UNIVERSIDADE FEDERAL DE MINAS GERAIS
Instituto de Ciências Exatas
Programa de Pós-graduação em Matemática

Marlon Stefano Fernandes Estanislau

Módulos de permutação p-ádicos para p-grupos abelianos elementares

Belo Horizonte
2022

Marlon Stefano Fernandes Estanislau

Módulos de permutação p-ádicos para p-grupos abelianos elementares

Versão final

Dissertação apresentada ao Programa de Pós-graduação em Matemática da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. John William MacQuarrie

Belo Horizonte
2022

Estanislau, Marlon Stefano Fernandes.

E79m Módulos de permutação *p*-ádicos para *p*-grupos abelianos elementares: [manuscrito] / Marlon Stefano Fernandes Estanislau – 2022.
78 f. il.

Orientador: John William MacQuarrie.
Dissertação (mestrado) - Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática.
Referências: f. 78.

1. Matemática – Teses. 2. Módulos (Álgebra)– Teses. 3. Grupos finitos– Teses. I. MacQuarrie, John William. II. Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática. IV.Título.

CDU 51 (043)

Ficha catalográfica elaborada pela bibliotecária Belkiz Inez Rezende Costa
CRB 6/1510 Universidade Federal de Minas Gerais - ICEx

Universidade Federal de Minas Gerais
Departamento de Matemática
Programa de Pós-Graduação em Matemática

FOLHA DE APROVAÇÃO

Módulos de permutação p-ádicos para p-grupos abelianos elementares

MARLON STEFANO FERNANDES ESTANISLAU

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

Prof. John William MacQuarrie
UFMG

Prof. Csaba Schneider
UFMG

Prof. Pavel Zalesskii
UnB

Belo Horizonte, 21 de fevereiro de 2022.

Av. Antônio Carlos, 6627 – Campus Pampulha - Caixa Postal: 702
CEP-31270-901 - Belo Horizonte – Minas Gerais - Fone (31) 3409-5963
e-mail: pgmat@mat.ufmg.br - home page: http://www.mat.ufmg.br/pgmat

Agradecimentos

Agradeço a minha mãe pelo apoio incondicional e a minha avó por sempre ter demonstrado de diversas formas a importância da educação. Aos meus irmãos agradeço pela colaboração em manter um ambiente propício para os meus estudos e pesquisa.

Ao Dr. John William MacQuarrie agradeço pela orientação e por todos os ensinamentos que contribuíram para meu crescimento acadêmico. Agradeço também aos professores Dr. Pavel Zalesskii e Dr. Csaba Schneider, que compuseram a banca, pelo olhar criterioso sobre o trabalho.

A CAPES agradeço pela concessão da bolsa que permitiu minha dedicação integral aos estudos e à pesquisa.

Resumo

Seja $\mathbb{Z}_p$ o anel dos inteiros p-ádicos e G um p-grupo finito. Recentemente, MacQuarrie e Zalesskii caracterizaram os $\mathbb{Z}_pG$-módulos de permutação apenas olhando para módulos para G/N, onde N é um subgrupo normal de G com ordem p. Esta caracterização é dada por duas condições e nesse trabalho mostramos que, em geral, não podemos retirar nenhuma dessas condições para caracterizar os $\mathbb{Z}_pG$-módulos de permutação. Os autores já sabiam que uma das condições não poderia ser retirada mas a necessidade da outra condição era desconhecida. Trabalhamos com uma correspondência devida a Butler para construir um $\mathbb{Z}_pG$-módulo que não é um $\mathbb{Z}_pG$-módulo de permutação e satisfaz a condição que não se sabia se era uma caracterização dos $\mathbb{Z}_pG$-módulos de permutação.

Palavras-chave: Módulos de permutação. p-grupos finitos.

Abstract

Let $\mathbb{Z}_p$ be the ring of p-adic integers and G be a finite p-group. Recently, MacQuarrie and Zalesskii characterized the $\mathbb{Z}_pG$-permutation modules by just looking at modules for G/N, where N is a normal subgroup of G with order p. This characterization is given by two conditions and in this work we show that, in general, we cannot remove either of these conditions to characterize the permutation $\mathbb{Z}_pG$-modules. The authors already knew that one of the conditions could not be removed but the necessity of the other condition was unknown. We work with a correspondence due to Butler to construct a $\mathbb{Z}_pG$-module that is not a $\mathbb{Z}_pG$-permutation module, but which satisfies the condition that might still have been a characterization of permutation $\mathbb{Z}_pG$-modules.

Keywords: Permutation modules. Finite p-groups.

Sumário

Capítulo 1

Introdução

Seja G um p-grupo finito e R um anel comutativo com unidade. Um RG-módulo de permutação é um RG-reticulado (isto é, um RG-módulo que é finitamente gerado e R-livre) que possui uma base que é invariante pela ação de G. Denotando o anel dos inteiros p-ádicos por $\mathbb{Z}_p$ e por $\mathbb{F}_p$ o seu corpo residual, em [5] MacQuarrie e Zalesskii mostram que um $\mathbb{Z}_pG$-módulo é de permutação se, e somente se, existe um subgrupo normal $N \lhd G$ com ordem p satisfazendo

1. U^N e U_N são $\mathbb{Z}_p[G/N]$-módulos de permutação e
2. $\left(U/U^N\right)_N$ é um $\mathbb{F}_p[G/N]$-módulo de permutação,

onde, U^N e U_N são, respectivamente, o maior submódulo e o maior quociente de U em que N age trivialmente. Denotando por I_N o núcleo do homomorfismo natural

$$\phi : \mathbb{Z}_pN \to \mathbb{Z}_p$$

$$\sum_{g\in N} \lambda_g g \mapsto \sum_{g\in N} \lambda_g,$$

temos explicitamente

$$U^N = \{u \in U; gu = u \ \forall g \in N\},$$

$$U_N = U/I_NU.$$

No artigo [5] os autores fornecem pequenos exemplos mostrando que não se pode apenas supor que um dos módulos U^N ou U_N é um $\mathbb{Z}_p[G/N]$-módulo de permutação para concluir que U é um $\mathbb{Z}_pG$-módulo de permutação, mas um problema que ficou em aberto é o seguinte: se U_N e U^N são $\mathbb{Z}_p[G/N]$-módulos de permutação, então U é um $\mathbb{Z}_pG$-módulo de permutação? Fornecemos uma resposta negativa para essa questão utilizando ferramentas construídas por Butler em [7]. Para $p = 3$ e $G = C_3 \times C_3$ (C_3 denota o grupo cíclico de ordem 3) construímos um $\mathbb{Z}_3G$-reticulado U para o qual existe um subgrupo $N \lhd G$ de ordem 3 tal que U^N e U_N são de permutação mas U não é um

$\mathbb{Z}_3G$-módulo de permutação. O reticulado obtido tem $\mathbb{Z}_p$-posto 11, como $\mathbb{Z}_3[C_3 \times C_3]$-reticulado é estruturalmente complicado e acreditamos que seria difícil encontrá-lo sem essas ferramentas.

Vamos assumir que o leitor tenha familiaridade com conceitos e resultados básicos de Álgebra Abstrata pertinentes a teoria de grupos, anéis, e módulos.

No Capítulo 2 introduzimos algumas noções e resultados básicos da teoria das representações de grupos e resultados da teoria dos módulos finitamente gerados sobre anéis comutativos com unidade que serão importantes para o desenvolvimento do trabalho. O Capítulo 3 é reservado para alguns resultados sobre RG-módulos de permutação. Dedicamos o Capítulo 4 para apresentar a construção da principal ferramenta que utilizamos para construir um $\mathbb{Z}_p[C_3 \times C_3]$-reticulado que fornece a resposta para a questão proposta.

Capítulo 2

$\mathbb{Z}_pG$-módulos

Nesse capítulo definimos algumas noções básicas da teoria das representações de grupos finitos e expomos alguns resultados que serão relevantes para o desenvolvimento do trabalho. Ao longo do texto, R denota um anel comutativo com unidade e G um grupo finito.

2.1 Representações de grupos

2.1.1 Definições e exemplos

Seja R um anel comutativo com unidade e G um grupo finito. Uma representação linear de G sobre R é um homomorfismo de grupos

$$\rho : G \longrightarrow \mathrm{GL}(U),$$

onde U é um R-módulo e $\mathrm{GL}(U)$ denota o grupo das transformações lineares invertíveis de U. Isso significa que ρ satisfaz

$$\rho(gh) = \rho(g)\rho(h)\ \forall g, h \in G$$

fornecendo $\rho(1) = 1$ e $\rho(g^{-1}) = (\rho(g))^{-1}$. O módulo U é chamado módulo de representação. Se ρ' é outra representação de G com módulo de representação W e existe uma transformação linear invertível $T : U \longrightarrow W$ satisfazendo

$$T\rho(g)T^{-1} = \rho'(g)\ \forall g \in G,$$

dizemos que ρ e ρ' são similares.

O homomorfismo ρ fornece uma ação de G em U definida por $g \cdot u = \rho(g)(u)$, que denotaremos por gu. Observe que essa ação cumpre

$$g(u + \lambda w) = gu + \lambda gw, \ \forall u, w \in U, \ \forall \lambda \in R,$$

$$(gh)u = g(hu), \ \forall g, h \in G, \ \forall u \in U$$

$$1_G u = u.$$

Uma ação desse tipo é chamada uma ação linear de G em U.

Se U é livre e finitamente gerado, digamos com R-posto r, dizemos que r é o grau da representação ρ. Fixada uma R-base B de U, para cada elemento $T \in \mathrm{GL}(U)$ associamos uma matriz $[T]_B \in M_{r\times r}(R)$, onde $[T]_B$ denota a matriz de T na base B e $M_{r\times r}(R)$ é o anel das matrizes $r \times r$ com entradas em R. Sabemos que essa associação fornece um isomorfismo de grupos entre $\mathrm{GL}(U)$ e $\mathrm{GL}(r, R)$, onde $\mathrm{GL}(r, R)$ denota o conjunto das matrizes não singulares de $M_{r\times r}(R)$. Nesse caso, uma representação linear ρ é um homomorfismo de G no grupo $\mathrm{GL}(r, R)$ e é chamada representação matricial. Como cada $u \in U$ possui uma única representação como combinação linear dos elementos da base $B = \{u_1, ..., u_r\}$, assim, se $u = \sum_{i=1}^{r} \lambda_i u_i$, então a ação de G em U é dada colocando

$$g \cdot u = \rho_g(u) = \sum_{i=1}^{r} \alpha_i u_i,$$

onde

$$\rho(g) \cdot \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_r \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix},$$

e $\rho_g \in \mathrm{End}_R(U)$ satisfaz $\rho(g) = [\rho_g]_B$.

Exemplo 2.1.1. *Seja R^* o conjunto dos elementos invertíveis de R. Defina*

$$\rho : G \longrightarrow R^*$$

por $\rho(g) = 1_R \ \forall g \in G$. Essa é uma representação de G chamada a representação trivial. O seu módulo de representação será denotado ao longo do texto simplesmente por R.

Exemplo 2.1.2. *Seja $R = \mathbb{C}$ o conjunto dos números complexos e $C_n, n > 1$, o grupo cíclico com n elementos. Seja g um gerador de C_n e defina*

$$\rho : C_n \longrightarrow \mathbb{C}\backslash\{0\}$$

pondo $\rho(g^r) = \lambda^r$, onde $\lambda \in \mathbb{C}$ é uma n-ésima raiz primitiva da unidade. Então, ρ é uma representação de grau 1 que não é trivial. O módulo de representação é $\mathbb{C}$, onde g age como uma multiplicação por λ. Em geral para um anel R com unidade e um grupo G, uma representação de grau 1 é especificada por um homomorfismo entre G e R^*.

Exemplo 2.1.3. *Seja $R = \mathbb{F}_p$ um corpo com característica $p > 0$ e $G = \langle g \rangle$ o grupo cíclico de ordem p. Defina*

$$\rho : G \longrightarrow GL(2, \mathbb{F}_p)$$
$$\rho(g^r) = \begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix}.$$

Como $\rho(g)$ possui ordem p, ρ é uma representação de grau 2.

2.2 RG-módulos e representações

Denote por RG o R-módulo livre com base G. Em RG podemos definir uma ação de G pondo $g \cdot h = gh \ \forall g, h \in G$, onde gh denota a multiplicação em G dos elementos $h, g \in G$. Como os elementos de RG são da forma $\lambda = \sum_{g \in G} \lambda_g g, \lambda_g \in R$, definimos uma multiplicação em RG da seguinte forma

$$\left(\sum_{g \in G} \lambda_g g \right) \left(\sum_{h \in G} \alpha_h h \right) = \sum_{g \in G} \sum_{h \in G} \lambda_g \alpha_h gh.$$

Com essa multiplicação, RG se torna um anel com unidade 1_G e também é um R-módulo que possui uma ação linear de G dada pela multiplicação de RG definida acima.

Dado um módulo de representação U, cada $g \in G$ age como uma transformação linear em U, assim, U se torna um RG-módulo com a sua ação linear de G. Agora, dado um RG-módulo U, esse possui uma ação linear de G e podemos construir uma representação linear para G da seguinte forma: para cada $g \in G$ associamos uma transformação linear $\rho_g \in \mathrm{GL}(U)$ definida por $\rho_g(u) = gu \ \forall u \in U$, daí, pomos $\rho(g) = \rho_g$, logo a ação linear de G em U fornece uma representação linear ρ de G.

Posto isso, vemos que lidar com módulos de representação para G é a mesma coisa que lidar com RG-módulos e vice-versa. Isso tem uma grande vantagem já que podemos utilizar a teoria de módulos para anéis com unidade para entender os módulos de representação para G.

Dado um RG-módulo U e $W \subseteq U$ um R-submódulo, dizemos que W é um RG-submódulo de U se W é invariante pela ação de G, isso é, se $gu \in W \ \forall g \in G$, e $\forall u \in W$.

Definição 2.2.1. *Sejam U e W dois RG-módulos e $\phi : U \longrightarrow W$ um R-homomorfismo. Dizemos que ϕ é um RG-homomorfismo se $\phi(gu) = g\phi(u) \ \forall g \in G$ e $\forall u \in U$. No caso em*

que ϕ também é uma bijeção, dizemos que ϕ é um isomorfismo de RG-módulos. Como de costume, denotamos por $\ker\phi$ *o núcleo do homomorfismo ϕ. Claramente, esse é um RG-submódulo de U.*

Exemplo 2.2.1. *Considere o mapa*

$$\phi : RG \longrightarrow R$$

dado por

$$\phi\left(\sum_{g\in G}\lambda_g g\right) = \sum_{g\in G}\lambda_g.$$

Segue da definição da multiplicação em RG que ϕ é um homomorfismo de anéis. Denotaremos por I_G o núcleo do homomorfismo ϕ, esse é amplamente conhecido como ideal de aumentação de RG. Observe que $\sum_{g\in G}\lambda_g g \in I_G$ se, e somente se, $\lambda_1 = -\sum_{g\neq 1}\lambda_g$, e disso segue que $\{g-1; 1 \neq g \in G\}$ é uma R-base para I_G. Quando G é cíclico e gerado por g, I_G é gerado por $(g-1)$ como ideal de RG.

Ao longo do texto, I_G sempre denotará o ideal de aumentação de RG. No contexto o anel R estará evidente e não haverá risco de confusão.

Definição 2.2.2. *Dizemos que um RG-módulo U é indecomponível se esse não possui RG-somando direto diferente de U e do módulo nulo. Dizemos que a representação ρ é indecomponível se o RG-módulo associado é indecomponível.*

Quando um RG-módulo U finitamente gerado possui uma decomposição em soma direta de RG-submódulos indecomponíveis, digamos

$$U = W_1 \oplus W_2 \oplus ... \oplus W_s,$$

onde cada W_i é indecomponível, a representação ρ associada a U se escreve como uma soma das restrições indecomponíveis $\rho|_{W_i}, i = 1, ..., s$.

Definição 2.2.3. *Seja U um RG-módulo. Dizemos que U é simples se os únicos RG-submódulos de U são o módulo nulo e ele próprio.*

Teorema 2.2.1 ([8], Proposição 6.2.1, pág.98)**.** *Seja K um corpo com característica $p > 0$ e G um p-grupo finito, então o módulo trivial é o único KG-módulo simples.*

Demonstração. Seja S um KG-módulo simples e seja $x \neq 0$ um gerador de S. Considere o grupo abeliano aditivo H que é gerado pelos elementos gx, com $g \in G$. Como S é um

K-espaço vetorial, p age como 0 em H, de modo que os elementos de H possuem ordem p e, assim, H é um p-grupo abeliano finito. Observe que H possui uma ação de G que é herdada da ação de G em S, já que H é gerado pelo conjunto $\{gx; g \in G\}$. Sendo G um p-grupo, o estabilizador em G de cada elemento $h \in H$ possui ordem igual a uma potência de p. Como a órbita de $0 \in H$ tem tamanho 1, deve existir outro elemento possuindo órbita com tamanho 1, pois caso contrário teríamos $|H| = 1+pk$ o que é uma contradição. Então, seja $y \neq 0$ um elemento cuja a órbita tem tamanho 1. Como S é simples, temos $S = \langle y \rangle_{KG} = K$ o módulo trivial. □

2.3 O Lema de Nakayama

Seja R um anel comutativo com unidade. A interseção de todos os ideais maximais de R é um ideal, denominado o ideal de Jacobson de R e denotado por $J(R)$. Quando o anel que estivermos trabalhando estiver claro no contexto, denotaremos $J(R)$ simplesmente por J. O ideal de Jacobson de um anel comutativo R pode ser caracterizado de outras maneiras, utilizaremos duas caracterizações que serão úteis para o desenvolvimento do trabalho. Como veremos, o ideal de Jacobson fornece uma ferramenta essencial na teoria dos R-módulos finitamente gerados que é conhecida como o Lema de Nakayama.

Teorema 2.3.1. *Seja R um anel comutativo com unidade e J o ideal de Jacobson de R, então o ideal de Jacobson pode ser caracterizado das seguintes formas*

1. $J = \{x \in R; xU = 0,$ *para todo R-módulo simples* $U\}$.

2. $J = \{x \in R; xy - 1$ *é invertível* $\forall y \in R\}$.

Demonstração. Primeiramente observe que se U é um módulo simples e u é um elemento não nulo de U, então $U = \langle u \rangle_R$. Assim, o homomorfismo definido por $\phi(x) = xu$ é um homomorfismo sobrejetivo e, daí, $U \simeq R/\ker(\phi)$. Como U é simples, segue que $\ker(\phi)$ é um ideal maximal de R.

Posto isso, dado $x \in R$ tal que x pertence a todo ideal maximal de R, temos necessariamente que x anula todo R-módulo simples. Reciprocamente, dado $x \in R$ que anula todo R-módulo simples, temos que x age como 0 em R/I para todo ideal maximal $I \subset R$ o que significa que x pertence a todos ideais maximais de R, assim, o Item 1 é uma caracterização de J.

Dado $x \in J$, suponha que para algum $y \in R$ tenhamos $xy - 1$ não invertível. Sendo R comutativo com unidade, deve existir um ideal maximal I contendo $xy-1$, como $x \in J \subseteq I$ devemos ter $xy \in I$, logo $1 \in I$ e concluímos que $I = R$, contradição. Reciprocamente, se $xy - 1$ é invertível para todo $y \in R$ e existe um ideal maximal I tal que $x \notin I$, então escolha $z \notin I$. Daí, temos $R/I = \langle z+I \rangle_R$, pois $z+I$ é invertível em R/I, sendo I maximal ele também é um ideal primo, logo $xz \notin I$ e temos que $R/I = \langle z+I \rangle_R = \langle xz+I \rangle_R$. Assim, deve existir $y \in R$ satisfazendo $y(xz + I) = z + I$ e obtemos que $(yx - 1)z \in I$. Como I é primo e $z \notin I$, devemos ter o elemento invertível $xy - 1$ pertencente a I, e obtemos uma contradição com o fato de I ser maximal. Portanto, o Item 2 é outra caracterização do ideal de Jacobson de R.

□

Seja U um R-módulo. Denote por U^r a soma direta de r cópias de U, também denote o homomorfismo identidade de U por id_U. Seja $\phi \in \mathrm{End}_R(U)$, convencionando que $\phi^0 = id_U$, denote por $R[\phi]$ o anel em que seus elementos são combinações lineares do

tipo

$$a_s\phi^s + a_{s-1}\phi^{s-1} + ... + a_0 id_U, a_j \in R, j = 0, 1, ..., s.$$

Claramente $R[\phi]$ é um anel comutativo com unidade.

Teorema 2.3.2 ([4], Proposição 2.4, pág.21)**.** *Seja U um R-módulo finitamente gerado e $\phi \in End_R(U)$. Suponha que exista um ideal $\mathfrak{a} \subseteq R$ tal que $\phi(U) \subseteq \mathfrak{a}U$, então ϕ satisfaz uma equação do tipo*

$$\phi^r + a_{r-1}\phi^{r-1} + ... + a_0 = 0, a_j \in \mathfrak{a}, j = 0, 1..., r-1.$$

Demonstração. Seja $\{v_1, ..., v_r\}$ um conjunto gerador de U, então

$$\phi(v_i) = \sum_{j=1}^{r} a_{ij}v_j, a_{ij} \in \mathfrak{a}, i, j = 1, ..., r.$$

Reescrevendo a última equação, obtemos

$$\sum_{j=1}^{r}(\delta_{ij}\phi - a_{ij}id_U)v_j = 0,$$

onde δ_{ij} é 1 se $i = j$ e $\delta_{ij} = 0$ caso contrário. Essa equação pode ser interpretada como a seguinte equação matricial

$$(\phi I_{U^r} - A)\begin{bmatrix} v_1 \\ \vdots \\ v_r \end{bmatrix} = 0,$$

onde as entradas da matriz A são $a_{ij}id_U \in R[\phi]$ e I_{U^r} é a matriz identidade $r \times r$ com entradas em $R[\phi]$. Agora, sendo $R[\phi]$ um anel comutativo, podemos aplicar o que conhecemos sobre matrizes com entradas em um anel comutativo. Sendo $adj(\phi I_{U^r} - A)$ a adjunta da matriz $\phi I_{U^r} - A$, sabemos que

$$[adj(\phi I_{U^r} - A)](\phi I_{U^r} - A) = det(\phi I_{U^r} - A)I_{U^r},$$

assim

$$[adj(\phi I_{U^r} - A)](\phi I_{U^r} - A)\begin{bmatrix} v_1 \\ \vdots \\ v_r \end{bmatrix} = det(\phi I_{U^r} - A)I_{U^r}\begin{bmatrix} v_1 \\ \vdots \\ v_r \end{bmatrix} = 0,$$

e logo

$$det(\phi I_{U^r} - A)v_i = 0, i = 1, ..., r.$$

Desenvolvendo o determinante obtemos

$$\phi^r + a_{r_1}\phi^{r-1} + ... + a_0 = 0 \in End_R(U), a_i \in \mathfrak{a}, i = 0, 1, ...r-1.$$

□

Corolário 2.3.1 ([4], Corolário 2.5, pág.21)**.** *Seja U um R-módulo finitamente gerado e $\mathfrak{a} \subseteq R$ um ideal. Suponha que $U = \mathfrak{a}U$, então existe $x \in R$ tal que $x - 1 \in \mathfrak{a}$ e $xU = 0$.*

Demonstração. Aplicando o último teorema ao homomorfismo identidade de U, obtemos

$$id_U^r + a_{r_1} id_U^{r-1} + ... + a_0 id_U = 0.$$

Escolhendo $x = 1 + a_{r-1} + ... + a_0$, temos que $xU = 0$ e $x - 1 \in \mathfrak{a}$. □

O próximo resultado é conhecido como o Lema de Nakayama.

Proposição 2.3.1 ([4], Proposição 2.6, pág.21)**.** *Seja U um R-módulo finitamente gerado e suponha que $J(R)U = U$, então U é o módulo nulo.*

Demonstração. Pelo Corolário 2.3.1, existe $x \in R$ tal que $x - 1 \in J(R)$ e $xU = 0$. Como $x - 1 \in J(R)$, x deve ser invertível pelo Teorema 2.3.1, portanto, $xU = 0$ implica $U = 0$. □

Corolário 2.3.2 ([4], Corolário 2.7, pág.22)**.** *Seja U um R-módulo finitamente gerado e suponha que existe $W \subseteq U$ um R-submódulo satisfazendo $U = W + J(R)U$, então $W = U$.*

Demonstração. Primeiramente, observe que

$$J(R)(U/W) = \left\{ \sum_{i=1}^{r} \lambda_i u_i + W; \lambda_i \in J(R), u_i \in U \right\} = \{u + w + W; u \in J(R)U, w \in W\}.$$

Como

$$(W + J(R)U)/W = \{u + w + W; u \in J(R)U, w \in W\},$$

obtemos da igualdade acima que

$$J(R)(U/W) = (W + J(R)U)/W.$$

Por hipótese $U = W + J(R)U$, donde obtemos $J(R)(U/W) = U/W$. Sendo U finitamente gerado, assim também o é U/W, e segue da Proposição 2.3.1 que $U/W = 0$, donde $W = U$. □

Dado um R-módulo U e $u \in U$, denote por $\bar{u}$ a classe de u em $U/J(R)U$.

