Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Extensões Cíclicas de Grupos Pro-p Livres e Representações Inteiras p-Ádicas

por
Anderson Luiz Pedrosa Porto

Brasília
2009

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Extensões Cíclicas de Grupos Pro-p Livres e Representações Inteiras p-Ádicas

por

Anderson Luiz Pedrosa Porto*

Tese apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

DOUTOR EM MATEMÁTICA

Brasília, 6 de novembro de 2009.

Comissão Examinadora:

Prof. Dr. Pavel A. Zalesskii - UnB (Orientador)

Prof. Dr. Pavel Shumyatsky - UnB

Prof. Dr. Aline Gomes da Silva Pinto - UnB

Prof. Dr. Mikhajolo Dokuchaev - USP

Prof. Dr. Dessislava Hristova Kochloukova - Unicamp

*O autor foi bolsista da CAPES e CNPQ durante parte da elaboração deste trabalho.

Abstract

Let F be a free pro-p group of finite rank and consider C_{p^n} the cyclic group of order p^n. In this thesis we exhibit the $\mathbb{Z}_pC_{p^n}$-lattices that can be obtained by factoring $F \rtimes C_{p^n}$ (semi-direct product pro-p) by the commutator subgroup $F' = \overline{[F, F]}$.

Keywords: virtually free pro-p groups, integral p-adic representations.

Resumo

Seja F um grupo pro-p livre de posto finito e considere C_{p^n} o grupo cíclico de ordem p^n. Nessa tese nós exibimos os $\mathbb{Z}_p C_{p^n}$-reticulados que podem ser obtidos pela fatoração de $F \rtimes C_{p^n}$ (produto semi-direto pro-p) pelo subgrupo comutador $F' = \overline{[F, F]}$.

Palavras-chave: grupos pro-p virtualmente livres e representações inteiras p-ádicas.

Agradecimentos

Primeiramente agradeço à Deus (Jesus Cristo) por ter me dado a vida e por ter me fortalecido nos momentos mais difícies do meu trabalho, por ter me dado paciência e tranquilidade para prosseguir. Agradeço a ele as ilustres idéias que ele me deu em sonhos e que me levaram a conquistar nesse ano de 2009 todos os objetivos que almejei, além daquelas que eu nem espereva.

Agradeço em especial a minha esposa Nascilaine Osanilha Costa Pedrosa, por todo o seu apoio e paciência durante a realização desse que para nós foi um encançável trabalho. Lembro-me muito bem dos momentos em que chegava em casa angustiado pelos fracassos que eu tinha durante alguns semestres do meu doutorado e que ela sabiamente sempre me entusiasmava e me dava forças para prosseguir. Na te amo.

A meu filho André, dedico não só o meu trabalho, mas toda a minha vida, voçê é muito especial para o papai. Espero que daqui em diante o papai tenha mais tempo de lhe dar mais atenção, te amo.

A minha família: Afonso Porto (Pai), Arlete (Mãe)(in memoriam), Amanda (irmã), Anna (irmã), João Felipe (sobrinho), Andréia e Lavínia (sobrinho) por onde comecei toda a minha caminhada, amo todos vocês e está conquista não é só minha é de todos nós. Ê saudades de Januária! As minhas vós Josefa e Maria, ao tio Ailton e família, a tia Zezina, tia Sandra e família.

A minha nova família de Diamantina que tanto me auxiliaram nessa etapa final da conclusão de meu trabalho, são eles: Dona Lucinda (êta comidinha boa, gente), Neil, Elisa, Joana, Seu João Vicente.

Agradeço ao meu orientador o Prof. Dr. Pavel A. Zalesskii pelos seus ensinamentos prestados em todos os cursos que eu eu fiz, além da orientação e direção que me deste para a obtenção dos resultados que conseguimos. Fica aqui os agradecimentos pelos papos descontraídos que tivemos e pelas palavras de incentivo que sempre me foram passados.

Sou grato também aos professores que aceitaram participar da banca e pelas sugestões que foram dadas para uma melhor conclusão do meu trabalho, em especial agradeço os professores Prof. Dr. Mikhajolo Dokuchaev - USP, pelas conversas que tivemos nos congressos, pelo incentivo e pelas observações que me ajudaram a enriquecer a conclusão do meu trabalho. Também o meu agradecimento à Prof. Dr. Dessislava Hristova Kochloukova - Unicamp, pelas diversas sugestões apontadas para a correção de minha tese.

Agradeço aos ilustríssimos professores do departamento que de forma brilhante me levaram a adquirir um rico conhecimento em várias áreas da matemática, são eles: Alexei Krassilnikov, Pavel Shumyatsky, Aline Pinto (pelas observações feitas para a melhora na escrita da tese e por todo conhecimento que me fora passado dentro e fora da sala de aula no estudo de lgebra Homológica), Hemar Godinho, Raderson, Cátia Gonçalvez, Rudolf Maier, Mauro Patrão.

Ao pessoal que dá o suporte técnico ao departamento, os mais sinceros agradecimentos por todo o auxílio prestado por todos esses anos que passei por aí: a Tânia, a Eveline, ao Gari, ao Manoel e até o Luisão (êta figura).

Aos professores da UFV que tanto me intusiasmaram para que eu prosseguisse os meus estudos, são eles: Olímpio, Rosane, Brás, Laerte, Sukarno, Oderli, Lana e a Marinês (por ter me mostrado que a álgebra era essa coisa tão bonita que eu me apaixonei).

Sobre os colegas de ralação, nem preciso comentar, saudades de vocês, espero que não venhamos a nos esquecer, são eles: Evander, Walter, Wagner, Magno, Luciene, Abilio, Nilton, Luciana, Luverci, Zhou, Leonardo, Leonardo Amorim, Allan Moura, Willian Vieira, Daniel, Felipe, os gêmeos, Tertuliano, Flávia, Igor, Aline, Jhone, Jorge, Gilberto, Fágner, Fabiana, Thiago, Eunice, Gaúcho, Anielle, Ivonildes, Miguel, Elson, Wallison Lustrino, dentre outros.

Deixo também um agradecimento aos meus ilustrissímos colegas de trabalho da UFVJM, em especial ao Prof. Dr Paulo César por todo incentivo e apoio que me deu para a finalização do meu trabalho.

Ao suporte financeiro prestado pelo CNPQ e CAPES, meus sinceros elogios.

Sumário

Lista de Símbolos

$\mathbb{N},\ \mathbb{Z},\ \mathbb{P}$	Os conjuntos dos números naturais, inteiros e primos.
$\mathbb{Z}_p,\ \hat{\mathbb{Z}}$	Os inteiros p-ádicos, completamento profinito de $\mathbb{Z}$.
$G, M, \ldots$	Grupos, módulos e anéis profinitos.
$G^{\text{abs}},\ M^{\text{abs}}, \ldots$	Grupos abstratos.
$x^y = y^{-1}xy$	O conjugado do elemento x por y.
$H \cong G$	H é isomorfo à G (como grupos, módulos ou anéis profinitos).
$H \leq_c G,\ H \lhd_c G$	H um subgrupo fechado de G, H é um subgrupo normal fechado próprio do grupo G.
$\overline{\langle X \rangle}$	Subgrupo fechado gerado topologicamente por X.
$C_G(H),\ N_G(H)$	Centralizador, normalizador de um subgrupo fechado H em G.
H^G	Fecho normal de H em G.
$A * B,\ A \coprod B$	Produto livre de grupos, produto livre pro-p de grupos pro-p.
$A \rtimes B$	Produto semi-direto ou Produto semi-direto de grupos pro-p.
$G' = \overline{[G, G]}$	Subgrupo derivado de um grupo profinito G.
$\overline{F} = \frac{F}{F'}$	A abelianização do grupo pro-p livre F.
$M \oplus N$	Soma direta de módulos.
$\twoheadrightarrow, \hookrightarrow$	Aplicação sobrejetora, Aplicação injetora .
f.g.	Finitamente gerado .
$x \circ \alpha$	A ação de x sobre o elemento α.
$\mathrm{ann}_R(M)$	O anulador do R-módulo M.
$\mathrm{rad}(M)$	O radical do R-módulo M.
$\mathrm{r}_p(M)$	O posto do $\mathbb{Z}_p$-módulo livre M.
$[[RG]],\ [RG] = RG$	Anel de grupo completo, Anel de grupo abstrato.

$B \lhd \cdot M$	B é um R-submódulo maximal de M.
$\left(H^{\text{abs}}\right)_{\hat{p}}$	Completamento pro-p de H^{abs}.
$\mathbb{Z}_p[t]$	O anel de polinômios sobre a variável t.
C_{p^n}	Grupo cíclico de ordem p^n.
F_r	Grupo pro-p livre de posto r.
F_r^{abs}	Grupo livre abstrato de posto r.

Introdução

Seja H um grupo finito e R um anel comutativo com 1. Nós dizemos que M é um RH-reticulado, se o mesmo é um RH-módulo que é R-livre de torção e finitamente gerado como um R-módulo.

Em 1938, Diederichsen em [2], mostrou que a quantidade de $\mathbb{Z}C_p$-reticulados indecomponíveis e não isomorfos é finita e o mesmo deu um exemplo incorreto mostrando que a quantidade de $\mathbb{Z}C_4$-reticulados indecomponíveis e não isomorfos era infinita. Contudo, mais tarde Roiter ([23]) e Troy ([30]), mostraram independentemente que essa quantidade é igual a 9.

Considere $\mathbb{Z}_p$ como sendo o anel dos inteiros p-ádicos. No contexto da teoria dos grupos pro-p, $\mathbb{Z}_p$ denotará o grupo pro-p livre de posto 1.

Defina $\mathrm{n}(RH)$ como sendo o número de RH-reticulados indecomponívies e não-isomorfos.

Em [9], Reiner e Heller mostraram que:

$$\mathrm{n}(\mathbb{Z}_p C_{p^n}) < \infty \text{ se, e somente se,} \mathrm{n}(\mathbb{Z} C_{p^n}) < \infty. \tag{1}$$

Assim, para sabermos sobre a finitude das representações inteiras, basta conhecermos a finitude das representações p-ádicas.

Em Berman-Gudivok [3] e [4], Reiner-Heller [9], [10] e em Curtis-Reiner [5], podemos encontrar o seguinte resultado:

Teorema: Seja G um grupo finito. Então o número de representações inteiras indecomponíveis de G é finito se, e somente se, os subgrupos de Sylow de G são de ordem $\leq p^2$.

Nos trabalhos [9] e [10] de Reiner e Heller e no livro de Curtis-Reiner [5], nós temos que:

$$n(\mathbb{Z}_p C_p) = 3, \;\; n(\mathbb{Z}_p C_{p^2}) = 4p + 1 \;\text{ e }\; n(\mathbb{Z}_p C_{p^s}) = \infty, \tag{2}$$

onde $s \geq 3$.

Observamos que a não finitude de $n(\mathbb{Z}_p C_{p^s})$ onde $s \geq 3$, também segue do **Teorema** acima juntamente com (1).

Além disso, nesses trabalhos os autores exibiram todos os reticulados nos casos p e p^2, contudo eles afirmaram que esta tarefa é praticamente impossível nos casos p^s onde $s \geq 3$, com exceção do caso $2^3 = 8$ (as representações mansas, veja Yakolev [31]).

Nós dizemos que um $\mathbb{Z}_pH$-reticulado M se levanta para um grupo pro-p virtualmente livre $G = F \rtimes H$, onde F é um grupo pro-p livre de posto finito se o $\frac{G}{F}$-módulo $\overline{F} = \frac{F}{F'}$ é isomorfo à M como um $\mathbb{Z}_pH$-módulo.

Seja $\mathbb{Q}_p$ o corpo p-ádico do anel de valoração $\mathbb{Z}_p$. Considere $\phi_p(x)$ como sendo o polinômio ciclotômico de ordem p e seja θ_p uma de suas raízes primitivas p-ésimas da unidade. Como podemos ver em Neukirch [19], temos que $\mathbb{Z}_p[\theta_p]$ é o único anel de valoração discreta completo (à menos de isomorfismo) do corpo local $\mathbb{Q}_p[\theta_p]$ contendo $\mathbb{Z}_p$.

Pavel Zalesskii e Wolfgang Herfort, mostraram no Lema 6 do artigo [8], uma relação muito interessante entre as representações p-ádicas do grupo C_p e certos grupos pro-p virtualmente livres (também veja o Teorema 51).

Como consequência deste lema, temos que:

- $\mathbb{Z}_p$ se levanta para $C_p \times \mathbb{Z}_p$;
- $\mathbb{Z}_p[\theta_p]$ se levanta para $C_p \coprod C_p$;
- $\mathbb{Z}_pC_p$ se levanta para $C_p \coprod \mathbb{Z}_p$.

Como podemos ver em [9]:

$$\mathbb{Z}_p, \mathbb{Z}_p[\theta_p] \text{ e } \mathbb{Z}_pC_p$$

são os únicos $\mathbb{Z}_pC_p$-reticulados indecomponíveis e não-isomorfos (para mais detalhes, veja também a Seção 1.4. desta tese).

Logo cada um dos $\mathbb{Z}_pC_p$-reticulados indecomponíveis de Reiner e Heller se levantam para algum grupo pro-p da forma $F \rtimes C_p$.

Uma questão natural que surgiu e que fora proposta por Pavel Zalesskii é a seguinte:

Quando um $\mathbb{Z}_pH$-reticulado dado se levanta para algum grupo profinito virtualmente livre?

Nessa tese, nós resolvemos esta questão para o caso em que $H \cong C_{p^n}$, onde $n \in \mathbb{N}$. Em resumo, obtivemos os seguintes resultados, no Capítulo 2, dessa tese:

Teorema 77(Teorema Principal) Considere $n \in \mathbb{N}$. Seja

$$G \cong F \rtimes C_{p^n}$$

um produto semi-direto pro-p de um grupo pro-p livre de posto finito por C_{p^n}. Suponha que a representação de C_{p^n} sobre $\overline{F} = \frac{F}{F'}$ induzida pela conjugação, é uma $\mathbb{Z}_p$-representação fiel e indecomponível. Então $\overline{F} = \frac{F}{F'}$ é de um dos tipos dados logo abaixo:

1. $$\overline{F} \cong \text{Ker } (\mathbb{Z}_pC_{p^n} \twoheadrightarrow 0) \cong \mathbb{Z}_pC_{p^n},$$

2.
$$\overline{F} \cong \text{Ker}\left(\mathbb{Z}_p C_{p^n} \twoheadrightarrow \mathbb{Z}_p C_{p^m}\right),$$
como um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, tal que $m \in \mathbb{N}$ satisfaz $0 \leq m \leq (n-1)$.

Além disso, os únicos $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis, com C_{p^n}-ação fiel, que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$, são dos tipos **1) e 2)** dados nesse Teorema.

Também mostramos que tais $\mathbb{Z}_p C_{p^n}$-reticulados do Teorema 77, se levantam respectivamente para os seguintes grupos pro-p virtualmente livres:

$$C_{p^n} \coprod \mathbb{Z}_p \quad \text{e}\ C_{p^n} \coprod C_{p^t},$$

onde $t \in \{1, \ldots, n\}$ (veja o Teorema 78).

A partir desses últimos resultados, nós exibimos as representações não-fiéis que se levantam e obtivemos os seguintes resultados:

Teorema 79 Seja $n \in \mathbb{N}$. Considere $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito e $C_{p^n} = \langle x \rangle$. Seja $k \in \{1, 2, \ldots, n\}$, de maneira que C_{p^k} seja o subgrupo maximal de C_{p^n} com a propriedade de agir trivialmente sobre $\overline{F} = \frac{F}{F'}$. Além disso, suponha que C_{p^n} age indecomponivelmente sobre $\overline{F}$. Então $\overline{F} = \frac{F}{F'}$ é de um dos tipos dados logo abaixo:

1.
$$\overline{F} \cong \text{ Ker}\left(\mathbb{Z}_p C_{p^{(n-k)}} \twoheadrightarrow 0\right) \cong \mathbb{Z}_p C_{p^{(n-k)}},$$

2.
$$\overline{F} \cong \text{Ker}\left(\mathbb{Z}_p C_{p^{(n-k)}} \twoheadrightarrow \mathbb{Z}_p C_{p^{m'}}\right)$$
como um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, tal que m' satisfaz $0 \leq m' \leq n-k-1$.

Além disso, esses são os únicos $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$, com as propriedades requeridas por esse Teorema.

Teorema 81 Seja $n \in \mathbb{N}$ e $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto $s \geq 2$. Suponhamos que $\overline{F}$ seja um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, onde C_{p^k} é o subgrupo maximal próprio e não-trivial de C_{p^n} agindo trivialmente sobre $\overline{F}$. Então

$$G \cong C_{p^n} \coprod_{C_{p^k}} \left(C_{p^k} \times \mathbb{Z}_p\right) \quad \text{ou} \quad G \cong C_{p^n} \coprod_{C_{p^k}} C_{p^t},$$

onde $t \in \{k+1, \ldots, n\}$.

Assim, foi possível exibir a quantidade exata de $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p virtualmente livre, este fato é o conteúdo do seguinte Corolário:

Corolário 82 Seja $n \in \mathbb{N}$. Considerem todos os $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis não-isomorfos. A quantidade de tais reticulados que se levantam para grupos pro-p da forma $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito, é igual a

$$\frac{(n+1)(n+2)}{2}.$$

Temos mais uma Proposição:

Proposição 83 Considere $n \in \mathbb{N}$, tal que $n \geq 2$. Então nem todos os $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis e não-isomorfos, se levantam para algum grupo pro-p da forma

$$F \rtimes C_{p^n},$$

onde F é um grupo pro-p livre de posto finito.

Por fim, no Capítulo 4 nós mostramos que basta estudar os levantamentos para $\mathbb{Z}_p C_{p^n}$-reticulados indecomponívieis, já que o caso dos decomponíveis, recai em uma soma direta finita de $\mathbb{Z}_p C_{p^n}$-reticulados indecomponívieis que se levantam. De forma mais precisa provamos os seguintes Teoremas:

Teorema 94 Considere $n \in \mathbb{N}$. Seja $G \cong F \rtimes C_{p^n}$, um produto semi-direto pro-p de um grupo pro-p livre F de posto finito, por C_{p^n}. Então $\overline{F}$ é uma soma direta única de $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis, que se levantam para algum grupo pro-p virtualmente livre da forma $F_k \rtimes C_{p^n}$.

Teorema 95 Seja M um $\mathbb{Z}_p C_{p^n}$-reticulado. Suponhamos que $M = \bigoplus_{i \in J < \infty} M_i$, onde os M_i são $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p virtualmente livre $F^i \rtimes C_{p^n}$. Então existe um grupo pro-p virtualmente livre $\tilde{G} = \tilde{F} \rtimes C_{p^n}$, tal que M se levanta para $\tilde{G}$ e $\tilde{F}$ é um grupo pro-p livre de posto finito.

Capítulo 1

Preliminares

Nesse capítulo vamos descrever vários fatos conhecidos à cerca da **Teoria de Grupos, Anéis e Módulos Pro-p**, sem demonstrá-los.

Também faremos uma seção para apresentarmos alguns fatos sobre álgebras de grupo.

Dedicaremos uma seção para a apresentação do **Teorema de Krull-Schmidt-Azumaya** que poderá ser encontrado em [1], [5] e [12].

Logo a seguir, veremos alguns fatos sobre **Módulos Indecomponíveis** que poderá ser visto em **Kasch** [12].

Por fim, vamos dedicar uma seção ao estudo das representações p-ádicas de Reiner e Heller, que podem ser vistos em [3], [5], [9] e [10].

1.1 Grupos Profinitos e Pro-p

Nessa seção vamos relembrar sem demonstrar alguns fatos da **Teoria de Grupos Profinitos** que nos serão muito úteis nessa tese.

1.1.1 Produto Semi-Direto Profinito e Grupos Pro-p Livres

Vamos relembrar nessa subseção, a definição de produto semi-direto profinito (pro-p). Para tanto, vamos nos basear nos livros de Wilson [32] e Ribes-Zalesskii [22].

Definição 1. *Seja G um grupo profinito(pro-p) que tem um subgrupo normal fechado K e um subgrupo fechado C. Um **produto semi-direto profinito(pro-p)** ou uma **extensão profinita (pro-p) cindida** de K por C, é um produto semi-direto de grupos abstratos, cuja ação é uma aplicação contínua. Notação:*

$$G = K \rtimes C = C \ltimes K.$$

O subgrupo C de G é dito ser um complemento para K em G. No livro de Wilson [32], página 22, temos a seguinte observação:

Observação 2. *Se $G = K \rtimes C$, então cada elemento $g \in G$ é escrito como $g = k'c' = ck$, para certos elementos unicamente determinados $c, c' \in C$ e $k, k' \in K$.*

Grupos Pro-p Livres

Seja X um conjunto finito com topologia discreta. Considere $F^{\text{abs}}(X)$ o grupo livre abstrato com base X (veja por exemplo Lyndon [16] ou Serre [29]). Tome a seguinte coleção de subgrupos de $F^{\text{abs}}(X)$:

$$\mathcal{N} = \left\{ N \lhd F^{\text{abs}}(X) \mid \frac{F^{\text{abs}}(X)}{N} \text{ é um } p\text{-grupo finito} \right\}.$$

Nós definimos o grupo pro-p livre com base X, como sendo o completamento de $F^{\text{abs}}(X)$ com respeito a coleção $\mathcal{N}$ (base filtrada para baixo e não-vazia), bem melhor,

$$F_{\hat{p}}(X) := \varprojlim_{N \in \mathcal{N}} \left[\frac{F^{\text{abs}}(X)}{N} \right] = \left(F^{\text{abs}}(X) \right)_{\hat{p}}.$$

Para mais detalhes consulte Wilson [32] ou Ribes-Zalesskii [22], capítulo 3. Nós denotaremos um grupo pro-p livre de posto n, simplesmente por F_n e o grupo livre abstrato de posto m, como sendo igual a F_m^{abs}.

1.1.2 O Produto Livre Amalgamado Pro-p e o Produto Livre Pro-p

Sejam G_1 e G_2 grupos pro-p. Considerem $f_i : H \longrightarrow G_i \, (i = 1, 2)$ monomorfismos contínuos de grupos pro-p. Um **produto livre amalgamado pro-p** de G_1 e G_2 com subgrupo amalgamado H, é definido pelo "pushout":

$$\begin{tikzcd} H \arrow[r, "f_1"] \arrow[d, "f_2"'] & G_1 \arrow[d, "\phi_1"] \\ G_2 \arrow[r, "\phi_2"'] & G \end{tikzcd}$$

na categoria de grupos pro-p, ou seja, um grupo pro-p G juntamente com homomorfismos contínuos $\phi_i : G_i \longrightarrow G \, (i = 1, 2)$ satisfazendo a seguinte propriedade universal: para quaisquer pares de homomorfismos contínuos $\Psi_1 : G_1 \longrightarrow K$, $\Psi_2 : G_2 \longrightarrow K$ em um grupo pro-p K, tal que $\Psi_1 \circ f_1 = \Psi_2 \circ f_2$, existe um único homomorfismo contínuo $\Psi : G \longrightarrow K$, tal que o seguinte diagrama é comutativo:

$$\begin{tikzcd}
H \arrow[r, "f_1"] \arrow[d, "f_2"'] & G_1 \arrow[d, "\phi_1"] \arrow[ddr, bend left, "\Psi_1"] & \\
G_2 \arrow[r, "\phi_2"'] \arrow[drr, bend right, "\Psi_2"'] & G \arrow[dr, dotted, "\Psi"] & \\
 & & K
\end{tikzcd}$$

O Lema a seguir não será demonstrado:

Lema 3. *Sejam G_1, G_2 e H grupos pro-p. Suponhamos que $f_i : H \longrightarrow G_i$ $(i = 1, 2)$ sejam monomorfismos contínuos. O produto livre amalgamado pro-p de G_1, G_2 com subgrupo amalgamado H existe e é único.*

Demonstração. Ver [22], páginas 376 e 377. ∎

Observação 4. *Indutivamente podemos definir o produto livre amalgamado de grupos pro-p G_i $(i = 1, 2, \ldots, n)$ com um subgrupo amalgamado H.*

Observação 5. *Na situação abstrata os homomorfismos canônicos de G_i em $G_1 *_H G_2$ são monomorfismos de grupos abstratos para cada $i = 1, 2$ (veja o Corolário 1 do Teorema 11 de Serre [29], página 45). Em contraste com o caso abstrato, o exemplo 9.2.9. da página 380 do livro de Ribes-Zalesskii [22], mostra que em geral no caso de grupos pro-p estas aplicações não são sempre monomorfismos.*

Definição 6. *Um produto livre amalgamado pro-p $G = G_1 \coprod_H G_2$ é dito ser próprio se os homomorfismos canônicos ϕ_i $(i = 1, 2)$ são monomorfismos. Nesse caso, nós identificamos G_1, G_2 e H com suas imagens em G.*

Agora temos o seguinte lema:

Lema 7. *Sejam G_1 e G_2 grupos pro-p com um subgrupo procíclico fechado comum H. Então $G_1 \coprod_H G_2$ é próprio.*

Demonstração. Veja o Teorema 3.2. em [21]. ∎

Observação 8. *Nessa tese todos os produtos livres amalgamados pro-p que aparecem nos Capítulos 3 e 4, são produtos cujo o subgrupo amalgamado (comum) é um p-grupo cíclico finito. Como os subgrupos amalgamados são canônicamente grupos procíclicos, segue do Lema 7 que os produtos livres amalgamados pro-p dessa tese são todos próprios.*

Observação 9. *Tomando $H = \{1\}$ na definição de produto livre amalgamado pro-p; obtemos o que chamamos de Produto livre pro-p dos grupos dados. Para mais detalhes veja Ribes-Zalesski [22], página 361.*

Observação 10. • *Seja $G = A * B$ um produto livre de grupos abstratos. Então*

$$G_{\hat{p}} = A_{\hat{p}} \coprod B_{\hat{p}},$$

onde para um grupo abstrato H denotaremos por $H_{\hat{p}}$ os seu completamento pro-p.

