de conjugação ([13], página 113) e tem, portanto, 5 caracteres irredutíveis.

Analogamente ao que fizemos acima para A_4, notamos que o automorfismo σ, definido por $\sigma(a + b\sqrt{5}) = a - b\sqrt{5}$ pertence ao grupo de Galois $Gal(\mathbb{Q} : \mathbb{Q}(\sqrt{5}))$. Assim, temos que ω e ω' são algebricamente conjugados.

Logo, $\mathcal{Z}(\mathbb{Q}A_5) \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\omega) = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\sqrt{5})$

Temos que as classes de conjugação de A_5, $K_0, K_1, \ldots, K_4$, tem cardinalidades $1, 12, 15$ e 20, onde duas classes tem cardinalidade igual a 12 ([13], página 113).

Seja $T = (t_{ij})$ a matriz que leva a base $\{y_0, y_1, \ldots, y_4\}$ de $\mathcal{Z}(\mathbb{C}A_5)$ na base $\{e_0, e_1, \ldots, e_4\}$ de idempotentes minimais ortogonais de $\mathcal{Z}(\mathbb{C}A_5)$.

Se chamarmos os representantes das classes de conjugação de $x_0, \ldots, x_4$, respectivamente, a tábua de caracteres $X = (x_{ij})$ é tal que $\chi_{ij} = \chi_i(x_j)$, para todo $i, j \in \{0, 1, \ldots, 4\}$.

Usando as notações definidas anteriormente, temos

$$S = \begin{bmatrix} \frac{1}{\chi_1(1)} & 0 & 0 & 0 \\ 0 & \frac{1}{\chi_2(1)} & 0 & 0 \\ 0 & 0 & \frac{1}{\chi_3(1)} & 0 \\ 0 & 0 & 0 & \frac{1}{\chi_4(1)} \end{bmatrix} .X. \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 20 & 0 & 0 & 0 \\ 0 & 0 & 15 & 0 & 0 \\ 0 & 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 0 & 12 \end{bmatrix} =$$

$$S = \begin{bmatrix} \frac{1}{\chi_1(1)} & 0 & 0 & 0 \\ 0 & \frac{1}{\chi_2(1)} & 0 & 0 \\ 0 & 0 & \frac{1}{\chi_3(1)} & 0 \\ 0 & 0 & 0 & \frac{1}{\chi_4(1)} \end{bmatrix} . \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & -1 & 0 & \omega & \omega' \\ 3 & -1 & 0 & \omega' & \omega \\ 4 & 0 & 1 & -1 & -1 \\ 5 & 1 & -1 & 0 & 0 \end{bmatrix} . \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 20 & 0 & 0 & 0 \\ 0 & 0 & 15 & 0 & 0 \\ 0 & 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 0 & 12 \end{bmatrix}$$

Logo,

$$S = \begin{bmatrix} 1 & 15 & 20 & 12 & 12 \\ 1 & -5 & 0 & 4\omega & 4\omega' \\ 1 & -5 & 0 & 4\omega' & 4\omega \\ 1 & 0 & -5 & -3 & -3 \\ 1 & 3 & -4 & 0 & 0 \end{bmatrix}$$

Temos ainda

$$T = \frac{1}{60}.\begin{bmatrix} 1 & 3 & 3 & 4 & 5 \\ 1 & -1 & -1 & 0 & 1 \\ 1 & 0 & 0 & 1 & -1 \\ 1 & \omega' & \omega & -1 & 0 \\ 1 & \omega & \omega' & -1 & 0 \end{bmatrix}.\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 9 & 9 & 16 & 25 \\ 1 & -3 & -3 & 0 & 5 \\ 1 & 0 & 0 & 4 & -5 \\ 1 & 3\omega' & 3\omega & -4 & 0 \\ 1 & 3\omega & 3\omega' & -4 & 0 \end{bmatrix}$$

Agora, escrevendo $u = \sum_{i=0}^{4} \gamma_i y_i = \sum_{i=0}^{4} \beta_i e_i$, temos

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \end{bmatrix} = S \begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \end{bmatrix}$$

e

$$\begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \end{bmatrix} = T \begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \end{bmatrix},$$

para todo $i \in \{1, \ldots, r\}$.
Logo,

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \end{bmatrix} = \begin{bmatrix} 1 & 15 & 20 & 12 & 12 \\ 1 & -5 & 0 & 4\omega & 4\omega' \\ 1 & -5 & 0 & 4\omega' & 4\omega \\ 1 & 0 & -5 & -3 & -3 \\ 1 & 3 & -4 & 0 & 0 \end{bmatrix}.\begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \end{bmatrix}$$