Corolário 2.3.3. *Seja U um R-módulo finitamente gerado e sejam $\bar{u}_1, ..., \bar{u}_r$ geradores de $U/J(R)U$. Então $U = \langle u_1, ..., u_r \rangle_R$.*

Demonstração. Com efeito, como $\bar{u}_1, ..., \bar{u}_r$ geram $U/J(R)U$, dado $u \in U$ podemos escrever $\bar{u} \in U/J(R)U$ como combinação linear dos elementos $\bar{u}_1, ..., \bar{u}_r$, digamos

$$\bar{u} = \lambda_1 \bar{u}_1 + ... + \lambda_r \bar{u}_r, \lambda_i \in R, i = 1, 2, ..., r.$$

Assim,

$$\bar{u} - \lambda_1 \bar{u}_1 - ... - \lambda_r \bar{u}_r = \bar{0},$$

consequentemente

$$u - \lambda_1 u_1 + ... + \lambda_r u_r \in J(R)U$$

e temos que $u = \lambda_1 u_1 + ... + \lambda_r u_r + w$, onde $w \in J(R)U$. Logo,

$$U = \langle u_1, ..., u_r \rangle_R + J(R)U$$

e segue do último corolário que $U = \langle u_1, ..., u_r \rangle_R$. □

2.4 Anéis de valorização e o ideal de Jacobson de RG

Nessa seção definimos o conceito de anéis de valorização e fornecemos uma descrição do ideal de Jacobson da álgebra de grupos RG quando R é um anel de valorização discreta, p é primo em R e G é um p-grupo abeliano finito.

Definição 2.4.1. *Seja K um corpo. Uma* valorização discreta (aditiva) *em K é um homomorfismo de grupos sobrejetivo $\nu : K^* \longrightarrow \mathbb{Z}$ satisfazendo a condição*

- $\nu(a+b) \geq min\{\nu(a), \nu(b)\}$.

Em alguns casos é conveniente estender a valorização para o corpo K, fazemos isso colocando $\nu(0) = +\infty$. O conjunto $R = \{a \in K : \nu(a) \geq 0\}$ é um anel chamado o anel de valorização de ν, ou anel de valorização do corpo K se não houver perigo de confusão.

Definição 2.4.2. *Se R é um domínio, dizemos que R é um anel de valorização discreta se esse é um anel de valorização para seu corpo de frações.*

Vejamos algumas consequências da valorização discreta em K sobre o seu anel de valorização R. Primeiramente, observamos que sendo ν um homomorfismo temos

$$\nu(1) = \nu(1^2) = 2\nu(1)$$

o que fornece $\nu(1) = 0$, logo $1 \in R$. Dado $a \in R$ invertível, obtemos pela definição de R e do fato que ν é um homomorfismo,

$$\nu(a) \geq 0 \text{ e } \nu(a^{-1}) = -\nu(a) \geq 0$$

fornecendo $\nu(a) = 0$. Por outro lado, se $a \in R$ é tal que $\nu(a) = 0$, então

$$\nu(a^{-1}) = -\nu(a) = 0$$

e segue que $a^{-1} \in R$, portanto, o conjunto dos elementos invertíveis de R é o conjunto

$$R^* = \{a \in R; \nu(a) = 0\}.$$

Dessas observações segue que o conjunto $\mathfrak{m} = \{a \in R : \nu(a) > 0\}$ é um ideal de R. Como $a \in R$ é invertível se, e somente se, $\nu(a) = 0$, o ideal $\mathfrak{m}$ é o único ideal maximal de R, de modo que R é um domínio local comutativo com unidade.

Se $a, b \in R$ são tais que $\nu(a) = \nu(b)$, então

$$\nu(a) - \nu(b) = 0$$

o que implica $\nu(ab^{-1}) = 0$ e $x = ab^{-1}$ é invertível em R, logo $\langle a\rangle_R = \langle b\rangle_R$. Como ν é um homomorfismo sobrejetivo, deve existir $\pi \in R$ tal que $\nu(\pi) = 1$ e, daí vem que se $a \in R$ devemos ter $\nu(a) = k = \nu(\pi^k)$ e consequentemente

$$\langle a\rangle_R = \langle \pi^k\rangle_R.$$

Isso também mostra que dado um ideal $\mathfrak{a} \subset R$ e $a \in \mathfrak{a}$ com a menor valorização possível (é possível escolher pela boa ordenação de $\mathbb{Z}$), digamos $\nu(a) = k$, devemos ter

$$\langle a\rangle = \langle \pi^k\rangle = \{b \in R; \nu(b) \geq k\} = \mathfrak{a},$$

pois todo elemento de $\mathfrak{a}$ deve ter valorização maior ou igual a k.

Posto isso, vemos que cada elemento de R é da forma $\pi^n a$, onde a é invertível em R. Além disso, $\mathfrak{m} = \langle\pi\rangle$ e todo ideal de R é da forma $\mathfrak{m}^k$. Também observe que o único ideal primo não nulo de R é $\mathfrak{m}$, e dado $a \in K^*$ temos $\nu(a) = l$ para algum $l \in \mathbb{Z}$, assim,

$$\nu(a) = \nu(\pi^l)$$

e obtemos que $a\pi^{-l} = b \in R$ e logo $a = \dfrac{b}{\pi^{-l}}$, daí, segue que K é o corpo de frações de R.

Exemplo 2.4.1. *Seja p um número primo. Cada número racional $q \neq 0$ pode ser escrito de forma única como $p^k\frac{r}{s}$, onde $k \in \mathbb{Z}, s > 0$, $p \nmid r$, $p \nmid s$ e $mdc(r,s) = 1$. Defina $\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z}$ por $\nu(q) = k$ e $\nu_p(0) = +\infty$, assim ν_p é uma valorização discreta em $\mathbb{Q}$ e o seu anel de valorização é o anel $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q}; p \nmid b\}$.*

Uma cadeia ascendente de ideais em um anel R é uma sequência crescente de ideais

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq ... \subseteq \mathfrak{a}_n \subseteq ....$$

Dizemos que essa cadeia é estacionaria se existe $m \geq 0$ tal que

$$\mathfrak{a}_m = \mathfrak{a}_i \ \forall i > m.$$

Um anel é dito Noetheteriano se toda cadeia ascendente de ideais é estacionária, o anel dos inteiros é um exemplo de tal anel.

Dada uma cadeia de ideais primos no anel R

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset ... \subset \mathfrak{p}_n$$

o numero n é chamado comprimento da cadeia. O supremo dos comprimentos das cadeias de ideais primos de R é denominado a dimensão de Krull de R. Por exemplo, um corpo tem dimensão de Krull zero e o anel dos inteiros $\mathbb{Z}$ tem dimensão de Krull igual a um.

Como observamos anteriormente, um anel de valorização discreta possui dimensão de Krull igual 1, e como esse possui uma única cadeia de ideais próprios

$$... \subset \mathfrak{m}^k \subset ... \subset \mathfrak{m}^1 = \mathfrak{m}$$

R é um anel Noetheriano. Temos visto que um anel de valorização discreta é um domínio local Noetheriano de dimensão de Krull um, no qual o único ideal maximal é principal. Como mostra o próximo teorema, essa é uma caracterização dos anéis de valorização discreta.

Teorema 2.4.1 ([4], Proposição 9.2, pág.94)**.** *Seja R um domínio Noetheriano local possuindo dimensão de Krull igual a 1. As seguintes afirmações são equivalentes*

1. *R é um anel de valorização discreta.*
2. *O ideal maximal $\mathfrak{m} \subset R$ é principal.*

Em algumas ocasiões é conveniente utilizar uma outra noção de valorização: a noção de valorização discreta multiplicativa. A grande diferença é que essa fornece uma métrica no corpo K em que está definida, assim, K se torna um espaço métrico. Quando K não é um espaço métrico completo com a topologia induzida pela métrica (fornecida pela valorização multiplicativa), é possível construir um novo corpo $\widehat{K}$ que é completo e contém K como subcorpo. O corpo $\widehat{K}$ é denominado o completamento de K com respeito a métrica induzida pela valorização multiplicativa, esse é o menor corpo no qual K é completo com essa métrica. A norma de $\widehat{K}$ é uma extensão da norma de K e, assim, toda sequência de Cauchy em K possui um limite em $\widehat{K}$.

Definição 2.4.3. *Uma valorização multiplicativa no corpo K é uma função $\phi : K \longrightarrow [0, +\infty)$ que satisfaz*

1. *$\phi(a) = 0 \Leftrightarrow a = 0$,*
2. *$\phi(ab) = \phi(a)\phi(b)$,*
3. *$\phi(a + b) \leq \phi(a) + \phi(b)$.*

As três condições fornecem que definindo $d(a, b) = \phi(a - b)$, d se torna uma métrica. A última condição é conhecida como a desigualdade triangular.

Exemplo 2.4.2. *Seja K um corpo e defina ϕ por $\phi(a) = 0$ se $a = 0$ e $\phi(a) = 1$ caso contrário. Então ϕ é uma valorização multiplicativa.*

Exemplo 2.4.3. *Seja K um subcorpo dos números complexos. Definindo $\phi(a) = |a|$, onde $|\ |$ denota a norma usual em $\mathbb{C}$, ϕ é uma valorização multiplicativa.*

O exemplo mais comum de um completamento via uma valorização é quando tomamos $K = \mathbb{Q}$ e ϕ para ser o valor absoluto (a norma usual em $\mathbb{C}$), o completamento de $\mathbb{Q}$ obtido é o conjunto dos números reais .

Uma valorização multiplicativa ϕ que satisfaz $\phi(a+b) \leq \max(\phi(a), \phi(b))$ é chamada valorização multiplicativa não arquimediana. Se ϕ é não arquimediana o conjunto

$$R_\phi = \{a \in K : \phi(a) \leq 1\}$$

é um anel denominado anel de valorização de ϕ. Dado $a \in R_\phi$ invertível em R_ϕ temos

$$0 < \phi(a) \leq 1,\ 0 < (\phi(a))^{-1} \leq 1,$$

assim, $\phi(a) = 1$. Por outro lado, dado $a \in R_\phi$ com $\phi(a) = 1$, então $\phi(a^{-1}) = (\phi(a))^{-1} = 1$ e logo $a^{-1} \in R_\phi$. Dessas observações segue que $\mathfrak{m} = \{a \in R_\phi; \phi(a) < 1\}$ é o único ideal maximal de R_ϕ.

Quando o conjunto $\phi(K^*)$ é um grupo cíclico infinito, dizemos que ϕ é uma valorização discreta multiplicativa, e nesse caso, podemos mostrar, com ideias análogas para o caso de uma valorização aditiva, que $\mathfrak{m}$ é principal e gerado pelo elemento $\pi \in R_\phi$ tal que $\phi(\pi)$ gera o grupo cíclico $\phi(K^*)$. Também podemos mostrar que todo ideal próprio de R é da forma $\mathfrak{m}^k, k \in \mathbb{N}$, assim, o único ideal primo não nulo em R_ϕ é $\mathfrak{m}$. Portanto, R_ϕ é um domínio local Noetheriano de dimensão de Krull igual a um no qual o ideal maximal é principal, logo um anel de valorização discreta pelo Teorema 2.4.1.

Exemplo 2.4.4 (valorização p-ádica)**.** *Seja p um número primo e seja ν_p a valorização discreta definida no Exemplo 2.4.1. Defina*

$$\phi_p : \mathbb{Q} \longrightarrow [0, +\infty)$$

colocando $\phi_p(a) = \left(\frac{1}{p}\right)^{\nu_p(a)}$ se $a \neq 0$ e $\phi_p(0) = 0$. Com essa definição, ϕ_p é uma valorização multiplicativa em $\mathbb{Q}$. Essa valorização é conhecida como a valorização p-ádica. Como $\nu_p(a+b) \geq min\{\nu_p(a), \nu_p(b)\}$ e $\frac{1}{p} < 1$, obtemos

$$\left(\frac{1}{p}\right)^{\nu_p(a+b)} \leq \left(\frac{1}{p}\right)^{min\{\nu_p(a),\nu_p(b)\}}$$

ou seja, $\phi_p(a+b) \leq max\{\nu_p(a), \nu_p(b)\}$ e ϕ é não arquimediana. Além disso, ϕ_p é discreta, já que $\phi_p(\mathbb{Q}^*)$ é gerado por p^{-1}. O anel de valorização de ϕ_p é a localização de $\mathbb{Z}$ em p, isso é, o anel $\mathbb{Z}_{(p)}$.

No último exemplo o completamento obtido para $\mathbb{Q}$ utilizando a métrica induzida por ϕ_p é conhecido como o conjunto dos números p-ádicos e denotado por $\mathbb{Q}_p$. É possível

mostrar (veja [1], Lema 4.1.2, pág.74) que ϕ_p possui uma extensão $\widehat{\phi}_p$ para todo $\mathbb{Q}_p$ e que $\widehat{\phi}_p(\mathbb{Q}_p^*) = \phi_p(\mathbb{Q}^*)$, assim, $\widehat{\phi}_p$ é uma valorização discreta e denotamos o seu anel de valorização por $\mathbb{Z}_p$ que é conhecido como o anel dos inteiros p-ádicos. Como vimos, $\mathbb{Z}_p$ é um anel de valorização discreta e seu ideal maximal é $p\mathbb{Z}_p$, já que $\widehat{\phi}_p(p) = \phi_p(p) = p^{-1}$ gera $\widehat{\phi}_p(\mathbb{Q}_p^*) = \phi_p(\mathbb{Q}^*)$.

Teorema 2.4.2. *Seja R um anel de valorização discreta com ideal maximal gerado por $\pi \in R$. Suponha que U seja um R-módulo finitamente gerado e livre de torção, e seja $u_1 \in U \backslash \pi U$, então u_1 gera um somando direto de U.*

Demonstração. Mantendo a notação do Corolário 2.3.3, como $u_1 \notin \pi U$ e $U/\pi U$ é um espaço vetorial sobre o corpo $R/\pi R$, deve existir uma base para $U/\pi U$ contendo $\bar{u}_1$, digamos $\{\bar{u}_1, ..., \bar{u}_n\}$. Pelo Corolário 2.3.3, $U = \langle u_1, ..., u_n \rangle$. Agora, observe que se

$$\lambda_1 u_1 + \lambda_2 u_2 + ... + \lambda_n u_n = 0 \Rightarrow \lambda_i \in \pi R$$

pois caso contrário, teríamos

$$\lambda_1 \bar{u}_1 + \lambda_2 \bar{u}_2 + ... + \lambda_n \bar{u}_n = \bar{0}$$

com algum $\lambda_i \notin \pi R$ e isso contraria a hipótese dos elementos $\bar{u}_1, ..., \bar{u}_n$, formarem uma base para o $R/\pi R$-espaço vetorial $U/\pi U$. Assim, $\lambda_i = \pi^{s_i} a_i$, onde a_i é invertível e $s_i > 0$. Seja $s = \min\{s_1, ..., s_n\}$, então podemos escrever

$$\pi^s(\pi^{s_1 - s} a_1 u_1 + ... + \pi^{s_n - s} a_n u_n) = 0.$$

já que U é livre de torção, devemos ter

$$\pi^{s_1 - s} a_1 u_1 + ... + \pi^{s_n - s} a_n u_n = 0,$$

e logo vamos obter uma contradição com o fato de $\{\bar{u}_1, ..., \bar{u}_n\}$ ser uma base para $U/\pi U$. Portanto, $\{u_1, ..., u_n\}$ é um conjunto linearmente independente e gera U, logo uma R-base para U. Daí, u_1 gera um somando direto de U. □

Terminamos essa seção com um teorema conhecido que diz respeito ao ideal de Jacobson da álgebra de grupo RG quando G é um p-grupo abeliano finito e p é primo no anel de valorização discreta R. Recordamos que I_G denota o ideal de aumentação de RG.

Teorema 2.4.3. *Seja G um p-grupo abeliano finito e R um anel de valorização discreta com ideal maximal pR. O ideal de Jacobson de RG é*

$$J(RG) = pRG + I_G.$$

Demonstração. De fato, se U é um RG-módulo, então pU também o é. Assim, se U é simples, devemos ter $pU = 0$ ou $pU = U$, mas a segunda opção somente ocorre quando $U = 0$, pelo Proposição 2.3.1. Posto isso, vemos que U deve ser um R/pR-espaço vetorial. O Teorema 2.2.1 garante que G age trivialmente em U, logo, pRG e I_G anulam todo RG-módulo simples. Por outro lado,

$$RG = \langle 1_{RG} \rangle_R \oplus I_G$$

como R-módulos, pois, como vimos na seção 2, o conjunto $\{g - 1; 1 \neq g \in G\}$ é uma R-base para I_G, além disso, como $1 \notin I_G$ devemos ter $\langle 1_{RG} \rangle_R \oplus I_G$ como R-módulos, mas como podemos obter os elementos de G como combinação linear de 1 e dos elementos de $\{g - 1; 1 \neq g \in G\} \subset I_G$, temos essa decomposição de RG. Assim,

$$RG/(pRG + I_G) = \langle 1 + (pRG + I_G) \rangle_R \simeq R/pR.$$

Daí, concluímos que $pRG + I_G$ é um ideal maximal de RG. Como o Teorema 2.3.1 fornece que $pRG + I_G \subseteq J(RG)$, pela definição de $J(RG)$, temos

$$J(RG) = pRG + I_G.$$

□

2.5 Decompondo o anel de grupo RG

Seja R um anel comutativo com unidade e G um grupo abeliano finito. Dois elementos $a, b \in RG$ são chamados ortogonais se $ab = 0$. Um elemento $e \in RG$ é dito idempotente se $e^2 = e$. O idempotente e é chamado de primitivo se ele não se escreve como uma soma de dois idempotentes ortogonais, o que equivale a dizer que RGe não se escreve como uma soma direta de ideais de RG não nulos.

Teorema 2.5.1 ([8], Proposição 3.6.1, pág.46)**.** *Seja R um anel comutativo com unidade e G um grupo abeliano finito. Cada decomposição de RG em soma direta de ideais bilaterais*

$$RG = \Lambda_1 \oplus \Lambda_2 \oplus ... \oplus \Lambda_r$$

corresponde a uma decomposição da identidade de RG

$$1 = e_1 + e_2 + ... + e_r$$

como soma de idempotentes ortogonais e vice-versa. Por essa correspondência, $\Lambda_i = RGe_i$ e se cada Λ_i é indecomponível, então e_i é primitivo e esses são os únicos idempotentes primitivos centrais de RG.

Demonstração. Se RG possui uma decomposição do tipo $RG = \Lambda_1 \oplus \Lambda_2 \oplus ... \oplus \Lambda_r$, onde cada Λ_i é um ideal de RG, então existem $e_i \in \Lambda_i, i = 1, ..., r$ tais que

$$1 = e_1 + e_2 + ... + e_r.$$

Sendo Λ_i um ideal de RG, obtemos que $e_i e_j \in \Lambda_i \cap \Lambda_j$. Como $\Lambda_i \cap \Lambda_j = 0$ se $i \neq j$, por consequência temos $e_i e_j = 0$ quando $i \neq j$.

Agora, observe que

$$e_i = e_i 1 = e_i(e_1 + e_2 + ... + e_r) = e_i^2 + \sum_{j \neq i} e_i e_j$$

e obtemos $e_i = e_i^2$, assim, os elementos $e_1, ..., e_r$, são idempotentes e ortogonais. Dado $\lambda_i \in \Lambda_i$, temos

$$\lambda_i = \lambda_i 1 = \lambda_i(e_1 + e_2 + ... + e_r) = \lambda_i e_i,$$

onde a última igualdade foi obtida da decomposição de RG como soma direta dos Λ_i. Dessa maneira, $\Lambda_i = RGe_i$.

Reciprocamente, dada uma decomposição da unidade de RG

$$1 = e_1 + e_2 + ... + e_r$$

como soma de idempotentes ortogonais, temos para cada $\lambda \in R$

$$\lambda = \lambda 1 = \lambda(e_1 + e_2 + ... + e_r) \in RGe_1 + RGe_2 + ... + RGe_r$$

e segue que $RG = RGe_1 + RGe_2 + ... + RGe_r$. Agora, se $\lambda_i \in RGe_i \cap \left(\sum_{i \neq j} RGe_j \right)$, então $\lambda_i = e_i\lambda_i = 0$, já que e_i age como 0 em $\sum_{i \neq j} RGe_j$. Assim,

$$RG = RGe_1 \oplus RGe_2 \oplus ... \oplus RGe_r.$$

Se cada RGe_i é indecomponível como anel, então $e_i, i = 1, 2, ..., r$, é primitivo, pois caso contrário teríamos

$$e_i = e_i' + e_i''$$

onde e_i' e e_i'' são idempotentes ortogonais, o que implicaria em $RGe_i = RGe_i' \oplus RGe_i''$. E de modo análogo vemos que e_i primitivo implica RGe_i indecomponível como anel.

Por outro lado, se existem outros idempotentes primitivos que são ortogonais, digamos $f_1, ..., f_s$, e que satisfazem

$$1 = e_1 + ... + e_r = f_1 + ... + f_s,$$

então para cada $i = 1, ..., r$ temos

$$e_i = e_i 1 = e_i \sum_{j=1}^{s} f_j.$$

Sendo e_i primitivo, devemos ter $e_i = e_i f_j$ para um único índice $j \in \{1, 2, ..., s\}$, pois $e_i f_l$ é idempotente e ortogonal a $e_i f_k$ se $l \neq k$. Para esse índice j, temos

$$f_j = f_j 1 = f_j \sum_{i=1}^{r} e_i,$$

e pelo mesmo argumento anterior obtemos $f_j = f_j e_k$ para algum índice $k \in \{1, 2, ..., s\}$. Como já obtemos $e_i f_j \neq 0$, devemos ter $f_j = e_i f_j$ e logo $f_j = e_i$. Note que se $i \neq j$, então e_i e e_j não podem cumprir $e_i = f_k$ e $e_j = f_k$, uma vez que e_i e e_j são ortogonais, portanto $r \leq s$. De forma análoga obtemos $s \leq r$, donde $r = s$.

□

Agora, considerando o anel dos inteiros p-ádicos $\mathbb{Z}_p$ e seu corpo de frações $\mathbb{Q}_p$, vamos fornecer uma descrição dos idempotentes primitivos da álgebra de grupo $\mathbb{Q}_p[C_p \times C_p]$. Vamos utilizar esses idempotentes em uma correspondência devida a Butler para a construção de um $\mathbb{Z}_p[C_p \times C_p]$-módulo conveniente.

Ao longo dessa seção, G denotará o grupo $C_p \times C_p$ e $p > 0$ um número primo. Observe que sendo G um grupo abeliano seus subgrupos são normais, assim, se H e H' são subgrupos de G com ordem p satisfazendo $H \cap H' = \{1_G\}$, então HH' é um subgrupo de G possuindo ordem p^2 e, daí, G é o produto direto dos subgrupos H e H' que são cíclicos. Também note que se $G = \langle g \rangle \times \langle h \rangle$ os subgrupos próprios de G são exatamente os $p+2$ subgrupos a seguir

$$\langle 1_G \rangle, H_1 = \langle g \rangle, H_2 = \langle h \rangle, H_{2+j} = \langle gh^j \rangle, j = 1, ..., p-1.$$

Isso segue de observar que se $1 \leq i \neq j \leq p-1$ não podemos ter $gh^i = (gh^j)^k$ para nenhum $k \in \mathbb{Z}$, pois caso contrário $k - 1 \in p\mathbb{Z}$ e consequentemente $h^i = h^j$, resultando em $i - j \in p\mathbb{Z}$ o que não ocorre.

Vamos denotar por $\widehat{H}_i$ a soma de todos elementos do subgrupo H_i e por $\widehat{G}$ a soma de todos elementos de G. Para cada subgrupo H_i defina o seguinte elemento de $\mathbb{Q}_pG$

$$e_i = \frac{1}{p^2}\left(p\widehat{H}_i - \widehat{G}\right).$$

Observe que

$$e_i e_i = \frac{1}{p^4}\left(p\widehat{H}_i - \widehat{G}\right)\left(p\widehat{H}_i - \widehat{G}\right) =$$

$$\frac{1}{p^4}\left(p^2\widehat{H}_i^2 - 2p\widehat{H}_i\widehat{G} + \widehat{G}^2\right) =$$

$$= \frac{1}{p^4}(p^3\widehat{H}_i - 2p^2\widehat{G} + p^2\widehat{G}) = e_i,$$

assim, e_i é idempotente. Além disso, quando $i \neq j$ temos $G = \bigcup_{k=1}^{p-1} h_i^k H_j$, onde $\langle h_i \rangle = H_i$, e a união é disjunta. Daí,

$$e_i e_j = \frac{1}{p^4}\left(p\widehat{H}_i - \widehat{G}\right)\left(p\widehat{H}_j - \widehat{G}\right) =$$

$$\frac{1}{p^4}\left(p^2\widehat{H}_i\widehat{H}_j - p\widehat{H}_i\widehat{G} - p\widehat{H}_j\widehat{G} + \widehat{G}^2\right) =$$

$$= \frac{1}{p^4}\left(p^2\widehat{G} - p^2\widehat{G} - p^2\widehat{G} + p^2\widehat{G}\right) = 0,$$

e temos e_i ortogonal a e_j se $i \neq j$. Definindo $e_0 = \frac{1}{p^2}\widehat{G}$, uma conta simples mostra que e_0 é idempotente e ortogonal a e_i para cada $i = 1, 2, ..., p+1$. Também temos

$$\sum_{i=0}^{p+1} e_i = \frac{1}{p^2}\left[p\left(\widehat{H_1} + \widehat{H}_2 + ... + \widehat{H}_{p+1}\right) - p\widehat{G}\right] = 1.$$

Segue do Teorema 2.5.1 que essa decomposição da unidade fornece a decomposição

$$\mathbb{Q}_pG = \mathbb{Q}_pGe_0 \oplus \mathbb{Q}_pGe_1 \oplus ... \oplus \mathbb{Q}_pGe_{p+1}.$$

Observação 2.5.1. *Observe que se $g \in H_i$, temos $ge_i = e_i$ e logo $\mathbb{Q}_pGe_i$ é um $\mathbb{Q}_p[G/H_i]$-módulo. Também note que se $g \in G\backslash H_i$, temos $(1 + g + g^2 + ... + g^{p-1})\widehat{H}_i = \widehat{G}$, logo*

$$(1 + g + ... + g^{p-1})e_i = \frac{1}{p^2}\left(p(1 + g + ... + g^{p-1})\widehat{H}_i - (1 + g + ... + g^{p-1})\widehat{G}\right) = 0.$$

Daí, $g \notin H_i$ implica em

$$(1 + g + g^2 + ... + g^{p-1})e_i = 0$$

e caso contrário $ge_i = e_i$.