• *Se F é um grupo livre pro-p de posto finito n, então:*

$$F \cong \underbrace{\mathbb{Z}_p \coprod \mathbb{Z}_p \coprod \cdots \coprod \mathbb{Z}_p}_{n \text{ vezes}}.$$

Nós vamos enunciar a seguir, uma versão pro-p do **Teorema do Subgrupo de Kurosh** (TSK) (Teorema 11) para subgrupos abertos de produtos livres pro-p de grupos pro-p. Observamos que nos restringiremos somente ao caso em que o número de fatores livres do produto livre pro-p é finito. Para uma situação mais geral, nós recomendamos a leitura de Mel'nikov [17]. Temos o seguinte lema:

Teorema 11 (Teorema do Subgrupo de Kurosh)**.** *Sejam $G_1, \ldots, G_n$ uma coleção finita de grupos pro-p. Considere D um subgrupo aberto do produto livre pro-p $G = G_1 \coprod \cdots \coprod G_n$. Então*

$$D = \coprod_{i=1}^{n} \left(\coprod_{g_{i,\tau} \in D \backslash G / G_i} \left(D \cap {g_{i,\tau}}^{-1} G_i g_{i,\tau} \right) \right) \coprod F$$

é um produto livre pro-p, onde:
a) para cada $i \in \{1, \ldots, n\}$, $g_{i,\tau}$ percorre um sistema de representantes de classes duplas para $D \backslash G / G_i$ contendo o 1, e
b) F é um grupo livre pro-p de posto igual à:

$$1 + (n-1)[G : D] - \sum_{i=1}^{n} |D \backslash G / G_i|.$$

Demonstração. Ver [22], páginas 367, 368 e 369. ∎

Para ver uma prova desse teorema para o caso de grupos abstratos, nós recomendamos a leitura de Serre [29] ou Kurosh [13].

Observação 12 (Geradores de Kurosch)**.** *Para mais detalhes sobre os geradores livres de F^{abs}, veja o livro de Kurosh [13], página 25, capítulo IX e seção 34, onde os tais geradores são descritos como sendo os elementos da forma $f_{\nu\delta}$.*

Observação 13. *À luz da prova do TSK (Teorema 11), considere o grupo abstrato $G^{\text{abs}} = G_1 * \ldots * G_n$. Pelo* ***Teorema do Subgrupo de Kurosh*** *para grupos abstratos, obtemos um subgrupo livre F^{abs} de $G^{\text{abs}} \cap D$, tal que $(F^{\text{abs}})_{\hat{p}} = F$, onde F é como no Teorema 11 (TSK). Assim no caso de produtos livres pro-p para encontrarmos os geradores de F como no Teorema 11 é necessário somente encontrar os geradores de F^{abs} como um subgrupo de $G^{\text{abs}} \cap F$, pela aplicação do Teorema do Subgrupo de Kurosh para grupos abstratos (veja*

Kurosh [13]) e como o subgrupo F^{abs} é denso em F, basta tomar o fecho topológico do subgrupo gerado pelos geradores livres que encontramos para F^{abs}. Agora, como podemos ver em Ribes-Zalesskii [22] página 95, temos que:

$$posto(F^{\mathrm{abs}}) = posto(F).$$

Observação 14. *Quando estivermos nessa tese, interessados em calcular o posto de F assim como no Teorema 11 (TSK), poderemos usar a **Teoria de Bass-Serre** (ver Serre [29]) para grupos abstratos, para calcularmos o posto de tais grupos pro-p livres. Além disso, esse cálculo poderá ser feito usando-se a fórmula da Característica de Euler-Poincaré-Wall que se encontra na página 123 do livro de Serre [29].*

Também temos uma versão pro-p do **Teorema de Grushko-Neumann** (Teorema 15), que pode ser encontrado em Ribes-Zalesskii [22], páginas 372 e 373.

Teorema 15 (Teorema de Grushko-Neumann)**.** *Seja $G = G_1 \coprod G_2$ um produto livre pro-p dos grupos pro-p G_1 e G_2. Então o número minimal de geradores topológicos de G, digamos $d(G)$, é igual à*

$$d(G) = d(G_1) + d(G_2).$$

Por fim apresentaremos, um resultado sobre o grupo de automorfismos de um grupo pro-p livre:

Lema 16. *Seja F um grupo pro-p livre de posto $2 \leq m < \infty$. Então o núcleo do epimorfismo canônico $\mathrm{Aut}(F) \twoheadrightarrow \mathrm{Aut}\left(\frac{F}{F'}\right)$ é um grupo pro-p livre de torção.*

Demonstração. Para o caso abstrato veja Lyndon-Schupp [16], página 27. Para o caso pro-p, consulte Lubotzky [15], página 323. ■

1.2 Anéis e Módulos

Nessa seção vamos relembrar alguns fatos que serão importantes nessa tese, que tratam sobre a teoria de anéis e módulos, tanto no caso abstrato, quanto para o caso profinito (pro-p).

1.2.1 Módulos Abstratos

Vamos admitir nessa seção conhecidas algumas definições e propriedades elementares dos módulos abstratos. Considere $(R, +, ., 1) = R$ um anel associativo com 1. Essa subseção será baseada nos livros de Kasch [12] e Rotman [24].

Relembramos que um R-módulo à esquerda é dito ser cíclico se existe um $x \in M$, tal que $M = \langle x \rangle = \{rx | r \in R\}$.

Os módulos cíclicos satisfazem o seguinte Lema:

Lema 17. *Um R-módulo à esquerda M é cíclico se, e somente se, $M \cong \frac{R}{I}$ para algum ideal à esquerda I de R. Se $M = \langle x \rangle$, então $I = \text{ann}_R(M) = \{r \in R | rx = 0\}$.*

Demonstração. Ver Rotman [24], página 26. ■

Vamos enunciar a seguir, o Lema 18, que trata de R-módulos f.g., para sua demonstração basta consultar Kasch [12], página 28.

Lema 18. *Seja M um R-módulo à esquerda f.g., então cada submódulo próprio à esquerda de M está contido em um submódulo à esquerda maximal de M.*

Módulos Livres Abstratos

Nessa subsubseção vamos relembrar alguns fatos sobre módulos livres e projetivos. Além disso, R-módulos significarão R-módulos à esquerda nessa tese. Começaremos com o seguinte Lema:

Lema 19. *Cada sequência exata curta $\{0\} \to A \to B \to P \to \{0\}$ de R-módulos à esquerda, onde P é um R-módulo projetivo, é cindida (split).*

Demonstração. Ver Rotman [24], página 63. ■

Lema 20. *Um R-módulo P é projetivo se, e somente se, ele é um somando direto de um R-módulo livre. Em particular, R-módulos livres são projetivos.*

Demonstração. Ver Rotman [24], página 63. ■

Antes de falarmos sobre o posto de um $\mathbb{Z}_p$-módulo livre, precisamos de uma definição que pode ser vista em Rotman [24], página 58.

Definição 21. *Um anel $(R, +, .)$ tem **IBN** (número invariante da base), se para cada R-módulo livre M, quaisquer duas de suas bases tem a mesma cardinalidade.*
Neste caso, o posto é definido como sendo a cardinalidade de alguma de suas bases e o mesmo será denotado por posto(M).

Lema 22. *Cada anel R comutativo, associativo com* 1, *tem **IBN**.*

Demonstração. Ver Rotman [24], página 58. ■

Observação 23. *O anel dos inteiros p-ádicos $\mathbb{Z}_p$ é um anel comutativo, associativo com* 1, *logo pelo Lema 22 temos que o mesmo tem **IBN**. No caso de $\mathbb{Z}_p$-módulos livres, vamos escrever o posto de tais módulos simplesmente como:*

$$r_p(M) := \text{posto}(M).$$

Por fim, vamos ver agora uma propriedade interessante dos R-módulos livres abstratos, onde R é um domínio de ideais principais (por exemplo, $\mathbb{Z}_p$ é um domínio de ideais principais, veja Neukirch [19]). Para sua prova, consulte Rotman [24], páginas 121 e 122.

Lema 24. *Seja R um domínio de ideais principais comutativo. Considere A um R-submódulo de um R-módulo livre F, então A é um R-módulo livre e o* $\text{posto}(A) \leq \text{posto}(F)$.

Anéis e Módulos Pro-p

Nessa subseção vamos relembrar algumas definições e propriedades básicas à cerca de anéis e módulos profinitos (pro-p), que nos serão muito úteis nessa tese.
Para isto, vamos nos basear nos livros de Ribes-Zalesskii [22] e Wilson [32].

Proposição 25. *Seja G um grupo profinito e $\hat{\mathbb{Z}}$ o completamento profinito de $\mathbb{Z}$. Considere $\iota : \mathbb{Z} \longrightarrow \hat{\mathbb{Z}}$ a aplicação canônica de $\mathbb{Z}$ em seu completamento profinito. Então:*
a) Existe uma única aplicação contínua $\hat{\mathbb{Z}} \times G \longrightarrow G$, tal que $(n, g) \longmapsto g^n$ para todo $n \in \mathbb{Z}$. Assim, se $g \in G$ e $z \in \hat{\mathbb{Z}}$, então g^z é bem definido;
b)Se $g \in G$ e $z_1, z_2 \in \hat{\mathbb{Z}}$, então $g^{z_1+z_2} = g^{z_1}g^{z_2}$ e $(g^{z_1})^{z_2} = g^{z_1z_2}$;
c)Se $g_1, g_2 \in G$, $z \in \hat{\mathbb{Z}}$ e se g_1 e g_2 comutam, então $(g_1g_2)^z = g_1^z g_2^z$.

Demonstração. Ver [32], página 29. ■

Note que a Proposição 25, implica que cada grupo abeliano profinito tem naturalmente uma única estrutura de $\hat{\mathbb{Z}}$-módulo. Visto que $\mathbb{Z}_p$ é um subanel de $\hat{\mathbb{Z}}$ e que cada grupo pro-p é um grupo profinito, temos que cada grupo abeliano pro-p tem naturalmente uma estrutura de $\mathbb{Z}_p$-módulo.

1.2.2 Álgebra de Grupo Completa e Álgebra de Grupo Abstrata

Definição 26. *Seja R um anel profinito comutativo com 1 e G um grupo profinito. A **álgebra de grupo completa** $[[RG]]$ é definida como o seguinte anel profinito:*

$$[[RG]] := \varprojlim[(R/I)\,(G/U)],$$

onde I e U percorrem os ideais abertos de R e os subgrupos normais abertos de G, respectivamente.

Se G é um grupo finito, temos $[[RG]] = [RG] = RG$. Para mais detalhes veja [22].

Para módulos profinitos temos a seguinte propriedade:

Lema 27. *Seja G um grupo profinito e R um anel profinito comutativo com 1. Então se A é ambos um G-módulo profinito e um R-módulo profinito com ações comutativas (isto é, se $r \in R, g \in G$ e $a \in A$, então $r(ga) = g(ra)$), então A é naturalmente um $[[RG]]$-módulo.*

Demonstração. Ver Ribes-Zalesskii [22], Proposição 5.3.6 da página 178. ∎

Definição 28. *Um anel R profinito comutativo com 1 é dito ser uma anel local se ele tem um único ideal maximal e aberto.*

A seguir, vamos enunciar o Lema 29, que não será demonstrado nessa tese.

Lema 29. *Seja K um anel profinito comutativo com 1 e G um grupo profinito. Então $[[KG]]$ é um anel local profinito se, e somente se, existe um $p \in \mathbb{P}$ tal que K é um anel local pro-p e G é um grupo pro-p.*

Demonstração. Ver Wilson[32], Proposição 7.5.3. e páginas 126 e 127. ∎

Como consequência imediata temos que se $G \cong C_{p^n}$ e $K = \mathbb{Z}_p$ é o anel dos inteiros p-ádicos, então $\mathbb{Z}_p C_{p^n}$ é um anel local pro-p (em particular, é um anel local abstrato).

Vamos exibir agora, um lema clássico que será usado nessa tese.

Lema 30. *Seja G um grupo profinito e considerem M_1, M_2 $K[[G]]$-módulos profinitos, onde K é um anel profinito comutativo com 1. Se $\theta : M_1 \longrightarrow M_2$ é ambos um K-homomorfismo contínuo e um G-homomorfismo de módulos, então θ é um $K[[G]]$-homomorfismo de módulos profinitos.*

Demonstração. Ver Wilson [32], página 119. ∎

O Lema e Observação a seguir são conhecidos e podem ser encontrados em Milies-Sehgal [28].

Lema 31. *Considere K um anel comutativo com 1. Seja $\phi : H_1 \longrightarrow H_2$ um homomorfismo de grupos. Considere $\tilde{\phi} : KH_1 \longrightarrow KH_2$ como sendo o homomorfismo canônico de anéis que estende linearmente ϕ. Então $\operatorname{Ker}\left(\tilde{\phi}\right) = \Delta(H_1, N)$ onde $N = \operatorname{Ker}(\phi)$ e $\Delta(H_1, N)$ é um ideal á esquerda do anel KH_1, gerado como um ideal pelos elementos $h - 1$, onde h é um gerador do grupo N.*

Observação 32. *Seja $N \triangleleft H_1$. Então o ideal $\Delta(H_1, N)$ é gerado como um K-módulo pelos elementos $x(h-1)$, onde $h \in N$ e x percorre um conjunto completo de representantes das classes laterais de N em H_1.*

Observação 33. *Considere o seguinte epimorfismo canônico de anéis:*
$$\Psi_m : \mathbb{Z}_p C_{p^n} \twoheadrightarrow \mathbb{Z}_p C_{p^m}$$
que aplica o gerador do grupo C_{p^n} no gerador do grupo C_{p^m}, onde $m \in \{0, 1, \ldots, (n-1)\}$ e admita que $C_{p^n} = \langle x \rangle$. Então, segue imediatamente a partir do Lema 31 e da Observação 32 que o $\mathrm{Ker}(\Psi_m)$ é um $\mathbb{Z}_p C_{p^n}$-módulo cíclico gerado por $\left(x^{p^m} - 1\right)$ e cujo o $\mathbb{Z}_p$-posto é igual a $p^n - p^m$.

Por fim, vamos provar o Lema a seguir que será usado na **Seção 3.1.**, para a construção dos $\mathbb{Z}_p C_{p^n}$-módulos indecomponíveis com ação não fiel do C_{p^n}, que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$.

Lema 34. *Considere $n \in \mathbb{N}$ e seja $C_{p^n} = \langle x \rangle$ e $C_{p^k} \leq C_{p^n}$.*
Então temos o seguinte isomorfismo de anéis (de $\mathbb{Z}_p$-álgebras):

$$\mathbb{Z}_p \left[\frac{\langle x \rangle}{\left\langle x^{p^{n-k}} \right\rangle} \right] \cong \frac{\mathbb{Z}_p \langle x \rangle}{\left(x^{p^{n-k}} - 1\right)}.$$

Demonstração. Considere o epimorfismo canônico dos p-grupos finitos dado abaixo:

$$\phi : \langle x \rangle \twoheadrightarrow \frac{\langle x \rangle}{\left\langle x^{p^{n-k}} \right\rangle}.$$

Como

$$\frac{\langle x \rangle}{\left\langle x^{p^{n-k}} \right\rangle} \hookrightarrow \left(\mathbb{Z}_p \left[\frac{\langle x \rangle}{\left\langle x^{p^{n-k}} \right\rangle} \right] \right)^{\times},$$

segue da propriedade universal de $\mathbb{Z}_p \langle x \rangle$, que existe um único $\mathbb{Z}_p$-homomorfismo de álgebras, dado por:

$$\Phi : \mathbb{Z}_p \langle x \rangle \twoheadrightarrow \mathbb{Z}_p \left[\frac{\langle x \rangle}{\left\langle x^{p^{n-k}} \right\rangle} \right] \cong \mathbb{Z}_p C_{p^{n-k}},$$

que envia $x \longmapsto \overline{x} := x + \left\langle x^{p^{n-k}} \right\rangle$.
Agora, pela Observação 33, sabemos que o $\mathrm{Ker}(\Phi) = \left(x^{p^{n-k}} - 1\right)$.
Assim, segue do **Teorema do Isomorfismo para Anéis**, que:

$$\mathbb{Z}_p \left[\frac{\langle x \rangle}{\left\langle x^{p^{n-k}} \right\rangle} \right] \cong \frac{\mathbb{Z}_p \langle x \rangle}{\left(x^{p^{n-k}} - 1\right)}$$

como $\mathbb{Z}_p$-álgebras. ■

1.2.3 O Teorema de Krull-Schmidt-Azumaya

Começaremos essa subseção com as seguintes definições:

Definição 35 (indecomponível)**.** *Seja M um $\mathbb{Z}_p C_{p^n}$-módulo. Nós diremos que M é **indecomponível** se $M \neq 0$ e M não pode ser escrito como uma soma-direta de dois $\mathbb{Z}_p C_{p^n}$-submódulos próprios.*

Definição 36. *Seja M um C_{p^n}-módulo. Nós diremos que C_{p^n} age indecomponivelmente sobre M, se M é **indecomponível** como um $\mathbb{Z}_p C_{p^n}$-módulo.*

Definição 37 (+-indecomponível)**.** *Seja M um $\mathbb{Z}_p C_{p^n}$-módulo. Nós diremos que M é **+-indecomponível** se $M \neq 0$ e M não pode ser escrito como uma soma de dois $\mathbb{Z}_p C_{p^n}$-submódulos próprios.*

Segue imediatamente o seguinte lema:

Lema 38. *Seja M um R-módulo +-indecomponível, então M é um R-módulo indecomponível.*

Demonstração. É claro que $M \neq \{0\}$. Agora, suponhamos por absurdo que M não é indecomponível. Então existem C e D, R-submódulos próprios de M, tais que:

$$M = C \oplus D = C + D.$$

Mas isso implica que M não é +-indecomponível, um absurdo. ■

Um resultado fundamental que será usado muitas vezes na construção do **Teorema Principal** é o **Teorema de Krull-Schmidt-Azumaya(TSKA)**, que também não vamos provar nessa tese.

Teorema 39. *Seja M um A-módulo à esquerda finitamente gerado e assuma que uma das duas condições abaixo são satisfeitas:*
(i)Os A-submódulos de M satisfazem ambas as condições de cadeia, ou
(ii)A é uma R-álgebra, f.g. como um R-módulo, onde R é um anel local noetheriano, comutativo e completo (por exemplo, um anel de valoração discreta e completa). Então M é expresso como uma soma-direta finita de A-submódulos indecomponíveis. Além disso, se:

$$M = \bigoplus_{i=1}^{r} M_i = \bigoplus_{j=1}^{s} N_j$$

são duas tais somas, então $r = s$ e $M_1 \cong N_{j_1}, \ldots, M_r \cong N_{j_r}$, onde $\{j_1, \ldots, j_r\}$ é alguma permutação de $\{1, \ldots, r\}$. Em outra palavras, M é escrito de maneira única como uma soma direta finita de A-submódulos indecomponíveis, à menos de isomorfismos e ordens de ocorrências dos somandos diretos.

Demonstração. Ver Curtis-Reiner[5], capítulo 6 e páginas 128 e 129. ■

Observamos que originalmente este Teorema não continha a parte (ii) de sua hipótese e era simplesmente conhecido como o **Teorema de Krull-Schimidt**; para mais detalhes veja o **Teorema de Krull-Schimidt** em [1], páginas 164 e 165 ou Kasch em [12], páginas 180 e 181.

Como sabemos, $\mathbb{Z}_pC_{p^n}$ é uma $\mathbb{Z}_p$-álgebra de grupo gerada por C_{p^n} como um $\mathbb{Z}_p$-módulo. Além disso, $\mathbb{Z}_p$ é um anel de valoração discreta completo (veja Neukirch [19]). Assim, a parte (ii) do Teorema 39 é satisfeita para $\mathbb{Z}_pC_{p^n}$-módulos finitamente gerados.

Em outra palavras, nessa tese o Teorema 39 é aplicável, já que nosso interesse é de estudar $\mathbb{Z}_pC_{p^n}$-módulos f.g.

1.3 O Radical de um Módulo e Alguns Fatos Sobre Módulos Indecomponíveis

Nessa seção, vamos relembrar algumas definições e fatos conhecidos da Teoria de Radicais de um dado R-módulo. A definição abaixo, pode ser vista no livro de Kasch [12], páginas 213 e 214.

Definição 40. *O R-submódulo de um R-módulo M dado por:*

$$\bigcap_{B \triangleleft\cdot M} B$$

é dito ser o radical de M se M tem submódulos maximais, caso contrário, o radical de M será igual a M. Notação: $\mathrm{rad}(M)$.

Exemplo 41. *1.* $\mathrm{rad}({}_{\mathbb{Z}}\mathbb{Z}) = \{0\}$;

2. $\mathrm{rad}({}_{\mathbb{Z}}\mathbb{Q}) = \mathbb{Q}$, *já que* $(\mathbb{Q}, +)$ *não tem subgrupos maximais.*

Por fim, vamos enunciar o fato a seguir, que pode ser encontrado em Kasch [12], página 304.

Lema 42. *Seja M um R-módulo tal que o* $\mathrm{rad}(M) \neq M$. *Então as seguintes afirmações são equivalentes:*
(a)M é um R-módulo $+$-indecomponível;
(b) Para todo X submódulo próprio de M, temos que $\frac{M}{X}$ é um R-módulo indecomponível.

1.4 Representações p-Ádicas do Grupo C_{p^n}

Nessa seção vamos fazer um breve estudo sobre as representações p-ádicas dos grupos cíclicos de ordem p^n, onde $n \in \mathbb{N}$. Nosso estudo será baseado nos trabalhos de **Reiner e**

Heller, que podem ser encontrados em [9], [10], [20] e [5].

Começaremos com a definição a seguir, que poderá ser vista em Reiner [20], Kang [11] ou no livro de Curtis-Reiner [5], página 522, onde a definição é feita para o caso de R ser um Domínio de Dedekind ou na página 254 de [5].

Definição 43 (Reticulados)**.** *Considere G um grupo finito. Seja M um $\mathbb{Z}_pG$-módulo à esquerda. Nós dizemos que M é um $\mathbb{Z}_pG$-reticulado se o mesmo é $\mathbb{Z}_p$-livre de torção e f.g. como um $\mathbb{Z}_p$-módulo.*

Temos a seguir a definição de uma R-representação de um grupo G sobre um R-módulo M. Essa definição pode ser vista no livro de Lang [14], página 664.

Definição 44 (R-representação de um grupo G sobre M)**.** *Sejam R um anel associativo, comutativo com 1 e G um grupo finito. Considere um R-módulo M. Nós dizemos que um homomorfismo de grupos:*

$$\rho : G \longrightarrow \mathrm{Aut}_R(M)$$

é uma R-representação do grupo G sobre M.

Temos imediatamente a seguinte observação:

Observação 45. *Estudar as R-representações de um dado grupo G sobre um R-módulo M, é o mesmo que estudar os $R[G]$-módulos.*

Demonstração. Para mais detalhes, veja Lang [14], página 664. ■

A partir de agora, estaremos interessados em estudar os $\mathbb{Z}_pC_{p^n}$-reticulados, onde $n \in \mathbb{N}$.

Os $\mathbb{Z}_pC_p$-Reticulados

Essa seção é baseada no artigo de **Reiner e Heller** [9]. Seja $\phi_p(x)$ o p-ésimo polinômio ciclotômico (veja Nagell [18] ou Lang [14]) e θ_p uma raiz primitiva p-ésima da unidade. Considere $\mathbb{Z}_p[\theta_p]$ o único anel de valoração discreta completa do corpo local $\mathbb{Q}_p[\theta_p]$, contendo $\mathbb{Z}_p$ (para mais detalhes, veja Neukirch [19]). Denote $C_p = H = \langle h \rangle$.

Nós temos os seguintes isomorfismos de anéis:

$$\frac{\mathbb{Z}_pH}{(h-1)\,\mathbb{Z}_pH} \cong \mathbb{Z}_p \quad \text{e} \quad \frac{\mathbb{Z}_pH}{(\phi_p(h))\,\mathbb{Z}_pH} \cong \mathbb{Z}_p\,[\theta_p]\,,$$

dados respectivamente por $h \longmapsto 1$ e $h \longmapsto \theta_p$.
Como ambos $\mathbb{Z}_p$ e $\mathbb{Z}_p\,[\theta_p]$ são anéis quocientes de $\mathbb{Z}_pH$, eles são canonicamente $\mathbb{Z}_pH$-módulos anulados respectivamente pelos ideais bilaterais de $\mathbb{Z}_pH$:

$$(h-1) \;\text{ e }\; (\phi_p(h))\,.$$

Como o ideal $(h-1)$ anula $\mathbb{Z}_p$, temos que o mesmo é o $\mathbb{Z}_pH$-módulo trivial.

Temos o seguinte Teorema:

Teorema 46. *Os únicos $\mathbb{Z}_pC_p$-reticulados indecomponíveis, não-isomorfos são:*

$$\mathbb{Z}_p, \ \ \mathbb{Z}_p\left[\theta_p\right] \ \ e \ \mathbb{Z}_pC_p.$$

Demonstração. Ver A. Heller e I. Reiner em [9]. ■

Os $\mathbb{Z}_pC_{p^2}$-Reticulados

Nas seções 3 e 4 do artigo [9], os autores A. Heller e I. Reiner, provaram o seguinte fato, que nós resumimos no seguinte Teorema:

Teorema 47. *O número de $\mathbb{Z}_pC_{p^2}$-reticulados indecomponíveis e não-isomorfos é finito. Além disso, esse número é precisamente igual a $4p+1$.*

Demonstração. Essa demonstração pode ser vista em Reiner e Heller [9], que provaram este fato independentemente de Berman e Gudivok em [3]. Também podemos ver essa prova em Curtis e Reiner [5]. ■

Os $\mathbb{Z}_pC_{p^n}$-Reticulados, Para $n \geq 3$

Os autores Reiner e Heller mostraram no artigo [10], página 327, que a **quantidade de $\mathbb{Z}_pC_{p^3}$-reticulados indecomponíveis e não-isomorfos** é **infinita**.