Assim, obtemos o seguinte sistema:

$$I = \begin{cases} \beta_0 = \gamma_0 + 15\gamma_1 + 20\gamma_2 + 12\gamma_3 + 12\gamma_4 \\ \beta_1 = \gamma_0 - 5\gamma_1 + 4\omega\gamma_3 - 4\omega'\gamma_4 \\ \beta_2 = \gamma_0 - 5\gamma_1 + 4\omega'\gamma_3 - 4\omega\gamma_4 \\ \beta_3 = \gamma_0 + 5\gamma_1 - 3\gamma_3 - 3\gamma_4 \\ \beta_4 = \gamma_0 + 3\gamma_1 - 4\gamma_3 \end{cases}$$

Temos também

$$\begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \end{bmatrix} = \frac{1}{60} \begin{bmatrix} 1 & 9 & 9 & 16 & 25 \\ 1 & -3 & -3 & 0 & 5 \\ 1 & 0 & 0 & 4 & -5 \\ 1 & 3\omega^{'} & 3\omega & -4 & 0 \\ 1 & 3\omega & 3\omega^{'} & -4 & 0 \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \end{bmatrix}$$

Gerando o sistema

$$II = \begin{cases} \gamma_0 = \frac{1}{60}\left(\beta_0 + 9\beta_1 + 9\beta_2 + 16\beta_3 + 25\beta_4\right) \\ \gamma_1 = \frac{1}{60}\left(\beta_0 - 3\beta_1 - 3\beta_2 + 5\beta_4\right) \\ \gamma_2 = \frac{1}{60}\left(\beta_0 + 4\beta_3 - 5\beta_4\right) \\ \gamma_3 = \frac{1}{60}\left(\beta_0 + 3\omega\beta_1 + 3\omega^{'}\beta_2 + 4\beta_3\right) \\ \gamma_4 = \frac{1}{60}\left(\beta_0 + 3\omega^{'}\beta_1 + 3\omega\beta_2 - 4\beta_4\right) \end{cases}$$

Poderíamos calcular as unidades em $\mathcal{Z}(\mathbb{Q}A_5)$ e, através desse procedimento, achar $\mathcal{U}(\mathcal{Z}(\mathbb{Z}A_5))$, as unidades de $\mathcal{Z}(\mathbb{Z}A_5)$. O teorema que segue nos dá as unidades de $\mathcal{Z}(\mathbb{Z}A_5)$ de maneira direta.

Teorema 4.1.8. *Seja $\mathcal{U} = \mathcal{U}\left(\mathcal{Z}(\mathbb{Z}A_5)\right)$ o grupo de unidades do centro do anel de grupo $\mathbb{Z}A_5$. Então $\mathcal{U} = \langle -1\rangle \times \langle u\rangle$. Além disso, $\langle u\rangle$ é um grupo cíclico infinito e*

$$u = 49y_0 - 16y_1 + 26y_3 - 10y_4 = e_0 + (161 + 72\sqrt{5})e_1 + (161 - 72\sqrt{5})e_2 + e_3 + e_4,$$

cujo inverso é

$$u^{-1} = 49y_0 - 16y_1 - 10y_3 + 26y_4 = e_0 + (161 - 72\sqrt{5})e_1 + (161 + 72\sqrt{5})e_2 + e_3 + e_4$$

Demonstração. Seja $\varepsilon : \mathbb{Z}A_5 \longrightarrow \mathbb{Z}$ a função aumento definida por

$$\varepsilon\left(\sum_{x\in A_5} a_x x\right) = \sum_{x\in A_5} a_x.$$

Seja V o grupo de unidades normalizadas do centro do anel de grupo $\mathbb{Z}A_5$ dado por $V = \{v \in \mathcal{U} | \varepsilon(v) = 1\}$. Consideremos v um elemento arbitrário em V. Logo, $v = \sum_{i=0}^{4} \gamma_i y_i = \sum_{i=0}^{4} \beta_i e_i$. Já que $|K_0| = 1$, $|K_1| = 15$, $|K_2| = 20$ e $|K_3| = |K_4| = 12$, temos que

$$\varepsilon(v) = \gamma_0 + 15\gamma_1 + 20\gamma_2 + 12\gamma_3 + 12\gamma_4 = 1$$

Logo, a primeira equação do sistema I acima é igual a 1.

Agora vamos provar alguns Lemas para podermos concluir a demonstração do teorema:

Lema 4.1.1. $\beta_3 = \beta_4 = 1$

Demonstração. Primeiramente, notemos que $\beta_3, \beta_4 \in \mathbb{Z}$.