Nosso objetivo é mostrar que $\mathbb{Q}_pGe_i$ é um $\mathbb{Q}_pG$-módulo simples para cada $i = 1, 2, ..., p+1$. Para tanto, vamos precisar de alguns resultados.

Proposição 2.5.1. *Seja $g \notin H_i$, então os elementos $e_i, ge_i, ..., g^{p-2}e_i$ formam uma base para $\mathbb{Q}_pGe_i$ sobre $\mathbb{Q}_p$.*

Demonstração. Seja $g \notin H_i$, como G é o produto direto de H_i com o subgrupo gerado por g, e H_i age trivialmente em $\mathbb{Q}_pGe_i$, todo elemento de $\mathbb{Q}_pGe_i$ pode ser escrito da forma

$$(a_0 + a_1g + ... + a_{p-2}g^{p-2} + a_{p-1}g^{p-1})e_i, a_j \in \mathbb{Q}_p.$$

Pela Observação 2.5.1 temos

$$g^{p-1}e_i = -(1 + g^2 + ... + g^{p-2})e_i,$$

assim, apenas os elementos $e_i, ge_i, ..., g^{p-2}e_i$ são necessários para gerar $\mathbb{Q}_pGe_i$. Por outro lado,

$$(a_0 + a_1g + ... + a_{p-2}g^{p-2})e_i = (a_0 + a_1g + ... + a_{p-2}g^{p-2})\frac{1}{p^2}\left(p\widehat{H}_i - \widehat{G}\right) =$$

$$= \frac{1}{p^2}\left(p(a_0 + a_1g + ... + a_{p-2}g^{p-2})\widehat{H}_i - (a_0 + a_1 + ... + a_{p-2})\widehat{G}\right).$$

Como

$$\widehat{G} = \widehat{H}_i + g\widehat{H}_i + ... + g^{p-1}\widehat{H}_i,$$

obtemos

$$\frac{1}{p^2}\left(p(a_0 + a_1g + ... + a_{p-2}g^{p-2})\widehat{H}_i - (a_0 + a_1 + ... + a_{p-2})\widehat{G}\right) =$$

$$= \frac{1}{p^2}\left(pa_0 - \sum_{j=0}^{p-2} a_j\right)\widehat{H}_i + \frac{1}{p^2}\left(pa_1 - \sum_{j=0}^{p-2} a_j\right) g\widehat{H}_i + ...$$

$$+\frac{1}{p^2}\left(pa_{p-2} - \sum_{j=0}^{p-2} a_j\right) g^{p-2}\widehat{H}_i - \left(\frac{1}{p^2}\sum_{j=0}^{p-2} a_i\right) g^{p-1}\widehat{H}_i.$$

Assim,

$$(a_0 + a_1 g + ... + a_{p-2}g^{p-2})e_i = 0 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} pa_i = \sum_{j=0}^{p-2} a_j \quad i = 0, 1, ..., p-2 \\ \sum_{j=0}^{p-2} a_j = 0 \end{cases}$$

donde, $a_j = 0, i = 0, 1, ..., p-2$, pois $G = \bigcup_{k=1}^{p-1} g^k H_i$ é uma base para $\mathbb{Q}_p G$ e essa união é disjunta. Por consequência, os elementos $e_i, ge_i, ..., g^{p-2}e_i$, são linearmente independentes sobre $\mathbb{Q}_p$, como eles geram $\mathbb{Q}_p G e_i$, segue que o conjunto $\{e_i, ge_i, ..., g^{p-2}e_i\}$ é uma $\mathbb{Q}_p$-base para $\mathbb{Q}_p G e_i$. □

Observação 2.5.2. *Considere o grupo cíclico C_p e seja $g \in C_p$ um gerador desse grupo. Podemos definir um homomorfismo de álgebras ϕ entre a álgebra de polinômios $\mathbb{Q}_p[x]$ e $\mathbb{Q}_p C_p$ colocando*

$$\phi(a_0 + a_1 x + ... + a_n x^n) = a_0 + a_1 g + ... + a_n g^n.$$

Como ϕ é sobrejetiva temos $\mathbb{Q}_p C_p \simeq \mathbb{Q}_p[x]/\ker\phi$. Agora, observe que

$$\langle x^p - 1\rangle \subseteq \ker\phi.$$

Por outro lado, se $f \notin \langle x^p - 1\rangle$, então existem únicos polinômios q e r em $\mathbb{Q}_p[x]$ tais que $f = q(x^p - 1) + r$, onde $r \neq 0$ e o grau de r é menor do que p. Assim, $\phi(f) = \phi(r) \neq 0$, já que os elementos $1, g, ..., g^{p-1}$ formam uma base para $\mathbb{Q}_p C_p$, logo $\ker\phi = \langle x^p - 1\rangle$ e $\mathbb{Q}_p C_p \simeq \mathbb{Q}_p[x]/\langle x^p - 1\rangle$.

Denote por f_0 o polinômio $x^{p-1} + x^{p-2} + ... + x + 1 \in \mathbb{Z}_p[x]$.

Proposição 2.5.2. *O polinômio f_0 é irredutível em $\mathbb{Z}_p[x]$ e consequentemente também irredutível em $\mathbb{Q}_p[x]$.*

Demonstração. Como $\mathbb{Z}_p$ é um domínio de fatoração única e p é primo em $\mathbb{Z}_p$, podemos aplicar o critério de Eisenstein (veja [11], Teorema 3.2.8, pág.80) ao polinômio $f_0(x+1)$ para obter que $f_0(x+1)$ é irredutível em $\mathbb{Z}_p[x]$. Ora, $f_0(x)$ é irredutível se, e somente se,

$f_0(x+1)$ o é. Observe que

$$f_0(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + ... + (x-1) + 1 = \frac{(x+1)^p - 1}{(x+1) - 1} =$$

$$\frac{x^p + \binom{p}{1}x^{p-1} + ... + \binom{p}{p-1}x + 1 - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + ... + \binom{p}{p-2}x + p,$$

onde $\binom{p}{i} = \frac{p!}{(p-i)!i!}$. Uma vez que $p|\binom{p}{i}$ quando $0 < i < p$ e $p^2 \nmid p$, temos que $f_0(x+1)$ é irredutível pelo critério de Eisenstein. Como f_0 é primitivo e irredutível em $\mathbb{Z}_p[x]$, segue do Lema de Gauss (ver [11] Lema 2.3.6, pág.60) que f_0 é irredutível em $\mathbb{Q}_p[x]$. □

Uma consequência imediata da proposição anterior é que o ideal gerado por f_0 é maximal em $\mathbb{Q}_p[x]$. Além disso, f_0 é um fator de $x^p - 1$, e daí vem que $\langle f_0\rangle/\langle x^p - 1\rangle$ é um ideal de $\mathbb{Q}_p[x]/\langle x^p - 1\rangle$. Como vimos na Observação 2.5.2, $\mathbb{Q}_pC_p \simeq \mathbb{Q}_p[x]/\langle x^p - 1\rangle$ como $\mathbb{Q}_p$-álgebras, assim, $\langle f_0\rangle/\langle x^p-1\rangle$ é um $\mathbb{Q}_pC_p$-módulo. Agora, o quociente de $\mathbb{Q}_p[x]/\langle x^p-1\rangle$ pelo $\mathbb{Q}_pC_p$-submódulo gerado pela classe de f_0 é isomorfo ao quociente $\mathbb{Q}_p[x]/\langle f_0\rangle$ que é um corpo. Denote por g um gerador de C_p. Como g age em $\mathbb{Q}_p[x]/\langle f_0\rangle$ como uma multiplicação pela classe de x, qualquer $\mathbb{Q}_pC_p$-submódulo de $\mathbb{Q}_p[x]/\langle f_0\rangle$ é um ideal do mesmo, portanto, $\mathbb{Q}_p[x]/\langle f_0\rangle$ é um $\mathbb{Q}_pC_p$-módulo simples. Também observe que como o grau de f_0 é $p-1$, a dimensão de $\mathbb{Q}_p[x]/\langle f_0\rangle$ sobre $\mathbb{Q}_p$ deve ser $p-1$. Com essas observações temos o seguinte resultado:

Proposição 2.5.3. *$\mathbb{Q}_p[x]/\langle f_0\rangle$ é um $\mathbb{Q}_pC_p$-módulo simples.*

Fixado $i \in \{1, 2, ..., p+1\}$, temos visto que podemos tratar $\mathbb{Q}_p[x]/\langle f_0\rangle$ como um $\mathbb{Q}_p[G/H_i]$-módulo em que um gerador g de G/H_i age como uma multiplicação pela classe do x em $\mathbb{Q}_p[x]/\langle f_0\rangle$. Posto isso, temos o seguinte resultado:

Teorema 2.5.2. *Fixado $i \in \{1, 2, ..., p+1\}$, os $\mathbb{Q}_p[G/H_i]$-módulos $\mathbb{Q}_pGe_i$ e $\mathbb{Q}_p[x]/\langle f_0\rangle$ são isomorfos .*

Demonstração. Seja $h \in \mathbb{Q}_p[x]$ e denote por $\bar{h} = a_0 + a_1\bar{x} + ... + a_{p-1}\bar{x}^{p-2}$ a sua classe em $\mathbb{Q}_p[x]/\langle f_0\rangle$. Seja $g \in G\backslash H_i$ e defina $\phi : \mathbb{Q}_p[x]/\langle f_0\rangle \longrightarrow \mathbb{Q}_pGe_i$ por

$$\phi(a_0 + a_1\bar{x} + ... + a_{p-2}\bar{x}^{p-2}) = (a_0 + a_1g + ... + a_{p-2}g^{p-2})e_i.$$

Sendo $\{\bar{1}, \bar{x}, ..., \bar{x}^{p-2}\}$ uma $\mathbb{Q}_p$-base para $\mathbb{Q}_p[x]/\langle f_0\rangle$, ϕ está bem definida. Como vimos na Proposição 2.5.1, o conjunto $\{e_i, ge_i, ..., g^{p-2}e_i\}$ é uma base para $\mathbb{Q}_pGe_i$, assim, ϕ é um isomorfismo de $\mathbb{Q}_p$-espaços vetoriais. Agora, $\phi(\bar{1}) = e_i, \phi(\bar{x}) = ge_i, \phi(\bar{x}^2) = g^2e_i, ..., \phi(\bar{x}^{p-2}) = g^{p-2}e_i$. Daí, como g age em $\mathbb{Q}_p[x]/\langle f_0\rangle$ por uma multiplicação pela classe de x, obtemos $\forall k \in \{0, 1, ..., p-2\}$, e $\forall i \in \{1, ..., p\}$,

$$\phi(g^j(\bar{x}^k)) = \phi(\bar{x}^j\bar{x}^k) = \phi(\bar{x}^{j+k}) =$$

$$= g^{j+k}e_i = g^j(g^k e_i) = g^j\phi(\bar{x}^k).$$

Assim, ϕ é um $\mathbb{Q}_p[G/H_i]$-isomorfismo, mas sendo $G = H_i \times \langle g\rangle$, ϕ também é um $\mathbb{Q}_pG$-isomorfismo. □

Corolário 2.5.1. *$\mathbb{Q}_pGe_i$ é um $\mathbb{Q}_pG$-módulo simples para cada $i \in \{1, ..., p+1\}$.*

Demonstração. Com efeito, a Proposição 2.5.3 garante que $\mathbb{Q}_p[x]/\langle f_0\rangle$ é um $\mathbb{Q}_pG$-módulo simples. Pelo último teorema temos $\mathbb{Q}_pGe_i \simeq \mathbb{Q}_p[x]/\langle f_0\rangle$. □

Observação 2.5.3. *Note que tratando $\mathbb{Q}_p[x]/\langle f_0\rangle$ como uma $\mathbb{Q}_p$-álgebra a aplicação ϕ definida no teorema anterior é um homomorfismo de $\mathbb{Q}_p$-álgebras. Mas sendo ϕ uma bijeção, ϕ é um isomorfismo de $\mathbb{Q}_p$-álgebras.*

Corolário 2.5.2. *Os idempotentes $e_0, ..., e_{p+1}$ são idempotentes primitivos ortogonais da álgebra de grupo $\mathbb{Q}_pG$.*

Demonstração. De fato, já vimos que eles são ortogonais. Como que $\mathbb{Q}_pGe_0 \simeq \mathbb{Q}_p$, temos e_0 primitivo. Utilizando o Corolário 2.5.1 obtemos que $\mathbb{Q}_pGe_i$ é simples para cada $i \in \{1, ..., p+1\}$, portanto, indecomponível. □

Vamos terminar a seção mostrando que o domínio $\mathbb{Z}_pGe_i \subset \mathbb{Q}_pGe_i$ é um anel de valorização discreta com ideal maximal $J\mathbb{Z}_pGe_i$, onde J denota o ideal de Jacobson de $\mathbb{Z}_pG$. Esse fato será de grande utilidade para o desenvolvimento do trabalho.

Começamos observando que $\mathbb{Z}_p[x]/\langle f_0\rangle$ é uma $\mathbb{Z}_p$-álgebra que é isomorfa a $\mathbb{Z}_pGe_i$,$i = 1, ..., p+1$. Mostramos isso da mesma forma que fizemos no Teorema 2.5.2 e na Observação 2.5.3, pois os coeficientes lideres dos polinômios f_0 e $x^p - 1$ são invertíveis em $\mathbb{Z}_p$, desse modo podemos realizar divisão por eles em $\mathbb{Z}_p[x]$.

Sendo $\mathbb{Z}_p$ Noetheriano de dimensão de Krull igual a um, o anel $\mathbb{Z}_p[x]$ é Noetheriano com dimensão de Krull igual a 2 (veja [3], Teorema 15.4, pág.117). Assim, se $\mathfrak{p} \subset \mathbb{Z}_p[x]$ é um ideal primo não nulo, então o domínio Noetheriano $\mathbb{Z}_p[x]/\mathfrak{p}$ tem dimensão de Krull igual a 1, pois cada ideal primo não nulo de $\mathbb{Z}_p[x]/\mathfrak{p}$ é da forma $\mathfrak{p}'/\mathfrak{p}$, onde $\mathfrak{p}'$ é um ideal primo de $\mathbb{Z}_p[x]$ que contém $\mathfrak{p}$. Daí, concluímos que $\mathbb{Z}_pGe_i$ é um domínio Noetheriano de dimensão de Krull igual a 1, já que $\mathbb{Z}_pGe_i \simeq \mathbb{Z}_p[x]/\langle f_0\rangle$ e o ideal $\langle f_0\rangle \subset \mathbb{Z}_p[x]$ é primo.

Denote por J o ideal de Jacobson de $\mathbb{Z}_pG$. Pelo Teorema 2.4.3, temos

$$J = p\mathbb{Z}_pG + I_G.$$

Teorema 2.5.3. *Os anéis $\mathbb{Z}_pGe_i$ são de valorização discreta para cada $i = 0, 1, ..., p+1$, e com ideal maximal $J(\mathbb{Z}_pGe_i)$.*

Demonstração. Primeiramente observe que e_i é a identidade de $\mathbb{Z}_pGe_i$. Para $i = 0$ não temos nada para fazer, já que $\mathbb{Z}_pGe_0 \simeq \mathbb{Z}_p$. Quando $i > 0$ e $g \notin H_i$ temos

$$pe_i = (p - 1 - g - g^2 - ... - g^{p-1})e_i,$$

pois, pela Observação 2.5.1

$$(1 + g + g^2 + ... + g^{p-1})e_i = 0.$$

Como

$$(p - 1 - g - g^2 - ... - g^{p-1}) = (1 - g) + (1 - g^2) + ... + (1 - g^{p-1}),$$

pela definição de I_G, temos $(p - 1 - g - g^2 - ... - g^{p-1}) \in I_G$. Daí, $pe_i \in I_{\langle g\rangle}\mathbb{Z}_pGe_i$.

Sendo $I_{\langle g\rangle} = \langle g - 1\rangle_{\mathbb{Z}_p\langle g\rangle}$, temos $pe_i \in (g - 1)\mathbb{Z}_pGe_i$. Como $G = H_i \times \langle g\rangle$ e H_i age trivialmente em $\mathbb{Z}_pGe_i$, obtemos

$$J(\mathbb{Z}_pGe_i) = (p\mathbb{Z}_pG + I_G)\mathbb{Z}_pGe_i = (p\mathbb{Z}_p\langle g\rangle + I_{\langle g\rangle})\mathbb{Z}_pGe_i = I_{\langle g\rangle}\mathbb{Z}_pGe_i,$$

onde a última igualdade foi obtida do fato de que $pe_i \in I_{\langle g\rangle}\mathbb{Z}_pGe_i$. Com isso, temos $J(\mathbb{Z}_pGe_i) = (g - 1)e_i\mathbb{Z}_pGe_i$ e $J(\mathbb{Z}_pGe_i)$ é um ideal principal de $\mathbb{Z}_pGe_i$.

Agora, se $\lambda \in J$ e $\lambda' \in \mathbb{Z}_pG$, então $\lambda\lambda' e_i - e_i = (\lambda\lambda' - 1)e_i$, mas, pela definição de J, $\lambda\lambda' - 1$ é invertível. Logo, $(\lambda\lambda' - 1)e_i$ é invertível em $\mathbb{Z}_pGe_i$, consequentemente λe_i está no ideal de Jacobson de $\mathbb{Z}_pGe_i$.

Ora, $\mathbb{Z}_pGe_i/J\mathbb{Z}_pGe_i$ é um $\mathbb{F}_p$-espaço vetorial gerado pela classe de e_i, pois G age trivialmente nesse quociente e $pe_i \in J(\mathbb{Z}_pGe_i)$. Então, temos que $\mathbb{Z}_pGe_i/J(\mathbb{Z}_pGe_i) \simeq \mathbb{F}_p$ e $J(\mathbb{Z}_pGe_i)$ é maximal, disso segue que $J(\mathbb{Z}_pGe_i)$ é o ideal de Jacobson de $\mathbb{Z}_pGe_i$.

Concluímos que $\mathbb{Z}_pGe_i$ é um domínio Noetheriano local possuindo dimensão de Krull igual a 1 no qual o ideal maximal é principal, então, pelo Teorema 2.4.1, $\mathbb{Z}_pGe_i$ é um anel de valorização discreta. □

Capítulo 3

RG-módulos de permutação

Nesse capítulo apresentamos a noção de RG-módulos de permutação e alguns resultados importantes relacionados com eles. Quando G é um p-grupo finito e $R = \mathbb{Z}_p$, dois dos principais resultados indicam uma maneira de decidir quando um $\mathbb{Z}_pG$-módulo é de permutação.

3.1 Módulos de permutação

Seja U um RG-módulo. Dizemos que U é um RG-reticulado ou simplesmente reticulado, se U é R-livre e finitamente gerado. Dizemos que U é um RG-módulo de permutação se U é um RG-reticulado que possui uma R-base que é preservada pela ação de G.

Exemplo 3.1.1. *Seja $G = S_n$ o grupo simétrico e U um R-módulo com R-base $\{u_1, u_2, ..., u_n\}$. Defina $\sigma u_i = u_{\sigma(i)}$, e estenda para todo U a ação de forma linear, desse modo, U é um RS_n-módulo de permutação.*

Exemplo 3.1.2. *Considere o anel de grupo RG. Esse é um módulo de permutação para RG, já que $\{g; g \in G\}$ é uma R-base preservada por G.*

Exemplo 3.1.3. *O RGmodulo trivial R, é um RG-módulo de permutação, já que $g \cdot 1 = 1 \forall g \in G$.*

Exemplo 3.1.4. *Seja $p > 0$ um número primo. Seja $R = \mathbb{Z}_p$ e $G = \langle g \rangle$ o grupo cíclico de ordem p. Considere o ideal de aumentação I_G de $\mathbb{Z}_pG$. Como $I_G = \langle g - 1 \rangle_{\mathbb{Z}_pG}$, $1 + g + g^2 + ... + g^{p-1}$ age como uma multiplicação por 0 em I_G, uma vez que*

$$(g - 1)(1 + g + g^2 + ... + g^{p-1}) = 1 - g^p = 0.$$

Desse modo, não se pode ter uma base para I_G preservada pela ação de G, pois caso tivesse, a soma de todos os elementos dessa base, digamos $u \in I_G$, seria um ponto fixo de

G. Como $(1+g+g^2+...+g^{p-1})u = pu = 0$, pela escolha de u, obtemos uma contradição. Assim, I_G não é um $\mathbb{Z}_pG$-módulo de permutação.

Um G-conjunto é um conjunto Ω não vazio com uma ação de G. Em geral, um RG-módulo de permutação é especificado por um G-conjunto. De fato, considere o R-módulo livre $R\Omega$ com base Ω. Sendo Ω um G-conjunto, então $R\Omega$ é um RG módulo de permutação. Por outro lado, um módulo de permutação U possui uma base B que é um G-conjunto e, claro, temos $U = RB$.

Seja G um grupo abeliano e Ω um G-conjunto. Para cada $x \in \Omega$ denote por $\mathfrak{O}(x)$ a órbita de x. Como Ω se decompõe em uma união disjunta de órbitas, digamos

$$\Omega = \bigcup_{i=1}^{r} \mathfrak{O}(x_i)$$

daí, devemos ter $R\Omega = R\mathfrak{O}(x_1) \oplus ... \oplus R\mathfrak{O}(x_r)$. Denote por H_i o estabilizador de x_i, então $\mathfrak{O}(x_i)$ é um G/H_i-conjunto e, desse modo, $R\mathfrak{O}(x_i)$ é um $R[G/H_i]$-módulo de permutação. Sejam $\bar{1}, \bar{g}_1, ..., \bar{g}_s$ representantes distintos das classes laterais de H_i em G, então o conjunto $\{\bar{1}, \bar{g}_1, ..., \bar{g}_s\}$ é uma base para $R[G/H_i]$. Como $\mathfrak{O}(x) = \{x, g_1x, g_2x, ..., g_sx\}$, segue que definindo

$$\phi : R[G/H_i] \longrightarrow R\mathfrak{O}(x)$$

por $\phi(\bar{1}) = x, \phi(\bar{g}_i) = g_ix, i = 1, ..., s$, obtemos um isomorfismo de RG-módulos. Com essas observações acabamos de provar o seguinte teorema:

Teorema 3.1.1. *Seja G um grupo abeliano e R um anel comutativo com unidade. Suponha que U é um RG-módulo de permutação, então U possui uma decomposição em soma direta de RG-módulos do tipo $R[G/H]$.*

Observação 3.1.1. *O último teorema também é válido quando G não é abeliano.*

Embora um RG-módulo de permutação U possua uma decomposição em soma direta de RG-módulos de permutação, pode acontecer que esse tenha uma decomposição em soma direta de RG-módulos que não são de permutação, por exemplo, quando $G = C_p \times C_p$, $\mathbb{Q}_pG$ é uma soma direta dos módulos $\mathbb{Q}_pGe_i, i = 0, 1, ..., p+1$, e apenas $\mathbb{Q}_pGe_0$ é um $\mathbb{Q}_pG$-módulo de permutação. Mas quando G é um p-grupo, não necessariamente abeliano, e R é um anel de valorização discreta completo no qual p é primo ou um corpo de característica p, então os somandos de um RG-módulo de permutação são sempre RG-módulos de permutação como afirma o próximo teorema.

Teorema 3.1.2 ([2], Teorema 7.1, pág.433)**.** *Seja R um corpo de característica $p > 0$ ou um anel de valorização discreta completo em que p é primo. Suponha que G é um p-grupo e que U é um RG-módulo com uma decomposição*

$$U = U_1 \oplus ... \oplus U_s$$

então U é um RG- módulo de permutação se, e somente se, cada $U_i, i = 1, ..., s$, o é.

3.2 Caracterizando os módulos de permutação

Em geral, decidir quando um RG-reticulado é de permutação não é uma tarefa simples, e os mesmos possuem aplicações importantes na teoria das representações de grupos. Desse modo, é conveniente encontrar formas de decidir quando um RG-reticulado é de permutação. O primeiro resultado que apresentamos nessa direção é para o caso no qual $R = \mathbb{Z}_p$ e G é cíclico de ordem p. Para tanto, precisamos de um resultado fundamental sobre a classificação dos $\mathbb{Z}_pC_p$-reticulados indecomponíveis.

Lema 3.2.1 ([9], Teorema 2.6, pág.79)**.** *Os únicos $\mathbb{Z}_pC_p$-reticulados indecomponíveis (a menos de isomorfismos) são $\mathbb{Z}_p, \mathbb{Z}_pC_p$ e I_{C_p}.*

Observação 3.2.1. *Seja g um gerador de C_p e denote $\mathbb{Z}_pC_p$ por U. Como U possui um elemento u tal que o conjunto $\{u, gu, g^2u, ..., g^{p-1}u\}$ é uma $\mathbb{Z}_p$-base para U, o conjunto*

$$\left\{u, (g-1)u, (g^2-u), ..., (g^{p-1}-1)u\right\}$$

também é uma $\mathbb{Z}_p$-base para U. Observe que o conjunto

$$\left\{(g-1)u, (g^2-u), ..., (g^{p-1}-1)u\right\} \subset I_{C_p}U$$

é uma $\mathbb{Z}_p$-base para $I_{C_p}U$. Assim, se $\bar{u}$ denota a classe de u no quociente $U/I_{C_p}U$, temos que $\bar{u}$ gera $U/I_{C_p}U$ como $\mathbb{Z}_p$-módulo. Já que $\{u, (g-1)u, (g^2-u), ..., (g^{p-1}-1)u\}$ é uma $\mathbb{Z}_p$-base para U, temos que $U/I_{C_p}U$ é $\mathbb{Z}_p$-livre e $\bar{u}$ forma uma base para esse módulo, ou seja, $U/I_{C_p}U \simeq \mathbb{Z}_p$ é um reticulado.