Agora, seja $C_{p^n} = \langle x \rangle$ e $C_{p^3} = \langle g \rangle$.
Considere o epimorfismo canônico de C_{p^n} em C_{p^3}, dado por $x \longmapsto g$.
Pela propriedade universal da álgebra de grupo $\mathbb{Z}_pC_{p^n}$, temos que existe um único epimorfismo canônico de $\mathbb{Z}_p$-álgebras:

$$\mathbb{Z}_pC_{p^n} \twoheadrightarrow \mathbb{Z}_pC_{p^3},$$

que estende a aplicação $x \longmapsto g$ e cujo núcleo é igual a $\left(x^{p^3}-1\right)$, pelo Lema 33.
Portanto, temos o seguinte isomorfismo de anéis:

$$\frac{\mathbb{Z}_pC_{p^n}}{(x^{p^3}-1)} \cong \mathbb{Z}_pC_{p^3}.$$

Assim, cada $\mathbb{Z}_pC_{p^3}$-módulo é um $\mathbb{Z}_pC_{p^n}$-módulo, anulado por $\left(x^{p^3}-1\right)$.
Por fim, juntando-se todas as informações obtidas nessa subsubseção, concluí-mos:

Teorema 48. *A quantidade de $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis e não-isomorfos, para $n \geq 3$, é infinita.*

Demonstração. Ver Reiner e Heller [10], páginas 318 ou 327. ■

O $\mathbb{Z}_p C_{p^n}$-Módulo Trivial

Seja $n \in \mathbb{N}$ e $C_{p^n} = \langle g \rangle$. Considere o seguinte isomorfismo canônico de anéis:

$$\frac{\mathbb{Z}_p C_{p^n}}{(g-1)} \cong \mathbb{Z}_p,$$

que envia $g \longmapsto 1$. Nesse caso, temos que $\mathbb{Z}_p$ é naturalmente um $\mathbb{Z}_p C_{p^n}$-módulo anulado por $(x-1)$, ou de outra maneira, $\mathbb{Z}_p$ é o $\mathbb{Z}_p C_{p^n}$-módulo indecomponível e trivial, como podemos ver no Teorema 46.

Capítulo 2

Capítulo Principal

2.1 Introdução ao Capítulo Principal

Seja $G = F \rtimes C_{p^n}$ um produto semi-direto pro-p, onde F é um grupo pro-p livre de posto finito em G e $n \in \mathbb{N}$.

Neste capítulo vamos provar que se C_{p^n} age fielmente e indecomponivelmente sobre o $\mathbb{Z}_p$-módulo livre F/F', então a abelianização de F é de um dos tipos dados a seguir:

- $$F/F' \cong Ker\,(\mathbb{Z}_pC_{p^n} \twoheadrightarrow \mathbb{Z}_pC_{p^m})$$
  para um certo m tal que $m \in \{0, 1, \ldots, (n-1)\}$
- $$F/F' \cong \mathbb{Z}_pC_{p^n}$$

como $\mathbb{Z}_pC_{p^n}$-módulos.

Para isso, vamos usar alguns fatos da **Teoria de Bass-Serre** (veja em Serre[29]), alguns resultados sobre módulos indecomponíveis em Kasch [12] e um Teorema de **Pavel Zalesskii** e **Wolfgang Herfort** sobre produto pro-p de normalizadores que se encontra em [8].

2.2 Resultados e Definições Auxiliares

Seja $G = F \rtimes C_{p^n}$ um produto semi-direto pro-p, onde F é um grupo pro-p livre e de posto finito em G e $n \in \mathbb{N}$.

Segue da Definição 1 que C_{p^n} age continuamente sobre F. Agora, como a aplicação canônica $F \twoheadrightarrow \frac{F}{F'}$ é aberta, segue que C_{p^n} também age continuamente sobre $\frac{F}{F'}$.
Segundo a Proposição 25, que se encontra em Wilson [32], temos que F/F' é $\mathbb{Z}_p$-módulo livre. Pela ação dada pela conjugação de C_{p^n} sobre F, temos que $\frac{F}{F'}$ é um C_{p^n}-módulo. Assim, temos que F/F' é naturalmente um $\mathbb{Z}_pC_{p^n}$-módulo, como podemos ver no Lema 27.

A partir de agora, escreveremos simplesmente $\overline{F}$ para significar:

$$\overline{F} := \frac{F}{F\,'} = F^{\text{ab}} = \frac{F}{\overline{[F,F]}}.$$

Note que esta é a mesma notação usada para o fecho topológico de um dado subgrupo. Quando houver alguma ambiguidade na notação, nós vamos fazer as devidas ressalvas nessa tese.

Definição 49. *[Levantamento] Seja M um $\mathbb{Z}_pC_{p^n}$-reticulado. Nós diremos que M* ***se levanta para um grupo pro-p*** *$G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito e $n \in \mathbb{N}$, se o $\mathbb{Z}_p$-módulo livre $\overline{F}$ é isomorfo à M como um $\mathbb{Z}_pC_{p^n}$-módulo.*

2.2.1 Caracterização dos Grupos da Forma $F \rtimes C_{p^n}$ e um Teorema Sobre Levantamentos de P. Zalesskii e W. Herfort

Vamos caracterizar nessa subseção como são os grupos da forma:

$$G = F \rtimes C_{p^n},$$

onde F é um grupo pro-p livre de posto finito em G e $n \in \mathbb{N}$.
O resultado abaixo será fundamental na prova do **Teorema Principal** dessa tese e o mesmo não será demonstrado. A prova de tal fato pode ser encontrada em Herfort-Zalesskii [7].

Teorema 50. *Seja G uma extensão cíclica de um grupo pro-p livre F, isto é, $G \cong F \rtimes C_n$. Então*

$$G \cong \left(\coprod_{x \in X} N_G(C_x)\right) \coprod H\,,$$

onde H é um subgrupo pro-p livre de F e $\{C_x \,|\, x \in X\}$ é um sistema de representantes de classes de conjugação de subgrupos de ordem p em G.

Além desse lema, temos à seguir o resultado que impulsionou o problema central dessa tese, ou seja, o Lema 6 em [8], que nessa tese é o:

Teorema 51. *Seja G uma extensão cindida (split) de um grupo pro-p livre F de posto finito por um grupo de ordem p, isto é,*

$$G \cong F \rtimes C_p \, .$$

Então :
(a) G tem decomposição livre como

$$G = \left(\coprod_{a \in A} (C_a \times H_a) \right) \amalg H,$$

onde $C_a \cong C_p$, H_a e H são subgrupos pro-p livres de F e A é um espaço booleano.
(b)Seja $M := \frac{F}{F'}$. Fixe $a_0 \in A$ e um gerador $c_{a_0} = c$ de C_{a_0}. Então a conjugação por c induz uma ação de C_{a_0} sobre M. O C_{a_0}-módulo M se decompõe na forma:

$$M = M_1 \oplus M_p \oplus M_{p-1},$$

onde M_p é um $\langle c \rangle$-módulo livre, c age trivialmente sobre M_1 e $\phi_p(c)$ age como a aplicação nula sobre M_{p-1}.

Observação 52. *A parte (i) do Teorema 51, foi provada por* ***C. Scheiderer*** *em [26].*

2.2.2 A Álgebra de Grupo $\mathbb{Z}_p C_{p^n}$ e Algumas de Suas Propriedades Elementares

Vamos provar nesta subseção, que se $\langle x \rangle \cong C_{p^n}$ e $m \in \{0, 1, \ldots, (n-1)\}$, onde $n \in \mathbb{N}$, então os núcleos dos epimorfismos canônicos de anéis

$$\operatorname{Ker}(\mathbb{Z}_p C_{p^n} \twoheadrightarrow \mathbb{Z}_p C_{p^m})$$

são $\mathbb{Z}_p C_{p^n}$-módulos indecomponíveis. Pelo livro de Sehgal [27], Lema 38.1, página 219, sabemos que $\mathbb{Z}_p C_{p^n}$ é um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível. Nessa tese, nós temos o interesse de provar que o mesmo é $+$-indecomponível. Temos o seguinte Lema:

Lema 53. *Seja G um p-grupo finito. Então $\mathbb{Z}_p G$ é um $\mathbb{Z}_p G$-módulo livre e $+$-indecomponível. Em particular, $\mathbb{Z}_p G$ é indecomponível.*

Demonstração. Sabemos que $\{0\} \neq \mathbb{Z}_p G$ é um $\mathbb{Z}_p \langle x \rangle$-módulo livre.
Suponhamos por absurdo que $\mathbb{Z}_p G$ seja escrito como

$$\mathbb{Z}_p G = A + B,$$

onde A e B são $\mathbb{Z}_p G$-submódulos próprios de $\mathbb{Z}_p G$.
Pelo Lema 29, vimos que $\mathbb{Z}_p G$ é um anel local comutativo pro-p (anel local comutativo abstrato).
Considere N seu único ideal bilateral maximal. Pelo Lema 18, temos que $A \subset N$ e $B \subset N$.
Logo, temos que $A + B \subset N \neq \mathbb{Z}_p G$, um absurdo.
Portanto $\mathbb{Z}_p G$ é um $\mathbb{Z}_p G$-módulo **$+$-indecomponível**. Do Lema 38, temos que $\mathbb{Z}_p G$ também é **indecomponível**. ∎

Observação 54. *Nem todo módulo livre de posto* 1 *(módulo regular) é indecomponível.*

Exemplo 55. *Considere* $(\frac{\mathbb{Z}}{6\mathbb{Z}}, +, .)$ *o anel de resíduos módulo* 6*. Então* $\frac{\mathbb{Z}}{6\mathbb{Z}} = \langle \overline{1} \rangle$ *como um* $\frac{\mathbb{Z}}{6\mathbb{Z}}$*-módulo livre (cíclico). Mas*

$$\frac{\mathbb{Z}}{6\mathbb{Z}} = \langle \overline{3} \rangle \oplus \langle \overline{2} \rangle \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$$

como um $\frac{\mathbb{Z}}{6\mathbb{Z}}$*-módulo decomponível.*

Vamos mostrar a partir de agora, que para todo $m \in \{0, 1, \ldots, (n-1)\}$, temos que os núcleos dos epimorfismos canônicos:

$$\Psi_m : \mathbb{Z}_p C_{p^n} \twoheadrightarrow \mathbb{Z}_p C_{p^m}$$

são $\mathbb{Z}_p C_{p^n}$-módulos **indecomponíveis**.

Temos a seguinte proposição:

Proposição 56. *Seja* $n \in \mathbb{N}$ *e* $m \in \{0, 1, \ldots, (n-1)\}$*. Considerem os epimorfismos canônicos de grupos* $C_{p^n} \longrightarrow C_{p^m}$*. Então os núcleos dos epimorfismos canônicos de anéis* $\Psi_m : \mathbb{Z}_p C_{p^n} \longrightarrow \mathbb{Z}_p C_{p^m}$ *são* $\mathbb{Z}_p C_{p^n}$*-módulos* ***indecomponíveis****, para cada* $m \in \{0, 1, \ldots, (n-1)\}$*.*

Demonstração. Considere $C_{p^n} = \langle x \rangle$. Os núcleos dos epimorfismos Ψ_m são os ideais bilaterais

$$\left(x^{p^m} - 1\right)$$

de $\mathbb{Z}_p \langle x \rangle$, para todos os m, como podemos ver na Observação 33.
Note que cada $\operatorname{Ker}(\Psi_m)$ é um $\mathbb{Z}_p C_{p^n}$-módulo cíclico.

Agora, observe que:

$$\{0\} \neq \operatorname{ann}_{\mathbb{Z}_p\langle x \rangle} \left(\left(x^{p^m} - 1\right)\right) \neq \mathbb{Z}_p \langle x \rangle .$$

De fato, se o $\operatorname{ann}_{\mathbb{Z}_p\langle x \rangle} \left(\left(x^{p^m} - 1\right)\right) = \mathbb{Z}_p \langle x \rangle$, então $1 \cdot \left(x^{p^m} - 1\right) = x^{p^m} - 1 = 0$, o que implicaria que $x^{p^m} = 1$ e a ordem de x seria igual a p^m, uma contradição. Agora, note que:

$$x^{p^n} - 1 = \left(x^{p^m} - 1\right) \cdot \phi_{p^{m+1}}(x) \cdot \phi_{p^{m+2}}(x) \cdots \phi_{p^n}(x),$$

pela definição de polinômios ciclotômicos (para mais detalhes veja Nagell [18] ou Lang [14]). Mas em $\mathbb{Z}_p \langle x \rangle$ temos que $x^{p^n} - 1 = 0$, donde segue que

$$0 \neq \phi_{p^{m+1}}(x) \cdot \phi_{p^{m+2}}(x) \cdots \phi_{p^n}(x) \in \operatorname{ann}_{\mathbb{Z}_p\langle x \rangle} \left(\left(x^{p^m} - 1\right)\right).$$

Portanto o $\operatorname{ann}_{\mathbb{Z}_p\langle x \rangle} \left(\left(x^{p^m} - 1\right)\right)$ não é nulo.

Pelo Lema 17, temos que:

$$\operatorname{Ker}(\Psi_m) \cong \frac{\mathbb{Z}_p \langle x \rangle}{\operatorname{ann}_{\mathbb{Z}_p\langle x \rangle} \left(\left(x^{p^m} - 1\right)\right)}$$

como um $\mathbb{Z}_pC_{p^n}$-módulo.

Além disso, o Lema 53 nos garante que $\mathbb{Z}_p\langle x\rangle$ é um $\mathbb{Z}_p\langle x\rangle$-módulo **+-indecomponível**. Também temos que o $\mathrm{rad}(\mathbb{Z}_p\langle x\rangle)$ é um submódulo próprio, já que $\mathbb{Z}_p\langle x\rangle$ é um anel local pro-p (veja o Lema 29).

Logo, reunindo todas essas informações para aplicarmos o Lema 42, nós concluí-mos que:

$$\frac{\mathbb{Z}_p\langle x\rangle}{\mathrm{ann}_{\mathbb{Z}_p\langle x\rangle}\left((x^{p^m}-1)\right)} \cong \mathrm{Ker}\left(\Psi_m\right)$$

é um $\mathbb{Z}_p\langle x\rangle$-módulo **indecomponível**, para todo $m \in \{0,1,\ldots,(n-1)\}$. ■

Lema 57. *Seja $n \in \mathbb{N}$ e considere M um $\mathbb{Z}_pC_{p^n}$-módulo. Suponha que $C_{p^n} = \langle x\rangle$ e seja $C_{p^k} \leq C_{p^n}$. Então:*

M é um $\mathbb{Z}_pC_{p^n}$-módulo indecomponível anulado por $\left(x^{p^{n-k}}-1\right)$ se, e somente se, M é um $\mathbb{Z}_p\left[\frac{C_{p^n}}{C_{p^k}}\right]$-módulo indecomponível.

Demonstração. Pelo Lema 34, temos que:

$$\frac{\mathbb{Z}_pC_{p^n}}{\left(x^{p^{n-k}}-1\right)} = \frac{\mathbb{Z}_p\langle x\rangle}{\left(x^{p^{n-k}}-1\right)} \cong \mathbb{Z}_p\left[\frac{C_{p^n}}{C_{p^k}}\right] = \mathbb{Z}_p\left[\frac{\langle x\rangle}{\left\langle x^{p^{n-k}}\right\rangle}\right]$$

como $\mathbb{Z}_p$-álgebras, onde $x \longmapsto \overline{x} := x + C_{p^k}$.

Logo cada $\left[\mathbb{Z}_p\left[\frac{C_{p^n}}{C_{p^k}}\right]\right]$-módulo é um $\left[\frac{\mathbb{Z}_pC_{p^n}}{\left(x^{p^{n-k}}-1\right)}\right]$-módulo, e vice-versa.

Agora, observamos que um $\left[\frac{\mathbb{Z}_pC_{p^n}}{\left(x^{p^{n-k}}-1\right)}\right]$-módulo é um $\mathbb{Z}_pC_{p^n}$-módulo, anulado pelo ideal bilateral $\left(x^{p^{n-k}}-1\right)$, e vice-versa, como podemos ver em Rotman [24], página 24.

Como a ação de $\mathbb{Z}_pC_{p^n}$ sobre M, é a mesma que a ação de $\mathbb{Z}_p\left[\frac{C_{p^n}}{C_{p^k}}\right]$ sobre M, o Lema segue trivialmente. ■

2.3 Conexões entre Alguns $\mathbb{Z}_pC_{p^n}$-Reticulados e Certos Grupos Pro-p

Vamos provar nessa seção uma das Proposições mais importantes na prova do **Teorema Principal**.

Em resumo, temos:

Para certos grupos da forma $G \cong F \rtimes C_{p^n}$, onde F é um grupo pro-p livre, de posto finito, mostraremos que o grupo abeliano pro-p $\overline{F}$ é um $\mathbb{Z}_p C_{p^n}$-reticulado indecomponível.

Para isso, vamos usar o Teorema 11 (**TSK**) juntamente com a Observação 13 e os resultados da **Seção 1.2.**.

Antes de provarmos a tal Proposição, vamos provar o seguinte Lema:

Lema 58. *Considere $n \in \mathbb{N}$.*

1. *Seja $G \cong C_{p^n} \coprod \mathbb{Z}_p$. Então*
$$G \cong F_{p^n} \rtimes C_{p^n},$$
onde C_{p^n} age por conjugação sobre F_{p^n}.
2. *Seja $G \cong C_{p^n} \coprod C_{p^k}$, onde $1 \leq k \leq n$. Então, temos que*
$$G \cong F_{\left[p^n - p^{(n-k)}\right]} \rtimes C_{p^n},$$
onde C_{p^n} age por conjugação sobre $F_{\left[p^n - p^{(n-k)}\right]}$. Em particular, se $k = n$, então
$$G \cong F_{(p^n - 1)} \rtimes C_{p^n}.$$

Demonstração. Vamos provar primeiramente o item 1).

1. Considere
$$G = \langle x \rangle \coprod \overline{\langle \alpha \rangle},$$
onde $\langle x \rangle = C_{p^n}$ e $\overline{\langle \alpha \rangle} = \mathbb{Z}_p$.
Pela propriedade universal do produto livre pro-p, existe um único epimorfismo contínuo canônico de grupos pro-p, dado por:
$$\langle x \rangle \coprod \overline{\langle \alpha \rangle} \xrightarrow{\phi} \langle \omega \rangle \cong C_{p^n}$$
$$x \longmapsto \omega$$
$$\alpha \longmapsto 1.$$
Agora, note que Ker $(\phi) \triangleleft_c G$ e $\langle x \rangle = C_{p^n} <_c G$. Como
$$\text{Ker } (\phi) \cap \langle x \rangle = \{1\},$$
temos que
$$\text{Ker } (\phi) \rtimes \langle x \rangle \leq G.$$
Pela Observação 13 do Teorema **TSK** (11), temos que:
$$\text{Ker } (\phi) = \overline{\left\langle \alpha, \alpha^x, \ldots, \alpha^{x^{[p^n-1]}} \right\rangle} \cong F_{p^n}.$$
Agora temos que $\langle x \rangle \hookrightarrow$ Ker $(\phi) \rtimes \langle x \rangle$ e $\overline{\langle \alpha \rangle} \hookrightarrow$ Ker $(\phi) \rtimes \langle x \rangle$ (pela definição de ϕ.) Portanto temos que $G \cong F_{p^n} \rtimes C_{p^n}$.

2. Seja $G = \langle x \rangle \coprod \langle y \rangle$, onde $\langle x \rangle = C_{p^n}$ e $\langle y \rangle = C_{p^k}$. Além disso, suponha que k satisfaz $1 \leq k \leq n$.
Pela propriedade universal do produto livre pro-p, existe um único epimorfismo contínuo canônico de grupos pro-p
$$\eta : \langle x \rangle \coprod \langle y \rangle \twoheadrightarrow \langle \omega \rangle \cong C_{p^n},$$
dado por $x \longmapsto \omega$ e $y \longmapsto \omega^{\left(p^{[n-k]}\right)}$.
Agora, pela Observação 13 do Teorema **TSK** (11), temos que: Ker (η) é um subgrupo pro-p livre de G, dado por: Se $k = n$:
$$\text{Ker } (\eta) = \overline{\langle x^v y^{[-v]}, \text{ onde } v \in \{1, \ldots, (p^n - 1)\}\rangle}$$
e quando $k \neq n$, temos que:
$$\text{Ker } (\eta) = \overline{\left\langle x^{\left[p^n - vp^{(n-k)}\right]} y^v \,,\, x^m y^v x^{\left[p^n - vp^{(n-k)} - m\right]} \right\rangle},$$
onde $1 \leq v \leq (p^k - 1)$ e $1 \leq m \leq \left[p^{(n-k)} - 1\right]$.
Pela Observação 14 do Teorema 11, temos que Ker (η) é um subgrupo pro-p livre de G, cujo posto é igual à:
$$\text{posto}\,(\text{Ker } (\eta)) = 1 + p^n. \left(1 - \frac{1}{p^n} - \frac{1}{p^k}\right) = 1 + p^n - 1 - p^{(n-k)} = p^n - p^{(n-k)}\,.$$
Agora, note que Ker $(\eta) \lhd_c G$, $\langle x \rangle <_c G$ e $(\text{Ker } (\eta) \cap \langle x \rangle) = \{1\}$.
Assim, nós obtemos que Ker $(\eta) \rtimes \langle x \rangle <_c G$.
Observe que $x^{\left[p^n - p^{[n-k]}\right]} y \in \text{Ker } (\eta)$. Portanto, temos que:
$$\left(x^{\left[p^n - p^{[n-k]}\right]}\right)^{[-1]} \cdot \left[\left(x^{\left[p^n - p^{[n-k]}\right]}\right) y\right] = y \in \text{Ker } (\eta) \rtimes \langle x \rangle\,.$$
Logo,
$$G = \langle x \rangle \coprod \langle y \rangle \hookrightarrow \text{Ker } (\eta) \rtimes \langle x \rangle$$
e o lema está provado.

■

À luz do Lema 58, temos a seguinte Proposição:

Proposição 59. *Considere $n \in \mathbb{N}$. Seja*
$$G \cong C_{p^n} \coprod \mathbb{Z}_p \cong F_{p^n} \rtimes C_{p^n}.$$
Então
$$\overline{F_{p^n}} \cong \text{Ker } (\mathbb{Z}_p C_{p^n} \twoheadrightarrow 0) = \mathbb{Z}_p C_{p^n}$$
como um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível.

Demonstração. Pela introdução da **Seção 2.2.**, temos imediatamente que $\overline{F_{p^n}}$ é um $\mathbb{Z}_p C_{p^n}$-módulo.
Observamos também, que o fato do módulo ser indecomponível segue do Lema 53. Resta-nos assim, mostrar somente o isomorfismo desta proposição.

Considere

$$G = \langle x \rangle \coprod \overline{\langle \alpha \rangle} \cong C_{p^n} \coprod \mathbb{Z}_p \cong F_{p^n} \rtimes C_{p^n} \,.$$

Pelo Lema 58, temos que:

$$F_{p^n} = \overline{\left\langle \alpha, \alpha^x, \ldots, \alpha^{x^{[(p^n)-1]}} \right\rangle},$$

donde segue que:

$$G = \overline{\left\langle \alpha, \alpha^x, \ldots, \alpha^{x^{[(p^n)-1]}} \right\rangle} \rtimes \langle x \rangle \,.$$

Agora,

$$\overline{F_{p^n}} := \frac{F_{p^n}}{[F_{p^n}]'} = \left\langle \overline{\alpha}, \overline{\alpha^x}, \ldots, \overline{\alpha^{x^{[(p^n)-1]}}} \right\rangle$$

e como

$$x^k \circ \overline{\alpha} = \overline{\alpha^{x^k}}, \ \forall\ k = 0, 1, \ldots, p^n - 1\,,$$

temos que

$$\overline{F_{p^n}} \cong \mathbb{Z}_p C_{p^n}$$

como um $\mathbb{Z}_p C_{p^n}$-módulo. ∎

Proposição 60. *Considere $n \in \mathbb{N}$. Seja*

$$G \cong C_{p^n} \coprod C_{p^t} \cong F_{[p^n - p^{(n-t)}]} \rtimes C_{p^n},$$

onde $t \in \{1, 2, \ldots, n\}$. Então

$$\overline{F_{[p^n - p^{(n-t)}]}} \cong \operatorname{Ker}\left(\mathbb{Z}_p C_{p^n} \twoheadrightarrow \mathbb{Z}_p C_{p^{[n-t]}}\right)$$

como um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível.

Demonstração. Pela introdução da **Seção 2.2.**, temos imediatamente que $\overline{F_{[p^n - p^{(n-t)}]}}$ é um $\mathbb{Z}_p C_{p^n}$-módulo. Além disso, notamos que o fato do módulo ser indecomponível, segue da Proposição 56.
Resta-nos assim, mostrar somente o isomorfismo da assertiva desta proposição.
Dividiremos o restante da prova dessa Proposição, em dois casos, são eles:

Caso a): Quando $t = n$ e **Caso b)** Quando $t \in \{1, 2, \ldots, (n-1)\}$.

Caso a): Quando $t = n$. Neste caso, temos que $G \cong C_{p^n} \coprod C_{p^n}$. Considere $G = \langle x \rangle \coprod \langle y \rangle$.
Pelo Lema 58, temos que:

$$G = F_{p^n - 1} \rtimes \langle x \rangle \,.$$

Agora, pela Observação 13 do Teorema 11, temos que:

$$F_{p^n-1} = \overline{\left\langle \alpha_1 := xy^{-1}, \ldots, \alpha_{([p^n]-2)} := x^{([p^n]-2)}y^{-([p^n]-2)}, \alpha_{([p^n]-1)} := x^{[p^n]-1}y^{-([p^n]-1)} \right\rangle}.$$

Defina $M := \frac{F_{[p^n-1]}}{\left[F_{(p^n-1)}\right]'} =: \overline{F_{p^n-1}}$.

Como já discutimos na Proposição 59, temos que M é naturalmente um $\mathbb{Z}_p \langle x \rangle$-módulo. Escreveremos $\overline{m} := f + \left[F_{(p^n-1)}\right]' \in M$, onde $f \in F_{(p^n-1)}$.
Nosso objetivo a partir de agora, é de mostrar que M é um $\mathbb{Z}_p \langle x \rangle$-módulo cíclico, gerado por $\overline{\alpha_{(p^n-1)}}$.