Pelo teorema 4.1.5, temos

$$\mathcal{Z}(\mathbb{Q}A_5) \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\sqrt{5}),$$

via isomorfismo ψ. Seja v como tomamos acima, $v \in \mathcal{U}(\mathcal{Z}(\mathbb{Z}A_5))$. Como $\mathcal{Z}(\mathbb{Z}A_5) \subset \mathcal{Z}(\mathbb{Q}A_5)$, então $v \in \mathcal{Z}(\mathbb{Q}A_5)$. Sabemos, pela definição de ψ, que $\psi(v) = (\beta_0, \ldots, \beta_4)$. Logo, $\beta_i \in \mathbb{Q}$ ou $\beta_i \in \mathbb{Q}(\sqrt{5})$, para todo $i \in \{0, \ldots, 4\}$. Pelo Teorema 4.1.6, temos

$$\mathcal{U}(\mathcal{Z}(\mathbb{Q}A_5)) \simeq \mathcal{U}(\mathbb{Q}) \oplus \mathcal{U}(\mathbb{Q}) \oplus \mathcal{U}(\mathbb{Q}) \oplus \mathcal{U}(\mathbb{Q}(\sqrt{5})).$$

Dessa maneira, vem que $\beta_i \in \mathcal{U}(\mathbb{Q})$ ou $\beta_i \in \mathcal{U}(\mathbb{Q}(\sqrt{5}))$ e $\beta_i \in \mathbb{Z}$, para todo $i \in \{0, \ldots, 4\}$. Logo, $\beta_i = \pm 1$. No nosso caso, $\beta_3 = \beta_4 = \pm 1$.
Temos ainda que $\omega + \omega' = 1$ e $\beta_0 = 1$. Do sistema II, vem que

$$\gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 = \left(\frac{1}{60}\right)(4 + 0.\beta_1 + 0.\beta_2 - 4\beta_3 + 0.\beta_4) = \left(\frac{1}{15}\right)(1 - \beta_3)$$

Como $\gamma_i \in \mathbb{Z}$, para todo $i \in \{0, \ldots, 4\}$, então $\beta_3 = 1$. E ainda

$$\gamma_1 + \gamma_2 + \gamma_3 = \left(\frac{1}{60}\right)(3 - 8 + 5\beta_4) = \left(\frac{1}{12}\right)(\beta_4 - 1),$$

o que implica que $\beta_4 = 1$, provando o Lema. □

Lema 4.1.2. $\beta_1\beta_2 = 1$ *e*

$$x = \frac{\beta_1 + \beta_2}{2} = 1 + 10(\gamma_3 + \gamma_4), y = \frac{\beta_1 - \beta_2}{4\sqrt{5}} = 1 + 10(\gamma_3 - \gamma_4)$$

são inteiros. Além disso, $x^2 - 20y^2 = 1$.

Demonstração. Vamos reescrever o sistema II, com $\beta_0 = \beta_3 = \beta_4 = 1$:

$$\begin{cases} \gamma_0 = (1/60)\,(9\beta_1 + 9\beta_2 + 42) \\ \gamma_1 = (1/60)\,(-3\beta_1 - 3\beta_2 + 6) \\ \gamma_2 = (1/60)\,(1 + 4 - 5) = 0 \\ \gamma_3 = (1/60)\,\left(3\omega\beta_1 + 3\omega^{'}\beta_2 - 3\right) \\ \gamma_4 = (1/60)\,\left(3\omega^{'}\beta_1 + 3\omega\beta_2 - 3\right) \end{cases}$$

Logo, obtemos um novo sistema:

$$III = \begin{cases} \gamma_0 = (1/20)\,(3\beta_1 + 3\beta_2 + 14) \\ \gamma_1 = (1/20)\,(-\beta_1 - \beta_2 + 2) \\ \gamma_2 = 0 \\ \gamma_3 = (1/20)\,\left(\omega\beta_1 + \omega^{'}\beta_2 - 1\right) \\ \gamma_4 = (1/20)\,\left(\omega^{'}\beta_1 + \omega\beta_2 - 1\right) \end{cases}$$

Temos que $\omega + \omega^{'} = 1$ e, portanto, $\gamma_3 + \gamma_4 = \dfrac{1}{20}(\beta_1 + \beta_2 - 2) = \dfrac{\beta_1 + \beta_2}{20} - \dfrac{1}{10}$. Daí que que

$$x = \frac{\beta_1 + \beta_2}{2} = \frac{1}{2}\left(\gamma_3 + \gamma_4 + \frac{1}{10}\right).20 = 10(\gamma_3 + \gamma_4) + 1$$

Além disso,

$$\gamma_3 + \gamma_4 = \frac{1}{20}\left[(\omega - \omega^{'})\beta_1 + (\omega^{'} - \omega)\beta_2\right] = \frac{1}{20}\left[((\omega - \omega^{'})(\beta_1 - \beta_2)\right] = \frac{\sqrt{5}}{20}\,(\beta_1 - \beta_2)$$