Quando $U = I_{C_p}$, como visto no Exemplo 3.1.4, o elemento $(p-1-g-g^2-...-g^{p-1}) \in \mathbb{Z}_pC_p$ age como uma multiplicação por p em U, logo $(p-1-g-g^2-...-g^{p-1})U = pU$. Agora,

$$(p-1-g-g^2-...-g^{p-1}) = (1-g)+(1-g^2)+...+(1-g^{p-1}) \in I_{C_p},$$

assim, $pU \subseteq I_{C_p}U$. Portanto, $U/I_{C_p}U$ não é $\mathbb{Z}_p$-livre, uma vez que $\mathbb{Z}_p$ é um domínio de ideais principais.

Para $U = \mathbb{Z}_p$, é imediato que $U/I_{C_p} \simeq \mathbb{Z}_p$, assim, U/I_{C_p} é um reticulado.

Teorema 3.2.1 ([5], Lema 8, pág.5)**.** *Seja U um $\mathbb{Z}_pC_p$ reticulado, então U é um $\mathbb{Z}_pC_p$-módulo de permutação se, e somente se, $U/I_{C_p}U$ é um reticulado.*

Demonstração. A classificação dos $\mathbb{Z}_pC_p$-reticulados fornece que U é uma soma direta dos módulos $\mathbb{Z}_p, \mathbb{Z}_pC_p$ e I_{C_p}. Como vimos no Exemplo 3.1.4, o $\mathbb{Z}_pC_p$-módulo I_{C_p} não é de permutação. Logo, pelo Teorema 3.1.2, U é de permutação se, e somente se, U não possui somando isomorfo a I_{C_p}.

Por outro lado, pela Observação 3.2.1, o único $\mathbb{Z}_p$-reticulado U indecomponível para o qual $U/I_{C_p}U$ não é um reticulado é o $\mathbb{Z}_pC_p$-módulo I_{C_p}. Assim, para um $\mathbb{Z}_pC_p$-reticulado U, $U/I_{C_p}U$ é um reticulado se, e somente se, U não possui $\mathbb{Z}_pC_p$-somando direto isomorfo a I_{C_p}. Portanto, um $\mathbb{Z}_pC_p$-reticulado U é um $\mathbb{Z}_pC_p$-módulo de permutação se, e somente se, $U/I_{C_p}U$ é um reticulado. □

Seja G um p-grupo finito e $\mathbb{F}_p$ o corpo residual de $\mathbb{Z}_p$. Dado $N \leqslant G$ denote por $U\downarrow_N$ o módulo U restrito aos escalares de $\mathbb{Z}_pN$ e por

$$U^N = \{u \in U; gu = u \ \forall g \in N\},$$

$$U_N = U/I_NU.$$

Um resultado importante na teoria das representações integrais, devido a Weiss é o seguinte:

Teorema 3.2.2 ([5], Teorema 1, pág. 1)**.** *Seja U um $\mathbb{Z}_pG$-reticulado e suponha que N é um subgrupo normal de G para o qual*

- *$U\downarrow_N$ é um $\mathbb{Z}_pN$-módulo livre e*
- *U^N é um $\mathbb{Z}_p[G/N]$-módulo de permutação.*

Então U é um $\mathbb{Z}_pG$-módulo de permutação.

Como um $\mathbb{Z}_pG$-módulo de permutação não precisa ser $\mathbb{Z}_pN$-livre (o módulo trivial $\mathbb{Z}_p$ é de permutação mas não é $\mathbb{Z}_pN$-livre) o Teorema 3.2.2 não é uma caracterização dos $\mathbb{Z}_pG$-módulos de permutação. Quando N tem ordem p, temos a seguinte caracterização dos $\mathbb{Z}_pG$-módulos de permutação devida a MacQuarrie e Zalesskii.

Teorema 3.2.3 ([5], Teorema 2, pág.2)**.** *Seja U um $\mathbb{Z}_pG$-reticulado e N um subgrupo normal de G com ordem p. Então, U é um $\mathbb{Z}_pG$-módulo de permutação se, e somente se*

1. *U^N e U_N são $\mathbb{Z}_p[G/N]$-módulos de permutação e*
2. *$\left(U/U^N\right)_N$ é um $\mathbb{F}_p[G/N]$-módulo de permutação.*

Em [5], MacQuarrie e Zalesskii fornecem dois exemplos em que a Condição 2 é verdadeira e apenas um dos módulos U^N e U_N é de permutação, mas U não é um $\mathbb{Z}_pG$-módulo de permutação. O objetivo do próximo capítulo é mostrar que, em geral, não podemos retirar a condição 2 no teorema acima e concluir que U é um $\mathbb{Z}_pG$-módulo de permutação.

Capítulo 4

A correspondência de Butler

Nesse capítulo vamos utilizar uma correspondência construída por Butler em [7] para mostrar que em geral somente a Condição 1 no Teorema 3.2.3 não caracteriza os $\mathbb{Z}_pG$-módulos de permutação. A correspondência de Butler vale para qualquer p-grupo abeliano e anéis de coeficientes (que são anéis de valorização discreta) mais gerais que $\mathbb{Z}_p$, mas fornecemos na Seção 4.1 a construção feita por Butler em [7] no caso especial em que $G = C_p \times C_p$ e o anel de coeficientes é $\mathbb{Z}_p$. Na Seção 4.4 utilizamos a ferramenta construída na Seção 4.1 para mostrar que, quando $p = 2$, U^N e U_N serem de permutação implica U de permutação, mas para $p > 2$ isso já não é válido, fornecendo um exemplo de um $\mathbb{Z}_3[C_3 \times C_3]$-módulo U em que U^N e U_N são de permutação, porém, U não é um $\mathbb{Z}_3[C_3 \times C_3]$-módulo de permutação. Vamos fixar algumas notações que serão usadas doravante: G denotará o grupo $C_p \times C_p$ e $\mathbb{F}_p$ o corpo residual de $\mathbb{Z}_p$. Manteremos as notações da Seção 2.5 para os idempotentes ortogonais primitivos $e_0, e_1, ..., e_{p+1}$ de $\mathbb{Q}_pG$, e para os subgrupos maximais $H_i, 0 < i \leq p+1$ de G. Também denotaremos por Λ o $\mathbb{Z}_pG$-módulo livre $\mathbb{Z}_pG$, e para cada $i \in A_{p+2} := \{0, 1, ..., p+1\}$, Λ_i denotará o $\mathbb{Z}_pG$-reticulado $\mathbb{Z}_pGe_i$ e J o ideal de Jacobson de $\mathbb{Z}_pG$.

4.1 Diagramas

Denote por $\mathcal{V}$ o conjunto de todos os $\mathbb{F}_pG$-módulos finitamente gerados. Também denote o produto cartesiano de $p+3$ cópias de $\mathcal{V}$ por $\mathcal{V}^{p+3}$.

Definição 4.1.1. *Uma $p+3$-upla $(V; V_0, V_1, ..., V_{p+1}) \in \mathcal{V}^{p+3}$ é um diagrama se são satisfeitas as seguintes condições*

1. $V_i \subseteq V \ \forall i \in A_{p+2}$,
2. *Fixado $i \in A_{p+2}$, temos* $V = \sum_{\substack{j \neq i \\ j \in A_{p+2}}} V_j$,

3. *Para cada* $i \in A_{p+2}$ *existem* $r_i \geq 0$ *e um epimorfismo* $\phi_i \in Hom_{\mathbb{Z}_pG}(\Lambda_i^{r_i}, V_i)$, *onde*

$$\bar{\phi} : \Lambda_i^{r_i}/J(\Lambda_i^{r_i}) \longrightarrow V_i/JV_i$$

$$\lambda_i + J(\Lambda_i^{r_i}) \mapsto \phi(\lambda_i) + JV_i$$

é um isomorfismo.

Observação 4.1.1. *Como vimos na demonstração do Teorema 2.5.3, para cada* $i \in A_{p+2}$ *temos*

$$\Lambda_i/J\Lambda_i \simeq \mathbb{F}_p.$$

Daí, $\dim_{\mathbb{F}_p} V_i/JV_i = r_i$. *Como para cada* $i \in A_{p+2}$ *existe um* $\mathbb{Z}_pG$*-homomorfismo sobrejetivo* $\phi_i \in Hom_{\mathbb{Z}_pG}(\Lambda_i^{r_i}, V_i)$, *necessariamente* V_0 *tem ação trivial de* G, *já que* Λ_0 *é trivial. Além disso, cada* V_i *é um* $\mathbb{F}_p[G/H_i]$*-módulo no qual, pela Observação 2.5.1, se* $g \in G \backslash H_i$ *o elemento* $(1 + g + g^2 + ... + g^{p-1})$ *age como uma multiplicação por* 0.

Exemplo 4.1.1. *Seja* $p = 2$ *e* $G = C_2 \times C_2$. *Pondo* $V = V_0 = V_1 = \mathbb{F}_2$, $V_2 = V_3 = 0$ *obtemos uma* 5*-upla*

$$(V, V_0, V_1, 0, 0)$$

que satisfaz as duas primeiras condições na Definição 4.1.1. Dado um gerador de V_0, *digamos* v_1, *pegamos para* V_0 *uma cópia de* Λ_0, *sendo* Λ_0 *gerado por* e_0 *como* $\mathbb{Z}_p$*-módulo, podemos definir um* $\mathbb{Z}_2G$*-homomorfismo sobrejetivo* $\phi_0 : \Lambda_0 \longrightarrow V_0$, *colocando* $\phi(e_0) = v_0$. *E de modo análogo, pegamos para* V_1 *uma cópia de* Λ_1 *e definimos* $\phi_1 : \Lambda_1 \longrightarrow V_1$ *colocando* $\phi_1(e_1) = v_0$. *Como um elemento de* G *age como uma multiplicação por* 1 *ou* -1 *em* Λ_1, *segue que* ϕ_1 *é um* $\mathbb{Z}_2G$*-homomorfismo sobrejetivo. Assim, a* 5*-upla* $(\mathbb{F}_2, \mathbb{F}_2, \mathbb{F}_2, 0, 0)$ *também satisfaz a última condição da Definição 4.1.1, portanto é um diagrama.*

Exemplo 4.1.2. *Sejam* $p = 3$ *e* $G = N \times C$, *onde* $N = \langle n \rangle$ *e* $C = \langle c \rangle$ *possuem ordem* 3. *Sejam*

$$H_1 = \langle n \rangle, H_2 = \langle c \rangle, H_3 = \langle nc \rangle, H_4 = \langle nc^2 \rangle,$$

os subgrupos maximais de G. *Considere o* $\mathbb{F}_3G$*-módulo* V *com base* $\{v_0, v_1, v_2\}$ *e multiplicação*

$$nv_0 = cv_0 = v_0, cv_1 = v_1 + v_0, nv_1 = v_1,$$

$$nv_2 = v_2 + v_0, cv_2 = v_2.$$

Observe que os seguintes $\mathbb{F}_3G$*-submódulos de* V

$$V_0 = \langle v_0 \rangle, V_1 = \langle v_0, v_1 \rangle, V_2 = \langle v_0, v_2 \rangle, V_3 = 0 \text{ e } V_4 = \langle v_0, v_0 + v_1 + v_2 \rangle$$

satisfazem as Condições 1 e 2 da Definição 4.1.1. Para a 6-upla

$$(V, V_0, V_1, V_2, 0, V_4)$$

ser um diagrama, precisamos verificar que essa também satisfaz a Condição 3 da Definição 4.1.1.

Observe que

$$JV_0 = 0, JV_1 = JV_2 = JV_4 = \langle v_0 \rangle,$$

logo

$$V_0/JV_0 = \langle v_0 + JV_0 \rangle, V_1/JV_1 = \langle v_1 + JV_1 \rangle, V_2/JV_2 = \langle v_2 + JV_2 \rangle, V_4/JV_4 = \langle v_0 + v_1 + v_2 + JV_4 \rangle.$$

Assim, cada V_i/JV_i é unidimensional. Escolha para cada V_i/JV_i uma copia de Λ_i. Da mesma forma que fizemos na Proposição 2.5.1, mostramos que os conjuntos $\{e_0\}$, $\{e_1, ce_1\}$, $\{e_2, ne_2\}$ e $\{e_4, ne_4\}$ são bases de $\Lambda_0, \Lambda_1, \Lambda_2$ e Λ_4, respectivamente. Denote os elementos desses conjuntos por

$$w_0 = e_0, w_1 = e_1, w_2 = ce_1,$$

$$w_3 = e_2, w_4 = ne_2,$$

$$w_5 = e_4, w_6 = ne_4.$$

Temos

$$nw_0 = cw_0 = w_0,$$

$$nw_1 = w_1, nw_2 = w_2, cw_1 = w_2, cw_2 = -w_1 - w_2;$$

$$cw_3 = w_3, cw_4 = w_4, nw_3 = w_4, nw_4 = -w_3 - w_4;$$

$$nc^2w_5 = w_5, nc^2w_6 = w_6, nw_5 = w_6, nw_6 = -w_5 - w_6.$$

Agora, defina os seguintes $\mathbb{Z}_3$-homomorfismos

$$\phi_0 : \Lambda_0 \longrightarrow V_0, w_0 \mapsto v_0,$$

$$\phi_1 : \Lambda_1 \longrightarrow V_1, w_1 \mapsto -v_1 + v_0, w_2 \mapsto -v_1,$$

$$\phi_2 : \Lambda_2 \longrightarrow V_2, w_3 \mapsto -v_2 + v_0, w_4 \mapsto -v_2,$$

$$\phi_4 : \Lambda_4 \longrightarrow V_4, w_5 \mapsto -v_1 - v_2, w_6 \mapsto -v_0 - v_1 - v_2.$$

Vamos verificar que de fato as aplicações definidas acima são homomorfismos de $\mathbb{Z}_3G$-módulos. Para ϕ_0 não temos nada a fazer, já que G age trivialmente em V_0 e Λ_0. Observe

que

$$\phi_1(cw_1) = \phi_1(w_2) = -v_1 = c(-v_1 + v_0) = c\phi_1(w_1)$$

$$\phi_1(c^2w_1) = \phi_1(cw_2) = \phi_1(-w_1 - w_2) = -v_0 + v_1 + v_1 = -v_0 - v_1 =$$

$$= c^2(v_0 - v_1) = c^2\phi_1(w_1),$$

$$\phi_1(cw_2) = \phi_1(c^2w_1) = c^2\phi_1(w_1) = -v_0 - v_1 = c(-v_1) = c\phi_1(w_2),$$

$$\phi_1(c^2w_2) = \phi_1(w_1) = -v_1 + v_0 = -v_1 - 2v_0 = c^2(-v_1) = c^2\phi_1(w_2).$$

$$\phi_2(nw_3) = \phi_2(w_4) = -v_2 = n(-v_2 + v_0) = n\phi_2(w_3),$$

$$\phi_2(n^2w_3) = \phi(nw_4) = \phi_2(-w_3 - w_4) = v_2 - v_0 + v_2 = -v_1 - v_0 =$$

$$= n^2(-v_2 + v_0) = n^2\phi_2(w_3),$$

$$\phi_2(nw_4) = -v_0 - v_2 = n(-v_2) = n\phi_2(w_4),$$

$$\phi_2(n^2w_4) = \phi_2(w_3) = -v_2 + v_0 = -v_2 - 2v_0 = n^2(-v_2) = n^2\phi_2(w_4).$$

$$\phi_4(cw_5) = \phi_4(w_6) = -v_0 - v_1 - v_2 = c(-v_1 - v_2) = c\phi_4(w_5),$$

$$\phi_4(c^2w_5) = \phi_4(cw_6) = \phi_4(-w_5 - w_6) = 2v_1 + 2v_2 + v_0 = -v_1 - v_2 - 2v_0 =$$

$$= c^2(-v_1 - v_2) = c^2\phi_4(w_5),$$

$$\phi_4(cw_6) = \phi_4(-w_5 - w_6) = 2v_1 + 2v_2 + v_0 = c(-v_0 - v_1 - v_2) = c\phi_4(w_6),$$

$$\phi_4(c^2w_6) = \phi_4(w_5) = -v_1 - v_2 = c^2(-v_0 - v_1 - v_2) = c^2\phi_4(w_6).$$

Então, fica verificado que ϕ_i é um homomorfismo de $\mathbb{Z}_3G$-módulos sobrejetivo para cada $i \in \{0, 1, 2, 4\}$.

Note que para cada $i \in \{0, 1, 2, 4\}$ o homomorfismo ϕ_i induz um novo homomorfismo sobrejetivo

$$\widehat{\phi_i} : \Lambda_i \longrightarrow V_i/JV_i,$$

$$x_i \mapsto \phi_i(x_i) + JV_i.$$

Para $i = 0$ é imediato que o mapa

$$\bar{\phi_0} : \lambda_0/J\Lambda_0 \longrightarrow V_0/JV_0$$

é um $\mathbb{Z}_pG$-isomorfismo. Seja $x_1 \in \Lambda_1$. Logo, existem escaleres $a_1, a_2 \in \mathbb{Z}_3$ tais que $x_1 = a_1w_1 + a_2w_2$. Assim,

$$x_1 \in \ker\phi_1 \Leftrightarrow \phi_1(x_1) \in JV_1 = \langle v_0\rangle_{\mathbb{F}_3} \Leftrightarrow \phi_1(x_1) = a_1v_0 + (-a_1 - a_2)v_1 \in JV_1.$$

Como v_0 e v_1 são linearmente independentes sobre $\mathbb{F}_3$, devemos ter $(a_1 + a_2) \in 3\mathbb{Z}_p$, ou seja, $a_1 = -a_2 + 3q, q \in \mathbb{Z}_3$. Daí,

$$x_1 = a_1w_1 + a_2w_2 = (-a_2 + 3q)w_1 + a_2w_2 = 3q_1w_1 + a_2(w_2 - w_1) =$$

$$= 3q_1w_1 + a_2(cw_1 - w_1) = 3q_1w_1 + a_2(c-1)w_1 \in J\Lambda_1.$$

Segue que $\ker \widehat{\phi}_1 \subseteq J\Lambda_1$, claramente $J\Lambda_1 \subseteq \ker \widehat{\phi}_1$, donde $J\Lambda_1 = \ker \widehat{\phi}_1$. Disso segue que o $\mathbb{Z}_pG$-homomorfismo induzido por ϕ_1

$$\bar{\phi}_1 : \Lambda_1/J\Lambda_1 \longrightarrow V_1/JV_1$$

$$x_1 + J\Lambda_1 \mapsto \phi_1(x_1) + JV_1$$

é um $\mathbb{Z}_pG$-isomorfismo. De modo análogo podemos mostrar que $\phi_i, i \in \{2, 4\}$, também induz um isomorfismo entre $\Lambda_i/J\Lambda_i$ e V_i/JV_i. Segue que a 6-upla

$$(V, V_0, V_1, V_2, 0, V_4)$$

também satisfaz a Condição 3 da Definição 4.1.1, portanto é um diagrama.

Definição 4.1.2. *Sejam $D_1 = (V, V_0, V_1, ..., V_{p+1})$ e $D_2 = \left(V', V_0', V_1', ..., V_{p+1}'\right)$ dois diagramas. Um morfismo ϕ entre os diagramas D_1 e D_2 é definido para ser um $\mathbb{Z}_pG$-homomorfismo $\phi \in Hom_{\mathbb{Z}_pG}(V, V')$ tal que $\phi(V_i) \subseteq V_i'$.*

Daqui em diante, denotaremos o conjunto dos morfismos entre dois diagramas D_1 e D_2 por $\mathrm{Hom}_{\mathbb{Z}_pG}(D_1, D_2)$.

Denote por $\mathfrak{V}$ a categoria cujos os objetos são diagramas da forma

$$D = (V, V_0, V_1, ..., V_{p+1}) \in \mathcal{V}^{p+3},$$

e os morfismos são como na última definição. O objetivo da próxima seção é estabelecer uma correspondência entre $\mathbb{Z}_pG$-reticulados reduzidos (vamos dar esta definição na próxima seção) e diagramas, de modo que $\mathbb{Z}_pG$-reticulados isomorfos estejam associados a diagramas isomorfos e vice-versa. A ideia central por trás dessa correspondência é que podemos entender certos $\mathbb{Z}_pG$-reticulados olhando apenas para o seu diagrama correspondente.

4.2 Associando reticulados a diagramas

Dado um $\mathbb{Z}_pG$-reticulado U, será conveniente para o nosso trabalho tratar U como sendo um $\mathbb{Z}_pG$-submódulo de algum $\mathbb{Q}_pG$-módulo. A melhor forma para isso é olhar para a imagem de U em $\mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U$ via a inclusão

$$i_{\mathbb{Z}_pG} : U \longrightarrow \mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U$$

$$u \mapsto 1 \otimes_{\mathbb{Z}_pG} u.$$

Quando U é $\mathbb{Z}_p$-livre, então $U \simeq i_{\mathbb{Z}_pG}(U)$. De fato, como U é livre, temos $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} U \simeq \mathbb{Q}_p^r$, onde r é o $\mathbb{Z}_p$-posto de U (veja [10], Corolário 18, pág.373). Assim, a inclusão

$$i_{\mathbb{Z}_p} : U \longrightarrow \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U$$

$$u \mapsto 1 \otimes_{\mathbb{Z}_p} u$$

é injetiva (ver [10], Corolário 8, pág.362) e $U \simeq i_{\mathbb{Z}_p}(U)$ como $\mathbb{Z}_p$-módulos. Agora, $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} U$ possui uma $\mathbb{Q}_p$-base em que os elementos são da forma $1 \otimes_{\mathbb{Z}_p} u$, pois $\mathbb{Q}_p$ é o corpo de frações de $\mathbb{Z}_p$. Já que U é um $\mathbb{Z}_pG$-módulo, podemos definir uma ação nos elementos $1 \otimes_{\mathbb{Z}_p} u \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U$ da seguinte forma

$$g(1 \otimes_{\mathbb{Z}_p} u) = 1 \otimes_{\mathbb{Z}_p} gu, \forall g \in G, \forall u \in U.$$

Uma vez que $i_{\mathbb{Z}_p}$ é injetiva, essa ação está bem definida, e como $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} U$ possui uma base na qual os elementos são da forma $1 \otimes_{\mathbb{Z}_p} u$, podemos estender essa ação para $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} U$. Assim, $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} U$ se torna um $\mathbb{Q}_pG$-módulo e $i_{\mathbb{Z}_p}$ é um $\mathbb{Z}_pG$-homomorfismo, donde $i_{\mathbb{Z}_p}(U) \simeq U$ como $\mathbb{Z}_pG$-módulos.

Pela propriedade universal do produto tensorial $\mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U$ (veja [10], Teorema 8, pág.362), deve existir um único homomorfismo de $\mathbb{Q}_pG$-módulos

$$\Psi : \mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U \longrightarrow \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U$$

satisfazendo $i_{\mathbb{Z}_p} = \Psi \circ i_{\mathbb{Z}_pG}$. Como $i_{\mathbb{Z}_p}$ é injetiva, assim deve ser $i_{\mathbb{Z}_pG}$, logo $U \simeq i_{\mathbb{Z}_pG}(U)$. Daqui em diante vamos identificar U com a sua imagem isomórfica $i_{\mathbb{Z}_pG}(U)$ em $\mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U$.

Observação 4.2.1. *Dado dois $\mathbb{Z}_pG$-reticulados U, W e um homomorfismo*

$$\phi \in Hom_{\mathbb{Z}_pG}(U, W),$$

como $\mathbb{Q}_p$-espaço vetorial, $\mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U$ é gerado por elementos da forma $1 \otimes u$ de tal

maneira que podemos definir

$$\Phi : \mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U \longrightarrow \mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} W$$

por $\Phi(1 \otimes u) = 1 \otimes \phi(u)$. *Desse modo,* Φ *está bem definida e quando estendemos essa de forma linear,* Φ *é um homomorfismo de* $\mathbb{Q}_pG$*-módulos. Observe que* Φ *é o único homomorfismo em* $Hom_{\mathbb{Q}_pG}(\mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U, \mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} W)$ *que quando restrito a* U *coincide com* ϕ. *Posto isso, passaremos a tratar um homomorfismo de* $\mathbb{Z}_pG$*-módulos como sendo a restrição de um único homomorfismo de* $\mathbb{Q}_pG$*-módulos.*

Seja U um $\mathbb{Z}_pG$-reticulado. Para cada $i \in \{0, 1, 2, ..., p+1\}$ considere o conjunto $e_iU := \{e_i \otimes u : u \in U\} \subset \mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U$. Claramente e_iU é um $\mathbb{Z}_pG$-módulo finitamente gerado, e como U é um reticulado, e_iU é um $\mathbb{Z}_pG$-reticulado para cada $i \in \{0, 1, ..., p+1\}$.

Denote por U_* o seguinte $\mathbb{Z}_pG$-submódulo de $\mathbb{Q}_pG \otimes_{\mathbb{Z}_pG} U$:

$$e_0U + e_1U + ... + e_{p+1}U.$$

Observação 4.2.2. *Observe que a soma*

$$e_0U + e_1U + ... + e_{p+1}U$$

é direta, pois os idempotentes são ortogonais. Também observe que, como

$$e_0 + e_1 + ... + e_{p+1} = 1,$$

temos para todo $u \in U$

$$1 \otimes u = (e_0 + e_1 + ... + e_{p+1}) \otimes u = \sum_{i=0}^{p+1} (e_i \otimes u) \in U_* \; e$$

$$e_i \otimes u = e_i \otimes u + \sum_{i=0}^{p+1} (e_i \otimes u) - \sum_{i=0}^{p+1} (e_i \otimes u) =$$

$$= 1 \otimes u - \sum_{\substack{j \neq i \\ j \in A_{p+2}}} (e_j \otimes u) \in U + \sum_{\substack{j \neq i \\ j \in A_{p+2}}} e_jU.$$

Logo, $U \subseteq U_*$ *e para cada* $i \in A_{p+2}$ *temos*

$$U_* = U + \sum_{\substack{j \neq i \\ j \in A_{p+2}}} e_jU.$$

Posto isso, daqui em diante vamos tratar U como sendo um $\mathbb{Z}_pG$-submódulo do $\mathbb{Z}_pG$-

módulo

$$U_* = \bigoplus_{i=0}^{p+1} e_i U.$$

Assim, iremos denotar o elemento $e_i \otimes u \in e_i U$ simplesmente por $e_i u$.