Considere $\overline{\alpha_0} := 0 =: \overline{\alpha_{p^n}}$.
Se $r \in \{0, 1, 2, \ldots, p^n - 2, p^n - 1\}$, temos que:

$$x^r \circ \overline{\alpha_{(p^n-1)}} = \overline{\alpha_{(p^n-r-1)}} - \overline{\alpha_{(p^n-r)}} .$$

De fato, isto ocorre já que:

$$\begin{array}{rcccl} x^r \circ \overline{\alpha_{(p^n-1)}} & = & \overline{x^{(-r)}x^{(p^n-1)}yx^r} & = & \overline{x^{-(r+1)}y^{(r+1)}y^{(-r)}x^r} \quad = \\ & = & \overline{x^{(p^n-(r+1))}y^{r+1}} - \overline{x^{(p^n-r)}y^r} & = & \overline{\alpha_{(p^n-r-1)}} - \overline{\alpha_{(p^n-r)}} , \end{array}$$

onde $y^{r+1} = \left(y^{(p^n-(r+1))}\right)^{(-1)}$ e $y^r = \left(y^{[p^n-r]}\right)^{(-1)}$.

Portanto, se já temos indutivamente que:

$$\overline{\alpha_s} \in \left\langle \overline{\alpha_{(p^n-1)}} \right\rangle ,$$

para qualquer

$$s \in \{2, \ldots, p^n - 1\},$$

então como:

$$x^{(p^n-s)} \circ \overline{\alpha_{(p^n-1)}} = \overline{\alpha_{(s-1)}} - \overline{\alpha_s} \in \left\langle \overline{\alpha_{(p^n-1)}} \right\rangle ,$$

segue que:

$$\overline{\alpha_s} + \left(\overline{\alpha_{(s-1)}} - \overline{\alpha_s}\right) = \overline{\alpha_{(s-1)}} \in \left\langle \overline{\alpha_{(p^n-1)}} \right\rangle .$$

Assim, por indução sobre s, temos que:

$$\overline{\alpha_1}, \overline{\alpha_2}, \ldots, \overline{\alpha_{(p^n-3)}}, \overline{\alpha_{(p^n-2)}}, \overline{\alpha_{(p^n-1)}}, \tag{2.1}$$

pertencem ao $\langle x \rangle$-submódulo de M gerado por $\overline{\alpha_{(p^n-1)}}$.
Portanto, temos que

$$M = \left\langle \overline{\alpha_{(p^n-1)}} \right\rangle$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo cíclico.

Denote por $\mathcal{A}$, o seguinte conjunto

$$\mathcal{A} = \{x^r \circ \overline{\alpha_{p^n-1}} \,|\, r = 0, \ldots, p^n - 2\}.$$

Como podemos ver em Neukirch [19], página 121, temos que $(\mathbb{Z}_p, +, .)$ é um domínio de

ideais principais. Logo, segue do Lema 24 que o $\mathbb{Z}_p$-submódulo de M gerado por $\mathcal{A}$ é um $\mathbb{Z}_p$-módulo livre, cujo $\mathbb{Z}_p$-posto é igual à $p^n - 1 = \mathrm{r}_p(M)$.
Donde concluí-mos que M é um $\mathbb{Z}_p$-módulo livre com base $\mathcal{A}$, já que quaisquer dos geradores de M como um $\mathbb{Z}_p$-módulo livre estão todos contidos no $\mathbb{Z}_p$-módulo livre gerado por $\mathcal{A}$.

Considere $\mathrm{I}(\mathbb{Z}_p\langle x\rangle) = (x-1)$, como sendo o ideal de augumentação de $\mathbb{Z}_p\langle x\rangle$. Sabemos pela Observação 33, que $\mathrm{I}(\mathbb{Z}_p\langle x\rangle)$ é um $\mathbb{Z}_p\langle x\rangle$-módulo cíclico, cujo o $\mathbb{Z}_p$-posto é igual à $p^n - 1$.
Além disso, note que $(x-1)$ é um $\mathbb{Z}_p$-módulo livre com base

$$\mathcal{B} = \{x^z \circ (x-1) \mid z \in \{0, 1, \ldots, p^n - 2\}\}.$$

Defina a seguinte aplicação de $\mathcal{B}$ para $\mathcal{A}$, que aplica

$$x^u \circ (x-1) = x^{u+1} - x^u \longmapsto x^u \circ \overline{\alpha_{p^n-1}} = \overline{\alpha_{p^n-(u+1)}} - \overline{\alpha_{p^n-u}},$$

para cada $u \in \{0, 1, \ldots, p^n - 2\}$ e a denote por $\phi_{\mathcal{B},\mathcal{A}}$.

A propriedade universal do $\mathbb{Z}_p$-módulo livre $(x-1)$, nos diz que existe um único $\mathbb{Z}_p$-homomorfismo $\lambda : (x-1) \longrightarrow M$, tal que $\lambda|_{\mathcal{B}} = \phi_{\mathcal{B},\mathcal{A}}$.

Agora, cada ϵ pertencente ao $\mathbb{Z}_p$-módulo livre $(x-1)$ é escrito da seguinte maneira:

$$\sum_{\substack{u \in \{0,\ldots,p^n-2\} \\ z_u \in \mathbb{Z}_p}} z_u x^u (x-1).$$

Assim, temos que

$$x^\omega \circ \epsilon = \sum_{\substack{u \in \{0,\ldots,p^n-2\} \\ z_u \in \mathbb{Z}_p}} z_u x^{u+\omega}(x-1),$$

para qualquer $\omega \in \{0, 1, \ldots, p^n - 1\}$.

Logo, temos que:

$$\lambda(x^\omega \circ \epsilon) = \sum_{\substack{u \in \{0,\ldots,p^n-2\} \\ z_u \in \mathbb{Z}_p}} z_u x^{u+\omega}(\overline{\alpha_{p^n-1}}) = x^\omega \circ \left(\sum_{\substack{u \in \{0,\ldots,p^n-2\} \\ z_u \in \mathbb{Z}_p}} z_u x^u (\overline{\alpha_{p^n-1}}) \right) = x^\omega \circ \lambda(\epsilon).$$

Portanto, λ é um $\langle x\rangle$-homomorfismo de $(x-1)$ para M.
Pelo Lema 30, temos que λ é um $\mathbb{Z}_p\langle x\rangle$-homorfismo.
Por fim, queremos provar que λ é um $\mathbb{Z}_p\langle x\rangle$-isomorfismo.
De fato, temos que:

$$\mathrm{r}_p(M) = \mathrm{posto}(F_{p^n-1}) = p^n - 1 = \mathrm{r}_p\left((x-1)\right).$$

Assim, λ é um isomorfismo dos $\mathbb{Z}_p$-módulos livres $(x-1)$ e M.
Em particular, λ é uma bijeção.
Finalizamos o seguinte:

$$\overline{F_{p^n-1}} = \langle \overline{\alpha_{p^n-1}} \rangle \cong (x-1) = I(\mathbb{Z}_p\langle x\rangle) = \mathrm{Ker}(\mathbb{Z}_p\langle x\rangle \twoheadrightarrow \mathbb{Z}_p)$$

como um $\mathbb{Z}_p C_{p^n}$-módulo.

Por fim, vamos provar o último caso:
Caso b) Quando $t \in \{1, 2, \ldots, (n-1)\}$. Neste caso, pelo Lema 58, temos que:

$$G \cong C_{p^n} \coprod C_{p^t} \cong F_{\left(p^n - p^{(n-t)}\right)} \rtimes C_{p^n}.$$

Admitamos que

$$G = \langle x \rangle \coprod \langle y \rangle = F_{\left(p^n - p^{(n-t)}\right)} \rtimes \langle x \rangle\,,$$

onde $\langle x \rangle = C_{p^n}$ e $\langle y \rangle = C_{p^t}$.

Suponha que $F_{\left(p^n - p^{(n-t)}\right)} = \overline{\langle \Xi \rangle}$, onde Ξ é um conjunto de geradores topológicos livres de $F_{p^n - p^{n-t}}$.
Agora, aplicando-se a Observação 13 do Teorema 11, podemos encontrar:

$$\Xi = \{x^{\left[p^n - sp^{(n-t)}\right]} y^s\,,\ x^k y^s x^{\left[p^n - sp^{(n-t)} - k\right]},\ \text{onde } 1 \leq s \leq (p^t - 1) \text{ e } 1 \leq k \leq \left[p^{(n-t)} - 1\right]\}\,.$$

Escreveremos a partir de agora:
Para $1 \leq s \leq (p^t - 1)$; $v_s := x^{\left[p^n - sp^{(n-t)}\right]} y^s$ e para $1 \leq k \leq \left[p^{(n-t)} - 1\right]$; $\beta_{k,s} := x^k y^s x^{\left[p^n - sp^{(n-t)} - k\right]}$.

Pelo Lema 27, temos que:

$$N := \frac{F_{\left(p^n - \left[p^{(n-t)}\right]\right)}}{\left[F_{\left(p^n - \left[p^{(n-t)}\right]\right)}\right]'} = \overline{F_{\left(p^n - \left[p^{(n-t)}\right]\right)}}$$

é um $\mathbb{Z}_p \langle x \rangle$-módulo.
Os geradores de N como um $\mathbb{Z}_p$-módulo livre, são os seguintes:

$$\overline{v_s} \text{ e } \overline{\beta_{k,s}},\ \text{ onde } 1 \leq s \leq (p^t - 1) \text{ e } 1 \leq k \leq \left[p^{(n-t)} - 1\right]\ .$$

FATO: $N := \overline{F_{\left(p^n - \left[p^{(n-t)}\right]\right)}}$ é um um $\mathbb{Z}_p \langle x \rangle$-módulo cíclico, gerado por $\overline{v_{(p^t-1)}}$.

JUSTIFICATIVA Primeiramente, vamos mostrar que para todo $j \in \{1, 2, \ldots, p^t - 1\}$, temos que cada $\overline{v_j}$ pertence ao $\mathbb{Z}_p \langle x \rangle$-submódulo de N, gerado por $\overline{v_{(p^t-1)}}$, isto é, para todo j, temos que

$$\overline{v_j} \in \left\langle \overline{v_{(p^t-1)}} \right\rangle := J\,.$$

Considere $\overline{v_0} := 0$ e $\overline{v_{-1}} = \overline{v_{p^t-1}}$. Em geral, se $u \in \{0, 1, 2, \ldots, p^t - 2, p^t - 1\}$, temos que:

$$
\begin{aligned}
x^{up^{(n-t)}} \circ \overline{v_{(p^t-1)}} &= \overline{x^{\left(p^n-[u-1]p^{(n-t)}\right)} y^{(p^t-1)} x^{up^{(n-t)}}} = \\
&= \overline{x^{\left(p^n-[u-1]p^{(n-t)}\right)} y^{(u-1)} y^{(p^t-1-(s-1))} x^{up^{(n-t)}}} = \overline{v_{(u-1)}} - \overline{v_u} \in J\,.
\end{aligned}
$$

Assim, dado qualquer $u \in \{0,1,2,\ldots,p^t-2\}$, se $\overline{v_{u-1}} \in J$, então temos que:

$$
-\overline{v_{u-1}} + \left(\overline{v_{(u-1)}} - \overline{v_u}\right) = -\overline{v_u} \in J\,.
$$

Portanto, temos pelo processo de indução sobre u, que:

$$
\overline{v_{(p^t-1)}}, \overline{v_1}, \overline{v_2}, \ldots, \overline{v_{(p^t-2)}} \in J. \tag{2.2}
$$

Para provarmos que N é um $\mathbb{Z}_p \langle x \rangle$-módulo cíclico, resta-nos provar que todos elementos da forma:

$$
\overline{\beta_{k,s}} := \overline{x^k y^s x^{\left[p^n - sp^{(n-t)} - k\right]}},\ \text{onde } 1 \leq s \leq p^t - 1 \text{ e } 1 \leq k \leq p^{(n-t)} - 1\}
$$

pertencem ao $\mathbb{Z}_p \langle x \rangle$-submódulo de N, dado por:

$$
J := \left\langle \overline{v_{(p^t-1)}} \right\rangle.
$$

Seja k um elemento fixo e arbitrário de $\{1,2,\ldots,p^{n-t}-1\}$. Como já sabemos os elementos:

$$
\overline{\beta_{k,1}}, \overline{\beta_{k,2}}, \ldots, \overline{\beta_{k,s}}, \ldots, \overline{\beta_{k,(p^t-2)}}, \overline{\beta_{k,(p^t-1)}}
$$

são geradores do $\mathbb{Z}_p$-módulo livre N.
Vamos provar que para todo $l \in \{1,2,\ldots,p^t-2,p^t-1\}$, temos que $\overline{\beta_{k,l}} \in J$.
Defina $\overline{\beta_{k,0}} := \overline{\beta_{k,(p^t-1)}}$ e $\overline{\beta_{k,p^t}} := 0$.

Para cada $\xi \in \{0,1,2,\ldots,(p^t-2)\}$, temos que:

$$
\begin{aligned}
x^{\left(p^{n-t}-k+\xi p^{n-t}\right)} \circ \overline{v_{p^t-1}} &= \overline{x^{\left[p^n-p^{(n-t)}+k-\xi p^{(n-t)}+p^{n-t}\right]} y^{p^t-1} x^{\left[p^{n-t}-k+\xi p^{(n-t)}\right]}} = \\
&= \overline{x^{p^n-\xi p^{n-t}+k} y^{p^t-1} x^{(\xi+1)p^{n-t}-k}} = \\
&= \overline{x^{p^n-\xi p^{n-t}+k} y^{\xi} x^{p^n-k} x^k y^{p^t-\xi-1} x^{(\xi+1)p^{n-t}-k}} = \\
&= -\overline{\beta_{k,(p^t-\xi)}} + \overline{\beta_{k,(p^t-\xi-1)}}\,.
\end{aligned}
$$

Em particular,

$$
x^{\left(p^{n-t}-k\right)} \circ \overline{v_{p^t-1}} = -\overline{\beta_{k,p^t}} + \overline{\beta_{k,(p^t-1)}} = \overline{\beta_{k,(p^t-1)}}.
$$

Suponhamos por indução que $\overline{\beta_{k,\epsilon}} \in J$, para um certo $\epsilon \in \{0,1,\ldots,(p^t-2)\}$.
Para $\xi = p^t - \epsilon - 1$, temos que:

$$
x^{\left[p^{(n-t)}-k+\left(p^t-\epsilon-1\right)p^{n-t}\right]} \circ \overline{v_{p^t-1}} = \overline{\beta_{k,\epsilon}} - \overline{\beta_{k,(\epsilon+1)}}.
$$

Logo,

$$\overline{\beta_{k,\epsilon}} - \left[-\overline{\beta_{k,(\epsilon+1)}} + \overline{\beta_{k,\epsilon}}\right] = \overline{\beta_{k,(\epsilon+1)}} \in J. \tag{2.3}$$

Assim, pela arbitrariedade do k, provamos que os $\overline{v_j}$ e os $\overline{\beta_{k,\tau}}$ pertencem a J, para

$$1 \leq j, \tau \leq (p^t - 1) \text{ e } 1 \leq k \leq (p^{n-t} - 1). \tag{2.4}$$

Portanto, temos que:

$$N = \left\langle \overline{v_{(p^t-1)}} \right\rangle = J$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo cíclico.

É claro que o conjunto de índices $\{up^{n-t}; (\xi+1)p^{n-t} - k \mid 0 \leq u \leq (p^t-2); 0 \leq \xi \leq (p^t-2); 1 \leq k \leq (p^{n-t}-1)\}$ percorre o conjunto de índices $\{0, 1, \ldots, p^n - p^{n-t} - 1\}$, um por um.

Agora, pelo Lema 24, temos que o $\mathbb{Z}_p$-submódulo de N gerado por

$$\Delta = \{x^{up^{n-t}} \circ \overline{v_{p^t-1}}\, ; x^{(\xi+1)p^{n-t}-k} \circ \overline{v_{p^t-1}} \mid 0 \leq u \leq (p^t-2); 0 \leq \xi \leq (p^t-2); 1 \leq k \leq (p^{n-t}-1)\}$$

é um $\mathbb{Z}_p$-módulo livre cujo posto é igual à $p^n - p^{n-t}$.

Assim, como vimos em (2.2), (2.3) e (2.4), temos que N está contido no $\mathbb{Z}_p$-módulo livre gerado por Δ, donde segue que N é o $\mathbb{Z}_p$-módulo livre com base Δ.

Já sabemos pela Observação 33 que os núcleos de $\Psi_{(n-t)} : \mathbb{Z}_p \langle x \rangle \twoheadrightarrow \mathbb{Z}_p C_{p^{n-t}}$, são $\mathbb{Z}_p \langle x \rangle$-módulos cíclicos gerados por $\left(x^{p^{n-t}} - 1\right)$.
Além disso, o núcleo $\mathrm{Ker}(\Psi_{(n-t)})$ é um $\mathbb{Z}_p$-módulo livre com base

$$\Omega := \left\{ x^\eta \circ \left(x^{p^{n-t}} - 1\right) \mid \eta \in \{0, 1, \ldots, (p^n - p^{n-t} - 1)\} \right\}.$$

Defina $\phi_{_{\Omega,\Delta}}$ como a aplicação que envia:

$$x^c \circ (x^{p^{n-t}} - 1) \longrightarrow x^c \circ \overline{v_{p^t-1}}$$

para todo $c \in \{0, 1, \ldots, (p^n - p^{n-t} - 1)\}$.
Pela propriedade universal do $\mathbb{Z}_p$-módulo livre $(x^{p^{n-t}} - 1)$, temos que existe um único $\mathbb{Z}_p$-homomorfismo:

$$\mu : (x^{p^{n-t}} - 1) \longrightarrow N = \langle \Delta \rangle,$$

tal que $\mu|_{\Omega} = \phi_{_{\Omega,\Delta}}$.

Vamos mostrar a partir de agora que μ é um $\langle x \rangle$-homomorfismo.
De fato, um elemento arbitrário θ do $\mathbb{Z}_p$-módulo livre $\left(x^{p^{n-t}} - 1\right)$, com base Ω, é da forma:

$$\theta = \sum_{\substack{\delta \in \{0, \ldots, (p^n - p^{n-t} - 1)\} \\ z_\delta \in \mathbb{Z}_p}} z_\delta x^\delta \left(x^{p^{n-t}} - 1\right).$$

Dado $x^{\tilde{u}} \in \langle x \rangle$, temos que:

$$\mu(x^{\tilde{u}} \circ \theta) = \sum_{\substack{\delta \in \{0,\ldots,(p^n - p^{n-t} - 1)\} \\ z_\delta \in \mathbb{Z}_p}} z_\delta x^{\tilde{u}+\delta} \circ \overline{v_{p^t - 1}} = x^{\tilde{u}} \circ \sum_{\substack{\delta \in \{0,\ldots,(p^n - p^{n-t} - 1)\} \\ z_\delta \in \mathbb{Z}_p}} z_\delta x^{\delta} \circ \overline{v_{p^t - 1}} = x^{\tilde{u}} \circ \mu(\theta) \, .$$

Portanto, pelo Lema 30, temos que μ é um $\mathbb{Z}_p \langle x \rangle$-homomorfismo de $\left(x^{p^{n-t}} - 1\right)$ para N. Agora, note que:

$$\mathrm{r}_p \left(\left(x^{p^{n-t}} - 1 \right) \right) = \mathrm{posto}(F_{p^n - p^{n-t}}) = p^n - p^{n-t} = \mathrm{r}_p(N).$$

Logo, μ é um isomorfismo de tais $\mathbb{Z}_p$-módulos livres.
Em particular, μ é uma bijeção.
Portanto, concluí-mos o seguinte:

$$\overline{F_{p^n - p^{n-t}}} := N = \langle \overline{v_{p^t-1}} \rangle \cong \left(x^{p^{n-t}} - 1\right) = \mathrm{Ker}(\mathbb{Z}_p \langle x \rangle \twoheadrightarrow \mathbb{Z}_p C_{p^{n-t}})$$

como $\mathbb{Z}_p C_{p^n}$-módulos. ∎

Por fim, vamos provar o seguinte lema:

Lema 61. *Seja $n \in \mathbb{N}$ e considere $G = C_{p^n} \coprod \mathbb{Z}_p = F_{p^n} \rtimes C_{p^n}$.*
Então o $\mathrm{ann}_{\mathbb{Z}_p C_{p^n}} \left(\frac{F_{p^n}}{F_{p^n}{}'} \right) = \{0\}$.

Demonstração. Considere $C_{p^n} = \langle x \rangle$ e $\mathbb{Z}_p = \overline{\langle \alpha \rangle}$. Como vimos na Proposição 59, temos que $\overline{F_{p^n}} = \langle \overline{\alpha} \rangle$ como um $\mathbb{Z}_p \langle x \rangle$-módulo.
Agora seja $p(x) = a_{[p^n-1]} x^{[p^n-1]} + a_{[p^n-2]} x^{[p^n-2]} + \cdots + a_1 x + a_0 \in \mathbb{Z}_p \langle x \rangle$, tal que:

$$p(x) \circ \overline{\alpha} = 0.$$

Então, nós temos que:

$$p(x) \circ \overline{\alpha} = a_{[p^n-1]} \overline{\alpha^{x^{[p^n-1]}}} + a_{[p^n-2]} \overline{\alpha^{x^{[p^n-2]}}} + \cdots + a_1 \overline{\alpha^x} + a_0 \overline{\alpha} = 0$$

em $\overline{F_{p^n}}$. Mas, $\overline{F_{p^n}}$ é um $\mathbb{Z}_p$-módulo livre com base $\{\overline{\alpha}, \ldots, \overline{\alpha^{x^{[(p^n)-1]}}}\}$.
Daí, segue que:

$$p(x) \circ \overline{\alpha} = 0 \Leftrightarrow a_j = 0, \;\; \forall j \in \{0, 1, \ldots, (p^n - 1)\}.$$

Portanto, $p(x) = 0$. Logo o $\mathrm{ann}_{\mathbb{Z}_p \langle x \rangle} \left(\frac{F_{p^n}}{[F_{p^n}]'} \right) = \{0\}$. ∎

2.4 Grupos Pro-p com Ação Fiel sobre o Grupo Abelianizado

Agora vamos caminhar para provarmos uma propriedade interessante dos grupos dados nas Proposições 59 e 60, ou seja, vamos mostrar que para os grupos:

$$C_{p^n} \coprod \mathbb{Z}_p \text{ e } C_{p^n} \coprod C_{p^t},$$

onde $t \in \{1, 2, \dots, n\}$, temos que C_{p^n} age fielmente sobre o grupo abelianizado, onde a ação é dada por conjugação. Esta proposição será fundamental na prova do **Teorema Principal**.

Para provarmos tal fato, vamos usar as Proposições 59 e 60, o Teorema 51 e as propriedades elementares do **módulo livre abstrato**.

Temos o seguinte resultado:

Proposição 62. *1. Se $G \cong C_{p^n} \coprod \mathbb{Z}_p$ e $n \in \mathbb{N}$. Então C_{p^n} age fielmente sobre $\overline{F}$.*

2. Seja $G \cong C_{p^n} \coprod C_{p^k}$, onde $k \in \{1, 2, \dots, (n-1), n\}$ e $n \in \mathbb{N}$. Então C_{p^n} age fielmente sobre $\overline{F}$.

Demonstração. 1. Considere

$$G = \langle x \rangle \coprod \overline{\langle \alpha \rangle},$$

onde $\langle x \rangle = C_{p^n}$ e $\overline{\langle \alpha \rangle} = \mathbb{Z}_p$.

Suponha por absurdo que C_{p^n} não age fielmente sobre $\overline{F}$.
Então existe um

$$1 \neq x^{p^{(n-t)}} \in \langle x \rangle \;,$$

tal que $x^{p^{(n-t)}}$ age trivialmente sobre $\frac{F}{F'}$.

Logo o ideal de $\mathbb{Z}_p \langle x \rangle$ dado por $\left(x^{p^{(n-t)}} - 1\right)$ anula $\overline{F}$.

Mas por outro lado, pelo Lema 61 nós vimos que o:

$$\operatorname{ann}_{\mathbb{Z}_p \langle x \rangle} \left(\overline{F}\right) = \{0\}.$$

Portanto, temos que $x^{p^{(n-t)}} - 1 = 0 \Rightarrow x^{p^{(n-t)}} = 1$, um absurdo.

2. Considere

$$G = \langle x \rangle \coprod \langle y \rangle \,,$$

onde $\langle x \rangle = C_{p^n}$ e $\langle y \rangle = C_{p^k}$.
Além disso, suponha por absurdo que $\langle x \rangle$ não age fielmente sobre $\overline{F}$.

Vamos fazer a nossa demonstração por partes.

- Caso A) Seja $n = 1$. Neste caso, a única possibilidade para k é $k = 1$. Assim, tomando-se $n = 1$ e $k = 1$ no Lema 58, obtemos que:

$$G \cong \left(C_p \coprod C_p\right) \cong F_{(p-1)} \rtimes C_p\,.$$

Pelo Teorema 51 e a **Teoria de Reiner e Heller** da **Seção 1.4.**, temos que:

$$\frac{F_{(p-1)}}{\left[F_{(p-1)}\right]'} \cong \mathbb{Z}_p[\theta_p]$$

como um $\mathbb{Z}_p\left\langle x\right\rangle$-módulo indecomponível.
Como $\left\langle x\right\rangle \cong C_p$ não age fielmente sobre $\frac{F_{(p-1)}}{\left[F_{(p-1)}\right]'}$, segue que existe um $1 \neq y \in \left\langle x\right\rangle$, tal que y fixa $\frac{F_{(p-1)}}{\left[F_{(p-1)}\right]'}$.
Mas, como a ordem de y é p, temos que $\left\langle x\right\rangle = \left\langle y\right\rangle$.
Portanto, nesta situação, temos que $\left\langle x\right\rangle$ age trivialmente sobre $\frac{F_{(p-1)}}{\left[F_{(p-1)}\right]'}$.
Logo, temos que

$$\frac{F_{(p-1)}}{\left[F_{(p-1)}\right]'} \cong \bigoplus_{j=1}^{(p-1)} \left[(\mathbb{Z}_p)_j\right]$$

como um $\mathbb{Z}_p\left\langle x\right\rangle$-módulo, onde os $(\mathbb{Z}_p)_j$ são o $\mathbb{Z}_p\left\langle x\right\rangle$-módulos indecomponíveis e triviais.
Seja $p = 2$, das observações acima, segue que:

$$\overline{F_1} \cong \mathbb{Z}_2 \cong \mathbb{Z}_2[\theta_2]$$

como $\mathbb{Z}_2C_2$-módulos, uma contradição pelo Teorema 46.
Seja $p > 2$, então temos que $\frac{F_{(p-1)}}{\left[F_{(p-1)}\right]'}$ é um $\mathbb{Z}_p\left\langle x\right\rangle$-módulo decomponível.
Agora, pelo Teorema 39 (T.K.S.A.) e pelo fato de $\frac{F_{(p-1)}}{\left[F_{(p-1)}\right]'} \cong \mathbb{Z}_p[\theta_p]$ ser um $\mathbb{Z}_p\left\langle x\right\rangle$-módulo indecomponível, temos novamente uma contradição.