Daí,

$$\frac{\sqrt{5}}{20}\,(\gamma_3 - \gamma_4) = \beta_1 - \beta_2$$

Portanto,

$$y = \frac{\beta_1 - \beta_2}{4\sqrt{5}} = 1 + 10(\gamma_3 - \gamma_4)$$

Consideremos

$$v^{-1} = \frac{1}{\beta_0}e_0 + \frac{1}{\beta_1}e_1 + \frac{1}{\beta_2}e_2 + \frac{1}{\beta_3}e_3 + \frac{1}{\beta_4}e_4 = \delta_0 y_0 + \delta_1 y_1 + \delta_2 y_2 + \delta_3 y_3 + \delta_4 y_4$$

Sabemos que a matriz T encontrada anteriormente é tal que

$$\begin{bmatrix} \delta_0 \\ \delta_1 \\ \delta_2 \\ \delta_3 \\ \delta_4 \end{bmatrix} = T. \begin{bmatrix} 1/\beta_0 \\ 1/\beta_1 \\ 1/\beta_2 \\ 1/\beta_3 \\ 1/\beta_4 \end{bmatrix}$$

Logo,

$$\begin{bmatrix} \delta_0 \\ \delta_1 \\ \delta_2 \\ \delta_3 \\ \delta_4 \end{bmatrix} = \frac{1}{60} \begin{bmatrix} 1 & 9 & 9 & 16 & 25 \\ 1 & -3 & -3 & 0 & 5 \\ 1 & 0 & 0 & 4 & -5 \\ 1 & 3\omega^{'} & 3\omega & -4 & 0 \\ 1 & 3\omega & 3\omega^{'} & -4 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1/\beta_1 \\ 1/\beta_2 \\ 1 \\ 1 \end{bmatrix}$$

Assim,

$$\begin{cases} \delta_0 = (1/60)\,(1 + 9/\beta_1 + 9/\beta_2 + 16\beta_3 + 16 + 25) \\ \delta_1 = (1/60)\,(1 - 3/\beta_1 - 3/\beta_2 + 5) \\ \delta_2 = 0 \\ \delta_3 = (1/60)\left(1 + 3\omega/\beta_1 + 3\omega^{'}/\beta_2 - 4\right) \\ \delta_4 = (1/60)\left(1 + 3\omega^{'}/\beta_1 + 3\omega/\beta_2 - 4\right) \end{cases}$$

Logo,

$$IV = \begin{cases} \delta_0 = (1/20)\,(14 + 3/\beta_1 + 3/\beta_2) \\ \delta_1 = (1/20)\,(2 - 1/\beta_1 - 1/\beta_2) \\ \delta_2 = 0 \\ \delta_3 = (1/20)\left(-1 + \omega/\beta_1 + \omega^{'}\right) \\ \delta_4 = (1/20)\left(-1 + \omega^{'}/\beta_1 + \omega/\beta_2\right) \end{cases}$$

Agora obtemos

$$\gamma = \delta_0 - 7\delta_1 = \left[\frac{1}{20}\left(14 + \frac{3}{\beta_1} + \frac{3}{\beta_2}\right) - \frac{1}{20}\left(14 - \frac{7}{\beta_1} - \frac{7}{\beta_2}\right)\right] = \left(\frac{\beta_1 + \beta_2}{2}\right)\left(\frac{1}{\beta_1\beta_2}\right)$$

e

$$\delta = \delta_3 - \delta_4 = \left[\frac{1}{20}\left(\frac{\omega}{\beta_1} - \frac{\omega^{'}}{\beta_1} + \frac{\omega^{'}}{\beta_2} - \frac{\omega}{\beta_2}\right)\right] = \frac{\sqrt{5}}{20}\left(\frac{\beta_2 - \beta_1}{\beta_2\beta_1}\right) = \left(\frac{\beta_2 - \beta_1}{4\sqrt{5}}\right)\left(\frac{1}{\beta_1\beta_1}\right)$$

Temos ainda que $\delta, \gamma \in \mathbb{Z}$, já que $\delta_i \in \mathbb{Z}$, para $i \in \{0, 1, 2, 3, 4\}$.

Assim,

$$x = \frac{\beta_1 + \beta_2}{2} = \gamma\beta_1\beta_2$$

e

$$y = \frac{\beta_1 - \beta_2}{4\sqrt{5}} = -\delta\beta_1\beta_2$$

Agora vamos achar uma expressão para $\beta_1\beta_2$. Fazendo $(\beta_1 + \beta_2)^2 - (\beta_2 - \beta_1)^2$, obtemos:

$$(\beta_1 + \beta_2)^2 - (\beta_2 - \beta_1)^2 = (\beta_1^2 + 2\beta_1\beta_2 + \beta_2^2) - (\beta_2^2 + 2\beta_1\beta_2 + \beta_1^2) = 4\beta_1\beta_2$$