Definição 4.2.1. *Um $\mathbb{Z}_p G$-reticulado U é dito reduzido se esse não possui somando direto isomorfo a Λ ou $\Lambda_i, i = 0, 1, ..., p+1$.*

Teorema 4.2.1. *Seja U um $\mathbb{Z}_p G$-reticulado. Então $e_i U$ é Λ_i-livre.*

Demonstração. Para $i = 0$ é imediato que $e_0 U$ é Λ_0-livre, já que $\Lambda_0 \simeq \mathbb{Z}_p$. Para $i > 0$ observe que $e_i U$ é um $\mathbb{Z}_p[G/H_i]$-reticulado em que, pela Observação 2.5.1,

$$(1 + g + g^2 + ... + g^{p-1})$$

age como zero se $g \notin H_i$. Como G/H_i é cíclico de ordem p, pela classificação dos $\mathbb{Z}_p C_p$-módulos (Lema 3.2.1), o único $\mathbb{Z}_p[G/H_i]$-reticulado em que $(1+g+g^2+...+g^{p-1}), g \notin H_i$, age como 0 é uma soma direta dos módulos $I_{[G/H_i]} \simeq \Lambda_i$. □

Proposição 4.2.1 (Butler)**.** *Seja U um $\mathbb{Z}_p G$-reticulado. Então U não possui somando isomorfo a Λ se, e somente se, $pe_i U \subseteq U \ \forall i = 0, 1, ..., p+1$.*

Demonstração. Suponha que U tenha um somando isomorfo a Λ. Já que Λ é gerado por 1 como $\mathbb{Z}_p G$-módulo, temos que existe $u \in U$ tal que $\langle u \rangle_{\mathbb{Z}_p G} \simeq \Lambda$ como $\mathbb{Z}_p G$-módulos, assim, $\sum_{g \in G} gu \notin p\langle u \rangle_{\mathbb{Z}_p G}$, pois $\{gu; g \in G\}$ é uma $\mathbb{Z}_p$-base para $\langle u \rangle_{\mathbb{Z}_p G}$. Daí, $\left(p \sum_{g \in H_i} g - \sum_{g \in G} g \right) u \notin pU$, donde $pe_i u \notin U \ \forall i = 0, 1, 2, ..., p+1$.

Reciprocamente, se $pe_i U \nsubseteq U$ para algum $i = 0, 1, ..., p+1$, escolha $u_0 \in U$ tal que $pe_i u_0 \notin U$ e seja $w = \sum_{g \in G} gu_0$. Observe que $w \notin pU$, pois caso contrário teríamos $w = \sum_{g \in G} gu_0 = pu'$ e logo $pe_0 u_0 \in U$. Como $e_0 - e_i = -\frac{1}{p} \sum_{g \in H_i} g$, temos $p(e_0 - e_i)u_0 \in U$ o que implica $pe_i u_0 \in U$, contradição. Daí, $w \notin pU$ e pelo Teorema 2.4.2, w gera um $\mathbb{Z}_p$-somando direto de U. Seja $W' \subset U$ tal que $U = \langle w \rangle_{\mathbb{Z}_p} \oplus W'$ e defina $\pi_{\langle w \rangle} \in \mathrm{Hom}_{\mathbb{Z}_p}(U, \langle w \rangle_{\mathbb{Z}_p})$ por $\pi_{\langle w \rangle}(u) = \lambda w$, onde $\lambda \in \mathbb{Z}_p$ e $u = \lambda w + w'$ com $w' \in W'$. Seja $\theta \in \mathrm{Hom}_{\mathbb{Z}_p}(\langle w \rangle, \mathbb{Z}_p)$ definida por $\theta(\lambda w) = \lambda$. Então, $\pi = \theta \circ \pi_{\langle w \rangle} \in \mathrm{Hom}_{\mathbb{Z}_p}(U, \mathbb{Z}_p)$ e cumpre $\pi(w) = 1$.

Defina $\varphi : U \longrightarrow \mathbb{Z}_p G$ por $\varphi(u) = \sum_{g \in G} g\pi(g^{-1}u) \ \forall u \in U$. Sendo π um homomorfismo de $\mathbb{Z}_p$-módulos entre U e $\mathbb{Z}_p$, ϕ está bem definida e é um homomorfismo de $\mathbb{Z}_p$-módulos. Para cada $h \in G$ temos

$$\varphi(hu) = \sum_{g \in G} g\pi(g^{-1}hu) = \sum_{g \in G} h(h^{-1}g)\pi((h^{-1}g)^{-1}u) =$$

$$= h\sum_{g\in G} g\pi(g^{-1}u),$$

logo $\varphi \in \mathrm{Hom}_{\mathbb{Z}_pG}(U, \mathbb{Z}_pG)$.

Agora,

$$\varphi(w) = \sum_{g\in G} g\pi\left(g^{-1}\sum_{g\in G} gu_0\right) = \sum_{g\in G} g\pi\left(\sum_{g\in G} gu_0\right) = \sum_{g\in G} g\pi(w) = \sum_{g\in G} g,$$

então $\varphi(w) = \sum_{g\in G} g\varphi(u_0) = \sum_{g\in G} g$. Sejam $\lambda_j \in \mathbb{Z}_p, j = 1, ..., p^2$, as coordenadas de $\varphi(u_0)$ relativamente a base canônica $\{g; g \in G\}$ de $\mathbb{Z}_pG$. Então $\sum_{j=1}^{p^2} \lambda_j = 1$, pois $h\sum_{g\in G} g = \sum_{g\in G} g$ e $\{g; g \in G\}$ é uma base para $\mathbb{Z}_pG$. Pela definição de I_G, temos $(\varphi(u_0)-1) \in I_G \subset J$. Pelo Teorema 2.3.1, $\varphi(u_0)$ é invertível. Sendo $\varphi(u_0)$ invertível, existe $\lambda \in \mathbb{Z}_pG$ satisfazendo $\lambda\varphi(u_0) = 1$. Como ϕ é um $\mathbb{Z}_pG$-homomorfismo, obtemos $\varphi(\lambda u_0) = 1$ e daí vem que φ é um $\mathbb{Z}_pG$-homomorfismo sobrejetivo. Segue que $U/\ker\varphi \simeq \Lambda$ e isso implica que $U/\ker\varphi$ é Λ-livre, portanto, temos $U \simeq \Lambda \oplus \ker\varphi$ como Λ-módulos.

□

Proposição 4.2.2 ([7], Proposição 3.3(a), pág.63)**.** *Seja U um $\mathbb{Z}_pG$-reticulado. Então U não possui somando isomorfo a Λ_i se, e somente se, $U \cap e_iU \subseteq Je_iU$.*

Demonstração. Observe que $e_i\Lambda_i \cap \Lambda_i = \Lambda_i \nsubseteq J\Lambda_i$. Assim, $U \cap e_iU \subseteq Je_iU$ implica que U não possui somando isomorfo a Λ_i.

Reciprocamente, se $e_iU \cap U \nsubseteq Je_iU$ para algum $i = 0, 1, ..., p+1$, escolha $u \in U$ tal que $e_iu \in U\backslash Je_iU$. Observe que $Je_iU = J\Lambda_i(e_iU)$. Pelo Teorema 2.5.3, $J\Lambda_i$ é o ideal maximal do anel de valorização discreta Λ_i. Como e_iU é Λ_i-livre e finitamente gerado, o Teorema 2.4.2 garante que e_iu gera um Λ_i-somando direto de e_iU. Seja W' um submódulo de e_iU tal que $e_iU = \Lambda_iu \oplus W'$ e considere o conjunto $W = \{u \in U; e_iu \in W'\}$. Então, W é um $\mathbb{Z}_pG$-submódulo de U tal que $W \cap \Lambda_iu = 0$. Dado $u' \in U$, temos $e_iu' = \lambda e_iu + e_iw$, onde $\lambda \in \mathbb{Z}_pG$, $w \in W$, logo $e_i(u' - \lambda e_iu - w) = 0 \in W'$. Daí, $u' - \lambda e_iu - w = w' \in W$ e temos $u' = \lambda e_iu + w + w'$. Portanto, $U = \Lambda_iu \oplus W$. □

Teorema 4.2.2 (Butler)**.** *Se U é um $\mathbb{Z}_pG$-reticulado, então U é reduzido se, e somente se,*

$$pe_iU \subseteq e_iU \cap U \subseteq Je_iU.$$

Demonstração. Segue imediatamente das Proposições 4.2.1 e 4.2.2. □

Se U é um $\mathbb{Z}_pG$-reticulado, vimos na Observação 4.2.2 que U é um $\mathbb{Z}_pG$-submódulo

do $\mathbb{Z}_pG$-módulo

$$U_* = \bigoplus_{i=0}^{p+1} e_iU$$

e que para cada $i \in A_{p+2}$

$$U_* = U + \sum_{\substack{j \neq i \\ j \in A_{p+2}}} e_jU.$$

Daí, U_*/U é um $\mathbb{Z}_pG$-módulo finitamente gerado com $\mathbb{Z}_pG$-submódulos $(e_iU+U)/U, i \in A_{p+2}$, que satisfazem para cada $i \in A_{p+2}$

$$U_*/U = \sum_{\substack{j \neq i \\ j \in A_{p+2}}} (e_jU + U)/U.$$

Se U é reduzido, temos, pelo Teorema 4.2.2, que $pe_iU \subseteq e_iU \cap U \subseteq Je_iU \ \forall i \in A_{p+2}$. Assim, cada $(e_iU+U)/U$ é um $\mathbb{F}_p$-espaço vetorial. Desse modo, denotando U_*/U por V e $(e_iU+U)/U$ por V_i, associamos a U uma $(p+3)$-upla

$$\Delta(U) = (V, V_0, V_1, ..., V_{p+1}),$$

que satisfaz as Condições 1 e 2 da Definição 4.1.1.

Defina

$$\pi_i : e_iU \longrightarrow (e_iU + U)/U$$

pondo $\pi_i(e_iu) = e_iu + e_iU \ \forall u \in U$. Note que $\ker \pi_i = U \cap e_iU \subseteq Je_iU$. Seja $\lambda \in J$ e observe que se $e_iu + e_iU = \lambda e_iu' + e_iU$, então $e_i(u - \lambda u') \in U \cap e_iU$. Como $e_iU \cap U \subseteq Je_iU$ e $\lambda e_iu' \in Je_iU$, obtemos que $e_iu \in Je_iU$. Disso segue que $\pi(e_iu) \in JV_i$ se, e somente se, $e_iu \in Je_iU$. Dessas observações segue que π_i induz um $\mathbb{Z}_pG$-isomorfismo entre e_iU/Je_iU e V_i/JV_i.

Pelo Teorema 4.2.1, existe $r_i \geq 0$ e um $\mathbb{Z}_pG$-isomorfismo $\varphi_i : \Lambda_i^{r_i} \to e_iU$, assim $\pi_i \circ \varphi_i \in \mathrm{Hom}_{\mathbb{Z}_pG}(\Lambda_i^{r_i}, V_i)$ induz um isomorfismo entre $\Lambda_i^{r_i}/J(\Lambda_i^{r_i})$ e V_i/JV_i. Portanto, $\Delta(U)$ também satisfaz a Condição 3 da Definição 4.1.1, logo é um diagrama para $\mathbb{Z}_pG$.

Denote por $\mathcal{L}_0$ a categoria dos $\mathbb{Z}_pG$-reticulados reduzidos. Segue das observações feitas acima que para cada reticulado $U \in \mathcal{L}_0$ podemos associar um diagrama $\Delta(U)$ na categoria $\mathfrak{V}$ dos diagramas para $\mathbb{Z}_pG$. Essa associação fornecerá a nossa principal ferramenta, mas precisamos de mais alguns resultados.

Dados dois $\mathbb{Z}_pG$-reticulados U, W, e $\phi \in \mathrm{Hom}_{\mathbb{Z}_pG}(U, W)$, lembramos da Observação 4.2.1 que esse é uma restrição de um homomorfismo de $\mathbb{Q}_pG$-módulos. Defina

$$\Delta(\phi) : \Delta(U) \longrightarrow \Delta(W)$$

por $\Delta(\phi)(e_iu + U) = e_i\phi(u) + W \ \ \forall u \in U$ e $\forall i \in A_{p+2}$. Observe que se $e_iu + U = e_iu' + U$,

então $e_i(u-u') \in U$ o que implica $\phi(e_iu - e_iu') = e_i\phi(u-u') \in W$, donde $e_i\phi(u)+W = e_i\phi(u')+W$. Então, $\Delta(\phi)$ é um mapa bem definido e claramente é um homomorfismo entre os diagramas $\Delta(U)$ e $\Delta(W)$. É fácil verificar que $\Delta : \mathcal{L}_0 \longrightarrow \mathfrak{V}$ é um funtor. Os próximos resultados fornecerão que Δ é uma aplicação injetiva sobre a classe de objetos isomorfos de $\mathcal{L}_0$.

Teorema 4.2.3 ([7], Propoição 2.4, pág.59)**.** *Sejam U e W dois $\mathbb{Z}_pG$-reticulados reduzidos. Então*

$$\Delta_{U,W} : Hom_{\mathbb{Z}_pG}(U,W) \longrightarrow Hom_{\mathbb{Z}_pG}(\Delta(U),\Delta(W))$$

$$\phi \mapsto \Delta_{U,W}(\phi) = \Delta(\phi),$$

é um homomorfismo sobrejetivo de $\mathbb{Z}_p$-módulos e $\forall \phi \in \ker \Delta_{U,U}$ existe $q>0$ tal que $1-\phi^q$ é invertível.

Demonstração. É claro que $\Delta_{U,W}$ é um homomorfismo de $\mathbb{Z}_p$-módulos e quando $U=W$, $\Delta_{U,W}$ é um homomorfismo de anéis. Seja $\phi \in \mathrm{Hom}_{\mathbb{Z}_pG}(\Delta(U),\Delta(W))$. Pelo teorema 4.2.1 e_iU é Λ_i-livre para cada $i=0,1,...,p+1$, daí, seja $\{e_iu_{1i},...,e_iu_{j_ii}\}$ uma Λ_i-base de e_iU. Para cada $i=0,1,...,p+1$, defina o Λ_i-homomorfismo $\Phi_i : e_iU \longrightarrow e_iW$ na Λ_i-base $\{e_iu_{1i},...,e_iu_{j_ii}\}$ pondo $\Phi_i(e_iu_{ri}) = e_iw_{ri}, r=1,...,j_i$, onde $\phi(e_iu_{ri}+U) = e_iw_{ri}+W$. Dado $\lambda \in \mathbb{Z}_pG$ temos

$$\Phi_i(\lambda e_iu_{ri}) = \Phi_i(\lambda e_ie_iu_{ri}) = (\lambda e_i)e_iw_{ri} = \lambda e_iw_{ri} = \lambda\Phi_i(e_iu_{ri}),$$

e Φ_i é um $\mathbb{Z}_pG$-homomorfismo. Definindo $\Phi : U_* \longrightarrow W_*$ coincidindo com Φ_i em e_iU, temos que $\Phi|_U \in \mathrm{Hom}_{\mathbb{Z}_pG}(U,W)$, pela definição e pelo fato de que todo elemento de U pode ser escrito como combinação linear dos elementos das bases de cada Λ_i. Agora,

$$\Delta(\Phi|_U)(e_iu_{ri}+U) = e_i\Phi|_U(u_{ri})+W = e_i\Phi(e_iu_{ri})+W = e_iw_{ri}+W = \phi(e_iu_{ri}+U),$$

donde $\Delta(\Phi|_U)=\phi$.

Observe que

$$\phi \in \ker\Delta_{U,U} \Leftrightarrow \phi(e_iU) \subseteq U \cap e_iU \ \forall i=0,1,...,p+1.$$

Sendo U reduzido, pelo Teorema 4.2.2, temos $\phi(e_iU) \subseteq Je_iU$. Por outro lado, existe $q>0$ tal que $J^q \subset p^2\mathbb{Z}_pG$, daí, $J^qe_iU \subseteq p^2e_iU$. Assim, $\phi^q(e_iU) \subseteq J^qe_iU \subseteq p^2e_iU$. Pelo Teorema 4.2.2 $p^2e_iU \subseteq pU$, o que fornece $\phi^q(U_*) \subseteq p^2U_* \subset pU$, logo $\phi^q(U) \subseteq pU$. Ora, ϕ^q-1 induz um homomorfismo sobrejetivo em U/pU, via $u+pU \mapsto (\phi^q-1)(u)+U$, já que $\phi^q(U) \subseteq pU$. Daí, $U = \mathrm{img}(\phi^q-1)+pU$ e, pelo Corolário 2.3.2, $U=\mathrm{img}(\phi^q-1)$, donde ϕ^q-1 é sobrejetiva. Como $\phi^q(U) \subseteq pU$, o Teorema 2.2.1 garante que ϕ^q satisfaz

uma equação do tipo

$$(\phi^q)^s + a_{s-1}(\phi^q)^{s-1} + ... + a_1\phi^q + a_0 = 0,$$

onde $a_j \in p\mathbb{Z}_p$, $\forall j = 0, 1..., s$, e s é o $\mathbb{Z}_p$-posto de U. Daí, dado $u \in U$ tal que $\phi^q(u) = u$, então $(1+a_0+...+a_{s-1})u = 0$, mas como $a_0+...+a_{s-1} \in p\mathbb{Z}_p$ temos que $1+a_0+...+a_{s-1}$ é invertível, donde $u = 0$. Portanto, $\phi^q - 1$ é um automorfismo de U. □

Corolário 4.2.1 ([7], Propoição 2.4, pág.59)**.** *Sejam U e W dois $\mathbb{Z}_pG$-reticulados reduzidos, então $U \simeq W$ se, e somente se, $\Delta(U) \simeq \Delta(W)$.*

Demonstração. Suponha que $\Delta(U) \simeq \Delta(W)$ e seja $\phi : U_*/U \longrightarrow W_*/W$ um isomorfismo. Pelo Teorema 4.2.3, existem $\theta \in \mathrm{Hom}_{\mathbb{Z}_pG}(U, W)$ e $\theta' \in \mathrm{Hom}_{\mathbb{Z}_pG}(W, U)$ tais que $\Delta(\theta) = \phi$ e $\Delta(\theta') = \phi^{-1}$, assim, temos que $\theta\theta' - 1_W \in \ker \Delta_{W,W}$ e $\theta'\theta - 1_U \in \ker \Delta_{U,U}$, pois $\Delta(\theta\theta') = \Delta(\theta) \circ \Delta(\theta') = 1 \in \mathrm{End}_{\mathbb{Z}_pG}(W_*/W)$ e $\Delta(\theta'\theta) = \Delta(\theta') \circ \Delta(\theta) = 1 \in \mathrm{End}_{\mathbb{Z}_pG}(U_*/U)$. O Teorema 4.2.3 garante que existe $q > 0$ tal que $(1 - \theta\theta')^q - 1$ e $(1 - \theta'\theta)^q - 1$ são ambos isomorfismos. Agora,

$$(1 - \theta\theta')^q - 1 = \theta\theta'((\theta\theta')^{q-1} + ... + q), (1 - \theta'\theta)^q - 1 = ((\theta'\theta)^{q-1} + ... + q)\theta'\theta.$$

Daí, a primeira igualdade fornece que θ é um homomorfismo sobrejetivo e a segunda garante que θ é injetiva, pois

$$(1 - \theta\theta')^q - 1, (1 - \theta'\theta)^q - 1$$

são isomorfismos. Portanto, θ é um isomorfismo. De modo análogo obtemos que θ' é um isomorfismo.

Reciprocamente, dado um isomorfismo $\phi \in \mathrm{Hom}_{\mathbb{Z}_pG}(U, W)$, temos que $\Delta(\phi)$ e $\Delta(\phi^{-1})$ são isomorfismos um inverso do outro, pois

$$\Delta(1_U) = \Delta(\phi^{-1} \circ \phi) = \Delta(\phi^{-1}) \circ \Delta(\phi) = 1_{U_*/U}$$

e

$$\Delta(1_W) = \Delta(\phi \circ \phi^{-1}) = \Delta(\phi) \circ \Delta(\phi^{-1}) = 1_{W_*/W}.$$

□

Vamos terminar essa seção com alguns exemplos.

Exemplo 4.2.1. *Seja $G = C_2 \times C_2 = \langle n \rangle \times \langle c \rangle$. Considere o $\mathbb{Z}_2G$-módulo U com base $\{u_1, u_2, u_3\}$ e multiplicação*

$$nu_1 = u_2 - u_1, cu_1 = u_2 + u_3 - u_1$$
$$nu_2 = u_2, cu_2 = u_2$$
$$nu_3 = -u_3, cu_3 = u_3.$$

Se $H_1 = \langle n \rangle, H_2 = \langle c \rangle, H_3 = \langle nc \rangle$, *temos*

$$e_0u_1 = \frac{1}{4}(1 + n + c + nc)u_1 =$$
$$= \frac{1}{4}(u_1 + (u_2 - u_1) + (u_2 + u_3 - u_1) + (u_2 - u_2 - u_3 + u_1)) = \frac{1}{2}u_2,$$
$$e_0u_2 = \frac{1}{4}(1 + n + c + nc)u_2 = u_2,$$
$$e_0u_3 = \frac{1}{4}(1 + n + c + nc)u_3 = \frac{1}{4}(u_3 - u_3 + u_3 - u_3) = 0;$$

$$e_1u_1 = \frac{1}{4}(1 + n - c - nc)u_1 =$$
$$= \frac{1}{4}(u_1 + (u_2 - u_1) - (u_2 + u_3 - u_1) - (u_2 - u_2 - u_3 + u_1)) = 0,$$
$$e_1u_2 = \frac{1}{4}(1 + n - c - nc)u_2 = 0,$$
$$e_1u_3 = \frac{1}{4}(1 + n - c - nc)u_3 = \frac{1}{4}(u_3 - u_3 - u_3 + u_3) = 0;$$

$$e_2u_1 = \frac{1}{4}(1 - n + c - nc)u_1 =$$
$$= \frac{1}{4}(u_1 - (u_2 - u_1) + (u_2 + u_3 - u_1) - (u_2 - u_2 - u_3 + u_1)) = \frac{1}{2}u_3,$$
$$e_2u_2 = \frac{1}{4}(1 - n + c - nc)u_2 = 0,$$
$$e_2u_3 = \frac{1}{4}(1 - n + c - nc)u_3 = u_3;$$

$$e_3u_1 = \frac{1}{4}(1 - n - c + nc)u_1 =$$
$$= \frac{1}{4}(u_1 - (u_2 - u_1) - (u_2 + u_3 - u_1) + (u_2 - u_2 - u_3 + u_1)) =$$
$$= u_1 + \frac{1}{2}(-u_2 - u_3),$$
$$e_3u_2 = \frac{1}{4}(1 - n - c + nc)u_2 = 0,$$

$$e_3u_3 = \frac{1}{4}(1-n-c+nc)u_3 = 0.$$

Assim, obtemos

$$e_0U = \left\langle 2^{-1}u_2 \right\rangle_{\mathbb{Z}_2},$$

$$e_1U = 0,$$

$$e_2U = \left\langle 2^{-1}u_3 \right\rangle_{\mathbb{Z}_2},$$

$$e_3U = \left\langle u_1 + 2^{-1}(-u_2 - u_3) \right\rangle_{\mathbb{Z}_2}.$$

Observe que $Je_iU = 2e_iU = U \cap e_iU, i = 0,1,2,3$, *assim, o Teorema 4.2.2 garante que* U *é reduzido. Por fim, observe que denotando* U_*/U *por* V, *e* $(e_iU+U)/U$ *por* V_i, *obtemos*

$$V_0 = \langle e_0u_1 + U\rangle_{\mathbb{F}_2} = \langle e_2u_1 + e_3u_1 + U\rangle_{\mathbb{F}_2}, V_1 = 0,$$

$$V_2 = \langle e_2u_1 + U\rangle_{\mathbb{F}_2}, V_3 = \langle e_3u_1 + U\rangle.$$

Posto isso, vemos que

$$\Delta(U) \simeq \left((\mathbb{F}_2)^2; \langle(1,1)\rangle_{\mathbb{F}_2}, 0, \langle(1,0)\rangle_{\mathbb{F}_2}, \langle(0,1)\rangle_{\mathbb{F}_2}\right)$$

onde $\{(1,0),(0,1)\}$ *é uma base para* $(\mathbb{F}_2)^2$.

Exemplo 4.2.2. *Seja* $G = C_p \times C_p$. *Denote por* U *o* $\mathbb{Z}_pG$*-módulo* $\mathbb{Z}_p[G/H_i]$ *e seja* $g \in G\backslash H_i$. *Como* U *possui um elemento* u *tal que* $\{u, gu, g^2u, ..., g^{p-1}u\}$ *é uma* $\mathbb{Z}_p$*-base de* U *obtemos*

$$e_0u = \frac{1}{p^2}\left(\widehat{H}_i + g\widehat{H}_i + ... + g^{p-1}\widehat{H}_i\right)u = \frac{1}{p}(1+g+...+g^{p-1})u$$

$$e_iu = \frac{1}{p^2}\left(p\widehat{H}_i - \widehat{H}_i - g\widehat{H}_i - ... - g^{p-1}\widehat{H}_i\right)u =$$

$$= \frac{1}{p^2}(p^2 - p - pg + pg^2 + ... + pg^{p-1})u = u - \frac{1}{p}(1+g+...+g^{p-1})u.$$

Se $h \in H_i$, $j \neq i$ *e* $j \neq 0$ *obtemos*

$$e_ju = \frac{1}{p^2}\left(p\widehat{H}_j - \widehat{H}_j - h\widehat{H}_j - ... - h^{p-1}\widehat{H}_j\right)u =$$

$$= \frac{1}{p^2}\left(p\widehat{H}_j - p\widehat{H}_j\right)u = 0.$$

Como

$$(g-1)(p+1+g^2+...+g^{p-1}) = p(g-1),$$

obtemos para $i > 0$, *que* $Je_iU = (g-1)e_iU \subseteq pe_iU$, *donde* $Je_iU = U \cap e_iU$. *Segue que* G

age trivialmente em V_i, assim,

$$(e_0U + U)/U = (e_iU + U)/U = \langle e_iu + U\rangle$$

e $(e_jU + U)/U = 0$ se $i \neq j$. Segue que

$$\Delta(U) \simeq (V; V_0, V_1, ..., V_{p+1}),$$

onde $V = V_0 = V_i \simeq \mathbb{F}_2$ e $V_j = 0$ se $j \neq i$ e $j \neq 0$.