- Caso B) Vamos assumir a partir de agora que $n \geq 2$. Mais uma vez, vamos supor por absurdo que $\left\langle x\right\rangle$ não age fielmente sobre $\overline{F}$.
Então existe um

$$1 \neq x^{p^{(n-t)}} \in \left\langle x\right\rangle$$

de ordem p^t, tal que o mesmo age trivialmente sobre $\overline{F}$.
- Considere $t = n$.
Pela nossa hipótese, temos que $\left\langle x\right\rangle$ age trivialmente sobre $\frac{F}{F'}$. Como vimos no Lema 58, temos que

$$G \cong C_{p^n} \coprod C_{p^k} \cong F_{p^n - p^{(n-k)}} \rtimes C_{p^n}.$$

Logo, nesta situação temos que:

$$\frac{F_{p^n-p^{(n-k)}}}{F_{p^n-p^{(n-k)}}{}'} \cong \bigoplus_{j=1}^{\left(p^n-p^{(n-k)}\right)} \left[(\mathbb{Z}_p)_j\right]$$

como um $\mathbb{Z}_p\langle x\rangle$-módulo decomponível, onde $(\mathbb{Z}_p)_j$ é o $\mathbb{Z}_p\langle x\rangle$-módulo indecomponível e trivial.
Mas por outro lado, a Proposição 60, nos diz que:

$$\overline{F_{p^n-p^{(n-k)}}} \cong \text{Ker } \left(\mathbb{Z}_p\langle x\rangle \twoheadrightarrow \mathbb{Z}_p C_{p^{(n-k)}}\right)$$

como um $\mathbb{Z}_p\langle x\rangle$-módulo indecomponível.
Novamente temos uma contradição pelo Teorema 39 (T.K.S.A.).

- Admitiremos a partir de agora que $t \in \{1, 2, \ldots, (n-1)\}$.
Nesse caso, pela hipótese temos que $x^{p^{(n-t)}} \neq 1, x$ e além disso o mesmo age trivialmente sobre $\frac{F}{F'}$. Portanto, $\left(x^{p^{(n-t)}}-1\right)$ anula $\overline{F}$. Logo, temos que o ideal:

$$\left(x^{p^{(n-t)}}-1\right) \subset \text{ann}_{\mathbb{Z}_p\langle x\rangle} \left(\overline{F}\right).$$

Vamos separar o final da prova de tal Proposição em duas partes, são elas:
Parte 1) Quando $k = n$ e **Parte 2)** Quando $k \neq n$.

- **Parte 1)**Quando $k = n$. Nesse caso,

$$G = \langle x\rangle \coprod \langle y\rangle \cong C_{p^n} \coprod C_{p^n}.$$

Pela Proposição 60, tínhamos que:

$$\overline{F} \cong \text{Ker } (\mathbb{Z}_p\langle x\rangle \twoheadrightarrow \mathbb{Z}_p) = (x-1)$$

como um $\mathbb{Z}_p\langle x\rangle$-módulo indecomponível.
Agora, pela hipótese, temos que o ideal $\left(x^{p^{(n-t)}}-1\right)$ de $\mathbb{Z}_p\langle x\rangle$ anula $\overline{F}$.
Assim, temos que $\left(x^{p^{(n-t)}}-1\right)\cdot(x-1) = x^{\left[p^{(n-t)}+1\right]} - x^{p^{[n-t]}} - x + 1 = 0$ em $\mathbb{Z}_p\langle x\rangle$.
Como $p^{(n-t)} \in \{p, p^2, \ldots, p^{(n-1)}\}$, temos que:

$$p^{(n-t)} < p^n, \ \forall\ t \in \{1, \ldots, (n-1)\}.$$

Além disso,

$$\left[p^{(n-t)}+1\right] < p^n \text{ e } p^{(n-t)}+1 \not\equiv p^{(n-t)} \pmod{p^n}\ \forall t.$$

Portanto, a equação:

$$x^{\left[p^{(n-t)}+1\right]} - x^{p^{[n-t]}} - x + 1 = 0,$$

não vale em $\mathbb{Z}_p\langle x\rangle$, visto que o mesmo é um $\mathbb{Z}_p$-módulo livre com base

$$\{1, x, \ldots, x^{p^{(n-t)}}, x^{\left[p^{(n-t)}+1\right]}, \ldots, x^{[p^n-1]}\}.$$

Considere por fim, a última parte de tal Proposição.

- **Parte 2)** Quando $k \in \{1, 2, \ldots, (n-1)\}$. Nesse caso,

$$G = \langle x \rangle \coprod \langle y \rangle \cong C_{p^n} \coprod C_{p^k},$$

onde $n \in \mathbb{N}$, $n \geq 2$ e $\langle x \rangle \cong C_{p^n}$. Além disso, pelo Lema 58, temos que $G \cong F_{p^n - p^{n-k}} \rtimes C_{p^n}$. Vamos escrever $F_{p^n - p^{n-k}}$ simplesmente como F.
Pela Proposição 60, tínhamos que:

$$\overline{F} \cong \text{Ker } \left(\mathbb{Z}_p \langle x \rangle \twoheadrightarrow \mathbb{Z}_p C_{p^{(n-k)}}\right) = \left(x^{p^{(n-k)}} - 1\right),$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo indecomponível.
Agora, pela hipótese, temos que o ideal $\left(x^{p^{(n-t)}} - 1\right)$ de $\mathbb{Z}_p \langle x \rangle$ anula $\overline{F}$.
Assim, temos que:

$$\left(x^{p^{(n-t)}} - 1\right) \cdot \left(x^{p^{(n-k)}} - 1\right) = x^{\left[p^{(n-t)} + p^{(n-k)}\right]} - x^{p^{(n-t)}} - x^{p^{(n-k)}} + 1 = 0 \quad (2.5)$$

em $\mathbb{Z}_p \langle x \rangle$.
Cabe-nos ressaltar que $\mathbb{Z}_p \langle x \rangle$ é um $\mathbb{Z}_p$-módulo livre com base

$$\{1, x, \ldots, x^{p^{(n-t)}}, \ldots, x^{[p^n - 1]}\}.$$

Para encerrar, basta mostrar que a equação (2.5), não vale em $\mathbb{Z}_p \langle x \rangle$.
Primeiramente, note que:

$$p^{(n-t)} \in \{p, p^2, \ldots, p^{(n-1)}\} \quad \text{e} \quad p^{(n-k)} \in \{p, p^2, \ldots, p^{(n-1)}\},$$

para todo $t \in \{1, 2, \ldots, n-1\}$ e para todo $k \in \{1, 2, \ldots, n-1\}$.
Assim, para todo t, temos que:

$$p^{(n-t)} \not\equiv 0 \pmod{p^n} \;\text{ e }\; p^{(n-k)} \not\equiv 0 \pmod{p^n}.$$

O que implica que $x^{p^{(n-t)}} \neq 1$ e $x^{p^{(n-k)}} \neq 1$, $\forall\, t, k$.

- Seja agora $t = k$. Então da equação (2.5), resta-nos somente:

$$x^{\left[2p^{(n-t)}\right]} - 2x^{p^{(n-t)}} + 1 = 0.$$

Independentemente dos valores possíveis que:

$$x^{\left[2p^{(n-t)}\right]}$$

assuma em $\mathbb{Z}_p \langle x \rangle$, pela variação da variável t; nós não podemos ter validade da equação (2.5) em $\mathbb{Z}_p \langle x \rangle$, dado que o mesmo é um $\mathbb{Z}_p$-módulo livre com base

$$\{1, x, \ldots, x^{p^{(n-t)}}, \ldots, x^{[p^n - 1]}\}.$$

- Seja agora $t \neq k$.
De maneira análoga a situação precedente temos novamente uma contradição, pelo fato de $\mathbb{Z}_p \langle x \rangle$ ser um $\mathbb{Z}_p$-módulo livre com base

$$\{1, x, \ldots, x^{[p^n - 1]}\}.$$

■

2.5 Caracterizando F e $\overline{F}$ em Função de $G = F \rtimes C_{p^n}$

Nessa seção, vamos usar a versão pro-p do (TSK), ou seja, o Teorema 11, para provarmos alguns Lemas que serão muito úteis nas seções posteriores. Vamos começar com o seguinte Lema, que foi provado por Herfort-Zalesskii em [8], sem demonstrá-lo.

Lema 63. *Cada grupo pro-p virtualmente livre e finitamente gerado, tem à menos de conjugação, somente um número finito de subgrupos finitos.*

A partir deste Lema, temos o seguinte corolário que nos será muito útil na prova dos resultados dessa seção:

Corolário 64. *Em um grupo pro-p virtualmente livre e finitamente gerado, temos que o número de classes de conjugação de subgrupos de ordem p, é finito.*

Demonstração. Segue diretamente do Lema 63, já que à menos de conjugação, a quantidade de subgrupos de ordem p em tais grupos é finita. ■

À luz do Corolário 64, temos o seguinte lema:

Lema 65. *Considere $n \in \mathbb{N}$. Seja $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito em G. Admita que G seja escrito como um produto livre pro-p de normalizadores de subgrupos de ordem p em G, assim como no Teorema 50, ou seja,*

$$G = \coprod_{i=1}^{k \geq 1} \left[N_G \left(\langle x_i \rangle \right) \right] \coprod F_m \,,$$

onde F_m é um subgrupo pro-p livre de F cujo posto é m. Além disso, o conjunto $\{\langle x_i \rangle, 1 \leq i \leq k\}$ é um sistema de representantes de classes de conjugação de subgrupos de ordem p em G. Seja $C_{p^n} = \langle x \rangle$ e admita que $\langle x \rangle \hookrightarrow N_G \left(\langle x_1 \rangle \right)$. Então

$$F = \left[F \cap N_G \left(\langle x_1 \rangle \right) \right] \coprod \left[\coprod_{d_{x_2} \in \Xi_2} \left[F \cap \{ N_G \left(\langle x_2 \rangle \right) \}^{d_{x_2}} \right] \right] \coprod$$

$$\coprod \cdots \coprod \left[\coprod_{d_{x_k} \in \Xi_k} \left[F \cap \{ N_G \left(\langle x_k \rangle \right) \}^{d_{x_k}} \right] \right] \coprod F_m \coprod {F_m}^{x} \coprod \cdots \coprod {F_m}^{x^{p^n - 1}} \coprod F_s,$$

onde F_s é um subgrupo pro-p livre de F, de posto igual a $s \in \mathbb{N}$ e os conjuntos Ξ_j são sistemas de representantes de classes duplas para $F \backslash G / N_G \left(\langle x_j \rangle \right)$, onde $2 \leq j \leq k$.

Demonstração. Primeiramente, pelo Corolário 64, temos que $k \in \mathbb{N}$. Vamos aplicar o Teorema 11 (TSK) para F como um subgrupo aberto de G.

Assim, temos que:

$$F = \left[F \cap \mathrm{N}_G \left(\langle x_1 \rangle \right) \right] \coprod \left[\coprod_{d_{x_2} \in \Xi_2} \left[F \cap \{ \mathrm{N}_G \left(\langle x_2 \rangle \right) \}^{d_{x_2}} \right] \right] \coprod$$

$$\coprod \cdots \coprod \left[\coprod_{d_{x_k} \in \Xi_k} \left[F \cap \{\mathrm{N}_G\ (\langle x_k \rangle)\}^{d_{x_k}} \right] \right] \coprod F_m \coprod {F_m}^x \coprod \cdots \coprod {F_m}^{x^{p^n-1}} \coprod F_s,$$

onde $F_s = \left(F_s^{\mathrm{abs}}\right)_{\hat{p}}$ e F_s^{abs} é o grupo livre abstrato que aparece quando aplicamos o **Teorema do Subgrupo de Kurosch para grupos abstratos** ao grupo $F \cap \Gamma$ como um subgrupo do grupo abstrato $\Gamma = \left(*_{i=1}^{k \geq 1}\ [\mathrm{N}_G\ (\langle x_i \rangle)] \right) * F_m$.

Por fim, como o posto(F) é finito, o Teorema 15 implica que o posto de cada um dos fatores livres dado acima é finito, em particular o posto$(F_s) = s \in \mathbb{N}$. ■

À luz do **Lema 65** e supondo que $C_{p^n} = \langle x \rangle$, considere para cada $2 \leq i \leq k$, elementos $y_i \in \mathrm{N}_G\ (\langle x_i \rangle)$ de tal forma que os mesmos tem ordem maximal e finita em cada um dos correspondentes normalizadores e sejam suas ordens respectivamente iguais a p^{t_i}, onde $1 \leq t_i \leq n$.
Agora, temos a imersão natural de

$$C_{p^n} \coprod C_{p^{t_i}} = \langle x \rangle \coprod \langle y_i \rangle = F_{p^n - p^{n-t_i}} \rtimes \langle x \rangle \hookrightarrow G \text{ (Lema 58).}$$

Defina para cada $i \in \{2, \ldots, k\}$, os seguintes grupos pro-p livres

$$F_{x,t_i} := F_{p^n - p^{n-t_i}}.$$

Note que, pela Observação 13 do Teorema 11 (TSK), se $t_i = n$, então

$$F_{p^n-1} = \overline{\langle x^u y^{(-u)} |\, 1 \leq u \leq (p^n - 1) \rangle}$$

e se $t_i \neq n$, temos que:

$$F_{p^n - p^{n-t_i}} = \overline{\left\langle x^{p^n - sp^{n-t_i}} y_i^s; x^r y_i^s x^{\left(p^n - sp^{[n-t_i]} - r\right)} |\, 1 \leq s \leq (p^{t_i} - 1); 1 \leq r \leq (p^{n-t_i} - 1) \right\rangle}.$$

Agora podemos provar o seguinte corolário:

Corolário 66. *Considere as hipóteses do Lema 65 e admita F_s como neste mesmo Lema. Então:*

$$F_s = F_{x,t_2} \coprod F_{x,t_3} \coprod \ldots \coprod F_{x,t_k}.$$

Demonstração. Considere o seguinte grupo abstrato

$$G^{\mathrm{abs}} = \left(*_{i=1}^{k \geq 1}\ [\mathrm{N}_G\ (\langle x_i \rangle)] \right) * F_m^{\mathrm{abs}},$$

onde $F_m = \left(F_m^{\mathrm{abs}}\right)_{\hat{p}}$ e além disso F_m^{abs} é o grupo livre abstrato sobre o mesmo conjunto de geradores topológicos livres de F_m.
Como podemos ver na Observação 10, temos que:

$$G = \left(G^{\mathrm{abs}}\right)_{\hat{p}}.$$

Seguindo as notações precedentes, sejam os seguintes subgrupos de G^{abs} :

$$\langle x\rangle * \langle y_i\rangle = F^{\text{abs}}_{p^n-p^{n-t_i}} \rtimes \langle x\rangle\,,$$

onde $F_{p^n-p^{n-t_i}} = \left(F^{\text{abs}}_{p^n-p^{n-t_i}}\right)_{\hat{p}}$.

Como vimos no Lema 65, temos que $F_s = \left(F^{\text{abs}}_s\right)_{\hat{p}}$, onde:

$$F^{\text{abs}}_s = F^{\text{abs}}_{p^n-p^{n-t_2}} * F^{\text{abs}}_{p^n-p^{n-t_3}} * \ldots * F^{\text{abs}}_{p^n-p^{n-t_k}}$$

pela Observação 13 do Teorema 11.
Portanto,

$$F_s = \left(F^{\text{abs}}_{p^n-p^{n-t_2}}\right)_{\hat{p}} \coprod \left(F^{\text{abs}}_{p^n-p^{n-t_3}}\right)_{\hat{p}} \coprod \cdots \coprod \left(F^{\text{abs}}_{p^n-p^{n-t_k}}\right)_{\hat{p}} = F_{x,t_2} \coprod F_{x,t_3} \coprod \cdots \coprod F_{x,t_k}.$$

■

Vamos usar a partir de agora a seguinte notação $F_{x_1} := [F \cap \mathrm{N}_G\left(\langle x_1\rangle\right)]$ e para todo $d_{x_k} \in \Xi_k$ como no Lema 65, escreveremos $F_{d_{x_k}} = \left[F \cap \{\mathrm{N}_G\left(\langle x_k\rangle\right)\}^{d_{x_k}}\right]$.
Assim, teremos as seguintes abelianizações:

$$\overline{F_{x_1}} = \frac{F_{x_1}}{F_{x_1}{}'} = \frac{[F \cap \mathrm{N}_G\left(\langle x_1\rangle\right)]}{[F \cap \mathrm{N}_G\left(\langle x_1\rangle\right)]\,'}$$

e

$$\overline{F_{d_{x_k}}} = \frac{F_{d_{x_k}}}{F_{d_{x_k}}{}'} = \frac{\left[F \cap \{\mathrm{N}_G\left(\langle x_k\rangle\right)\}^{d_{x_k}}\right]}{\left[F \cap \{\mathrm{N}_G\left(\langle x_k\rangle\right)\}^{d_{x_k}}\right]\,'}.$$

Vamos provar o seguinte Lema:

Lema 67. *Seja F um grupo pro-p livre de posto n, onde $n \in \mathbb{N}$. Suponhamos que F se fatora como um produto livre pro-p da seguinte maneira:*

$$F = F_d \coprod F_{(n-d)}\,,$$

onde $d \leq n$.
Então

$$\frac{F_d\,F\,'}{F\,'} \cong \frac{F_d}{F_d{}'} \quad e \quad \frac{F_{(n-d)}\,F\,'}{F\,'} \cong \frac{F_{(n-d)}}{F_{(n-d)}{}'}\,.$$

Em particular, temos que $F_d{}' = F_d \cap F\,'$ e $F_{(n-d)}{}' = F_{(n-d)} \cap F\,'$.

Demonstração. Basta provar o Lema, para o grupo F_d, pois o caso do grupo $F_{(n-d)}$ procede de maneira análoga.
Considere o epimorfismo canônico contínuo de grupos pro-p:

$$\phi : F \twoheadrightarrow \frac{F}{F\,'}\,.$$

Agora, temos que:

$$\phi(F_d) = \frac{F_d\, F'}{F'} \lhd_c \frac{F}{F'}\,.$$

Observamos que $\frac{F_d\, F'}{F'}$ é um grupo pro-p abeliano livre de posto igual ao de F_d.
Pelos **Teoremas dos Isomorfismos**, temos que:

$$\frac{F_d\, F'}{F'} \cong \frac{F_d}{F' \cap F_d}\,.$$

Agora, note que:

$$F_d{}' \subset (F_d \cap F') \subset F_d\,.$$

Assim, segue dos **Teoremas dos Isomorfismos**, que existe um epimorfismo canônico de grupos abelianos pro-p, dado abaixo:

$$\phi_d : \frac{F_d}{F_d{}'} \twoheadrightarrow \frac{F_d}{F' \cap F_d}\,,$$

onde o $\mathrm{Ker}\,(\phi_d) = \frac{F' \cap F_d}{F_d{}'}$.
Mas, note que:

$$\text{posto } \left(\frac{F_d}{F_d{}'}\right) = \text{posto } \left(F_d\right) = \text{posto } \left(\frac{F_d\, F'}{F'}\right) = \text{posto } \left(\frac{F_d}{F' \cap F_d}\right)\,.$$

Assim, segue que ϕ_d é um isomorfismo, já que os mesmos são grupos pro-p abelianos livres. Portanto, temos que:

$$\frac{F_d}{F_d{}'} \cong \frac{F_d}{F_d \cap F'} \cong \frac{F_d\, F'}{F'} \tag{2.6}$$

A parte final deste Lema, segue diretamente do isomorfismo (2.6) e do fato de que

$$F_d{}' \subset (F_d \cap F')\,.$$

■

A partir de agora, vamos provar uma Proposição que será o **alicerce** para as seções posteriores, essa Proposição terá um papel fundamental na demonstração do **Teorema Principal** dessa tese.

Proposição 68. *Considere $n \in \mathbb{N}$. Seja $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito. Admita que G seja escrito como um produto livre pro-p de normalizadores de subgrupos de ordem p em G, assim como no Teorema 50, ou seja,*

$$G = \coprod_{i=1}^{k} \left[N_G\left(\langle x_i \rangle\right)\right] \coprod F_m\,,$$

onde $k \geq 1$ e F_m é um subgrupo pro-p livre de F cujo posto é $m \in \mathbb{N}$. Além disso, o conjunto $\{\langle x_i \rangle, 1 \leq i \leq k\}$ é um sistema de representantes de classes de conjugação de subgrupos de ordem p em G. Suponha que $C_{p^n} = \langle x \rangle$ e além disso considere que $\langle x \rangle \hookrightarrow N_G(\langle x_1 \rangle)$. Então

$$\overline{F} \cong \overline{F_{\mathcal{X}}} \oplus \overline{F_M} \oplus \overline{F_s}$$

como um $\mathbb{Z}_p C_{p^n}$-módulo, onde:

$$F_{\mathcal{X}} := F_{x_1} \coprod \left[\coprod_{d_{x_2} \in \Xi_2} F_{d_{x_2}} \right] \coprod \cdots \coprod \left[\coprod_{d_{x_k} \in \Xi_k} F_{d_{x_k}} \right],$$

$$F_M := F_m \coprod {F_m}^x \coprod \cdots \coprod {F_m}^{x^{(p^n-1)}}$$

e além disso observamos que $F_{d_{x_i}}$ e F_s já foram definidos nas páginas 45 e 46.

Demonstração. Aplicando-se os Lemas 65 e 67, temos que:

$$\overline{F} \cong \overline{F_{\mathcal{X}}} \oplus \overline{F_M} \oplus \overline{F_s}$$

como um $\mathbb{Z}_p$-módulo livre. Daí segue que a interseção entre tais grupos abelianos pro-p, é nula.

Como $G = F \rtimes \langle x \rangle$, segue imediatamente que $\overline{F}$ é um $\langle x \rangle$-módulo.
Assim, segue da Proposição 27 que $\overline{F}$ é um $\mathbb{Z}_p \langle x \rangle$-módulo.

Precisamos provar somente que:

$$\overline{F_{\mathcal{X}}},\ \overline{F_M} \text{ e } \overline{F_s}$$

são $\mathbb{Z}_p \langle x \rangle$-módulos.

Vamos dividir o restante da prova em 3 partes, são elas:

1. $\overline{F_{\mathcal{X}}}$ é isomorfo a um $\mathbb{Z}_p \langle x \rangle$-submódulo de $\overline{F}$;
2. $\overline{F_M}$ é isomorfo a um $\mathbb{Z}_p \langle x \rangle$-submódulo de $\overline{F}$;
3. $\overline{F_s}$ é isomorfo a um $\mathbb{Z}_p \langle x \rangle$-submódulo de $\overline{F}$.

Parte 1) $\overline{F_{\mathcal{X}}}$ é um $\mathbb{Z}_p \langle x \rangle$-módulo.
Primeiramente, considere $F_{x_1} := F \cap \mathrm{N}_G(\langle x_1 \rangle)$, então

$$F_{x_1}^{\langle x \rangle} \subset \left[F^{\langle x \rangle} \cap [\mathrm{N}_G(\langle x_1 \rangle)]^{\langle x \rangle} \right] \subset [F \cap \mathrm{N}_G(\langle x_1 \rangle)] =: F_{x_1}$$

já que $\langle x \rangle \hookrightarrow \mathrm{N}_G(\langle x_1 \rangle)$.
Portanto, $\overline{F_{x_1}}$ é um $\langle x \rangle$-módulo. Logo, pela Proposição 27 temos que $\overline{F_{x_1}}$ é um $\mathbb{Z}_p \langle x \rangle$-módulo.

Precisamos estudar o que ocorre com a abelianização de cada grupo da forma $\left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)$, onde $a \in \{2,\ldots,k\}$.

Afirmação: $\overline{\left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)}$ é um $\mathbb{Z}_p\langle x\rangle$-módulo para cada $a \in \{2,\ldots,k\}$.

Justificativa: Seja $f \in \left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)$ e $z = c\tilde{f} \in F \rtimes \langle x\rangle = G$ um elemento arbitrário de G, onde $c \in \langle x\rangle$ e $\tilde{f} \in F$.

Relembrando que $\Xi_a \subseteq \langle x\rangle$, temos que

$$(f)^{c\tilde{f}} \in \left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)^{\tilde{f}} \subset \left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)^{F}. \tag{2.7}$$

Como

$$\left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)^{F} \subset \left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)^{G},$$

segue de (2.7) que:

$$\left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)^{G} = \left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)^{F}.$$

Em particular,

$$\left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)^{\langle x\rangle} \subset \left(\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}\right)^{F}.$$

Agora, módulo $F' = \overline{[F,F]}$, não existe conjugação não trivial por elementos de F, donde concluí-mos pelo Lema 67 que:

$$\left[\overline{\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}}\right]^{\langle x\rangle} \subset \left[\overline{\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}}\right] \cong \left(\bigoplus_{d_{x_a}\in\Xi_a} \overline{F_{d_{x_a}}}\right).$$

Portanto, pela Proposição 27 temos que $\overline{\coprod_{d_{x_a}\in\Xi_a} F_{d_{x_a}}}$ é um $\mathbb{Z}_p\langle x\rangle$-módulo para todo $a\in\{2,\ldots,k\}$.