Portanto,

$$\begin{aligned}
\beta_1\beta_2 &= \frac{1}{4}\left[(\beta_1 + \beta_2)^2 - (\beta_2 - \beta_1)^2\right] = \left(\frac{\beta_1 + \beta_2}{2}\right)^2 - 20\left(\frac{\beta_2 - \beta_1}{4\sqrt{5}}\right)^2 = \\
&= x^2 - 20y^2 = (\gamma\beta_1\beta_2)^2 - 20(-\delta\beta_1\beta_2)^2 = \gamma^2\beta_1^2\beta_2^2 - 20\delta^2\beta_1^2\beta_2^2 = \\
&= (\gamma^2 - 20\delta^2)(\beta_1^2\beta_2^2)
\end{aligned}$$

Logo,

$$\beta_1\beta_2(\gamma^2 - 20\delta^2) = 1$$

Dessa maneira, concluímos que $\beta_1\beta 2$ uma unidade em $\mathbb{Z}$. Logo, $\beta_1\beta_2 \pm 1$.

Agora, temos

$$\begin{aligned}\beta_1\beta_2 &= x^2 - 20y^2 = [10(\gamma_3+\gamma_4)+1]^2 - 20(\gamma_3-\gamma_4)^2 = \\ &= 100(\gamma_3+\gamma_4)^2 - 20(\gamma_3-\gamma_4) + 1 - 20(\gamma_3-\gamma_4)^2 = \\ &= 1 + 20(\gamma_3+\gamma_4+5(\gamma_3+\gamma_4)^2 - (\gamma_3-\gamma_4)^2) \equiv 1 \mod 20\end{aligned}$$

Assim, temos que $20|(\beta_1\beta_2-1)$. Caso $\beta_1\beta_2 = -1$, teríamos que $20|-2$, o que é um absurdo. Logo, concluímos que $\beta_1\beta_2 = 1$ Assim, temos que $x^2 - 20y^2 = \beta_1\beta_2 = 1$. Temos então que o par (x, y) satisfaz a chamada Equação de Pell. □

Seja d um inteiro positivo. A equação diofantina a ser considerada aqui é $x^2 - dy^2 = 1$. Em 1657, Fermat conjecturou que a mesma tinha um número infinito de soluções inteiras e algumas bibliografias dizem que isso foi demostrado por Lagrange, mas devido a um erro, foi atribuída a demonstração à Pell.

Proposição 4.1.4. *Se d é um inteiro positivo livre de quadrados, então $x^2 - dy^2 = 1$ tem infinitas soluções inteiras. Além disso, há uma solução (x_1, y_1) tal que toda solução tem a forma $(\pm x_n, \pm y_n)$, onde $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n, n \in \mathbb{Z}$.*

Demonstração. Ver Proposição 17.5.2, página 277 de [19]. □

Assim, temos o seguinte

Lema 4.1.3. *O conjunto das soluções da equação de Pell $x^2 - 20y^2 = 1$ é*

$$\left\{(\pm x_n, \pm y_n) | x_n + 2\sqrt{5}y_n = (9 + 4\sqrt{5}y_1)^n, n = 0, 1, 2, \dots\right\}.$$

Demonstração. Se d é um inteiro positivo livre de quadrados, então $x^2 - dy^2 = 1$ tem infinitas soluções inteiras. Além disso, há uma solução (x_1, y_1) tal que toda solução tem a forma $(\pm x_n, \pm y_n)$, onde $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d})^n$, pelo Teorema acima. Em nosso caso, $d = 20$ e, portanto $\sqrt{20} = 2\sqrt{5}$. Ainda, tomando $(x_1, y_1) = (9, 2)$ é solução para $x^2 - 20y^2 = 1$. Portanto, toda solução de $x^2 - 20y^2 = 1$ tem a forma $(\pm x_n, \pm y_n)$, com $x_n + 2\sqrt{5}y_n = (9 + 4\sqrt{5}y_1)^n, n = 0, 1, 2, \dots$. □

Lema 4.1.4.

$$\frac{\beta_1 + \beta_2}{2} = \frac{(9 + 4\sqrt{5})^{2n} + (9 - 4\sqrt{5})^{2n}}{2}$$

e

$$\frac{\beta_1 - \beta_2}{4\sqrt{5}} = \pm\frac{(9+4\sqrt{5})^{2n} - (9-4\sqrt{5})^{2n}}{4\sqrt{5}},$$

para algum inteiro n.

Demonstração. Pelos Lemas 4.1.2 e 4.1.3, temos $x + 2\sqrt{5}y = \pm(9+4\sqrt{5})^n$ e $x - 2\sqrt{5}y = \pm(9-4\sqrt{5})^n$. Logo, sendo $\mu = \pm 1$, temos

$$x = \mu\left[\frac{(9+4\sqrt{5})^n + (9-4\sqrt{5})^n}{2}\right],$$

onde $x = \dfrac{\beta_1 + \beta_2}{2} = 1 + 10(\gamma_3 + \gamma_4)$.