Exemplo 4.2.3. *Seja $G = C_p \times C_p$ e suponha que $U \in \mathcal{L}_0$ é de permutação. Pelo Teorema 3.1.1, temos*

$$U = (\mathbb{Z}_p[G/H_1])^{r_1} \oplus (\mathbb{Z}_p[G/H_2])^{r_2} \oplus ... \oplus (\mathbb{Z}_p[G/H_{p+1}])^{r_{p+1}}.$$

Segue do último exemplo que

$$e_iU = (e_i\mathbb{Z}_p[G/H_i])^{r_i} \simeq \Lambda_i^{r_i} \forall i > 0$$

e que $e_0U \simeq \mathbb{Z}_p^{r_1+...+r_{p+1}}$. Também vimos no último exemplo que

$$pe_iU = Je_iU = U \cap e_iU,$$

assim, $V_i = (e_iU + U)/U$ tem ação trivial de G para todo $i \in \{0, 1, ..., p + 1\}$. Agora, $\dim V_0 = r_1 + r_2 + ... + r_{p+1}$ e $\dim V_i = r_i$, pois, como vimos, a projeção canônica

$$\pi_i : e_iU \longrightarrow V_i$$

induz um isomorfismo

$$\bar{\pi}_i : e_iU/Je_iU \longrightarrow V_i/JV_i \simeq V_i.$$

Já que $V = V_1 + V_2 + ... + V_{p+1}$, temos que

$$\dim V \leq \dim V_1 + \dim V_2 + ... + \dim V_{p+1} = \dim V_0.$$

Logo, $\dim V = r_1 + r_2 + ... + r_{p+1}$. Agora, se a soma $V_1 + V_2 + ... + V_{p+1}$ não é direta, então

$$\dim V = \dim(V_1 + V_2 + ... + V_{p+1}) < \dim V_1 + \dim V_2 + ... + \dim V_{p+1} = \dim V,$$

contradição. Assim,

$$V = V_0 = V_1 \oplus V_2 \oplus ... \oplus V_{p+1}.$$

Teorema 4.2.4. *Seja $U \in \mathcal{L}_0$. Então U é um $\mathbb{Z}_pG$-módulo de permutação se, e somente se,*

$$\Delta(U) \simeq (V; V_0, V_1, V_2, ..., V_{p+1}),$$

onde $V = V_0 = V_1 \oplus V_2 \oplus ... \oplus V_{p+1}$.

Demonstração. Se $U \in \mathcal{L}_0$ é tal que $\Delta(U) \simeq (V; V_0, V_1, V_2, ..., V_{p+1})$, onde

$$V = V_0 = V_1 \oplus V_2 \oplus ... \oplus V_{p+1},$$

então, pelo exemplo anterior $\Delta(U)$ é um diagrama para um módulo de permutação, digamos, $W \in \mathcal{L}_0$. Pelo Corolário 4.2.1, $W \simeq U$, donde U é um $\mathbb{Z}_pG$-módulo de permutação. □

4.3 Associando diagramas a reticulados

Nessa seção vamos descrever como obter um $\mathbb{Z}_pG$-reticulado reduzido a partir de um diagrama para $\mathbb{Z}_pG$ e forneceremos alguns exemplos ilustrativos.

Teorema 4.3.1 ([7], Teorema 3.2.(a), pág.61)**.** *Para cada diagrama $D \in \mathfrak{V}$ existe um $\mathbb{Z}_pG$-reticulado $U \in \mathcal{L}_0$ satisfazendo $\Delta(U) \simeq D$.*

Demonstração. Sejam $D = (V; V_0, V_1, ..., V_{p+1}) \in \mathfrak{V}$ e $d_i = \dim V_i/JV_i$. Denote por $F_i = \Lambda_i^{d_i}$, $F = \bigoplus_{i=0}^{p+1} F_i$ e sejam $\phi_i \in \mathrm{Hom}_{\mathbb{Z}_pG}(F_i, V_i), i = 0, 1, ..., p+1$, $\mathbb{Z}_pG$-epimorfismos que induzem isomorfismos $\bar{\phi}_i$ entre F_i/JF_i e V_i/JV_i. Desse modo $\ker \phi_i \subseteq JF_i$. Defina

$$\phi : F \longrightarrow V$$

por $\phi = \sum_{i=0}^{p+1} \phi_i$. Então ϕ é um $\mathbb{Z}_pG$-epimorfismo. Denotando por $U = \ker \phi$, U é um $\mathbb{Z}_pG$-reticulado, pois F é um reticulado e $\mathbb{Z}_p$ é um domínio de ideais principais. Vamos mostrar que $U \in \mathcal{L}_0$, e que $\Delta(U) \simeq D$. Primeiramente, note que $e_iU \subseteq F_i$, pois $U \subset \bigoplus_{i=0}^{p+1} F_i$ e e_i age como zero em F_j se $i \neq j$. Dado $x_i \in F_i$ temos, pela definição de diagrama, que existem $x_j \in F_j, j \neq i$, tais que

$$\phi(x_i) = \sum_{\substack{j \neq i \\ j \in A_{p+2}}} \phi(x_j).$$

Pela definição de U, devemos ter $\sum_{i=0}^{p+1} x_i \in U$, assim

$$x_i \in \left\{ \sum_{\substack{j\neq i \\ j\in A_{p+2}}} x_j + u; u \in U \right\}.$$

Logo $x_i = e_i x_i \in e_i U$, e temos $e_i U = F_i$. Como $\ker \phi_i = U \cap F_i = U \cap e_i U$, temos $U \cap e_i U \subseteq JF_i = Je_i U$. Por outro lado, $pV = 0$, o que fornece $pe_i U \subseteq U \cap e_i U, i = 0, 1, ..., p+1$. Pelo Teorema 4.2.2, $U \in \mathcal{L}_0$. Agora, $F/\ker \phi \simeq V$ e é fácil ver que ϕ induz um isomorfismo de diagramas entre $\Delta(U)$ e D. □

Teorema 4.3.2 ([7], Teorema 3.2.(a), pág.61)**.** *O funtor $\Delta : \mathcal{L}_0 \longrightarrow \mathfrak{V}$ induz uma bijeção entre os conjuntos das classe de isomorfismos.*

Demonstração. Com efeito, dado dois $\mathbb{Z}_p G$-reticulados $U, W \in \mathcal{L}_0$, o Corolário 4.2.1 garante que $U \simeq W$ se, e somente se, $\Delta(U) \simeq \Delta(W)$. Por outro lado, o último teorema garante que para cada diagrama $D \in \mathfrak{V}$ existe um reticulado $U \in \mathcal{L}_0$ para o qual se tem $\Delta(U) \simeq D$. Assim, Δ induz uma bijeção na classe de objetos isomorfos. □

Vamos apresentar alguns exemplos que também serão revisitados nas próximas seções.

Exemplo 4.3.1. *Considere o diagrama $(\mathbb{F}_2 \oplus \mathbb{F}_2, \langle(1,1)\rangle, 0, \langle(1,0)\rangle, \langle(0,1)\rangle)$ que foi obtido no Exemplo 4.2.1. Mantendo a notação do Exemplo 4.2.1, observe que $JV_i = 0$, $\forall i \in \{0,1,2,3\}$. Assim, escolhemos para cada $V_i, i \in \{0,2,3\}$ uma copia de Λ_i. Denotando por w_0, w_1, w_2 os geradores, respectivamente, de Λ_0, Λ_2 e Λ_3, definimos*

$$\pi_0 : \Lambda_0 \longrightarrow V_0$$

$$w_0 \mapsto (1,1);$$

$$\pi_2 : \Lambda_2 \longrightarrow V_2$$

$$w_1 \mapsto (1,0);$$

$$\pi_3 : \Lambda_3 \longrightarrow V_3$$

$$w_2 \mapsto (0,1).$$

É claro que π_i é um $\mathbb{Z}_2 G$-homomorfismo, e que

$$\ker \phi_i = J\Lambda_i.$$

Defina

$$\pi : \Lambda_0 \oplus \Lambda_2 \oplus \Lambda_3 \longrightarrow \mathbb{F}_2 \oplus \mathbb{F}_2$$

por $\pi = \pi_0 + \pi_2 + \pi_3$.

Dado $u \in \Lambda_0 \oplus \Lambda_2 \oplus \Lambda_3$, *temos que existem únicos escalares* $\lambda_0, \lambda_1, \lambda_2 \in \mathbb{Z}_2$ *tais que*

$$u = \lambda_0 w_0 + \lambda_1 w_1 + \lambda_2 w_2.$$

Então

$$\pi(u) = 0 \Leftrightarrow$$

$$\Leftrightarrow \pi\left(\lambda_0 w_0 + \lambda_1 w_1 + \lambda_2 w_2\right) = \lambda_0(1,1) + \lambda_1(1,0) + \lambda_2(0,1) = 0 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \lambda_0 + \lambda_1 \in 2\mathbb{Z}_2 \\ \lambda_0 + \lambda_2 \in 2\mathbb{Z}_2 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \lambda_1 = -\lambda_0 + 2q_1 & \lambda_0, q_1 \in \mathbb{Z}_2 \\ \lambda_0 = -\lambda_2 + 2q_2 & \lambda_2, q_2 \in \mathbb{Z}_2 \end{cases}$$

Logo

$$\begin{cases} \lambda_1 = \lambda_2 + 2k_1 & \lambda_2, k_1 \in \mathbb{Z}_2 \\ \lambda_0 = -\lambda_2 + 2q_2 & \lambda_2, q_2 \in \mathbb{Z}_2 \end{cases}$$

Segue disso que

$$u = (-\lambda_2 + 2q_2)w_0 + (\lambda_2 + 2k_1)w_1 + \lambda_2 w_2 =$$

$$= \lambda_2(-w_0 + w_1 + w_2) + 2q_2 w_0 + 2k_1 w_1.$$

Assim, temos que $B = \{(-w_0 + w_1 + w_2), 2w_0, 2w_1\}$ *é uma base para* $\ker \pi$. *Denotando por*

$$\begin{aligned} u_1 &= (-w_0 + w_1 + w_2) \\ u_2 &= 2w_0, 2w_0, \\ u_3 &= 2w_1, \end{aligned}$$

Temos

$$\begin{aligned} nu_1 = -u_2 - u_1, cu_1 = -u_1 - u_2 + u_3 \\ nu_2 = u_2, cu_2 = u_2 \\ nu_3 = -u_3, cu_3 = u_3, \end{aligned}$$

e é imediato verificar que $\ker \pi \simeq U$, *onde* U *é o* $\mathbb{Z}_2G$*-reticulado do Exemplo* 4.2.1.

Exemplo 4.3.2. *Seja* $\{(1,0),(0,1)\}$ *uma base para* $\mathbb{F}_2 \oplus \mathbb{F}_2$ *e considere o diagrama*

$$D = (\mathbb{F}_2 \oplus \mathbb{F}_2, \mathbb{F}_2 \oplus \mathbb{F}_2, \langle(1,0)\rangle, \langle(1,0)\rangle, \langle(0,1)\rangle)$$

para $\mathbb{Z}_2G$. *Como* $\dim V_0 = 2$ *e* $\dim V_i = 1, i > 1$, *escolhemos duas cópias de* Λ_0 *e uma cópia de cada* $\Lambda_i, i > 0$. *Seja* $\{w_0, w_1\}$ *uma* $\mathbb{Z}_2$*-base de* Λ_0^2 *e denote por* w_2, w_3, w_4 *os geradores, respectivamente, de* Λ_1, Λ_2 *e* Λ_3. *Defina*

$$\pi_0 : \Lambda^2 \longrightarrow V_0$$
$$w_0 \mapsto (1,0)$$
$$w_1 \mapsto (0,1)$$
$$\pi_1 : \Lambda_1 \longrightarrow V_1$$
$$w_2 \mapsto (1,0)$$
$$\pi_2 : \Lambda_2 \longrightarrow V_2$$
$$w_3 \mapsto (1,0)$$
$$\pi_3 : \Lambda_3 \longrightarrow V_3$$
$$w_4 \mapsto (0,1)$$

e tome

$$\pi = \sum_{i=0}^{3} \pi_i : \Lambda_0^2 \oplus \Lambda_1 \oplus \Lambda_2 \oplus \Lambda_3 \longrightarrow V$$

Dado $u \in \Lambda_0^2 \oplus \Lambda_1 \oplus \Lambda_2 \oplus \Lambda_3$, *existem únicos escalares* $\lambda_i \in \mathbb{Z}_2, i = 0,1,2,3$, *tais que*

$$u = \sum_{i=0}^{4} \lambda_i w_i.$$

Então

$$\pi(u) = 0 \Leftrightarrow$$

$$\pi\left(\sum_{i=0}^{4} \lambda_i w_i\right) = \lambda_0(1,0) + \lambda_1(0,1) + \lambda_2(1,0) + \lambda_3(1,0) + \lambda_4(0,1) = 0 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \lambda_0 + \lambda_2 + \lambda_3 \in 2\mathbb{Z}_2 \\ \lambda_1 + \lambda_4 \in 2\mathbb{Z}_2 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \lambda_0 = \lambda_2 + \lambda_3 + 2q \\ \lambda_1 = \lambda_4 + 2k \end{cases} ; \lambda_2, \lambda_3, \lambda_4, q, k \in \mathbb{Z}_2.$$

Daí,

$$u = \sum_{i=0}^{4} \lambda_i w_i = (\lambda_2 + \lambda_3 + 2q)w_0 + (\lambda_4 + 2k)w_1 + \lambda_2 w_2 + \lambda_3 w_3 + \lambda_4 w_4 =$$

$$\lambda_2(w_0 + w_2) + \lambda_3(w_0 + w_3) + \lambda_4(w_1 + w_4) + 2qw_0 + 2kw_1.$$

Segue que $B = \{w_0 + w_2, w_0 + w_3, w_1 + w_4, 2w_0, 2w_1\}$ *é uma base para* $U = \ker \pi$. *Denotando por*

$$\begin{aligned} u_1 &= w_0 + w_2 \\ u_2 &= w_0 + w_3 \\ u_3 &= w_1 + w_4 \\ u_4 &= 2w_0 \\ u_5 &= 2w_1, \end{aligned}$$

obtemos a seguinte ação de G *na base* B*:*

$$\begin{aligned} nu_1 = u_1, cu_1 = u_4 - u_1 \\ nu_2 = u_4 - u_2, cu_2 = u_2 \\ nu_3 = u_5 - u_3, cu_3 = u_5 - u_3 \\ nu_4 = u_4, cu_4 = u_4 \\ nu_5 = u_5, cu_5 = u_5. \end{aligned}$$

Exemplo 4.3.3. *Seja* V *um* $\mathbb{F}_2$*-espaço vetorial com base* $\{v_1, v_2\}$. *Considere o diagrama*

$$(V, 0, \langle v_1 \rangle_{\mathbb{F}_2}, \langle v_1, v_2 \rangle_{\mathbb{F}_2}, \langle v_2 \rangle_{\mathbb{F}_2}).$$

Tome uma cópia de Λ_1, *duas de* Λ_2 *e uma de* Λ_3. *Sejam* w_1 *um gerador de* Λ_1, $\{w_2, w_3\}$ *uma base de* $\Lambda_2 \oplus \Lambda_2$ *e* w_4 *um gerador de* Λ_3. *Defina*

$$\pi_1 : \Lambda_1 \longrightarrow V_1$$

$$w_1 \mapsto v_1;$$

$$\pi_2 : \Lambda_2 \oplus \Lambda_2 \longrightarrow V_2$$

$$w_2 \mapsto v_1, w_3 \mapsto v_2;$$

$$\pi_3 : \Lambda_3 \longrightarrow V_3$$

$$w_4 \mapsto v_2.$$

Definindo

$$\pi : \Lambda_1 \oplus \Lambda_2 \oplus \Lambda_2 \oplus \Lambda_3 \longrightarrow V$$

por $\pi = \pi_1 + \pi_2 + \pi_3$, *observe que*

$$u = \sum_{i=1}^{4} \lambda_i w_i \in \ker \pi \Leftrightarrow$$

$$\Leftrightarrow \pi(u) = \lambda_1 v_1 + \lambda_2 v_1 + \lambda_3 v_2 + \lambda_4 v_2 = (\lambda_1 + \lambda_2)v_1 + (\lambda_3 + \lambda_4)v_2 = 0 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \lambda_1 = \lambda_2 + 2q_1 \\ \lambda_3 = \lambda_4 + 2q_3 \end{cases} ; \lambda_2, \lambda_4, q_1, q_2 \in \mathbb{Z}_2.$$

Assim,

$$u = (\lambda_2 + 2q_1)w_1 + \lambda_2 w_2 + (\lambda_3 + 2q_3)w_3 + \lambda_4 w_4 =$$

$$= \lambda_2(w_1 + w_2) + \lambda_4(w_3 + w_4) + 2q_1 w_1 + 2q_3 w_3.$$

Denotando por

$$u_1 = w_1 + w_2, u_2 = w_3 + w_4,$$
$$u_3 = 2w_1, u_4 = 2w_3$$

Obtemos que u_1, u_2, u_3 *e* u_4 *formam uma base para* $U = \ker \pi$ *na qual a multiplicação de* G *é dada por :*

$$nu_1 = -u_1 + u_3, nu_2 = -u_2, nu_3 = u_3, nu_4 = -u_4$$
$$cu_1 = u_1 - u_3, cu_2 = -u_2 + u_4, cu_3 = -u_3$$

Exemplo 4.3.4. *Considere o diagrama*

$$(V, V_0, V_1, V_2, 0, V_4)$$

para $\mathbb{Z}_3 G$ *do Exemplo 4.1.2. Mantendo a notação do Exemplo 4.1.2, lembramos que o conjunto* $\{v_1, v_2, v_3\}$ *é uma base para* V *na qual a multiplicação de* G *é dada por*

$$nv_0 = cv_0 = v_0, cv_1 = v_1 + v_0, nv_1 = v_1,$$

$$nv_2 = v_2 + v_0, cv_2 = v_2.$$

Também temos

$$V_0 = \langle v_0 \rangle, V_1 = \langle v_0, v_1 \rangle, V_2 = \langle v_0, v_2 \rangle, V_3 = 0 \text{ e } V_4 = \langle v_0, v_0 + v_1 + v_2 \rangle.$$

Como vimos no Exemplo 4.1.2, definindo os seguintes $\mathbb{Z}_3G$-homomorfismos

$$\phi_0 : \Lambda_0 \longrightarrow V_0, w_0 \mapsto v_0,$$

$$\phi_1 : \Lambda_1 \longrightarrow V_1, w_1 \mapsto -v_1 + v_0, w_2 \mapsto -v_1,$$

$$\phi_2 : \Lambda_2 \longrightarrow V_2, w_3 \mapsto -v_2 + v_0, w_4 \mapsto -v_2,$$

$$\phi_4 : \Lambda_4 \longrightarrow V_4, w_5 \mapsto -v_1 - v_2, w_6 \mapsto -v_0 - v_1 - v_2.$$

temos que cada ϕ_i é sobrejetivo e induz um isomorfismo entre $\Lambda_i/J\Lambda_i$ e V_i/JV_i. Posto isso, defina

$$\phi : \Lambda_0 \oplus \Lambda_1 \oplus \Lambda_2 \oplus \Lambda_4 \longrightarrow V,$$

por $\phi = \phi_0 + \phi_1 + \phi_2 + \phi_4$. Pelo Teorema 4.3.1 $U = ker\phi$ é um $\mathbb{Z}_3G$-módulo cujo o diagrama associado é $(V; V_0, V_1, V_2, 0, V_4)$. Vamos encontrar U.

Observe que dado $u \in \Lambda_0 \oplus \Lambda_1 \oplus \Lambda_2 \oplus \Lambda_4$ temos que existem únicos escalares $\lambda_i \in \mathbb{Z}_3, i = 0, 1, 2, 3, 4$, tais que $u = \sum_{i=0}^{6} \lambda_i w_i$. Assim

$$\phi(u) = 0 \Leftrightarrow$$

$$\Leftrightarrow \lambda_0\phi_0(w_0) + \phi_1(\lambda_1 w_1 + \lambda_2 w_2) + \phi_2(\lambda_3 w_3 + \lambda_4 w_4) + \phi_4(\lambda_5 w_5 + \lambda_6 w_6) = 0 \Leftrightarrow$$

$$\Leftrightarrow \lambda_0 v_0 + \lambda_1(v_0 - v_1) - \lambda_2 v_1 + \lambda_3(v_0 - v_2) - \lambda_4 v_2 + \lambda_5(-v_1 - v_2) - \lambda_6(v_0 + v_1 + v_2) = 0 \Leftrightarrow$$

$$(\lambda_0 + \lambda_1 + \lambda_3 - \lambda_6)v_0 + (-\lambda_1 - \lambda_2 - \lambda_5 - \lambda_6)v_1 + (-\lambda_3 - \lambda_4 - \lambda_5 - \lambda_6)v_2 = 0 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \lambda_0 = -\lambda_1 - \lambda_3 + \lambda_6 + 3q_0 \\ \lambda_2 = -\lambda_1 - \lambda_5 - \lambda_6 + 3q_2 \\ \lambda_4 = -\lambda_3 - \lambda_5 - \lambda_6 + 3q_4 \end{cases} ; \lambda_1, \lambda_3, \lambda_5, \lambda_6, q_0, q_2, q_4 \in \mathbb{Z}_3.$$

Assim,

$$u = \sum_{i=0}^{6} \lambda_i w_i = (-\lambda_1 - \lambda_3 + \lambda_6 + 3q_0)w_0 + \lambda_1 w_1 + (-\lambda_1 - \lambda_5 - \lambda_6 + 3q_2)w_2 + \lambda_3 w_3 +$$

$$+(-\lambda_3 - \lambda_5 - \lambda_6 + 3q_4)w_4 + \lambda_5 w_5 + \lambda_6 w_6 =$$

$$= \lambda_1(-w_0 + w_1 - w_2) + \lambda_3(-w_0 + w_3 - w_4) + \lambda_5(-w_2 - w_4 + w_5) +$$

$$+\lambda_6(w_0 - w_2 - w_4 + w_6) + 3q_0 w_0 + 3q_2 w_2 + 3q_4 w_4,$$

logo

$$\{3w_0, 3w_2, 3w_4, -w_0 + w_1 - w_2, -w_0 + w_3 - w_4, -w_2 - w_4 + w_5, w_0 - w_2 - w_4 + w_6\}$$

é uma base para $U = \ker \phi$.

Denotando por

$$u_1 = 3w_0, u_2 = 3w_2, u_3 = 3w_4,$$

$$u_4 = -w_0 + w_1 - w_2, u_5 = -w_0 + w_3 - w_4,$$

$$u_6 = -w_2 - w_4 + w_5, u_7 = w_0 - w_2 - w_4 + w_6,$$

Vemos que

$$cu_1 = nu_1 = u_1,$$

$$nu_2 = u_2, cu_2 = -u_2 - (u_1 + u_2 + 3u_4) = -2u_2 - u_1 - 3u_4,$$

$$nu_3 = -3v_4 - 3v_3 = -u_3 - (3u_5 + u_1 + u_3) = -2u_3 - 3u_5 - u_1, cu_3 = u_3,$$

$$nu_4 = u_4, cu_4 = -w_0 + w_2 + w_1 + w_2 = -w_0 + w_1 - w_2 + 3w_2 = u_4 + u_2,$$

$$nu_5 = -w_0 + w_4 + w_3 + w_4 = -w_0 + w_3 - w_4 + 3w_4 = u_5 + u_3, cu_5 = u_5,$$

$$nu_6 = -w_2 + w_4 + w_3 + w_6 = 3w_4 - w_0 + w_3 - w_4 + w_0 - w_2 - w_4 + w_6 = u_3 + u_5 + u_7,$$

$$cu_6 = w_2 + w_1 - w_4 + w_6 = w_0 - w_2 - w_4 + w_6 - w_0 + w_1 - w_2 + 3w_2 = u_7 + u_4 + u_2,$$

$$nu_7 = w_0 - w_2 + w_3 + w_4 - w_5 - w_6 = u_1 - u_2 + u_5 - u_6 - u_7,$$

$$cu_7 = w_0 + w_1 + w_2 - w_4 - w_5 - w_6 = u_1 + u_4 - u_6 - u_7 - u_3.$$

Logo U *possui a seguinte multiplicação de* G*:*

$$cu_1 = nu_1 = u_1,$$

$$nu_2 = u_2, cu_2 = -2u_2 - u_1 - 3u_4,$$

$$nu_3 = -2u_3 - 3u_5 - u_1, cu_3 = u_3,$$

$$nu_4 = u_4, cu_4 = u_4 + u_2,$$

$$nu_5 = u_5 + u_3, cu_5 = u_5,$$

$$nu_6 = u_3 + u_5 + u_7, cu_6 = u_7 + u_4 + u_2,$$

$$nu_7 = u_1 - u_2 + u_5 - u_6 - u_7, cu_7 = u_1 + u_4 - u_6 - u_7 - u_3.$$

4.4 $\mathbb{Z}_p[C_p \times C_p]$-módulos de permutação

Ao longo dessa seção, G denotará o grupo abeliano $N \times C$, onde N e C são grupos de ordem p, e $p > 0$ é primo. Seja U um $\mathbb{Z}_pG$-reticulado reduzido. Nessa seção encontramos condições necessárias e suficientes em $\Delta(U)$ para que U^N e U_N sejam $\mathbb{Z}_pC$-módulos de permutação e as utilizamos para a construção de um $\mathbb{Z}_pG$-reticulado reduzido U em que U^N e U_N são de permutação, mas U não é um $\mathbb{Z}_pG$-módulo de permutação. Esse exemplo mostra que apenas a Condição 1 no Teorema 3.2.3, em geral, não garante que um reticulado U seja de permutação.