Dado que

$$F_{\mathcal{X}} = F_{x_1}\coprod\left(\coprod_{d_{x_2}\in\Xi_2} F_{d_{x_2}}\right)\coprod\cdots\coprod\left(\coprod_{d_{x_k}\in\Xi_k} F_{d_x}\right),$$

juntando-se todas essas observaçẽs e aplicando-se o Lema 67, temos que:

$$\overline{F_{\mathcal{X}}}\cong\overline{F_{x_1}}\oplus\left[\bigoplus_{d_{x_2}\in\Xi_2}\overline{F_{d_{x_2}}}\right]\oplus\cdots\oplus\left[\bigoplus_{d_{x_k}\in\Xi_k}\overline{F_{d_{x_k}}}\right]$$

como um $\mathbb{Z}_p\langle x\rangle$-módulo.

Parte 2) $\overline{F_M}$ é um $\mathbb{Z}_p\langle x\rangle$-módulo.

Escrevamos $F_m=\overline{\langle\alpha_1,\ldots,\alpha_m\rangle}$. Pelo Lema 65, vimos que:

$$\begin{aligned}
F_M &= \overline{F_m\coprod[F_m]^x\coprod\cdots\coprod[F_m]^{x^{p^n-1}}} =\\
&= \overline{\left\langle\alpha_1,\ldots,(\alpha_1)^{x^{p^n-1}}\right\rangle}\coprod\cdots\coprod\overline{\left\langle\alpha_m,\ldots,(\alpha_m)^{x^{p^n-1}}\right\rangle} =\\
&= \left(\coprod_{j_1=0}^{p^n-1}\overline{\left\langle(\alpha_1)^{x^{j_1}}\right\rangle}\right)\coprod\cdots\coprod\left(\coprod_{j_m=0}^{p^n-1}\overline{\left\langle(\alpha_m)^{x^{j_m}}\right\rangle}\right).
\end{aligned}$$

Defina para cada $r\in\{1,2,\ldots,m\}$, o seguinte:

$$M_{\alpha_r} := \bigoplus_{j_r=0}^{p^n-1}\left[\frac{\overline{\left\langle{\alpha_r}^{x^{j_r}}\right\rangle}F'}{F'}\right].$$

Agora, $\forall r\in\{1,2,\ldots,m\}$, temos que:

$$\left[\left(\coprod_{j_r=0}^{p^n-1}\overline{\left\langle{\alpha_r}^{x^{j_r}}\right\rangle}\right)\right]^{\langle x\rangle}\subset\left(\coprod_{j_r=0}^{p^n-1}\overline{\left\langle{\alpha_r}^{x^{j_r}}\right\rangle}\right), \tag{2.8}$$

pois a ação de $\langle x\rangle$ permuta os conjugados de α_r e todos os possíveis conjugados do mesmo estão em

$$\left(\coprod_{j_r=0}^{p^n-1}\overline{\left\langle{\alpha_r}^{x^{j_r}}\right\rangle}\right).$$

É claro que M_{α_r} é um $\mathbb{Z}_p$-módulo livre e além disso por (2.8) temos que o mesmo é um $\langle x\rangle$-módulo. Logo, pela Proposição 27, temos que M_{α_r} é um $\mathbb{Z}_p\langle x\rangle$-módulo para cada $1\le r\le m$.
Portanto, concluí-mos que:

$$F_M\cong M_{\alpha_1}\oplus\cdots\oplus M_{\alpha_m}$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo.

Por fim, vamos provar a parte 3).

Parte 3) $\overline{F_s}$ é um $\mathbb{Z}_p \langle x \rangle$-módulo.

Como vimos no Corolário 66, temos que:

$$F_s = F_{x,t_2} \coprod F_{x,t_3} \coprod \cdots \coprod F_{x,t_k} \,,$$

onde os F_{x,t_r} são subgrupos pro-p livres e f.g. de F_s, dados por:

$$F_{x,n} = \overline{\left\langle x^u y_r^{[-u]}, \text{ onde } u \in \{1, \ldots, p^n - 1\} \right\rangle},$$

quando $t_r = n$ e quando $t_r \neq n$, temos que

$$F_{x,t_r} = \overline{\left\langle x^{\left[p^n - sp^{(n-t_r)}\right]} y_r^s \,,\ x^r y_r^s x^{\left[p^n - sp^{(n-t_r)} - r\right]} \right\rangle}\,,$$

onde $1 \leq s \leq (p^{t_r} - 1)$ e $1 \leq r \leq \left[p^{(n-t_r)} - 1\right]$.

Para cada r, a Proposição 60 nos garante que cada:

$$\overline{F_{x,t_r}} := \frac{F_{x,t_r}}{(F_{x,t_r})\,'}$$

é um $\mathbb{Z}_p \langle x \rangle$-módulo indecomponível, que se levanta para o grupo pro-p $F_{x,t_r} \rtimes \langle x \rangle$.

Agora, pelo Lema 67, temos que:

$$\overline{F_s} \cong \overline{F_{x,t_2}} \oplus \cdots \oplus \overline{F_{x,t_k}}$$

como um $\mathbb{Z}_p$-módulo livre.
Portanto, juntando-se todas estas informações, chegamos à:

$$\overline{F_s} \cong \overline{F_{x,t_2}} \oplus \cdots \oplus \overline{F_{x,t_k}}$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo. ■

Corolário 69. *Considere as mesmas hipóteses da Proposição 68 da página 47. Se $k \geq 2$ então $\overline{F_{x,t_i}} \neq \{0\}$, para todo $i = 2, 3, \ldots, k$.*

Demonstração. Pelo Corolário 66 temos que

$$F_s = F_{x,t_2} \coprod F_{x,t_3} \coprod \ldots \coprod F_{x,t_k},$$

onde

$$F_{x,t_i} := F_{p^n - p^{n-t_i}}$$

e $F_{p^n-p^{n-t_i}}$ é obtido a partir do grupo

$$C_{p^n} \coprod C_{p^{t_i}} = \langle x \rangle \coprod \langle y_i \rangle = F_{p^n-p^{n-t_i}} \rtimes C_{p^n},$$

como podemos ver na página 45. Além disso, note que

$$F_{p^n-p^{n-t_i}} = \left(F^{\text{abs}}_{p^n-p^{n-t_i}}\right)_{\hat{p}},$$

onde o grupo $F^{\text{abs}}_{p^n-p^{n-t_i}}$ é obtido a partir do grupo abstrato $\langle x \rangle * \langle y_i \rangle \cong C_{p^n} * C_{p^{t_i}}$.
Pela Observação 13 do Teorema 11, sabemos que pelo menos os elementos

$$x^{p^n-p^{n-t_i}} y_i \in \langle x \rangle * \langle y_i \rangle$$

são geradores livres de cada $F^{\text{abs}}_{p^n-p^{n-t_i}}$, para cada $i = 2, 3, \ldots, k$. Além disso, pela forma normal do produto livre abstrato (veja Lyndon [16]), temos que $x^{p^n-p^{n-t_i}} y_i \neq 1$.
Como $F_{x,t_i} = F_{p^n-p^{n-t_i}} = \left(F^{\text{abs}}_{p^n-p^{n-t_i}}\right)_{\hat{p}}$, segue que cada $F_{x,t_i} \neq \{1\}$ e por conseguinte $\overline{F_{x,t_i}} \neq \{0\}$, para todo $i = 2, 3, \ldots, k$. ■

Corolário 70. *Nas mesmas condições do Corolário 69, temos que* $\overline{F_s} \neq \{0\}$ *se* $k \geq 2$.

Demonstração. Como vimos na Proposição 68, temos que:

$$\overline{F_s} \cong \overline{F_{x,t_2}} \oplus \cdots \oplus \overline{F_{x,t_k}}$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo. Pelo Corolário 69 sabemos que cada um dos somandos diretos acima é não-nulo, donde segue que $F_s \neq \{0\}$. ■

2.6 Quando as Abelianizações Induzem Alguns Módulos Decomponíveis

Queremos provar nessa seção, alguns fatos muito interessantes, que serão usados na prova do **Teorema Principal**.
Estes fatos, caracterizam de certa maneira, como devem ser os grupos G da forma $F \rtimes C_{p^n}$, quanto a **quantidade e os tipos** de fatores livres que os mesmos podem ter, segundo o Teorema 50, para que $\overline{F}$ seja um $\mathbb{Z}_p C_{p^n}$-reticulado decomponível.

Por fim, mostraremos que se $G = F \rtimes C_{p^n}$ é escrito como um produto livre pro-p de normalizadores de subgrupos de ordem p e C_{p^n} age fielmente sobre $\overline{F}$, então G tem pelo menos dois fatores livres.

Para tanto, vamos usar às versões pro-p do **Teorema do Subgrupo de Kurosh**, veja o Teorema 11, a fórmula do posto que se encontra na parte b) do mesmo teorema e o **Teorema de Grushko-Neumann**, que nessa tese é o Teorema 15.

Começamos com o seguinte Lema:

Lema 71. *Seja $n \in \mathbb{N}$. Considere $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito em G. Admita que G seja escrito como um produto livre pro-p de normalizadores de subgrupos de ordem p em G, assim como no Teorema 50, ou seja,*

$$G = \coprod_{i=1}^{k\geq 1} \left[N_G \left(\langle x_i \rangle \right) \right] \coprod F_m \,,$$

onde F_m é um subgrupo pro-p livre de F cujo posto é $m \geq 2$. Além disso, o conjunto $\{\langle x_i \rangle, 1 \leq i \leq k\}$ é um sistema de representantes de classes de conjugação de subgrupos de ordem p em G. Também suponha que $C_{p^n} = \langle x \rangle \hookrightarrow N_G \left(\langle x_1 \rangle \right)$.
Então $\overline{F}$ é um $\mathbb{Z}_p C_{p^n}$-módulo decomponível.

Demonstração. Seja $G = F \rtimes \langle x \rangle$, onde $C_{p^n} = \langle x \rangle$ e considere $F_m = \overline{\langle \alpha_1, \ldots, \alpha_m \rangle}$.
Como vimos na Proposição 68, temos que:

$$\overline{F} \cong \overline{F_{\mathcal{X}}} \oplus \overline{F_M} \oplus \overline{F_s}$$

como um $\mathbb{Z}_p C_{p^n}$-módulo, tal que:

$$F_{\mathcal{X}} := F_{x_1} \coprod \left[\coprod_{d_{x_2} \in \Xi_2} F_{d_{x_2}} \right] \coprod \cdots \coprod \left[\coprod_{d_{x_k} \in \Xi_k} F_{d_{x_k}} \right] \quad \text{e}$$

$$\overline{F_M} = M_{\alpha_1} \oplus \cdots \oplus M_{\alpha_m},$$

onde cada:

$$M_{\alpha_r} := \bigoplus_{j_r=0}^{p^n-1} \left[\frac{\overline{\left\langle (\alpha_r)^{x^{j_r}} \right\rangle F'}}{F'} \right] \cong \bigoplus_{j_r=0}^{p^n-1} \left[\frac{\overline{\left\langle (\alpha_r)^{x^{j_r}} \right\rangle}}{\overline{\left\langle (\alpha_r)^{x^{j_r}} \right\rangle}'} \right] \cong \bigoplus_{j_r=0}^{p^n-1} \left[\overline{\left\langle (\alpha_r)^{x^{j_r}} \right\rangle} \right].$$

Já que $m \geq 2$, podemos supor sem perda de generalidade que pelo menos os somandos diretos M_{α_1} e M_{α_2} são não-nulos.
Defina o seguinte $\mathbb{Z}_p \langle x \rangle$-módulo:

$$L := M_{\alpha_2} \oplus \ldots \oplus M_{\alpha_m} \oplus \overline{F_{\mathcal{X}}} \oplus \overline{F_s}.$$

É claro que L é um $\mathbb{Z}_p \langle x \rangle$-módulo não nulo, já que pelo menos $\{0\} \neq M_{\alpha_2} \subset L$.

Portanto,

$$\overline{F} \cong M_{\alpha_1} \oplus L$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo decomponível. ∎

Observação 72. *Como vimos no Lema 71, nós devemos considerar $m = 0$ ou $m = 1$, para encontrarmos $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis, a partir de grupos pro-p da forma $F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito.*

Temos a seguinte proposição, onde G admite uma decomposição como um produto livre pro-p com mais do que 2 fatores livres.

Proposição 73. *Admita as mesmas hipóteses do Lema 71. Suponhamos que $m \in \mathbb{N}$, $k \geq 3$ e que $C_{p^n} = \langle x \rangle$. Então $\overline{F}$ é um $\mathbb{Z}_p C_{p^n}$-módulo decomponível.*

Demonstração. Pela Proposição 68, temos que:

$$\overline{F} \cong \overline{F_{\mathcal{X}}} \oplus \overline{F_M} \oplus \overline{F_s}$$

como um $\mathbb{Z}_p C_{p^n}$-módulo.
Além disso, pela Proposição 68 temos que:

$$\overline{F_s} \cong \overline{F_{x,t_2}} \oplus \overline{F_{x,t_3}} \oplus \cdots \oplus \overline{F_{x,t_k}}$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo não-nulo e decomponível, já que podemos supor sem perda de generalidade pelo Corolário 69, que pelo menos os dois primeiros somandos diretos de $\overline{F_s}$ são não-nulos, já que $k \geq 3$.

Defina o seguinte $\mathbb{Z}_p \langle x \rangle$-módulo:

$$U := \overline{F_{x,t_3}} \oplus \cdots \oplus \overline{F_{x,t_k}} \oplus \overline{F_s} \oplus \overline{F_M}.$$

Como $\{0\} \neq \overline{F_{x,t_3}} \subset U$, segue que U é um $\mathbb{Z}_p \langle x \rangle$-módulo não-nulo.

Portanto, temos que:

$$\overline{F} \cong \overline{F_{x,t_2}} \oplus U$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo decomponível. ■

Finalizaremos essa seção como o seguinte resultado:

Lema 74. *Seja $n \in \mathbb{N}$. Considere $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito em G.*
Admita que G seja escrito como:

$$G = \coprod_{i=1}^{k \geq 1} \left[N_G \left(\langle x_i \rangle \right) \right],$$

assim como no Teorema 50. Além disso, o conjunto $\{\langle x_i \rangle, 1 \leq i \leq k\}$ é um sistema de representantes de classes de conjugação de subgrupos de ordem p em G.
Se $\overline{F}$ é um $\mathbb{Z}_p C_{p^n}$-módulo com ação fiel do C_{p^n}, então $k \neq 1$.

Demonstração. Suponhamos por absurdo que k seja igual a 1. Consideremos $C_{p^n} = \langle x \rangle$.
Nesse, caso

$$G = \mathrm{N}_G \left(\left\langle x^{p^{(n-1)}} \right\rangle \right) = F \rtimes \langle x \rangle \cong F \rtimes C_{p^n},$$

onde observamos que G não é finito.

Pela hipótese, temos que $\left\langle x^{p^{(n-1)}} \right\rangle \lhd_c G$. Além disso,

$$\left[\left\langle x^{p^{(n-1)}} \right\rangle \cap F\right] \subset [\langle x \rangle \cap F] = \{1\} .$$

Donde segue que:

$$F \rtimes \left\langle x^{p^{(n-1)}} \right\rangle = F \times \left\langle x^{p^{(n-1)}} \right\rangle <_c F \rtimes \langle x \rangle = G .$$

Nesse caso, $\left\langle x^{p^{(n-1)}} \right\rangle$ age trivialmente sobre F e por conseguinte sobre $\overline{F}$.
Logo $C_{p^n} = \langle x \rangle$ não age fielmente sobre $\overline{F}$, uma contradição. ■

2.7 A Importância dos Grupos $C_{p^n} \coprod C_{p^t}$

Proposição 75. *Seja $n \in \mathbb{N}$. Considere $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito em G. Admita que G seja escrito como:*

$$G = \coprod_{i=1}^{k \geq 1} \left[N_G\left(\langle x_i \rangle\right)\right] ,$$

assim como no Teorema 50, onde o conjunto $\{\langle x_i \rangle, 1 \leq i \leq k\}$ é um sistema de representantes de classes de conjugação de subgrupos de ordem p em G. Além disso suponha que $\overline{F}$ seja um $\mathbb{Z}_p C_{p^n}$-reticulado indecomponível com ação fiel do C_{p^n}. Considere $\langle x \rangle \hookrightarrow \left[N_G\left(\langle x_1 \rangle\right)\right]$. Então os únicos grupos G para os quais $\overline{F}$ tem essas propriedades, são da forma:

$$C_{p^n} \coprod C_{p^t},$$

onde $1 \leq t \leq n$.

Demonstração. Se $k \geq 3$, a Proposição 73 nos garante que $\overline{F}$ é um $\mathbb{Z}_p C_{p^n}$-reticulado decomponível e tais grupos não satisfazem a nossa hipótese.
Seja $k = 1$. Pelo Lema 74, devemos ter uma ação não fiel do C_{p^n} sobre o $\overline{F}$, uma contradição pela nossa hipótese.
Portanto, vamos considerar a partir de agora somente o caso em que $k = 2$. Nessa situação G se decompõe como um produto livre da seguinte maneira:

$$\left[\mathrm{N}_G\left(\langle x_1 \rangle\right)\right] \coprod \left[\mathrm{N}_G\left(\langle x_2 \rangle\right)\right] .$$

Segue do Lema 65, que:

$$F = F_{x_1} \coprod \left[\coprod_{d_{x_2} \in \Xi_2} F_{d_{x_2}}\right] \coprod F_s,$$

onde F_s é um subgrupo pro-p livre de F, cujo posto é $s \in \mathbb{N}$ e Ξ_2 é um conjunto de representantes de classes duplas para $F \setminus G/\mathrm{N}_G\left(\langle x_2\rangle\right)$.

Pela Proposição 68, temos que:

$$\overline{F} \cong \overline{F_{x_1}} \oplus \left[\bigoplus_{d_{x_2}\in\Xi_2} \overline{F_{d_{x_2}}}\right] \oplus \overline{F_s}$$

como um $\mathbb{Z}_p\langle x\rangle$-módulo. Pelo Corolário 70, temos que $\overline{F_s} \neq \{0\}$, já que $k = 2$.

Para que $\overline{F}$ seja um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível devemos ter

$$\overline{F_{x_1}} = \{0\} \ \text{ e } \ \overline{F_{x_2}} := \left[\bigoplus_{d_{x_2}\in\Xi_2} \overline{F_{d_{x_2}}}\right] = \{0\}.$$

Para $i = 1, 2$, temos que:

$$\left[\bigoplus_{d_{x_i}\in\Xi_i} \overline{F_{d_{x_i}}}\right] := \left[\bigoplus_{d_{x_i}\in\Xi_i} \left(\frac{\left(F \cap \{\mathrm{N}_G\left(\langle x_i\rangle\right)\}^{d_{x_i}}\right)}{\left(F \cap \{\mathrm{N}_G\left(\langle x_i\rangle\right)\}^{d_{x_i}}\right)'}\right)\right] \cong \overline{\coprod_{d_{x_i}\in\Xi_i}\left[F \cap \{\mathrm{N}_G\left(\langle x_i\rangle\right)\}^{d_{x_i}}\right]}$$

como grupos pro-p abelianos livres, onde as barras superiores indicam a abelianização dos grupos dados.

Agora, para que $\left[\bigoplus_{d_{x_i}\in\Xi_i} \overline{F_{d_{x_i}}}\right] = \{0\}$, devemos ter $\coprod_{d_{x_i}\in\Xi_i}\left[F \cap \{\mathrm{N}_G\left(\langle x_i\rangle\right)\}^{d_{x_i}}\right] = \{1\}$. Em particular, devemos ter $F \cap \mathrm{N}_G\left(\langle x_i\rangle\right) = \{1\}$, para cada $i = 1, 2$.

Note que $F \cap \mathrm{N}_G\left(\langle x_i\rangle\right) \lhd_c \mathrm{N}_G\left(\langle x_i\rangle\right)$, para cada $i = 1, 2$. Logo pelo Teorema do Isomorfismo, temos que:

$$\frac{\mathrm{N}_G\left(\langle x_i\rangle\right)}{F \cap \mathrm{N}_G\left(\langle x_i\rangle\right)} \cong \frac{F\mathrm{N}_G\left(\langle x_i\rangle\right)}{F} \leq \frac{G}{F} \cong C_{p^n}. \tag{2.9}$$

Já que devemos ter $F \cap \mathrm{N}_G\left(\langle x_i\rangle\right) = \{1\}$, segue de (2.9) que o $\mathrm{N}_G\left(\langle x_i\rangle\right)$ é finito para cada $i = 1, 2$.

Como $G = F \rtimes C_{p^n}$ e $\langle x\rangle \hookrightarrow \mathrm{N}_G\left(\langle x_1\rangle\right) \hookrightarrow F \rtimes C_{p^n}$, temos que:

$$\mathrm{N}_G\left(\langle x_1\rangle\right) \cong C_{p^n} \ \text{ e } \ \mathrm{N}_G\left(\langle x_2\rangle\right) \cong C_{p^t},$$

para algum $t \in \{1, 2, \ldots, n\}$.

Portanto, concluí-mos que $G \cong C_{p^n} \coprod C_{p^t}$, para algum $t \in \{1, 2, \ldots, n\}$. ■

2.8 O Caso em que $m = 1$.

Considere nessa seção, grupos pro-p da forma $F \rtimes C_{p^n}$, onde $n \in \mathbb{N}$ e F é um grupo pro-p livre de posto finito. Pela Observação 72, basta considerarmos $m = 0$ ou 1 para encontrarmos $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis a partir de grupos pro-p da forma $F \rtimes C_{p^n}$. Na **Seção 2.7.**, nós consideramos o caso em que $m = 0$.
Agora, nosso objetivo nessa seção será o de encontrar no caso em que $m = 1$, grupos pro-p da forma $F \rtimes C_{p^n}$, tais que o $\overline{F}$ seja um $\mathbb{Z}_p C_{p^n}$-reticulado indecomponível.
Visto as observações acima, vamos considerar a partir de agora grupos G da forma:

$$G = \coprod_{i=1}^{k} \left[\mathrm{N}_G\left(\langle x_i \rangle\right)\right] \coprod \mathbb{Z}_p,$$

assim como no Teorema 50.

Temos a seguinte proposição:

Proposição 76. *Sejam $n \in \mathbb{N}$ e $k \geq 1$. Considere $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito em G. Admita que G seja escrito como:*

$$G = \coprod_{i=1}^{k \geq 1} \left[N_G\left(\langle x_i \rangle\right)\right] \coprod \mathbb{Z}_p,$$

assim como no Teorema 50, onde $k \in \mathbb{N}$ e $\{\langle x_i \rangle, 1 \leq i \leq k\}$ é um sistema completo de representantes de classes de conjugação de subgrupos de ordem p em G.
Suponha que $\overline{F}$ seja um $\mathbb{Z}_p C_{p^n}$-reticulado indecomponível.
Então o único grupo G para o qual $\overline{F}$ tem essas propriedades é

$$C_{p^n} \coprod \mathbb{Z}_p.$$

Demonstração. Se $k \geq 3$, então a Proposição 73, nos diz que $\overline{F}$ é um $\mathbb{Z}_p C_{p^n}$-módulo decomponível, o que não pode ocorrer pela nossa hipótese juntamente com o Teorema 39.

Resta-nos estudar somente os casos em $k = 1$ ou 2.

Considere primeiramente $k = 2$. Seja $C_{p^n} = \langle x \rangle$ e $\mathbb{Z}_p = \overline{\langle \alpha \rangle}$. Além disso, suponha sem perda de generalidade que $\langle x \rangle \hookrightarrow \mathrm{N}_G\left(\langle x_1 \rangle\right)$.
Pela Proposição 68, temos que:

$$\overline{F} \cong \overline{F_{x_1}} \oplus \left[\bigoplus_{d_{x_2} \in \Xi_2} \left(\overline{F_{d_{x_2}}}\right)\right] \oplus M_\alpha \oplus \overline{F_s},$$

como um $\mathbb{Z}_p C_{p^n}$-módulo, onde relembramos que

$$M_\alpha := \bigoplus_{j=0}^{x^{p^n}-1} \left[\frac{\overline{\langle \alpha^{x^j} \rangle} F'}{F'}\right] \cong \bigoplus_{j=0}^{x^{p^n}-1} \left[\overline{\langle \alpha^{x^j} \rangle}\right].$$

Como $\overline{\langle\alpha\rangle} = \mathbb{Z}_p$, temos que $M_\alpha \neq \{0\}$.
Logo para que $\overline{F}$ seja um $\mathbb{Z}_pC_{p^n}$-módulo indecomponível, devemos ter:

$$\overline{F_{x_1}} = \{0\}, \left[\bigoplus_{d_{x_2}\in\Xi_2}\left(\overline{F_{d_{x_2}}}\right)\right] = \{0\} \text{ e } \overline{F_s} = \{0\}.$$

Agora, pelo Corolário 70 temos que

$$\overline{F_s} \neq \{0\}.$$

Portanto, se $k = 2$ temos que $\overline{F}$ é um $\mathbb{Z}_pC_{p^n}$-módulo decomponível, que não satisfaz a nossa hipótese.

Assim, devemos considerar somente o caso em que $k = 1$.
Nesse caso, a Proposição 68, nos diz que $\overline{F}$ se reduz ao seguinte $\mathbb{Z}_pC_{p^n}$-módulo:

$$\overline{F} \cong \overline{F_{x_1}} \oplus M_\alpha.$$

Novamente como $M_\alpha \neq \{0\}$, devemos considerar $\overline{F_{x_1}} = \{0\}$, para obtermos o $\mathbb{Z}_pC_{p^n}$-módulo indecomponível $\overline{F}$.
Mas isso ocorre somente se $F \cap \mathrm{N}_G\left(\langle x_1\rangle\right) = \{1\}$. Assim como procedemos na Proposição 75 (2.9), temos que $\mathrm{N}_G\left(\langle x_1\rangle\right)$ é finito.