Temos também

$$y = \pm\left[\frac{(9+4\sqrt{5})^n - (9-4\sqrt{5})^n}{4\sqrt{5}}\right],$$

onde $y = \dfrac{\beta_1 - \beta_2}{4\sqrt{5}} = (\gamma_3 - \gamma_4)$.

Usando a expansão binomial de Newton, temos

$$\begin{aligned}
y &= \pm\frac{1}{4\sqrt{5}}\left[(9+4\sqrt{5})^n - (9-4\sqrt{5})^n\right] = \sum_{i=0}^{n}\binom{n}{i}9^{n-i}(4\sqrt{5})^i - \sum_{i=0}^{n}\binom{n}{i}9^{n-i}(-4\sqrt{5})^i = \\
&= \frac{1}{4\sqrt{5}}\sum_{i=0}^{n}\binom{n}{i}(9^{n-i}(4\sqrt{5})^i)(1-(-1)^i) = \frac{2}{4\sqrt{5}}\sum_{1\leqslant i\leqslant\left\lfloor\frac{n+1}{2}\right\rfloor}\binom{n}{2i-1}9^{n-2i+1}(4\sqrt{5})^{2i-1} = \\
&= \pm 2\sum_{1\leqslant i\leqslant\left\lfloor\frac{n+1}{2}\right\rfloor}\binom{n}{2i-1}9^{n-2i+1}(4\sqrt{5})^{2i-2} = \pm 2\sum_{1\leqslant i\leqslant\left\lfloor\frac{n+1}{2}\right\rfloor}\binom{n}{2i-1}9^{n-2i+1}80^{i-1}
\end{aligned}$$

Logo, concluímos que $y = \gamma_3 - \gamma_4$ é par.

Então podemos escrever $\gamma_3 - \gamma_4 = 2t$, para algum $t \in \mathbb{Z}$. Assim, temos que $\gamma_3 = 2t + \gamma_4$. Portanto, $\gamma_3 + \gamma_4 = 2t + \gamma_4 + \gamma_4 = 2(t + \gamma_4)$. Ou seja, $\gamma_3 + \gamma_4$ é par.

Chamemos $m = \gamma_3 + \gamma_4$. Temos que $m \in \mathbb{Z}$ e m é par.

Temos então que

$$\begin{aligned} x &= 1+10m = \frac{\mu}{2}\left[(9+4\sqrt{5})^n-(9-4\sqrt{5})^n\right] = \\ &= \frac{\mu}{2}\sum_{i=0}^{n}\binom{n}{i}(9^{n-i}(4\sqrt{5})^i)+(9^{n-i}(-4\sqrt{5})^i) = \\ &= \frac{\mu}{2}\sum_{i=0}^{n}\binom{n}{i}((9^{n-i}(4\sqrt{5})^i))(1+(-1)^i) = \\ &= 2.9^n.\frac{\mu}{2}\sum_{1\leqslant i\leqslant\left\lfloor\frac{n}{2}\right\rfloor}\binom{n}{2i}9^{2n-i}80^i = \\ &= 9^n\mu+80\sum_{1\leqslant i\leqslant\left\lfloor\frac{n}{2}\right\rfloor}\binom{n}{2i}9^{2n-i}80^{i-1} \end{aligned}$$

Daí vem que

$$m=\frac{x-1}{10}=\frac{9^n\mu+80\sum_{1\leqslant i\leqslant\left\lfloor\frac{n}{2}\right\rfloor}\binom{n}{2i}9^{2n-i}80^{i-1}-1}{10}=\frac{\mu 9^n-1}{10}+8\sum_{1\leqslant i\leqslant\left\lfloor\frac{n}{2}\right\rfloor}\binom{n}{2i}9^{2n-i}80^{i-1}$$

Logo, para que m seja par, $\dfrac{\mu 9^n-1}{10}$ deve ser par.

Temos que

$$\begin{aligned} \frac{\mu(10-1)^n-1}{10} &= \frac{((-1)+10)^n-1}{10}=\frac{\mu\left(\sum_{i=0}^{n}\binom{n}{i}(-1)^{n-i}10^i\right)-1}{10}= \\ &= \frac{\mu\left[(-1)^n+10n(-1)^{n-1}+100\sum_{i=2}^{n}10^{n-i-2}(-1)^i\right]-1}{10}= \\ &= \frac{-1+\mu(-1)^n+10n(-1)^{n-1}}{10}+10\sum_{i=2}^{n}10^{n-i-2}(-1)^i \end{aligned}$$