4.4.1 Analisando diagramas

Relembramos que os idempotentes ortogonais primitivos de $\mathbb{Q}_pG$ são

$$e_0 = \frac{1}{p^2}\sum_{h\in G} h, e_i = \frac{1}{p^2}\left(p\sum_{h\in H_i} h - \sum_{h\in G} h\right), i \in \{1, 2, 3, ..., p+1\},$$

onde H_i é um subgrupo de ordem p. Denote os subgrupos de G com ordem p por

$$H_1 = \langle n\rangle, H_2 = \langle c\rangle, H_3 = \langle nc\rangle, H_4 = \langle nc^2\rangle, ..., H_{p+1} = \langle nc^{p-1}\rangle.$$

Seja U um $\mathbb{Z}_pG$-reticulado. Como vimos na Seção 4.2, podemos trabalhar com U como sendo um $\mathbb{Z}_pG$-submódulo do $\mathbb{Z}_pG$-módulo

$$U_* = e_0U \oplus e_1U \oplus ... \oplus e_{p+1}U,$$

onde $e_iU \simeq \Lambda_i^{r_i}$, $pe_iU \subseteq U \cap e_iU \subseteq Je_iU$, $r_i \geq 0$ $\forall i = 0, 1, ..., p+1$. Assim, associamos a esse um diagrama $\Delta(U)$, onde

$$\Delta(U) = (V, V_0, V_1, ..., V_{p+1})$$

e

$$V = U_*/U = \sum_{i=0}^{p+1}(e_iU + U)/U, V_i = (e_iU + U)/U, i \in A_{p+2}.$$

Ao longo do texto, denotamos e_iU por F_i e por x_i um elemento de F_i. A projeção de x_i em $V_i = (e_iU + U)/U$ será denotada por $\bar{x}_i$.

Começamos observando que, uma vez que cada $u \in U$ pode ser expresso unicamente da forma

$$u = \sum_{i=0}^{p+1} x_i, x_i \in F_i,$$

temos,

$$\bar{u} = \bar{x}_0 + \bar{x}_1 + ... + \bar{x}_{p+1} = 0 \in V.$$

Assim, por exemplo, se $u = x_1 + x_2 + ... + x_{p+1}$ obtemos que

$$\bar{x}_1 = -\sum_{i=2}^{p+1} \bar{x}_i \in V_1 \cap (V_2 + V_3 + ... + V_{p+1}).$$

Agora, cada elemento de $V_1 \cap (V_2 + V_3 + ... + V_{p+1})$ é da forma

$$\bar{x}_1 = \bar{x}_2 + \bar{x}_3 + ... + \bar{x}_{p+1}$$

logo

$$\bar{x}_1 - \bar{x}_2 - \bar{x}_3 - ... - \bar{x}_{p+1} = 0 \in V = U_*/U,$$

donde $x_1 - x_2 - ... - x_{p+1} \in U$. Assim, a associação

$$\sum_{i=1}^{p+1} x_i \mapsto \bar{x_1} = -\bar{x}_2 - \bar{x}_3 - ... - \bar{x}_{p+1}$$

é bem definida e fornece um $\mathbb{Z}_pG$ homomorfismo sobrejetivo de $U \cap (F_1 + F_2 + ... + F_{p+1})$ em $V_1 \cap (V_2 + V_3 + ... + V_{p+1})$. Vamos generalizar essa ideia em um Lema.

Lema 4.4.1. *Seja $B_r := \{i_1, .., i_r\} \subset \{0, 1, 2, 3, ..., p+1\}, r > 1$. Para cada $i_j \in B_r$, existe um homomorfismo sobrejetivo de*

$$U \cap (F_{i_1} \oplus F_{i_2} \oplus ... \oplus F_{i_r}) \text{ em } V_{i_j} \cap \left(\sum_{\substack{i_s \neq i_j \\ i_s \in B_r}} V_{i_s} \right).$$

Demonstração. Dado $i_j \in B_r$ defina

$$\varphi_{i_j} : U \cap (F_{i_1} \oplus F_{i_2} \oplus ... \oplus F_{i_r}) \longrightarrow V_{i_j} \cap \left(\sum_{\substack{i_s \neq i_j \\ i_s \in B_r}} V_{i_s} \right)$$

por $\varphi_{i_j} \left(\sum_{s=1}^{r} x_{i_s} \right) = \bar{x}_{i_j} = -\sum_{\substack{i_s \neq i_j \\ i_s \in B_r}} \bar{x}_{i_s}$. Esse é claramente um homomorfismo, e dado

$$\bar{x}_{i_j} = -\sum_{\substack{i_s \neq i_j \\ i_s \in B_r}} \bar{x}_{i_s} \in V_{i_j} \cap \left(\sum_{\substack{i_s \neq i_j \\ i_s \in B_r}} V_{i_s} \right),$$

temos que

$$\sum_{s=1}^{r} \bar{x}_{i_s} = 0 \in V = \sum_{i=0}^{p+1} (e_i U + U)/U \Rightarrow$$

$$\Rightarrow \sum_{s=1}^{r} x_{i_s} \in U \cap (F_{i_1} \oplus F_{i_2} \oplus ... \oplus F_{i_r}),$$

donde a associação $\sum_{s=1}^{r} x_{i_s} \mapsto \bar{x}_{i_j} = -\sum_{\substack{i_s \neq i_j \\ i_s \in B_r}} \bar{x}_{i_s}$ é sobrejetiva. □

Dado um $\mathbb{Z}_pG$-módulo reduzido U, passamos a estabelecer condições necessárias e suficientes em $\Delta(U)$ para que U^N e U_N sejam $\mathbb{Z}_pC$-módulos de permutação. Daqui em diante quando estivermos trabalhando com um certo reticulado reduzido U, V e V_i, sempre denotarão as componentes de $\Delta(U) = (V; V_0, ..., V_{p+1})$. Antes de começarmos a estabelecer os resultados vamos conferir, através de alguns exemplos, o que ocorre no diagrama para um $\mathbb{Z}_pG$- reticulado U quando um dos módulos U^N e U_N não são de permutação.

Exemplo 4.4.1. *Para o diagrama do exemplo 4.3.2:*

$$D = (\mathbb{F}_2 \oplus \mathbb{F}_2; \mathbb{F}_2 \oplus \mathbb{F}_2, \langle(1,0)\rangle, \langle(1,0)\rangle, \langle(0,1)\rangle)$$

obtemos um $\mathbb{Z}_pG$-reticulado U com uma base $\{u_1, u_2, u_3, u_4, u_5\}$ com a seguinte ação de G:

$$\begin{aligned} nu_1 = u_1, cu_1 = u_4 - u_1 \\ nu_2 = u_4 - u_2, cu_2 = u_2 \\ nu_3 = u_5 - u_3, cu_3 = u_5 - u_3 \\ nu_4 = u_4, cu_4 = u_4 \\ nu_5 = u_5, cu_5 = u_5. \end{aligned}$$

Daí, vemos que $\{u_4 - u_1, u_1, u_5\}$ é uma base para U^N. Assim, U^N é de permutação.

Por outro lado, o conjunto $\{u_4 - 2u_1, u_5 - 2u_3, \}$ é uma base para I_NU, como $B' = \{u_1, u_2, u_3, u_4 - 2u_2, u_5 - 2u_3\}$ é uma base para U, logo U/I_NU é um reticulado. Note que I_CU_N não é um reticulado, daí, pelo Teorema 3.2.1, U_N não é um $\mathbb{Z}_2[G/N]$-módulo de permutação. Veja que a soma $V_1 + V_2 + V_3$ não é direta, e que $V_1, V_2, V_3 \subset V_0 = V$.

Exemplo 4.4.2. *Considere o diagrama do Exemplo 4.3.3:*

$$(V, 0, \langle v_1\rangle_{\mathbb{F}_2}, \langle v_1, v_2\rangle_{\mathbb{F}_2}, \langle v_2\rangle_{\mathbb{F}_2}).$$

Obtemos no Exemplo 4.3.3 que o reticulado U, associado ao diagrama acima, possui uma base $\{u_1, u_2, u_3, u_4\}$ na qual a multiplicação de G é dada por :

$$nu_1 = -u_1 + u_3, nu_2 = -u_2,$$
$$nu_3 = u_3, nu_4 = -u_4$$
$$cu_1 = u_1 - u_3, cu_2 = -u_2 + u_4,$$
$$cu_3 = -u_3.$$

Observe que U^N é gerado por u_3, e como $cu_3 = -u_3$, esse não pode ser um $\mathbb{Z}_2C$-módulo de permutação. Também observe que

$$I_N U = \langle -2u_1 + u_3, -2u_2, -2u_4 \rangle.$$

Como $u_4 \notin I_N U$ e $2u_4 \in I_N U$, então U_N não é um reticulado.

Observe que no diagrama para U temos $V_1 \nsubseteq V_0$, a soma $V_2 + V_3 + V_4$ não é direta e $V_2 + V_3 + V_4 \nsubseteq V_0 + V_1$.

Exemplo 4.4.3. *Seja U o reticulado obtido no Exemplo 4.3.4. Vimos que o diagrama associado a U é*

$$(V, V_0, V_1, V_2, 0, V_4),$$

onde o conjunto $\{v_1, v_2, v_3\}$ é uma base para V na qual a multiplicação de G é dada por

$$nv_0 = cv_0 = v_0, cv_1 = v_1 + v_0, nv_1 = v_1,$$

$$nv_2 = v_2 + v_0, cv_2 = v_2.$$

Também temos

$$V_0 = \langle v_0 \rangle, V_1 = \langle v_0, v_1 \rangle, V_2 = \langle v_0, v_2 \rangle, V_3 = 0 \text{ e } V_4 = \langle v_0, v_0 + v_1 + v_2 \rangle.$$

Agora, observe que como U possui uma base $\{u_1, u_2, ..., u_7\}$ na qual a multiplicação de G é dada por

$$cu_1 = nu_1 = u_1,$$

$$nu_2 = u_2, cu_2 = -2u_2 - u_1 - 3u_4,$$

$$nu_3 = -2u_3 - 3u_5 - u_1, cu_3 = u_3,$$

$$nu_4 = u_4, cu_4 = u_4 + u_2,$$

$$nu_5 = u_5 + u_3, cu_5 = u_5,$$

$$nu_6 = u_3 + u_5 + u_7, cu_6 = u_7 + u_4 + u_2,$$

$$nu_7 = u_1 - u_2 + u_5 - u_6 - u_7, cu_7 = u_1 + u_4 - u_6 - u_7 - u_3.$$

Observe que $U^N = \langle u_1, u_2, u_4, \rangle$ *e que*

$$(c-1)u_2 = -3u_2 - u_1 - 3u_4,$$

$$(c^2-1)u_2 = -u_2+c(-2u_2-u_1-3u_4) = -u_2-2(-2u_2-u_1-3u_4)-u_1-3(u_4+u_2) = u_1+3u_4$$

$$(c-1)u_4 = u_2, (c^2-1)u_4 = -u_4+c(u_4+u_2) = -u_4+u_4+u_2-2u_2-u_1-3u_4 = -u_2-u_1-3u_4.$$

Logo $I_C U^N = \langle u_1 + 3u_4, u_2 \rangle$, *como* $\{u_1 + 3u_4, u_2, u_4\}$ *também é base de* U^N *segue que* $U^N/I_C U^N = \langle \bar{u}_4 \rangle$ *é um reticulado. Portanto, pelo Teorema 3.2.1,* U^N *é um* $\mathbb{Z}_3 C$*-módulo de permutação.*

Por outro lado, U_N *não é de permutação. De fato, temos*

$$(n-1)u_3 = -3u_3 - 3u_5 - u_1,$$

$$(n^2-1)u_3 = -u_3 + n(-2u_3 - 3u_5 - u_1) =$$

$$-u_3 - 2(-2u_3 - 3u_5 - u_1) - 3(u_5 + u_3) - u_1 = 3u_5 + u_1,$$

$$(n-1)u_5 = u_3,$$

$$(n^2-1)u_5 = -u_5 + n(u_5 + u_3) = -u_5 + u_5 + u_3 - 2u_3 - 3u_5 - u_1 = -u_3 - 3u_5 - u_1,$$

$$(n-1)u_6 = -u_6 + u_3 + u_5 + u_7,$$

$$(n^2-1)u_6 = -u_6 + n(u_3 + u_5 + u_7) =$$

$$-u_6 - 2u_3 - 3u_5 - u_1 + u_5 + u_3 + u_1 - u_2 + u_5 - u_6 - u_7 =$$

$$= -2u_6 - u_5 - u_3 - u_2 - u_7,$$

$$(n-1)u_7 = u_1 - u_2 + u_5 - u_6 - 2u_7$$

$$(n^2-1)u_7 = -u_7 + n(u_1 - u_2 + u_5 - u_6 - u_7) =$$

$$= -u_7 + u_1 - u_2 + u_5 + u_3 - (u_3 + u_5 + u_7) - (u_1 - u_2 + u_5 - u_6 - u_7) =$$

$$= -u_7 - u_5 + u_6.$$

Assim,

$$I_N U = \langle u_3, 3u_5 + u_1, -2u_6 - u_5 - u_2 - u_7, -u_7 - u_5 - u_6 \rangle,$$

como $\{u_3, u_4, u_5, u_6, 3u_5 + u_1, -2u_6 - u_5 - u_2 - u_7, -u_7 - u_5 - u_6\}$ *também é base de* U*, segue que*

$$U_N = \langle \bar{u_4}, \bar{u_5}, \bar{u_6} \rangle,$$

e U_N *é um reticulado. Agora,*

$$c\bar{u}_6 = \bar{u}_7 + \bar{u}_4 + \bar{u}_2 = \bar{u}_7 + \bar{u}_4 + \bar{u}_2 - 2\bar{u}_6 - \bar{u}_5 - \bar{u}_2 - \bar{u}_7 = \bar{u}_4 - 2\bar{u}_6 - \bar{u}_5,$$

$$c\bar{u}_4 = \bar{u}_4 + \bar{u}_2 = \bar{u}_4 + \bar{u}_2 - 3\bar{u}_6 - \bar{u}_2 = \bar{u}_4 - 3\bar{u}_6,$$

$$c^2\bar{u}_6 = \bar{u}_4 - 3\bar{u}_6 - 2(\bar{u}_4 - 2\bar{u}_6 - \bar{u}_5) - \bar{u}_5 = -\bar{u}_4 + \bar{u}_6 + \bar{u}_5,$$

$$c^2\bar{u}_4 = \bar{u}_4 - 3\bar{u}_6 - 3(\bar{u}_4 - 2\bar{u}_6 - \bar{u}_5) = -2\bar{u}_4 + 3\bar{u}_6 + 3\bar{u}_5.$$

Daí, obtemos

$$I_C U_N = \langle -3\bar{u}_6, -\bar{u}_4 + \bar{u}_5 \rangle.$$

Como $\bar{u}_6 \notin I_C U_N$ *e* $3\bar{u}_6 \in I_C U_N$*, segue que* $U_N / I_C U_N$ *não é livre de torção. Então, pelo Teorema 3.2.1,* U_N *não é um* $\mathbb{Z}_3 C$*-módulo de permutação.*

Observe que no diagrama para U *temos que todo* G*-ponto fixo de* V_1 *está contido em* V_0*. Dado* $v \in V_2 + V_3 + V_4$*, já que* $\{v_0, v_2, v_0 + v_2 + v_1\}$ *é uma* $\mathbb{F}_3$*-base para* $V_2 + V_3 + V_4$*, existem escalares (únicos módulo o ideal* $3\mathbb{Z}_3$*)* $\lambda_0, \lambda_1, \lambda_2, \in \mathbb{Z}_3$*, tais que* $v = \lambda_0 v_0 + \lambda_1 v_2 + \lambda_2(v_0 + v_1 + v_2)$*. Logo,*

$$(n-1)v = (\lambda_1 + \lambda_2)w_0 = 0 \Leftrightarrow \lambda_1 + \lambda_2 \in 3\mathbb{Z}_3.$$

Segue que $v = \lambda_0 v_0 - \lambda_2 v_2 + \lambda_2(v_0 + v_1 + v_2) = \lambda_0 + \lambda_2(v_0 + v_1) \in V_0 + V_1$*, assim, temos que*

$$\{v \in V_2 + V_3 + V_4; (n-1)v = 0\} \subseteq V_0 + V_1.$$

Por fim, observe que $V_1 \cap (V_2 + V_3 + V_4) \nsubseteq I_G V_1$*.*

Observação 4.4.1. *Já que* $U \subset F_0 \oplus F_1 \oplus ... \oplus F_{p+1}$*, cada* $u \in U$ *pode ser expresso unicamente como*

$$u = \sum_{i=0}^{p+1} x_i, x_i \in F_i.$$

Daí,

$$(n-1)u = 0 \Leftrightarrow (n-1)\sum_{i=2}^{p+1} x_i = 0,$$

pois n *age trivialmente em* F_0 *e* F_1*. Por outro lado, segue da Observação 2.5.1 que o único* N*-ponto fixo de* $F_i, i > 1$*, é* 0*. Assim,*

$$\sum_{i=2}^{p+1} x_i = 0$$

e $u = x_0 + x_1$*, donde* $U^N = \{x_0 + x_1 \in F_0 \oplus F_1; x_0 + x_1 \in U\} = U \cap (F_0 + F_1)$*.*

Proposição 4.4.1. *Seja U um $\mathbb{Z}_pG$-reticulado reduzido, então U^N é um $\mathbb{Z}_2[G/N]$-módulo de permutação se, e somente se, $I_CU^N = U \cap F_1$.*

Demonstração. Pela observação anterior temos $U^N = U \cap (F_0 + F_1)$. Como c age trivialmente em F_0, obtemos $I_CU^N \subseteq U \cap F_1$. Se existe $x_1 \in U \backslash I_CU^N$, então, pela Observação 2.5.1,

$$[(1-c) + (1-c^2) + ... + (1-c^{p-1})] = (p - (1 + c + c^2 + ... + c^{p-1}))x_1 = px_1 \in I_CU^N,$$

portanto, U^N/I_CU^N não é um reticulado. Segue do Teorema 3.2.1 que U^N não pode ser um $\mathbb{Z}_2C$-módulo de permutação. Portanto, se U^N é de permutação, então $I_CU^N = U \cap F_1$.

Reciprocamente, $I_CU^N = U \cap F_1$ implica que U^N/I_CU^N é livre de torção, pois se $x_0 + x_1 \in U$ e $a(x_0 + x_1) \in I_CU^N, a \in \mathbb{Z}_p$, então $x_0 = 0$ e $x_1 \in U \cap F_1 = I_CU^N$. Sendo $\mathbb{Z}_p$ um domínio de ideais principais e U^N/I_CU^N $\mathbb{Z}_p$-livre de torção, temos U^N/I_CU^N reticulado e, pelo Teorema 3.2.1, U^N é um $\mathbb{Z}_pC$-módulo de permutação. □

Observação 4.4.2. *Dado $u \in U$, u se escreve de forma única como $u = x_0 + x_1 + ... + x_{p+1}$, onde $x_i \in F_i, i = 0, 1, 2, ..., p+1$. Agora, $I_NU = (n-1)U$ já que I_N é gerado por $(n-1)$ como $\mathbb{Z}_pN$-módulo. Como n age trivialmente em F_0 e F_1 devemos ter*

$$I_NU \subseteq U \cap (F_2 + F_3 + ... + F_{p+1}).$$

De modo análogo obtemos

$$I_CU \subseteq U \cap (F_1 + F_3 + F_4 + ... + F_{p+1}),$$

já que c age trivialmente em F_0 e F_2.

Proposição 4.4.2. *Seja U um $\mathbb{Z}_pG$-reticulado reduzido, então U_N é um reticulado se, e somente se, $U \cap (F_2 + F_3 + ... + F_{p+1}) = I_NU$.*

Demonstração. Pela observação anterior temos

$$I_NU \subseteq U \cap (F_2 + F_3 + ... + F_{p+1}).$$

Se existe $u = \sum_{i=2}^{p+1} x_i \in U \backslash I_NU$, então, ja que pela Observação 2.5.1

$$(1 + n + n^2 + ... + n^{p-1}) \sum_{i=2}^{p+1} x_i = 0,$$

temos

$$[(1-n) + (1-n^2) + ... + (1-n^{p-1})] \sum_{i=2}^{p+1} x_i =$$

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

$$= p \sum_{i=2}^{p+1} x_i = pu \in I_N U,$$

e U_N não é um reticulado, pois como $u \notin I_N U$ a sua projeção em $U/I_N U$ é não nulo, mas o mesmo não ocorre com pu, já que $pu \in I_N U$. Portanto, U_N reticulado implica $U \cap (F_2 + F_3 + ... + F_{p+1}) = I_N U$.

Reciprocamente, $U \cap (F_2 + F_3 + ... + F_{p+1}) = I_N U$ implica que U_N é livre de torção, pois se $u = x_0 + x_1 + ... + x_{p+1} \in U$ e existe $0 \neq a \in \mathbb{Z}_p$ com $au \in I_N U$, então $x_0 = x_1 = 0$ e $x_2 + x_3 + ... + x_{p+1} \in U \cap (F_2 + F_3 + ... + F_{p+1}) = I_N U$, logo $u \in I_N U$. Como $\mathbb{Z}_p$ é um domínio de ideais principais e $U/I_N U$ é livre de torção, segue que é um reticulado. □

Observação 4.4.3. *Como I_G é gerado pelo conjunto $\{(g-1); g \in G, g \neq 1\}$, os elementos de $I_G U$ são combinações lineares sobre $\mathbb{Z}_p$ de elementos da forma $(g-1)u$ tal que $u \in U$. Sendo $G = N \times C$ cada $g \in G$ é da forma $n^i c^k, k, i \in \mathbb{Z}$ e logo*

$$(n^i c^k - 1) = (n^i c^k - n^i n^{-i}) = n^i (c^k - n^{-i}) = n^i [(c^k - 1) - (n^{-i} - 1)].$$

Assim,

$$(n^i c^k - 1)u = n^i [(c^k - 1) - (n^{-i} - 1)] = (c^k - 1)n^i u - (n^{-i} - 1)n^i u \in I_N U + I_C U.$$

Disso segue que $I_G U = I_N U + I_C U \subseteq U \cap (F_1 + F_2 + F_3 + ... + F_{p+1})$.

Proposição 4.4.3. *Seja U um $\mathbb{Z}_p G$-reticulado reduzido e suponha que U_N é um reticulado. Então U_N é de permutação se, e somente se, $I_G U = U \cap (F_1 + F_2 + ... + F_{p+1})$.*

Demonstração. Pela observação anterior temos $I_G U \subseteq U \cap (F_1 + F_2 + F_3 + ... + F_{p+1})$. Pelo Teorema 3.2.1, U_N é de permutação se, e somente se, $(U_N)_C = U_N / I_C U_N \simeq U/I_G U$ é reticulado. Daí, se existe $\sum_{i=1}^{p+1} x_i \in U \backslash I_G U$, então existe $r > 0$ tal que $p^r \sum_{i=1}^{p+1} x_i \in I_G U$, já que pela Observação 2.5.1 se $g \in H_i$, então $(p - (1 + g + g^2 + ... + g^{p-1})) \in I_G$, age como zero em F_i e F_0, e como uma multiplicação por p em $F_j, j \neq i, 0$. Assim, se $I_G U$ está contido propriamente em $U \cap (F_1 + F_2 + F_3 + ... + F_{p+1})$, então $(U_N)_C$ não é um reticulado e, portanto, U_N não pode ser de permutação.

Reciprocamente, $I_G U = U \cap (F_1 + F_2 + F_3 + ... + F_{p+1})$ implica que $U/I_G U \simeq (U_N)_C$ é $\mathbb{Z}_p$-livre de torção, logo um reticulado. □

Teorema 4.4.1. *Seja U um $\mathbb{Z}_p G$-reticulado reduzido, então U^N é de permutação se, e somente se, todo G-ponto fixo de V_1 pertence a V_0.*

Demonstração. Suponha que U^N seja de permutação. Pela Proposição 4.4.1 temos $I_C U^N = U \cap F_1$. Dado $\bar{x}_1 \in V_1$ tal que $(c-1)\bar{x}_1 = 0$, temos $(c-1)x_1 \in U$. Como $U \cap F_1 = I_C U^N$, existe $x_0 \in F_0$ com $x_0 + x_1 \in U$. O Lema 4.4.1 fornece que $\bar{x}_1 \in V_0$.