Portanto, como $C_{p^n} = \langle x\rangle \hookrightarrow \mathrm{N}_G\left(\langle x_1\rangle\right)$ e $G = F \rtimes C_{p^n}$, temos que

$$\mathrm{N}_G\left(\langle x_1\rangle\right) = \langle x\rangle \cong C_{p^n}.$$

Logo, a única possibilidade para o grupo G é seguinte:

$$G \cong C_{p^n} \coprod \mathbb{Z}_p.$$

■

2.9 O Teorema Principal

Nessa seção, vamos provar o resultado principal desta tese, que diz o seguinte:

Teorema 77. *Considere $n \in \mathbb{N}$. Seja*

$$G \cong F \rtimes C_{p^n}$$

um produto semi-direto pro-p de um grupo pro-p livre de posto finito por C_{p^n}. Suponha que a representação de C_{p^n} sobre $\overline{F} = \frac{F}{F'}$ induzida pela conjugação, é uma $\mathbb{Z}_p$-representação fiel e indecomponível. Então $\overline{F} = \frac{F}{F'}$ é de um dos tipos dados logo abaixo:

1. $$\overline{F} \cong \text{Ker}\ (\mathbb{Z}_p C_{p^n} \twoheadrightarrow 0) \cong \mathbb{Z}_p C_{p^n},$$

2. $$\overline{F} \cong \text{Ker}\ (\mathbb{Z}_p C_{p^n} \twoheadrightarrow \mathbb{Z}_p C_{p^m}),$$

   como um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, tal que $m \in \mathbb{N}$ satisfaz $0 \leq m \leq (n-1)$.

*Além disso, os únicos $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis, com C_{p^n}-ação fiel, que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$, são dos tipos **1) e 2)** dados nesse Teorema.*

Antes de provarmos o **Teorema Principal**, vamos demonstrar o seguinte Teorema:

Teorema 78. *Considere $n \in \mathbb{N}$. Os únicos grupos pro-p G da forma*

$$F \rtimes C_{p^n},$$

onde F é um grupo pro-p livre de posto finito, tais que $\overline{F}$ é um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível com ação fiel do C_{p^n} são de uma das seguintes formas dadas abaixo:

1. $C_{p^n} \coprod \mathbb{Z}_p = F_{p^n} \rtimes C_{p^n}$
2. $C_{p^n} \coprod C_{p^t} = F_{p^n - p^{n-t}} \rtimes C_{p^n}$, *onde* $1 \leq t \leq n$.

Demonstração. Primeiramente, pelo Teorema 50 sabemos que

$$G = \coprod_{i=1}^{k} \left[\text{N}_G\ (\langle x_i \rangle)\right] \coprod F_m$$

onde F_m é um subgrupo pro-p livre de posto finito de F (o posto finito segue do Teorema 15, já que F_m é um fator livre de F pelo Teorema 11); o conjunto $\{\langle x_i \rangle, 1 \leq i \leq k\}$ é um sistema completo de representantes de classes de conjugação de subgrupos de ordem p em G e $1 \leq k < \infty$.

Pela Observação 72, temos que considerar somente os casos em que $m = 0$ ou $m = 1$, para encontrarmos grupos pro-p da forma $F \rtimes C_{p^n}$, cujo grupo $\overline{F}$ é um $\mathbb{Z}_p C_{p^n}$-reticulado indecomponível.

- Vamos considerar primeiramente o caso em que $m = 0$. Nesse caso, a Proposição 75 nos garante que os únicos grupos G com as propriedades da assertiva deste corolário são os seguintes:
$$C_{p^n} \coprod C_{p^t},$$
para algum $t \in \{1, \ldots, n\}$.

- Por fim, suponhamos $m = 1$. Para essa situação, a Proposição 76 nos garante que o único grupo $G = F \rtimes C_{p^n}$, para o qual o grupo $\overline{F}$ é um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, é o grupo
$$C_{p^n} \coprod \mathbb{Z}_p = F_{p^n} \rtimes C_{p^n}.$$

Além disso, pela Proposição 62, temos que C_{p^n} age fielmente sobre $\overline{F_{p^n}}$ e o corolário está provado.

■

Agora podemos provar o principal resultado desta tese, o **Teorema 77:**

Demonstração. Pelo Teorema 78, sabemos que os únicos grupos da forma:
$$F \rtimes C_{p^n},$$
com as propriedades requeridas na hipótese do Teorema Principal, são de um dos tipos abaixo:
$$\text{ou} \;\; C_{p^n} \coprod \mathbb{Z}_p \;\; \text{ou} \; C_{p^n} \coprod C_{p^t} \,,$$
para qualquer $t \in \{1, \ldots, n\}$.
Escreva $m := n - t$, então temos obviamente que $m \in \{0, 1, \ldots, (n-1)\}$.
Agora, se
$$G \cong C_{p^n} \coprod \mathbb{Z}_p \;\; \text{ou} \;\; G \cong C_{p^n} \coprod C_{p^t} \,,$$
então pelas Proposições 59 e 60, chegamos respectivamente à:
$$\overline{F} \cong \operatorname{Ker}(\mathbb{Z}_p C_{p^n} \twoheadrightarrow 0) \cong \mathbb{Z}_p C_{p^n} \tag{2.10}$$
ou
$$\overline{F} \cong \operatorname{Ker}\,(\mathbb{Z}_p C_{p^n} \twoheadrightarrow \mathbb{Z}_p C_{p^m}) \tag{2.11}$$
como um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, onde $0 \leq m \leq (n-1)$.

Por fim, como os únicos grupos com as propriedades do Teorema são dos tipos:
$$\text{ou} \;\; C_{p^n} \coprod \mathbb{Z}_p \;\; \text{ou} \;\; C_{p^n} \coprod C_{p^t} \,,$$
temos que os únicos $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis com C_{p^n}-ação fiel, que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$, são dos tipos (2.10) e (2.11) dados acima. ■

Capítulo 3

Consequências do Resultado Principal

Nosso objetivo nesse capítulo é o de mostrarmos várias consequências do **Teorema Principal** (o Teorema 77).
Começaremos com a **Seção 3.1.**, onde provaremos que alguns dos $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis com ação não fiel do C_{p^n}, também se levantam para algum grupo pro-p da forma:

$$F \rtimes C_{p^n}.$$

Os reticulados referidos acima, surgem naturalmente das representações fiéis, estudadas por nós no **Capítulo 2**.
A seguir, mostraremos uma proposição que caracterizará todos os $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$.
Além disso, exibiremos uma fórmula que dará explicitamente a quantidade de tais reticulados indecomponíveis que possuem a propriedade de se levantarem para algum grupo pro-p da forma $F \rtimes C_{p^n}$.

Na **Seção 3.2.**, veremos um contraste entre os Teoremas 77, 79 e à Teoria de Reiner e Heller da **Seção 1.4.**.

Por fim, vamos fazer a última seção desse capítulo (a **Seção 3.3.**), onde iremos provar o seguinte fato:

Se $G \cong F_k \rtimes C_{p^n}$, onde $n \in \mathbb{N}$ e $k \geq p^n + 1$, então $\overline{F_k}$ é um $\mathbb{Z}_p C_{p^n}$-reticulado decomponível.

3.1 As Representações Não Fiéis que se Levantam

No **Teorema Principal** (o Teorema 77), caracterizamos todos os $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$, onde C_{p^n} age fielmente e indecomponivelmente sobre $\overline{F} := \frac{F}{F'}$.

Nesta seção, queremos exibir quais são os outros $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que tem a propriedade de se levantarem para algum grupo pro-p da forma:

$$F \rtimes C_{p^n} \,,$$

cuja a ação de C_{p^n} não é fiel sobre $\frac{F}{F'}$.

Além disso, no final dessa seção vamos provar uma proposição que dará a quantidade exata de representações p-ádicas indecomponíveis que se levantam para grupos pro-p da forma:

$$F \rtimes C_{p^n} \,.$$

Começaremos provando o seguinte Teorema:

Teorema 79 (Não-fiéis)**.** *Seja $n \in \mathbb{N}$. Considere $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito e $C_{p^n} = \langle x \rangle$. Seja $k \in \{1, 2, \ldots, n\}$, de maneira que C_{p^k} seja o subgrupo maximal de C_{p^n} com a propriedade de agir trivialmente sobre $\overline{F} = \frac{F}{F'}$. Além disso, suponha que C_{p^n} age indecomponivelmente sobre $\overline{F}$. Então $\overline{F} = \frac{F}{F'}$ é de um dos tipos dados logo abaixo:*

1.

$$\overline{F} \cong \operatorname{Ker}\left(\mathbb{Z}_p C_{p^{(n-k)}} \twoheadrightarrow 0\right) \cong \mathbb{Z}_p C_{p^{(n-k)}},$$

2.

$$\overline{F} \cong \operatorname{Ker}\left(\mathbb{Z}_p C_{p^{(n-k)}} \twoheadrightarrow \mathbb{Z}_p C_{p^{m'}}\right)$$

como um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, tal que m' satisfaz $0 \leq m' \leq n - k - 1$.

Além disso, esses são os únicos $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$, com as propriedades requeridas por esse Teorema.

Demonstração. Primeiramente, considere $k = n$.
Nesse caso, C_{p^n} age trivialmente sobre o $\mathbb{Z}_p C_{p^n}$-reticulado indecomponível $\overline{F}$, pela nossa hipótese. Portanto, vale a parte (1) do Teorema já que:

$$\overline{F} \cong \mathbb{Z}_p \cong \mathbb{Z}_p C_{p^{(n-n)}}$$

como um $\mathbb{Z}_p C_{p^n}$-reticulado trivial e indecomponível.

Vamos supor a partir de agora $k \neq n$. Pela Definição 1, temos que C_{p^n} age continuamente sobre F. Dado que a aplicação canônica $F \twoheadrightarrow \frac{F}{F'}$ é uma aplicação aberta, segue que C_{p^n} também age continuamente sobre $\overline{F}$. Além disso, note que $\frac{C_{p^n}}{C_{p^k}}$ também age continuamente sobre $\overline{F}$ e sua ação é dada pela ação dos representantes das classes laterais de C_{p^n} sobre C_{p^k}.
Agora, pela nossa hipótese juntamente com o Lema 57, temos que $\frac{C_{p^n}}{C_{p^k}}$ age indecomponivelmente sobre $\overline{F}$ e além disso temos que $\{1\} \neq \frac{C_{p^n}}{C_{p^k}}$ age fielmente sobre o $\overline{F}$.

Portanto, pelo Teorema 78, sabemos que $\overline{F}$ se levanta para algum grupo pro-p da forma $F \rtimes \frac{C_{p^n}}{C_{p^k}} := \tilde{G}$.

Donde obtemos pelo Teorema 77 que:

$$\text{ou } \overline{F} \cong \mathbb{Z}_p \left[\frac{C_{p^n}}{C_{p^k}} \right]$$

$$\text{ou } \overline{F} \cong \operatorname{Ker} \left(\mathbb{Z}_p \left[\frac{C_{p^n}}{C_{p^k}} \right] \twoheadrightarrow \mathbb{Z}_p C_{p^{m'}} \right)$$

como um $\mathbb{Z}_p \left[\frac{C_{p^n}}{C_{p^k}} \right]$-módulo indecomponível, onde $m' \in \{0, 1, \ldots, n-k-1\}$.

O Lema 34, nos garante que cada $\mathbb{Z}_p \left[\frac{C_{p^n}}{C_{p^k}} \right]$-módulo é naturalmente um $\mathbb{Z}_p C_{p^n}$-módulo anulado pelo ideal bilateral $\left(x^{p^{n-k}} - 1 \right)$, onde $\left\langle x^{p^{n-k}} \right\rangle = C_{p^k}$ e
$k \in \{1, 2, \ldots, (n-1)\}$.

Portanto, segue que:

$$\text{ou } \overline{F} \cong \mathbb{Z}_p C_{p^{n-k}}$$

$$\text{ou } \overline{F} \cong \operatorname{Ker} \left(\mathbb{Z}_p C_{p^{n-k}} \twoheadrightarrow \mathbb{Z}_p C_{p^{m'}} \right)$$

como um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, anulado por $\left(x^{p^{n-k}} - 1 \right)$, onde
$m' \in \{0, 1, \ldots, (n-k-1)\}$. ∎

Visto que provamos o Teorema 79, podemos encontrar a partir de agora, todos os $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis e não-isomorfos que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$, onde F é um grupo pro-p livre f.g. Isto pode ser resumido no seguinte:

Corolário 80. *Seja $n \in \mathbb{N}$. Os únicos $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis e não-isomorfos que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de* posto *finito, são isomorfos como $\mathbb{Z}_p C_{p^n}$-módulos, a um dos tipos dados abaixo:*

1. *Se C_{p^n} age fielmente, então ou $\overline{F} \cong \mathbb{Z}_p C_{p^n}$, ou $\overline{F} \cong \operatorname{Ker} (\mathbb{Z}_p C_{p^n} \twoheadrightarrow \mathbb{Z}_p C_{p^m})$, onde $m \in \{0, 1, \ldots, n-1\}$;*

2. *Para todo $k \in \{1, 2, \ldots, (n-1)\}$, se $C_{p^k} \neq \{1\}$ é o subgrupo maximal de C_{p^n}, agindo trivialmente sobre $\overline{F}$, então ou $\overline{F} \cong \mathbb{Z}_p C_{p^{n-k}}$, ou $\overline{F} \cong \operatorname{Ker} \left(\mathbb{Z}_p C_{p^{n-k}} \twoheadrightarrow \mathbb{Z}_p C_{p^{m_k}} \right)$ como $\mathbb{Z}_p C_{p^n}$-módulos, onde $m_k \in \{0, 1, \ldots, n-k-1\}$.*

3. *Se C_{p^n} age trivialmente sobre $\overline{F}$, então $\overline{F} \cong \mathbb{Z}_p$, ou seja, $\overline{F}$ é isomorfo ao $\mathbb{Z}_p C_{p^n}$-módulo trivial e indecomponível (veja a **Seção 1.4.**, dessa tese).*

Demonstração. 1. Segue diretamente do Teorema 77.

2. Segue do Teorema 79, fazendo-se a aplicação desse fato para cada $k \in \{1, \ldots, (n-1)\}$.

3. Segue trivialmente pelo Teorema 79.

$\blacksquare$

Agora vamos exibir quais são os grupos que se levantam para os reticulados que aparecem no Corolário 80.

Note que o $\mathbb{Z}_p C_{p^n}$-módulo trivial e indecomponível $\mathbb{Z}_p$, se levanta para o grupo pro-p $C_{p^n} \times \mathbb{Z}_p$, onde $r_p(\mathbb{Z}_p) = 1$.

Teorema 81. *Seja $n \in \mathbb{N}$ e $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto $s \geq 2$. Suponhamos que $\overline{F}$ seja um $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, onde C_{p^k} é o subgrupo maximal próprio e não-trivial de C_{p^n} agindo trivialmente sobre $\overline{F}$. Então*

$$G \cong C_{p^n} \coprod_{C_{p^k}} \left(C_{p^k} \times \mathbb{Z}_p\right) \quad ou \quad G \cong C_{p^n} \coprod_{C_{p^k}} C_{p^{t^*}},$$

onde $t^* \in \{k+1, \ldots, n\}$.

Demonstração. Como $G = F \rtimes C_{p^n}$, existe um homomorfismo contínuo de grupos pro-p, dado abaixo:

$$\Psi : C_{p^n} \longrightarrow \mathrm{Aut}(F).$$

Além disso, como $F' = \overline{[F, F]}$ é um subgrupo característico de F, temos o homomorfismo induzido dos grupos abaixo:

$$\xi : \mathrm{Aut}(F) \longrightarrow \mathrm{Aut}\left(\frac{F}{F'}\right).$$

Pela Proposição 4.5.4. no livro de Ribes-Zalesskii [22], temos que ξ é um epimorfismo de grupos pro-p.

Assim temos a seguinte composição

$$\xi \circ \Psi : C_{p^n} \longrightarrow \mathrm{Aut}(F) \twoheadrightarrow \mathrm{Aut}\left(\frac{F}{F'}\right).$$

Agora, a ação de C_{p^k} sobre F, é dada pela ação de $\Psi(C_{p^k})$ sobre F e como pela nossa hipótese C_{p^k} age trivialmente sobre $\overline{F}$, temos que $\Psi(C_{p^k}) \in \mathrm{Ker}(\xi)$.
Pelo Lema 16, sabemos que o $\mathrm{Ker}(\xi)$ é um grupo livre de torção pro-p. Como $\Psi(C_{p^k})$ é finito, segue que o mesmo é trivial em $\mathrm{Aut}(F)$. Mas isto implica que C_{p^k} age trivialmente sobre F. Portanto

$$C_{p^k} \subseteq Z(F \rtimes C_{p^n}) = Z(G),$$

donde segue que C_{p^k} é um subgrupo normal de G.
Vamos considerar a partir de agora o grupo pro-p $\frac{G}{C_{p^k}} = F \rtimes \left[\frac{C_{p^n}}{C_{p^k}}\right]$.

Note que $\frac{C_{p^n}}{C_{p^k}}$ age fielmente e indecomponivelmente sobre $\overline{F}$, o que implica pelo Teorema 78 que:

$$\frac{G}{C_{p^k}} \cong \frac{C_{p^n}}{C_{p^k}} \coprod \mathbb{Z}_p \quad \text{ou} \quad \frac{G}{C_{p^k}} \cong \frac{C_{p^n}}{C_{p^k}} \coprod \frac{C_{p^{t^*}}}{C_{p^k}},$$

onde $t^* \in \{k+1, \ldots, n\}$.

Vamos dividir a prova do restante desse Teorema em duas partes, são elas:

- **Parte 1)** Quando $\frac{G}{C_{p^k}} \cong \frac{C_{p^n}}{C_{p^k}} \coprod \mathbb{Z}_p$ e
- **Parte 2)** Quando $\frac{G}{C_{p^k}} \cong \frac{C_{p^n}}{C_{p^k}} \coprod \frac{C_{p^{t^*}}}{C_{p^k}}$.

Parte 1) Considere $\frac{G}{C_{p^k}} \cong \frac{C_{p^n}}{C_{p^k}} \coprod \mathbb{Z}_p$.

Assim como fizemos no Lema 58, temos que $\frac{C_{p^n}}{C_{p^k}} \coprod \mathbb{Z}_p \cong F_{p^{n-k}} \rtimes \left[\frac{C_{p^n}}{C_{p^k}}\right]$, onde $C_{p^n} := \langle x \rangle$ e $\mathbb{Z}_p := \overline{\langle \beta \rangle}$.
Além disso, considere o seguinte epimorfismo canônico contínuo dos grupos pro-p :

$$\omega : G \twoheadrightarrow \frac{G}{C_{p^k}} = F_{p^{n-k}} \rtimes \left[\frac{C_{p^n}}{C_{p^k}}\right].$$

Claramente $\frac{C_{p^n}}{C_{p^k}} = \left\langle \overline{x} := x + C_{p^k} \right\rangle$ em $\frac{G}{C_{p^k}}$.
Considere agora o seguinte grupo pro-p virtualmente livre

$$\tilde{G} = C_{p^n} \coprod_{C_{p^k}} \left(C_{p^k} \times \mathbb{Z}_p\right),$$

onde $C_{p^n} = \langle a \rangle$, $C_{p^k} = \langle b \rangle$ e $\mathbb{Z}_p = \overline{\langle \alpha \rangle}$.
A propriedade universal do produto livre amalgamado pro-p, nos diz que existe um único epimorfismo contínuo $\gamma : \tilde{G} \twoheadrightarrow \langle \omega \rangle \cong C_{p^n}$, que aplica $a \longmapsto \omega$, $b \longmapsto \omega^{p^{n-k}}$ e $\alpha \longmapsto 1$.
Agora note que o Ker(γ) é um grupo pro-p livre de torção, pois caso contrário, considere $1 \neq y \in \text{Ker}(\gamma)$ de ordem p^s onde $1 \leq s \leq n$. Segue de Ribes-Zalesskii [25] (Teorema 4.2., item b) que ou $\langle y \rangle \subseteq \left\langle a^{d_a} \right\rangle$ ou $\langle y \rangle \subseteq \left\langle b^{d_b} \right\rangle$, para alguns $d_a, d_b \in \tilde{G}$ (note que $\langle y \rangle \cap \overline{\langle \alpha \rangle} \cong C_{p^s} \cap \mathbb{Z}_p = \{1\}$). Mas pela definição de γ, sabemos que $\left\langle a^{d_a} \right\rangle$ e $\left\langle b^{d_b} \right\rangle$ não estão contidos no Ker(γ), uma contradição já que $y \in \ker(\gamma)$.
Além disso, note que o índice de Ker (γ) é igual a p^n, donde segue que Ker$(\gamma) \triangleleft_o \tilde{G}$.
Pelo Lema 7, sabemos que $\tilde{G}$ é próprio. Assim seja

$$\tilde{G}^{\text{abs}} = \langle a \rangle *_{\langle b \rangle} (\langle b \rangle \times \langle \alpha \rangle)$$

o produto livre amalgamado desses grupos. Temos obviamente que $\tilde{G}^{\text{abs}} \hookrightarrow \tilde{G}$.
Agora considere Ker$(\gamma) \cap \tilde{G}^{\text{abs}}$ como um subgrupo de $\tilde{G}^{\text{abs}}$. O mesmo é livre de torção já

que $\mathrm{Ker}(\gamma)$ também o é. Como $\tilde{G}^{\mathrm{abs}}$ é virtualmente livre (veja Serre [29], Corolário da Proposição 11), segue de Serre [29] (Proposição 11, letra b, página 120) que $\mathrm{Ker}(\gamma)\cap\tilde{G}^{\mathrm{abs}}$ é um subgrupo livre de $\tilde{G}^{\mathrm{abs}}$, cujo índice é igual a p^n.
Novamente pela Observação 14 e por Serre (Exercício 3 da página 123), segue que o posto de $\mathrm{Ker}(\gamma)\cap\tilde{G}^{\mathrm{abs}}$ é igual a:

$$1+p^n\left(\frac{1}{p^k}+\frac{1}{p^k}-\frac{1}{p^k}-\frac{1}{p^n}\right)=1+p^{n-k}+p^{n-k}-p^{n-k}-1=p^{n-k}.$$

Como $\tilde{G}^{\mathrm{abs}}$ é um subgrupo denso em $\tilde{G}$ e $\mathrm{Ker}(\gamma)\lhd_o \tilde{G}$, segue do Exercício 3, do Livro do J. Wilson [32], página 9, que:

$$\left(\mathrm{Ker}(\gamma)\cap\tilde{G}^{\mathrm{abs}}\right)_{\hat{p}}=\overline{\mathrm{Ker}(\gamma)\cap\tilde{G}^{\mathrm{abs}}}=\mathrm{Ker}(\gamma).$$

Assim pela Proposição 3.3.6. em Ribes-Zalesskii [22], temos que:

$$\mathrm{posto}(\mathrm{Ker}(\gamma))=\mathrm{posto}\left(\mathrm{Ker}(\gamma)\cap\tilde{G}^{\mathrm{abs}}\right)=p^{n-k}.$$

Portanto, $\tilde{G}\cong F_{p^{n-k}}\rtimes C_{p^n}$.
Agora, pela propriedade universal do produto livre amalgamado pro-p, existe um único homomorfismo contínuo de grupos pro-p

$$\Theta:\tilde{G}\longrightarrow G,$$

tal que $a\longmapsto x$ e $b\longmapsto x^{p^{n-k}}$ e $\alpha\longmapsto\kappa$, onde $\kappa\in G$ é tal que $\omega(\kappa)=\beta$.
Observamos que κ é um elemento sem torção de G.
Além disso, note que

$$\frac{\tilde{G}}{\langle b\rangle}\cong\frac{C_{p^n}}{C_{p^k}}\coprod\mathbb{Z}_p\cong\frac{G}{C_{p^k}}.$$

Seja $\gamma:\frac{\tilde{G}}{\langle b\rangle}\longrightarrow\frac{G}{C_{p^k}}$ o tal isomorfismo que aplica $\overline{a}\longmapsto\overline{x}$ e $\alpha\longmapsto\beta$.

Assim temos o seguinte diagrama comutativo de grupos pro-p :

$$\begin{tikzcd}
1 \arrow[r] & \langle b\rangle \arrow[r, hook] \arrow[d, "\iota"] & \tilde{G} \arrow[r, two heads, "\tilde{\omega}"] \arrow[d, "\Theta"] & \frac{\tilde{G}}{\langle b\rangle} \arrow[r] \arrow[d, "\gamma"] & 1 \\
1 \arrow[r] & C_{p^k} \arrow[r, hook] & G \arrow[r, two heads, "\omega"] & \frac{G}{C_{p^k}} \arrow[r] & 1,
\end{tikzcd}$$

onde $C_{p^k}=\left\langle x^{p^{n-k}}\right\rangle$ e $\tilde{\omega}$ é o epimorfismo canônico de $\tilde{G}$ em $\frac{\tilde{G}}{\langle b\rangle}$.

Agora, este diagrama é comutativo já que o primeiro quadrado é o resultado da restrição de Θ ao subgrupo $\langle b\rangle$; além disso temos que:

$$(\gamma\circ\tilde{\omega})(a)=\gamma(\overline{a})=\overline{x}=\omega(x)=\omega(\Theta(a))=(\omega\circ\Theta)(a)$$

e

$$(\gamma\circ\tilde{\omega})(\alpha)=\gamma(\alpha)=\beta=\omega(\kappa)=\omega(\Theta(\alpha))=(\omega\circ\Theta)(\alpha).$$

Observe que ι e γ são isomorfismos, donde concluí-mos que Θ é um isomorfismo topológico de $\tilde{G}$ em G (este fato é conhecido como Five Lema, por exemplo veja Rotman [24]).
Portanto provamos que

$$G \cong C_{p^n} \coprod_{C_{p^k}} \left(C_{p^k} \times \mathbb{Z}_p\right).$$

Parte 2) Considere $\frac{G}{C_{p^k}} \cong \frac{C_{p^n}}{C_{p^k}} \coprod \frac{C_{p^{t^*}}}{C_{p^k}}$, onde $t^* \in \{k+1, \ldots, n\}$.