Sabemos que a última parcela é par. Agora vamos analisar $-1+\mu(-1)^n$. Temos que essa

expressão assume dois valores: -2 e 0. Com efeito:

- $\mu = 1$ e n par $\Longrightarrow -1 + \mu(-1)^n = 0$
- $\mu = 1$ e n ímpar $\Longrightarrow -1 + \mu(-1)^n = -2$
- $\mu = -1$ e n par $\Longrightarrow -1 + \mu(-1)^n = -2$
- $\mu = -1$ e n ímpar $\Longrightarrow -1 + \mu(-1)^n = 0$

Mas $\dfrac{-1+\mu(-1)^n}{10}$ é inteiro, então $-1 + \mu(-1)^n = 0$. Temos também que $\dfrac{10n(-1)^{n-1}}{10} = n(-1)^{n-1}$ é par se n é par. Logo, concluímos que $\mu = 1$.

Agora, vamos dar continuidade à demonsração do Teorema 4.1.8:

Pelo Lema 4.1.4, temos

$$\frac{\beta_1 + \beta_2}{2} = \frac{(9+4\sqrt{5})^{2n} + (9-4\sqrt{5})^{2n}}{2} = \frac{(\beta_1 + \beta_2)}{2}$$

e

$$\frac{\beta_1 - \beta_2}{4\sqrt{5}} = \pm\frac{(9+4\sqrt{5})^{2n} - (9-4\sqrt{5})^{2n}}{4\sqrt{5}} = \frac{(\beta_1 - \beta_2)}{4\sqrt{5}},$$

para algum inteiro n. □

Somando $(\beta_1 + \beta_2)$ e $(\beta_1 - \beta_2)$, temos que $\beta_1 = (9+4\sqrt{5})^{2n}$ ou $\beta_1 = (9-4\sqrt{5})^{2n}$.

Uma vez que $(9+4\sqrt{5})^{-1} = 9 - 4\sqrt{5}$, vamos assumir que, para o gerador u de V, $\beta_1 = (9+4\sqrt{5})^2 = 161 + 72\sqrt{5}$.

Pelo Lema 4.1.2, temos que $\beta_2 = \frac{1}{\beta_1}$. Então $\beta_2 = 161 - 72\sqrt{5}$.

Assim, obtemos todos os valores de β_i, com $i = 0, 1, 2, 3, 4$: $\beta_0 = \beta_3 = \beta_4 = 1$, $\beta_1 = 161 + 72\sqrt{5}$ e $\beta_2 = 161 - 72\sqrt{5}$.

Logo, $u = e_0 + (161 + 72\sqrt{5})e_1 + (161 - 72\sqrt{5})e_2 + e_3 + e_4$.

Agora, vamos escrever u em função de $\gamma_0, \gamma_1, \gamma_2, \gamma_3$ e γ_4.

Através do sistema III, obtemos $\gamma_0 = 49, \gamma_1 = -16, \gamma_2 = 0, \gamma_3 = 26$ e $\gamma_4 = -10$.

Daí vem que $u = 49y_0 - 16y_1 + 26y_3 - 10y_4$.

Temos ainda que $u^{-1} = e_0 + \frac{1}{161+72\sqrt{5}}e_1 + \frac{1}{161-72\sqrt{5}}e_2 + e_3 + e_4$, isto é, $u = e_0 + (161-72\sqrt{5})e_1 + (161+72\sqrt{5})e_2 + e_3 + e_4$.

Agora basta provar que $\langle u \rangle$ é um grupo cíclico infinito.

Temos que $\mathcal{Z}(\mathbb{Z}G)$ e o anel dos inteiros de $\mathcal{Z}(\mathbb{Q}G)$ são $\mathbb{Z}$-ordens em $\mathcal{Z}(\mathbb{Q}G)$. Além disso, $\mathcal{Z}(\mathbb{Z}G)$ está contido nesse anel de inteiros. Temos ainda que $\mathbb{Z}(\sqrt{5})$ é o anel de inteiros algébricos de $\mathbb{Q}(\sqrt{5})$, que é uma extensão quadrática de $\mathbb{Q}$, portanto tem 2 imersões reais. Daí, pelo Teorema de Unidades de Dirichlet (1.4.2), o posto de $\mathbb{Z}(\sqrt{5})$ é $2-1=1$. Como o posto de $\mathcal{U}(\mathcal{Z}(\mathbb{Z}A_5))$ é igual ao posto de $\mathcal{U}(\mathcal{Z}(\mathbb{Z}(\sqrt{5})))$, temos que $\pm u$ gera $\mathcal{U}(\mathcal{Z}(\mathbb{Z}A_5))$.