Reciprocamente, dado $(c-1)x_1 \in U \cap F_1 \subseteq JF_1$ temos que $(c-1)\bar{x}_1 = 0$. Logo $\bar{x}_1$ é G-ponto fixo de V_1. Como $\bar{x}_1 \in V_0$, temos que existe $x_0 \in F_0$ tal que $\bar{x}_0 = \bar{x}_1$ o que implica $x_0 - x_1 \in U$, donde $(c-1)x_1 \in I_C U^N$. Assim, $I_C U^N = U \cap F_1$ e a Proposição 4.4.1 garante que U^N é de permutação. □

Teorema 4.4.2. *Seja U um $\mathbb{Z}_pG$-reticulado reduzido, então U_N é um reticulado se, e somente se, são válidas*

1. $V_i \cap \left(\sum\limits_{\substack{j \neq 0,1,i \\ j \in A_{p+2}}} V_j \right) \subseteq I_N V_i, i \geq 2.$

2. $\left\{ \sum\limits_{i=2}^{p+1} \bar{x}_i \in V; (n-1) \sum\limits_{i=2}^{p+1} \bar{x}_i = 0 \right\} \subseteq V_0 + V_1.$

Demonstração. Suponha que U_N seja um reticulado. Pela Proposição 4.4.2 temos

$$U \cap (F_2 + F_3 + ... + F_{p+1}) = I_N U,$$

daí, o Lema 4.4.1 garante que

$$V_i \cap \left(\sum_{\substack{j \neq 0,1,i \\ j \in A_{p+2}}} V_j \right) \subseteq I_N V_i.$$

Seja $\sum\limits_{i=2}^{p+2} \bar{x}_i \in V$ tal que $(n-1) \sum\limits_{i=2}^{p+1} \bar{x}_i = 0$. Então,

$$(n-1) \sum_{i=2}^{p+1} x_i \in U$$

e por hipótese

$$(n-1) \sum_{i=2}^{p+1} x_i \in I_N U,$$

assim, existe $\sum\limits_{i=0}^{p+1} y_i \in U$ com

$$(n-1) \sum_{i=0}^{p+1} y_i = (n-1) \sum_{i=2}^{p+1} x_i.$$

Já que $1+n+...+n^2$ age como 0 em $F_i, i>1$, o único N-ponto fixo de $F_i, i>1$, é nulo. Daí, obtemos $x_i = y_i, \forall i > 1$. Por outro lado,

$$\bar{y}_0 + \bar{y}_1 = -\sum_{i=2}^{p+1} \bar{y}_i \in V_0 + V_1,$$

portanto

$$\sum_{i=2}^{p+1} \bar{x}_i \in V_0 + V_1.$$

Reciprocamente, pelo Lema 4.4.1, já que U é reduzido, o Item 1 garante que

$$U \cap (F_2 + F_3 + ... + F_{p+1}) \subseteq I_N(F_2 + F_3 + ... + F_{p+1}).$$

Daí, dado $\sum_{i=2}^{p+1} x_i \in U$ temos

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

logo $(n-1)\sum_{i=2}^{p+1} \bar{y}_i = 0$ e por hipótese,

$$\sum_{i=2}^{p+1} \bar{y}_i \in V_0 + V_1,$$

assim, existe $y_0 + y_1 \in F_0 + F_1$ tal que

$$\sum_{i=0}^{p+1} y_i \in U \text{ e } \sum_{i=2}^{p+1} x_i = (n-1)\sum_{i=0}^{p+1} y_i \in I_N U.$$

A Proposição 4.4.2 garante que U_N é um reticulado.

□

Teorema 4.4.3. *Seja U um $\mathbb{Z}_pG$-reticulado reduzido e suponha que U_N seja um reticulado. Então U_N é de permutação se, e somente se, são válidas*

1. $V_i \cap \left(\sum_{\substack{j \neq 0,i \\ j \in A_{p+2}}} V_j \right) \subseteq I_G V_i, \forall i > 0,$ *e*

2. *Cada elemento de $V_1 \cap (V_2 + V_3 + V_4 + ... + V_{p+1})$ é da forma*

$$(n-1)\left(\sum_{i=2}^{p+1} \bar{x}_i + \sum_{i=3}^{p+1} \lambda_i \bar{y}_i \right),$$

onde

$$(c-1)\bar{y}_1 = (n-1)\left(\sum_{i=2}^{p+1}\bar{x}_i + \sum_{i=3}^{p+1}\lambda_i\bar{y}_i\right),$$

$$\sum_{i=2}^{p+1}\bar{x}_i \in V_0+V_1,\ \bar{y}_1 - \sum_{i=3}^{p+1}\bar{y}_i \in V_0+V_2,\ e\ (n-1)\lambda_i y_i = (c-1)y_i,\ \lambda_i \in \mathbb{Z}_pG.$$

Demonstração. Se U_N é de permutação, temos pela Proposição 4.4.3

$$U \cap (F_1+F_2+F_3+...+F_{p+1}) = I_GU.$$

Daí, dado $u \in U \cap (F_1+F_2+...+F_{p+1})$ temos que existem $\sum_{i=0}^{p+1}x_i \in U$ e $\sum_{i=0}^{p+1}y_i \in U$ tais que

$$u = (n-1)\sum_{i=2}^{p+1}x_i + (c-1)y_1 + (c-1)\sum_{i=3}^{p+1}y_i.$$

Como c age em $F_i, i>2$, igual a uma potência de n, existe $\lambda_i \in \mathbb{Z}_pN, i>2$, satisfazendo $(c-1)y_i = (n-1)\lambda_i y_i$. Assim,

$$u = (c-1)y_1 + (n-1)\left(\sum_{i=2}^{p+1}x_i + \sum_{i=3}^{p+1}\lambda_i y_i\right),$$

e pelo Lema 4.4.1

$$(c-1)\bar{y}_1 = -(n-1)\left(\sum_{i=2}^{p+1}\bar{x}_i + \sum_{i=3}^{p+1}\lambda_i\bar{y}_i\right) \in V_1 \cap (V_2+V_3+...V_{p+1}).$$

Como $\sum_{i=0}^{p+1}x_i \in U$ e $\sum_{i=0}^{p+1}y_i \in U$, temos $\bar{x}_0+\bar{x}_1 = -\sum_{i=2}^{p+1}\bar{x}_i \in V_0+V_1$ e de modo análogo obtemos $\bar{y}_1 + \sum_{i=3}^{p+1}\bar{y}_i \in V_0+V_2$.

Assim, o Lema 4.4.1 garante a Condição 2 e a Condição 1 é uma aplicação direta do mesmo, uma vez que $U \cap (F_1+F_2+F_3+...+F_{p+1}) = I_GU$.

Reciprocamente, o fato de ser U reduzido garante que $\bar{x}_i \in JV_i \Leftrightarrow x_i \in J\Lambda_i$. Isso juntamente com a Condição 1 e o Lema 4.4.1 garantem que $U \cap (F_1+F_2+...+F_{p+1}) \subseteq I_G(F_1+F_2+...+F_{p+1})$. Daí, dado $u \in U \cap (F_1+F_2+...+F_{p+1})$, existem $\sum_{i=0}^{p+1}x_i \in U_*$ e $\sum_{i=0}^{p+1}y_i \in U_*$ tais que

$$u = (n-1)\sum_{i=2}^{p+1}x_i + (c-1)y_1 + (c-1)\sum_{i=3}^{p+1}y_i = (c-1)y_1 + (n-1)\left(\sum_{i=2}^{p+1}x_i + \sum_{i=3}^{p+1}\lambda_i y_i\right).$$

Logo,

$$(c-1)\bar{y}_1 = -(n-1)\left(\sum_{i=2}^{p+1}\bar{x}_i + \sum_{i=3}^{p+1}\lambda_i\bar{y}_i\right) \in V_1 \cap (V_2 + V_3 + ... + V_{p+1}).$$

Daí, a Condição 2 fornece que existe $(n-1)\left(\sum_{i=2}^{p+1}\bar{x'}_i + \sum_{i=3}^{p+1}\lambda'_i\bar{y'}_i\right) \in V_1 \cap (V_2+V_3+...+V_{p+2})$, onde $\sum_{i=2}^{p+1}\bar{x'}_i \in V_0 + V_1$, $-\bar{y}_1 + \sum_{i=3}^{p+1}\bar{y'}_i \in V_0 + V_2$, $(n-1)\lambda'_i y'_i = (c-1)y'_i$ e

$$(c-1)\bar{y}_1 = (n-1)\left(\sum_{i=2}^{p+1}\bar{x'}_i + \sum_{i=3}^{p+1}\lambda'_i\bar{y'}_i\right).$$

Disso segue que

$$w' = (c-1)y_1 - (n-1)\left(\sum_{i=2}^{p+1}x'_i + \sum_{i=3}^{p+1}\lambda'_i y'_i\right) = -(n-1)\sum_{i=2}^{p+1}x'_i + (c-1)y_1 - (c-1)\sum_{i=3}^{p+1}y'_i \in I_G U,$$

pois existe $y'_0 + y'_2 \in F_0 + F_2$ tal que

$$\bar{y'}_0 + \bar{y'}_2 = -\bar{y}_1 + \sum_{i=3}^{p+1}\bar{y'}_i \in V_0 + V_2$$

e existe $x'_0 + x'_1 \in F_0 + F_1$ tal que

$$\bar{x'}_0 + \bar{x'}_1 = \sum_{i=2}^{p+1}\bar{x'}_i \in V_0 + V_1.$$

Como

$$-(n-1)\left(\sum_{i=2}^{p+1}\bar{x}_i + \sum_{i=3}^{p+1}\lambda_i\bar{y}_i\right) = (n-1)\left(\sum_{i=2}^{p+1}\bar{x'}_i + \sum_{i=3}^{p+1}\lambda'_i\bar{y'}_i\right),$$

temos que

$$w = (n-1)\left(\sum_{i=2}^{p+1}x_i + \sum_{i=3}^{p+1}\lambda_i y_i\right) + (n-1)\left(\sum_{i=2}^{p+1}x'_i + \sum_{i=3}^{p+1}\lambda'_i y'_i\right) \in U \cap (F_2 + F_3 + ... + F_{p+2}).$$

Como $I_N U$ é reticulado, pela Proposição 4.4.2, temos $I_N U = U \cap (F_2 + F_3 + ... + F_{p+2})$, assim, $w \in I_N U$. Agora observe que

$$u = w + w' = (n-1)\left(\sum_{i=2}^{p+1}x_i + \sum_{i=3}^{p+1}\lambda_i y_i\right) + (c-1)y_1 \in I_G U,$$

já que $w \in I_N U$ e $w' \in I_G U$. Portanto, $U \cap (F_1 + F_2 + ... + F_{p+2}) = I_G U$ e pela Proposição 4.4.3 U_N é de permutação.

□

Suponha que U é um $\mathbb{Z}_p G$-reticulado reduzido para o qual U^N e U_N são $\mathbb{Z}_p[G/N]$-módulos de permutação, e além disso $Je_iU = pe_iU$. Então, $\Delta(U)$ é um diagrama em que V tem ação trivial de G e, daí, o Teorema 4.4.1 fornece que $V_1 \subseteq V_0$. Pelo Teorema 4.4.2, temos $V_j \subseteq V_0$, já que $V_1 \subseteq V_0$. E finalmente, o Teorema 4.4.3 fornece

$$V = V_0 = V_1 \oplus V_2 \oplus ... \oplus V_{p+1}.$$

Posto isso, vemos que

$$\Delta(U) \simeq (\mathbb{F}_p^{r_1+...+r_{p+1}}; \mathbb{F}_p^{r_1+...+r_{p+1}}, \mathbb{F}_p^{r_1}, ..., \mathbb{F}_p^{r_{p+1}}),$$

onde $r_i = \dim V_i, i > 0$. Segue do Teorema 4.2.4 que

$$U \simeq (\mathbb{Z}_p[G/H_1])^{r_1} \oplus (\mathbb{Z}_p[G/H_2])^{r_2} \oplus ... (\mathbb{Z}_p[G/H_{p+1}])^{r_{p+1}},$$

portanto, U é um $\mathbb{Z}_p G$-módulo de permutação. Com essa observação acabamos de provar o

Teorema 4.4.4. *Seja $U \in \mathcal{L}_0$. Então U é um $\mathbb{Z}_p G$-módulo de permutação se, e somente se,*

1. *U^N e U_N são $\mathbb{Z}_p[G/N]$-módulos de permutação e*
2. *$Je_iU = pe_iU \ \forall i = 0, 1, ..., p+1$.*

Teorema 4.4.5. *Seja $p = 2$ e $U \in \mathcal{L}_0$. Então U é um $\mathbb{Z}_2 G$-módulo de permutação se, e somente se, U^N e U_N são $\mathbb{Z}_2[G/N]$-módulos de permutação.*

Demonstração. De fato, para $p = 2$, temos $Je_i = 2e_iU \ \forall i = 0, 1, 2, 3$, pois dado $g \in G$, $(1 - g)$ age como uma multiplicação por 0 ou por 2 em Λ_i. Logo, o resultado segue do teorema anterior. □

Em posse desses resultados vamos estabelecer o nosso principal resultado: em geral, a Condição 1 no Teorema 3.2.3 não caracteriza os $\mathbb{Z}_p G$-módulos de permutação. Para tanto, consideremos $p = 3$ e passamos a analisar os $\mathbb{Z}_3 G$-reticulados reduzidos e seus diagramas associados.

Considere o seguinte $\mathbb{F}_3G$-módulo V com base $\{v_1, v_2, v_3, v_4, v_5\}$ possuindo a seguinte multiplicação

$$\begin{aligned} nv_1 = cv_1 = v_1, \\ nv_2 = v_2, cv_2 = v_1 + v_2 \\ nv_3 = v_3 + v_1, cv_3 = v_3 \\ nv_4 = cv_4 = v_1 + v_4, nc^2v_4 = v_4 \\ nv_5 = v_1 + v_5 = c^2v_5, \\ cv_5 = n^2v_5 = 2v_1 + v_5, \\ ncv_5 = v_5. \end{aligned}$$

Assim, vemos que $V = \sum_{i \neq j} V_i, i, j \in \{0, 1, ..., 4\}$ onde

$$V_0 = \langle v_1, v_3 + v_5 + v_4, -v_3 + v_2 + v_5 \rangle, V_1 = \langle v_1, v_2 \rangle, V_2 = \langle v_1, v_3 \rangle,$$

$$V_3 = \langle v_1, v_5 \rangle, V_4 = \langle v_1, v_4 \rangle.$$

Observe que

$$V_0/JV_0 = V_0, V_1/JV_1 = \langle v_2 + JV_1 \rangle, V_2/JV_2 = \langle v_3 + JV_2 \rangle, V_3/JV_3 = \langle v_5 + JV_3 \rangle,$$

$$V_4/JV_4 = \langle v_4 + JV_4 \rangle.$$

Lembramos que se $g \notin H_i$, então $\{e_i, ge_i, ..., g^{p-2}e_i\}$ é uma $\mathbb{Z}_p$base de Λ_i. Escolha três copias de Λ_0 e denote um gerador de cada cópia por $w_i, i = 0, 1, 2$. Utilizando a seguinte notação:

$$\begin{aligned} w_3 = e_1, w_4 = ce_1 \\ w_5 = e_2, w_6 = ne_2 \\ w_7 = e_3, w_8 = ne_3 \\ w_9 = e_4, w_{10} = ne_4, \end{aligned}$$

temos

$$\Lambda_0^3 = \langle w_0, w_1, w_2 \rangle$$

$$\Lambda_1 = \langle w_3, w_4 \rangle; cw_3 = w_4, cw_4 = -w_3 - w_4, nw_4 = w_4, nw_3 = w_3,$$

$$\Lambda_2 = \langle w_5, w_6 \rangle; nw_5 = w_6, nw_6 = -w_5 - w_6, cw_5 = w_5, cw_6 = w_6,$$

$$\Lambda_3 = \langle w_7, w_8 \rangle; nw_7 = w_8, nw_8 = -w_7 - w_8, cw_7 = n^2w_7, cw_8 = n^2w_8,$$

$$\Lambda_4 = \langle w_9, w_{10} \rangle; nw_9 = w_{10}, nw_{10} = -w_9 - w_{10}, cw_9 = nw_9, cw_{10} = nw_{10}.$$

Defina os seguintes $\mathbb{Z}_3$-homomorfismos

$$\phi_0 : \Lambda_0^3 \to V_0$$

$$w_0 \mapsto v_1$$

$$w_1 \mapsto v_3 + v_5 + v_4$$

$$w_2 \mapsto -v_3 + v_2 + v_5,$$

$$\phi_1 : \Lambda_1 \mapsto V_1$$

$$w_3 \mapsto v_1 - v_2, w_4 \mapsto -v_2,$$

$$\phi_2 : \Lambda_2 \mapsto V_2$$

$$w_5 \mapsto v_1 - v_3, w_6 \mapsto -v_3,$$

$$\phi_3 : \Lambda_3 \mapsto V_3$$

$$w_7 \mapsto v_1 - v_5, w_8 \mapsto -v_5,$$

$$\phi_4 : \Lambda_4 \mapsto V_4$$

$$w_9 \mapsto v_1 - v_4, w_{10} \mapsto -v_4.$$

Vamos verificar que esses são $\mathbb{Z}_pG$-homomorfismos.

$$\phi_1(cw_3) = \phi_1(w_4) = -v_2 = c(v_1 - v_2) = c\phi_1(w_3),$$

$$\phi_1(cw_4) = \phi_1(-w_3 - w_4) = v_2 - v_1 + v_2 = -v_1 - v_2 = c(-v_2) = c\phi_1(w_4);$$

$$\phi_2(nw_5) = \phi_2(w_6) = -v_3 = n(v_1 - v_3) = n\phi_2(w_5),$$

$$\phi_2(nw_6) = \phi_2(-w_5 - w_6) = v_3 - v_1 + v_3 = -v_3 - v_1 = n(-v_3) = n\phi_2(w_6);$$

$$\phi_3(nw_7) = \phi_3(w_8) = -v_5 = n(v_1 - v_5) = n\phi_3(w_7),$$

$$\phi_3(nw_8) = \phi_3(-w_7 - w_8) = v_5 - v_1 + v_5 = -v_5 - v_1 = n(-v_5) = n\phi_3(w_8),$$

$$\phi_3(cw_7) = \phi_3(n^2w_7) = n^2\phi_3(w_7) = c\phi_3(w_7),$$

$$\phi_3(cw_8) = \phi_3(n^2w_8) = n^2\phi_3(w_8) = c\phi_3(w_8);$$

$$\phi_4(nw_9) = \phi_4(w_{10}) = -v_4 = n(v_1 - v_4) = n\phi_4(w_9),$$

$$\phi_4(nw_{10}) = \phi_4(-w_9 - w_{10}) = v_4 - v_1 + v_4 = n(-v_4) = n\phi(w_{10}).$$

É claro que $\phi_i, i = 0, 1, 2, 3, 4$, é sobrejetiva, também observe que definindo

$$\widehat{\phi_i} : \Lambda_i \to V_i/JV_i$$

$$x_i \mapsto \phi_i(x_i) + JV_i,$$

temos $\ker \widehat{\phi}_i = JV_i$, assim,

$$\bar{\phi}_i : \Lambda_i/J\Lambda_i \to V_i/JV_i$$

$$x_i + J\Lambda_i \mapsto \phi_i(x_i) + JV_i,$$

é um isomorfismo. Fica verificado que $(V; V_0, ..., V_{p+1})$ é um objeto em $\mathfrak{V}$.

Agora, vamos verificar que o reticulado U, associado ao diagrama acima, satisfaz U^N e U_N de permutação. Primeiramente, observe que o submódulo maximal trivial de V_1 é gerado por $v_1 \in V_0$, assim, pelo Teorema 4.4.1, U^N é de permutação. Dado $v \in \sum_{i\neq 0,1} V_i$ com $(n-1)v = 0$, temos $v = \lambda_1 v_1 + \lambda_2 v_3 + \lambda_3 v_4 + \lambda_4 v_5$, $\lambda_j \in \mathbb{Z}_3$, e $(n-1)v = (\lambda_2+\lambda_3+\lambda_4)v_1 = 0$, então $\lambda_2 + \lambda_3 + \lambda_4 \in 3\mathbb{Z}_3$ e, daí,

$$v = \lambda_1 v_1 + (-\lambda_3 - \lambda_4)v_3 + \lambda_3 v_4 + \lambda_4 v_5 = \lambda_1 v_1 + \lambda_3(v_4 - v_3) + \lambda_4(v_5 - v_3).$$

Note que

$$v_5 - v_3 = (-v_3 + v_2 + v_5) - v_2 \in V_0 + V_1,$$

$$v_4 - v_3 = (v_5 - v_3) + (v_3 + v_5 + v_4) + (-v_3 + v_2 + v_5) - v_2 \in V_0 + V_1,$$

também temos

$$\langle v_1 \rangle = V_2 \cap (V_3 + V_4) = V_3 \cap (V_2 + V_4) = V_4 \cap (V_2 + V_3).$$

Então, pelo Teorema 4.4.2, U_N é um reticulado.

Observe que se $v \in (V_1+V_3+V_4)\cap(V_0+V_2)$, então $(c-1)v = 0$. Dado, $v \in V_1+V_3+V_4$ existem escalares $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{Z}_p$ (únicos módulo o ideal $3\mathbb{Z}_3$) tais que

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_4 + \lambda_4 v_5.$$

Assim,

$$(c-1)v = (\lambda_2 + \lambda_3 + 2\lambda_4)v_1 = 0 \Leftrightarrow \lambda_2 + \lambda_3 + 2\lambda_4 \in 3\mathbb{Z}_3,$$

logo

$$v = \lambda_1 v_1 + (-\lambda_3 - 2\lambda_4)v_2 + \lambda_3 v_4 + \lambda_4 v_5 =$$

$$= \lambda_1 v_1 + \lambda_3(v_4 - v_2) + \lambda_4(v_5 - 2v_2).$$

Observe que $v_2 + v_5 = v_5 - 2v_2 \in V_0 + V_2$ e $v_4 + v_5 \in V_0 + V_2$, assim, $v_4 - v_2 \in V_0 + V_2$. Logo $v \in V_0 + V_2$, e segue que

$$(V_0 + V_2) \cap (V_1 + V_3 + V_4) = \langle v_1, v_4 - v_2, v_5 - v_2 \rangle.$$

Claramente

$$\langle v_1 \rangle = V_1 \cap (V_2 + V_3 + V_4) = V_2 \cap (V_1 + V_3 + V_4) =$$

$$= V_3 \cap (V_1 + V_2 + V_4) = V_4 \cap (V_1 + V_2 + V_3),$$

e V também satisfaz a Condição 1 do Teorema 4.4.3. Por outro lado, dado $v \in (V_0 + V_2) \cap (V_1 + V_3 + V_4)$ temos

$$v = \lambda_1 v_1 + (-\lambda_3 - 2\lambda_4)v_2 + \lambda_4 v_5 + \lambda_3 v_4,$$

observe que dado $v' \in (V_0 + V_1) \cap (V_2 + V_3 + V_4)$, temos $(n-1)v' = 0$, também observe que

$$(c-1)v_5 = (n^2 - 1)v_5 = (n-1)(n+1)v_5$$

e $(c-1)v_4 = (n-1)v_4$. Assim,

$$(n-1)(v' + (n+1)\lambda_4 v_5 + \lambda_3 v_4) = (n+1)\lambda_4 v_1 + \lambda_3 v_1 = (2\lambda_4 + \lambda_3)v_1 \in V_1 \cap (V_2 + V_3 + V_4) = \langle v_1 \rangle.$$

Agora,

$$(c-1)(\lambda_1 v_1 + (-\lambda_3 - 2\lambda_4)v_2) = -(2\lambda_4 + \lambda_3)v_1,$$

e logo

$$(c-1)(\lambda_1 v_1 + (-\lambda_3 - 2\lambda_4)v_2) = -(n-1)(v' + (n+1)\lambda_4 v_5 + \lambda_3 v_4),$$

onde $v' \in (V_0 + V_1) \cap (V_2 + V_3 + V_4)$ e $\lambda_1 v_1 + (-\lambda_3 - 2\lambda_4)v_2 + \lambda_4 v_5 + \lambda_3 v_4 \in V_0 + V_2$. Portanto, a Condição 2 do Teorema 4.4.3 também é satisfeita. Segue do Teorema 4.4.3 que U_N é de permutação.

Como V tem ação não trivial de G, U não pode ser um $\mathbb{Z}_3 G$-módulo de permutação pelo Teorema 4.4.4.

Alternativamente, poderíamos ter calculado direto que

$$U_N \simeq \mathbb{Z}_3[G/N] \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \simeq U^N$$

por encontrar uma base para o reticulado U como fizemos nos exemplos da Seção 4.3. Se assim fosse feito, encontraríamos que com respeito a uma base de U as matrizes de n e c

são respectivamente

$$\begin{pmatrix}
1 & 0 & -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -2 & 0 & 0 & -1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & -2 & 0 & -1 & -1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & -2 & -1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & -3 & 0 & 0 & -1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & -3 & 0 & -1 & -1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & -3 & -1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

e

$$\begin{pmatrix}
1 & -1 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & -2 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & -2 & -1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & -3 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 3 & 0 & 1 & 1 & 0 & 0 & -2 & 0 \\
0 & 0 & 0 & 0 & -3 & -1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

Referências Bibliográficas

[1] GOUVEA. F.Q. *p-adic Numbers An Introduction*. Springer, 3 edition, 2020.

[2] KARPILOVSKY. Gregory. *Induced Modules Over Group Algebras*. North-Holland, 1 edition, 1990.

[3] MATSUMURA. HIDEYUKI. *Commutative ring theory*. Cambridge University Press, 1 edition, 2006.

[4] ATIYAH. M.F.; MCDONALD. I.G. *Introduction to Commutative Algebra*. Addison-Wesley, 1 edition, 1969.

[5] ZALESSKII. P.A.; MACQUARRIE. J.W. A characterization of permutation modules extending a theorem of Weiss. *Doc. Math*, 25:1159–1169, 2020.

[6] BUTLER. M.C.R. The 2-adic representations of Kleins's four group. In *Proceedings of the Second International Conference on The Theory of Groups*, pages 197–203. Springer, 1973.

[7] BUTLER. M.C.R. On the classification of local integral representations of finite abelian p-groups. In *Representations of Algebras*, pages 54–70. Springer, 1974.

[8] WEBB. Peter. *A Course in Finite Group Representation Theory*. Cambridge University Press, 1 edition, 2016.

[9] HELLER A.; REINER.I. Representations of cyclic groups in rings of integers. *Annals of Mathematics*, 76:73–92, 1962.

[10] DUMMIT. D.S.; FOOTE. R.M. *Abstract Algebra*. John Wiley and Sons, 3 edition, 2004.

[11] GARCIA. A.; LEQUAIN. Y. *Elementos de Álgebra*. IMPA, 6 edition, 2018.