Agora, temos que as classes de conjugação de A_5 são:

$$K_0 = \{1_{A_5}\}$$

$$K_1 = \begin{array}{ccccc} \{(12)(34), & (12)(35), & (12)(45), & (13)(25), & (13)(24), \\ (13)(45), & (14)(25), & (14)(35), & (14)(23), & (14)(24), \\ (15)(23), & (15)(34), & (23)(45), & (24)(35), & (25)(43)\} \end{array}$$

$$K_2 = \begin{array}{ccccc} \{(123), & (132), & (124), & (142), & (125), \\ (152), & (134), & (143), & (135), & (153), \\ (145), & (154), & (234), & (243), & (235), \\ (253), & (245), & (254), & (345), & (354)\} \end{array}$$

$$K_3 = \begin{array}{cccc} \{(12345), & (15432), & (12453), & (13542), \\ (15243), & (13425), & (15324), & (14235), \\ (12534), & (14352), & (13254), & (14523)\} \end{array}$$

$$K_4 = \begin{array}{cccc} \{(13524), & (14253), & (14325), & (15234), \\ (12354), & (14532), & (13452), & (12543), \\ (15423), & (13245), & (12435), & (15342)\} \end{array}$$

Então u é tal que $u \neq \pm g$ com $g \in A_5$.

Suponhamos que u tenha ordem finita. Então, pelo Corolário 1.3.3, $u = \pm g$, o que é um absurdo. Concluímos então que $\langle u \rangle$ é um grupo cíclico infinito.

□

O último resultado desse trabalho determina as unidades de certos anéis de grupos, cujos grupos são grupos alternados, que, para certas ordens, tem apenas unidades triviais, provado por Ferraz, em [9]:

Teorema 4.1.9. *O grupo* $\mathcal{Z}(\mathcal{U}(\mathbb{Z}A_n))$ *é trivial se, e somente se,* $n \in H = \{1, 2, 3, 4, 7, 8, 9, 12\}$.

Referências Bibliográficas

[1] R. Z. Aleev. Higman's central unit theory, units of integral group rings of finite cyclic groups and fibonacci numbers. *Int. J. Algebra and Comput*, 4(3):309–358, 1994.

[2] R. Zh. Aleyev and G. A. Panina. The units of cyclic groups of orders 7 and 9. *Russian Mathematics*, 43(11):80–83, 1999.

[3] Z. I. Borevich and I. R. Shafarevich. *Number Theory*. Academic Press, 1st edition, 1973.

[4] D. B. Coleman. Finite group with isomorphic group algebras. *Trans. Amer. Math. Soc.*, (105):1–8, 1962.

[5] E. C. Dade. Deux groups finis ayant la meme algébre de group sur tout corps. *Math. Z.*, (119):345–348, 1971.

[6] W. E. Deskins. Finite abelian groups with isomorphic group algebras. *Duke Math*, (23):35–40, 1956.

[7] H. Edwards. *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*. Mir, 1st edition, 1987.

[8] O. Endler. *Teoria dos números algébricos*. IMPA, 2nd edition, 2006.

[9] R. A. Ferraz. Simple components and central units in group algebras. *Journal of Algebra*, (279):191–203, 2004.

[10] R. A. Ferraz. Units of $\mathbb{Z}C_p$. *Contemporary Mathematics*, (499):107–119, 2009.

[11] G. Higman. The units of group rings. *Proc. London Math. Soc.*, 46(2):231–248, 1940.

[12] J. M. Howie. *Fields and Galois Theory*. Springer, 1st edition, 2006.

[13] G. James and M. Liebeck. *Representations and Characters of Groups*. Cambridge Mathematical Textbooks, 2st edition, 2001.

[14] P. M. Kitani. *Unidades de $\mathbb{Z}C_{p^n}$*. Tese de Doutorado, Universidade de São Paulo, 2012.

[15] Y. Li and Parmenter M. M. Central units of the integral group ring $\mathbb{Z}\mathrm{A}_5$. *Proc. Amer. Math. Soc.*, (125):61–65, 1997.

[16] C. P. Milies and S. K. Sehgal. *An Introduction to group rings*. Kluwer, 1st edition, 2002.

[17] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften 322, Springer, 1st edition, 1999.

[18] S. Perlis and Walker G. L. Abelian groups algebras of finite order. *Trans. Amer. Math. Soc.*, (68):420–426, 1950.

[19] M. Rosen and K. Ireland. *A Classical Introduction to Modern Number Theory*. Springer, 2st edition, 1990.

[20] R. R. M. Silva. *Unidades de $\mathbb{Z}C_{2p}$*. Tese de Doutorado, Universidade de São Paulo, 2012.

[21] L. Washington. *Introduction to cyclotomic fields*. Springer, 1st edition, 1980.

[22] A. Weiss. Rigidity of p-adic torsion. *Ann. Math.*, (127):317–332, 1988.

[23] A. Whitcomb. *The group ring problem*. Ph.D. Thesis, University of Chicago, 1968.