Sejam $\frac{C_{p^n}}{C_{p^k}} = \langle u \rangle$, $\frac{C_{p^{t^*}}}{C_{p^k}} = \langle v \rangle$ e $\tau : G \twoheadrightarrow \frac{G}{C_{p^k}}$ o epimorfismo canônico dos grupos pro-p, onde $C_{p^k} = \left\langle x^{p^{n-k}} \right\rangle$.
Considere o seguinte grupo pro-p

$$\ddot{G} = C_{p^n} \coprod_{C_{p^k}} C_{p^{t^*}},$$

onde $C_{p^n} = \langle a \rangle$ e $C_{p^{t^*}} = \langle b \rangle$.
Escolha $s \in G$, tal que $\tau(s) = v$. É claro que a ordem de s é igual a p^{t^*}, já que a ordem de v é igual a p^{t^*-k}.
Pela propriedade universal do produto livre amalgamado pro-p, temos que existe um único homomorfismo contínuo

$$\Delta : \ddot{G} \longrightarrow G,$$

tal que $a \longmapsto x$ e $b \longmapsto s$.
Note que

$$\frac{\ddot{G}}{\left\langle a^{p^{n-k}} \right\rangle} \cong C_{p^{n-k}} \coprod C_{p^{t^*-k}} \cong \frac{G}{\left\langle x^{p^{n-k}} \right\rangle}.$$

Denote por Ψ o tal isomorfismo acima que aplica $\overline{a} \longmapsto u$ e $\overline{b} \longmapsto v$.
Como a ordem de $\tau(x)$ é igual a p^{n-k}, podemos escolher sem perda de generalidade $\tau(x) = u$. De fato, se $\tau(x) \in \langle u \rangle \coprod \langle v \rangle \cong C_{p^{n-k}} \coprod C_{p^{t^*-k}}$, segue que $\tau(x) = u^{g_u}$, para algum $g_u \in \langle u \rangle \coprod \langle v \rangle = \frac{G}{C_{p^k}}$
Então pelo exercício 9.1.22. no livro de Ribes-Zalesskii (ver [22]), podemos reescrever

$$\frac{G}{\left\langle x^{p^{n-k}} \right\rangle} = \langle u^{g_u} \rangle \coprod \langle v \rangle = \langle u \rangle \coprod \langle v \rangle.$$

Assim escolha $s_u \in G$, tal que $\tau(s_u) = g_u$ e então troque x por $x^{s_u^{-1}}$ em G, de maneira que

$$\tau(x^{s_u^{-1}}) = (u^{g_u})^{g_u{}^{-1}} = u.$$

Agora temos o seguinte diagrama comutativo de grupos pro-p, dado abaixo:

$$
\begin{tikzcd}
1 \arrow[r] & \left\langle a^{p^{n-k}} \right\rangle \arrow[r, hook] \arrow[d, "\epsilon"] & \ddot{G} \arrow[r, two heads, "\ddot{\tau}"] \arrow[d, "\Delta"] & \frac{\ddot{G}}{\left\langle a^{p^{n-k}} \right\rangle} \arrow[r] \arrow[d, "\Psi"] & 1 \\
1 \arrow[r] & \left\langle x^{p^{n-k}} \right\rangle \arrow[r, hook] & G \arrow[r, two heads, "\tau"] & \frac{G}{\left\langle x^{p^{n-k}} \right\rangle} \arrow[r] & 1,
\end{tikzcd}
$$

onde $\ddot{\tau}$ é o epimorfismo canônico de $\ddot{G}$ em $\frac{\ddot{G}}{\left\langle a^{p^{n-k}} \right\rangle}$ e ϵ é a restrição de Δ ao subgrupo $\left\langle a^{p^{n-k}} \right\rangle$ de $\ddot{G}$.

De fato, este diagrama é comutativo já que o primeiro quadrado é o resultado da restrição de Δ ao subgrupo $\left\langle a^{p^{n-k}} \right\rangle$ e além disso temos que:

$$(\Psi \circ \ddot{\tau})(a) = \Psi(\overline{a}) = u = \tau(x) = \tau(\Delta(a)) = (\tau \circ \Delta)(a)$$

e

$$(\Psi \circ \ddot{\tau})(b) = \Psi(\overline{b}) = v = \tau(s) = \tau(\Delta(b)) = (\tau \circ \Delta)(b).$$

Como ϵ e Ψ são isomorfismos, segue que Δ é um isomorfismo topológico de $\ddot{G}$ em G. Portanto provamos que

$$G \cong C_{p^n} \coprod_{C_{p^k}} C_{p^{t^*}}$$

onde $t^* \in \{k+1, \ldots, n\}$.

■

Por fim, nesta seção vamos provar um Corolário que dará a quantidade exata de representações inteiras p-ádicas indecomponíveis do grupo C_{p^n}, que se levantam para algum grupo pro-p da forma $F \rtimes C_{p^n}$.

Corolário 82. *Seja $n \in \mathbb{N}$. Considerem todos os $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis não-isomorfos.*
A quantidade de tais reticulados que se levantam para grupos pro-p da forma $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito, é igual à

$$\frac{(n+1)(n+2)}{2}.$$

Demonstração. É uma consequência direta do Corolário 80.
De fato, o item 1) deste Corolário apresenta exatamente $(n+1)$ $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam.
O item 2) apresenta as seguintes quantidades:
Se $k = 1$, temos

$$1 + (n - 1 - 1) + 1 = n - 2 + 2 = n$$

$\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam.
Pelo processo de indução sobre k, chegamos depois de alguns passos ao seguinte:
Quando $k = (n-1)$, temos

$$1 + (n - (n-1) - 1) + 1 = 1 + n - n + 1 - 1 + 1 = 2$$

$\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam.
Por fim, se $k = n$, ou bem melhor, se C_{p^n} age trivialmente sobre $\overline{F}$, então o único $\mathbb{Z}_p C_{p^n}$-reticulado indecomponível que se levanta, é o $\mathbb{Z}_p C_{p^n}$-reticulado trivial $\mathbb{Z}_p$, como podemos ver no item 3) do Corolário 80.

Portanto, a quantidade total desses reticulados é obtida somando-se cada um destes valores, e o resultado é o seguinte:

$$(n+1) + n + (n-1) + \cdots + 3 + 2 + 1 = \frac{(n+1)(n+2)}{2} < \infty.$$

$\blacksquare$

3.2 Algumas Relações Entre o Teorema Principal e a Teoria de Reiner e Heller

Nessa seção, estamos interessados em responder a seguinte questão:

Considere um certo $\mathbb{Z}_p C_{p^n}$-reticulado indecomponível. Será que sempre existe um grupo pro-p da forma $G = F \rtimes C_{p^n}$, cujo o grupo abelinizado $\overline{F}$ seja isomorfo ao reticulado dado?
A resposta para essa questão é negativa. E esse será o nosso interesse a partir de agora.

3.2.1 Todos os $\mathbb{Z}_p C_p$-Reticulados Indecomponíveis se Levantam

Seja $C_p = \langle h \rangle$ e considere $\phi_p(h)$ o p-ésimo polinômio ciclotômico.
Relembramos da **Seção 1.4.** e do Teorema 46, que os únicos $\mathbb{Z}_p C_p$-reticulados indecomponíveis e não-isomorfos são os três listados logo abaixo:

$$\mathbb{Z}_p, \ \mathbb{Z}_p[\theta_p] \text{ e } \mathbb{Z}_p C_p.$$

Agora, pelos Teoremas 78 e 77, temos que:

- $\mathbb{Z}_p C_p$ se levanta para $C_p \coprod \mathbb{Z}_p$.
- $\mathbb{Z}_p[\theta_p]$ se levanta para $C_p \coprod C_p$.
  Além disso, como já observamos na última seção, temos que:
- $\mathbb{Z}_p$ se levanta para $C_p \times \mathbb{Z}_p$.

De outra maneira, o Corolário 82, nos diz que o número de $\mathbb{Z}_pC_p$-reticulados indecomponíveis não-isomorfos que se levantam é igual à:

$$\frac{(n+1)(n+2)}{2} = \frac{2 \cdot 3}{2} = 3.$$

Portanto, quando $n = 1$, temos que todos os $\mathbb{Z}_pC_p$-reticulados indecomponíveis não-isomorfos, se levantam para algum grupo pro-p da forma $F \rtimes C_p$. Assim, para $n = 1$ a questão proposta nesta seção, tem resposta afirmativa.

3.2.2 Nem Todos os $\mathbb{Z}_pC_{p^n}$-Reticulados se Levantam, se $n \geq 2$

Vamos mostrar nessa subseção que a reposta para a questão proposta no ínicio desta seção tem resposta negativa para o caso em que $n \geq 2$.
Para tanto, vamos provar nessa subseção, o seguinte fato:

Proposição 83. *Considere $n \in \mathbb{N}$, tal que $n \geq 2$.*
Então nem todos os $\mathbb{Z}_pC_{p^n}$-reticulados indecomponíveis não-isomorfos, se levantam para algum grupo pro-p da forma

$$F \rtimes C_{p^n},$$

onde F é um grupo pro-p livre de posto finito.

Demonstração. Considere primeiramente $n = 2$. Pelo Teorema 47, sabemos que o número de $\mathbb{Z}_pC_{p^2}$-reticulados indecomponíveis, não-isomorfos é igual à $4p+1$, para todo $p \in \mathbb{P}$.
Agora, o Corolário 82, nos diz que o número de $\mathbb{Z}_pC_{p^2}$-reticulados indecomponíveis, não-isomorfos que se levantam é igual à

$$\frac{(2+1)(2+2)}{2} = \frac{3 \cdot 4}{2} = 6.$$

Como, $4p + 1 \geq 9 > 6$, para todo $p \in \mathbb{P}$, temos que nem todos os $\mathbb{Z}_pC_{p^2}$-reticulados indecomponíveis e não-isomorfos que se levantam para algum grupo pro-p livre da forma $F \rtimes C_{p^2}$.

Suponhamos a partir de agora $n \geq 3$.
Pelo Teorema 48, temos que a quantidade de $\mathbb{Z}_pC_{p^n}$-reticulados indecomponíveis e não-isomorfos é infinita.
Segue novamente pelo Corolário 82, que o número de $\mathbb{Z}_pC_{p^n}$-reticulados indecomponíveis, não-isomorfos que se levantam é igual à

$$\frac{(n+1)(n+2)}{2} < \infty.$$

Logo, nem todos os $\mathbb{Z}_pC_{p^n}$-reticulados indecomponíveis e não-isomorfos, se levantam para algum grupo pro-p livre da forma $F \rtimes C_{p^n}$, quando $n \geq 3$.
Juntando-se os dois fatos acima, a prova de tal Proposição segue. ∎

Por fim, vamos fazer as seguintes observações muito interessantes:

Observação 84. *A propriedade de que um* $\mathbb{Z}_pC_{p^n}$*-reticulado se levanta para algum grupo pro-p da forma* $G = F \rtimes C_{p^n}$*, não implica na existência de um único grupo* G*, à menos de isomorfismo, com as tais propriedades.*
Se um tal grupo G *existe e a ação de* C_{p^n} *sobre o grupo* $\overline{F}$ *é indecomponível e fiel, então o grupo* G *é único com as tais propriedades, como podemos ver no Teorema Principal 77.*

Observação 85. *Sejam dados os seguintes grupos pro-p :*

$$G_1 = (C_p \times \mathbb{Z}_p) \coprod (C_p \times \mathbb{Z}_p) \ \text{ e } G_2 = (C_p \times F_2) \coprod C_p.$$

É claro que $G_1 \ncong G_2$*, já que em* G_2 *existe um normalizador finito para um subgrupo de ordem p, e em* G_1*, cada normalizador de subgrupos de ordem p, são não finitos.*
Pela fórmula do posto do Teorema 11, letra (b), chegamos à:

$$G_1 = F_{p+1} \rtimes_{\theta_1} C_p \ \text{ e } \ G_2 = F_{p+1} \rtimes_{\theta_2} C_p.$$

Agora, pelo Teorema 51, temos que em quaisquer dos casos, o grupo $\overline{F_{p+1}}$ *é isomorfo como um* $\mathbb{Z}_pC_p$*-módulo decomponível à:*

$$V := \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p[\theta_p],$$

ou seja, o $\mathbb{Z}_pC_p$*-reticulado* V*, tem duas* C_p*-conexões distintas.*

3.3 Uma Propriedade Interessante Com Relação ao posto de F

Consideraremos mais uma vez, grupos pro-p da forma $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito.
Nesta seção vamos provar mais uma consequência imediata do Teorema Principal (77). Esta se refere a decomposição do módulo $\overline{F}$; quando o grupo pro-p livre aberto F tem seu posto maior do que p^n.
Para isto, vamos usar o fato de $\mathbb{Z}_p$ ser um anel com **IBN**, já que o mesmo é um anel comutativo (ver Lema 22).

Temos a seguinte Proposição:

Proposição 86. *Seja* $n \in \mathbb{N}$*. Considere* G *um grupo pro-p da forma* $F_k \rtimes C_{p^n}$*, onde* F_k *é um grupo pro-p livre de* posto *igual a* k*.*
Suponhamos que $k \geq p^n + 1$*. Então* $\overline{F}$ *é um* $\mathbb{Z}_pC_{p^n}$*-reticulado decomponível.*

Demonstração. Seja $C_{p^n} = \langle x \rangle$. Vamos provar o tal fato por contradição.

Suponhamos por absurdo, que $\overline{F}$ seja um $\mathbb{Z}_pC_{p^n}$-reticulado indecomponível. Temos uma das duas possibilidades:

- C_{p^n} age fielmente sobre $\overline{F}$,
- C_{p^n} não age fielmente sobre $\overline{F}$.

Se C_{p^n} age fielmente sobre $\overline{F}$, o Teorema 77, nos diz que:

$$\overline{F_k} \cong \mathbb{Z}_p C_{p^n} \quad \text{ou} \quad \overline{F_k} \cong \operatorname{Ker}\left(\mathbb{Z}_p C_{p^n} \twoheadrightarrow \mathbb{Z}_p C_{p^t}\right), \tag{3.1}$$

onde $t \in \{0, 1, \ldots, (n-1)\}$.

Caso a ação de C_{p^n} sobre $\overline{F}$ não seja fiel, considere $\left\langle x^{p^{t'}} \right\rangle \cong C_{p^{n-t'}}$, onde $t' \in \{0, 1, \ldots, (n-1)\}$; como sendo o subgrupo maximal de $\langle x \rangle$, com a propriedade de que o mesmo age trivialmente sobre $\overline{F_k}$.

Pelo Teorema 79, temos que:

$$\overline{F_k} \cong \mathbb{Z}_p C_{p^{t'}} \tag{3.2}$$

ou

$$\overline{F_k} \cong \operatorname{Ker}\left(\mathbb{Z}_p C_{p^{t'}} \twoheadrightarrow \mathbb{Z}_p C_{p^{t^*}}\right) \tag{3.3}$$

como $\mathbb{Z}_p C_{p^n}$-módulo indecomponível, anulado pelo ideal bilateral $\left(x^{p^{t'}} - 1\right)$, tal que $t' \in \{0, 1, \ldots, (n-1)\}$ e $t^* \in \{0, 1, \ldots, (t'-1)\}$.

Agora os isomorfismos em (3.1), (3.2) e (3.3), nos dizem que:

$$\mathrm{r}_p\left(\overline{F_k}\right) = p^n \quad \text{ou} \quad p^n - p^t \quad \text{ou}\ p^{t'} \quad \text{ou}\ p^{t'} - p^{t^*}.$$

Em quaisquer dos casos acima, temos que:

$$k \geq p^n + 1 > p^n, p^n - p^t, p^{t'}, p^{t'} - p^{t^*},$$

pelas definições de t, t', t^*.

Portanto, em (3.1), (3.2) e (3.3), temos um isomorfismo de $\mathbb{Z}_p \langle x \rangle$-módulos ($\mathbb{Z}_p$-módulos livres), de postos diferentes, um absurdo, já que $(\mathbb{Z}_p, +, .)$ tem **IBN**(ver Lema 22).

Portanto, $\overline{F_k}$ é um $\mathbb{Z}_p C_{p^n}$-reticulado decomponível. ∎

Finalizaremos este Capítulo com o Exemplo a seguir:

Exemplo 87. *Seja*

$$G = (C_p \times \mathbb{Z}_p) \coprod (C_p \times \mathbb{Z}_p) = F_{p+1} \rtimes C_p.$$

Como o posto$(F_{p+1}) = p + 1 > p$, *segue da Proposição 86 que* $\overline{F_{p+1}}$ *é um* $\mathbb{Z}_p C_p$*-reticulado decomponível.*

De fato, pela Observação 85, temos que:

$$\overline{F_{p+1}} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p[\theta_p]$$

como um $\mathbb{Z}_pC_p$-módulo decomponível.

Capítulo 4

Módulos Decomponíveis que se Levantam

Neste capítulo vamos mostrar que se G é um produto semi-direto de um grupo pro-p livre F de posto finito, por um grupo cíclico de ordem p^n, então a abelianização de F será um $\mathbb{Z}_pC_{p^n}$-reticulado decomponível, cujos somandos diretos são $\mathbb{Z}_pC_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p da forma $F_k \rtimes C_{p^n}$.
Além disso, essa soma direta é única à menos da posição de seus somandos diretos e à menos de isomorfismos.
Para isso, vamos usar vários de nossos resultados que foram obtidos nos Capítulos 2 e 3 dessa tese.

4.1 Caracterizando F em Função dos Normalizadores de Ordem p

Nessa seção vamos considerar $n \in \mathbb{N}$ e $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito e $C_{p^n} = \langle x \rangle$.

Pelo Lema 65, sabemos que

$$F = F_{x_1} \coprod \left(\coprod_{d_{x_2} \in \Xi_2} F_{d_{x_2}} \right) \coprod \cdots \coprod \left(\coprod_{d_{x_k} \in \Xi_k} F_{d_{x_k}} \right) \coprod F_m \coprod {F_m}^x \coprod {F_m}^{x^{p^n-1}} \coprod F_s,$$

onde

$$F_{\mathcal{X}} := F_{x_1} \coprod \left[\coprod_{d_{x_2} \in \Xi_2} F_{d_{x_2}} \right] \coprod \cdots \coprod \left[\coprod_{d_{x_k} \in \Xi_k} F_{d_{x_k}} \right]$$

e

$$F_M := F_m \coprod {F_m}^x \coprod \cdots \coprod {F_m}^{x^{(p^n-1)}}.$$

Defina a partir de agora $F_{x_r} := \left(\coprod_{d_{x_r} \in \Xi_r} F_{d_{x_r}} \right)$ para cada $r = 1, 2, \ldots, k$, onde relembramos da página 46 que $F_{d_{x_r}} := F \cap \mathrm{N}_G \left(\langle x_r \rangle \right)^{d_{x_r}}$, onde $d_{x_r} \in \Xi_r$ e $\Xi_r \subseteq \langle x \rangle$ são os representantes de classes laterais duplas para $F \backslash G / \mathrm{N}_G \left(\langle x_r \rangle \right)$.

Agora, o Corolário 66, nos diz que:

$$F_s = F_{x,t_2} \coprod F_{x,t_3} \coprod \cdots \coprod F_{x,t_k},$$

onde F_{x,t_w} é obtido a partir do grupo pro-p

$$\langle x \rangle \coprod \langle y_w \rangle = F_{x,t_w} \rtimes \langle x \rangle ,$$

para cada $w = 2, \ldots, k$ e os y_w são elementos de ordem maximal e finita no $\mathrm{N}_G \left(\langle x_w \rangle \right)$.

Seja $F_m = \overline{\langle \alpha_1, \ldots, \alpha_m \rangle}$. Como vimos na Proposição 68, temos que:

$$F_M = \left(\coprod_{j_1=0}^{p^n-1} \overline{\left\langle (\alpha_1)^{x^{j_1}} \right\rangle} \right) \coprod \cdots \coprod \left(\coprod_{j_m=0}^{p^n-1} \overline{\left\langle (\alpha_m)^{x^{j_m}} \right\rangle} \right).$$

Precisamos, exibir a partir de agora, de forma mais explícita quem é o $F_{\mathcal{X}}$ que aparece no Lema 65. Para tanto, basta estudar a estrutura de cada $F_{x_r} \neq \{1\}$.

Relembramos também que na Proposição 68, nós mostramos que cada $\overline{F_{x_r}}$ é um $\mathbb{Z}_p \langle x \rangle$-módulo.

Observação 88. *Seja $G = F \rtimes C_{p^n}$, onde F é um grupo pro-p livre de posto finito. Se $G = N_G \left(\langle x_1 \rangle \right)$, onde a ordem de x_1 é igual a p, então pelo Lema 74, temos que C_{p^n} não age fielmente sobre $\overline{F}$. Assim existe no normalizador acima um elemento de ordem finita e maximal agindo trivialmente sobre $\overline{F}$.*

Temos o seguinte Lema:

Lema 89. *Seja $G = F \rtimes C_{p^n}$, onde $n \in \mathbb{N}$ e F é um grupo pro-p livre de posto finito. Seja H um subgrupo fechado de G. Então H é um grupo pro-p livre-por-cíclico.*

Demonstração. Considere o subgrupo $H \cap F$ de H. Como $F \triangleleft G$, temos que $[H \cap F] \triangleleft_c H$. Além disso $H \cap F <_c F$, donde segue pelo livro de Ribes-Zalesskii [22], página 286, que $H \cap F$ é um grupo pro-p livre.
Para que H seja um grupo pro-p livre-por-cíclico, basta mostrar que $\frac{H}{H \cap F}$ é um p-grupo cíclico finito.

Mas de fato, pelos Teoremas do Isomorfismos, temos que:

$$\frac{H}{H \cap F} \cong \frac{HF}{F} \leq \frac{G}{F} \cong C_{p^n}.$$

■

Observação 90. *No artigo de Herfort-Zalesskii [7], Teorema 2.2. página 523, nós observamos que o* $N_G(\langle x_i \rangle)$ *é um produto semi-direto pro-p de um grupo pro-p livre aberto por um grupo cíclico de ordem* p^{k_i}*, já que o mesmo é livre-por-cíclico pelo Lema 89. Denotaremos o*

$$N_G(\langle x_i \rangle) = F_{N_G(\langle x_i \rangle)} \rtimes C_{p^{k_i}},$$

onde $1 \leq k_i \leq n$*; para todo* $i = 1, 2, \ldots, k$*.*

Mediante a Observação 88, podemos escolher em cada normalizador um elemento de ordem maximal e finita, digamos y_{t_i} tal que $\langle y_{t_i} \rangle \cong C_{p^{t_i}}$ e $C_{p^{t_i}}$ age trivialmente sobre o $\overline{F_{\mathrm{N}_G(\langle x_i \rangle)}}$.

Lema 91. *Com as notações precedentes, temos que* $C_{p^{t_i}} \subset Z(N_G(\langle x_i \rangle))$*, para cada* $i = 1, 2, \ldots, k$*.*

Demonstração. De fato, pela hipótese, existem os homorfismos canônicos de grupos pro-p logo abaixo:

$$C_{p^{k_i}} \xrightarrow{\Psi} \mathrm{Aut}\left(F_{\mathrm{N}_G(\langle x_i \rangle)}\right) \overset{\Phi}{\twoheadrightarrow} \mathrm{Aut}\left(\overline{F_{\mathrm{N}_G(\langle x_i \rangle)}}\right).$$

Como $C_{p^{t_i}}$ trivializa $\overline{F_{\mathrm{N}_G(\langle x_i \rangle)}}$, segue que $\Psi\left(C_{p^{t_i}}\right)$ está no núcleo de Φ.
Agora pelo Lema 16, sabemos que tal núcleo é um grupo livre de torção pro-p.
Donde segue que $C_{p^{t_i}}$ age trivialmente sobre $F_{\mathrm{N}_G(\langle x_i \rangle)}$.
Assim,

$$C_{p^{t_i}} \subset Z\left(F_{\mathrm{N}_G(\langle x_i \rangle)} \rtimes C_{p^{k_i}}\right) = Z(\mathrm{N}_G(\langle x_i \rangle)).$$

■

Vamos descrever agora a estrutura de F_{x_i}, para cada $i = 1, 2, \ldots, k$.

Lema 92. *Para cada* $i = 1, \ldots, k$ *tal que* $F_{x_i} \neq \{1\}$*, temos que* F_{x_i} *se decompõe como um produto livre pro-p de subgrupos pro-p livres de posto finito da seguinte maneira:*

$$F_{x_i} = F^{i_0} \coprod F^{i_1} \coprod \cdots \coprod F^{i_u} \coprod F^{s_{i_0}} \coprod \cdots \coprod F^{s_{i_v}},$$

onde $0 \leq u < \infty$*;* $0 \leq v < \infty$*; u e v não são zero simultaneamente e para algum dos* F^{i_t} *ou* $F^{s_{i_j}}$ *temos que o seu posto é maior ou igual a* 1*.*

Demonstração. Relembramos pelo Lema 90 que

$$\mathrm{N}_G(\langle x_i \rangle) = F_{\mathrm{N}_G(\langle x_i \rangle)} \rtimes C_{p^{k_i}},$$

onde $C_{p^{k_i}} = \langle n_{k_i} \rangle$. Em $G = F \rtimes \langle x \rangle$ vamos amalgamar o subgrupo $\left\langle x^{p^{n-t_i}} \right\rangle$ de $\langle x \rangle$ com o subgrupo central $C_{p^{t_i}}$ do $N_G(\langle x_i \rangle)$.
Considere os seguintes subgrupos de G :

$$A_\epsilon = \langle x \rangle \coprod_{\left\langle x^{p^{n-t_i}} = y_{t_i} = z_\epsilon{}^{p^{t_\epsilon - t_i}} \right\rangle} \langle z_\epsilon \rangle \cong C_{p^n} \coprod_{C_{p^{t_i}}} C_{p^{t_\epsilon}},$$

onde os $\langle z_\epsilon \rangle \cong C_{p^{t_\epsilon}}$ não são conjugados de $C_{p^{k_i}}$ no $\mathrm{N}_G\,(\langle x_i \rangle)$, $p^{t_\epsilon} > p^{t_i}$, $\epsilon = i_0, i_1, \ldots, i_u$ e $\langle z_\epsilon \rangle < \mathrm{N}_G\,(\langle x_i \rangle)$.

Pelo Lema 7 sabemos que cada A_ϵ é próprio. A propriedade universal do produto livre amalgamado pro-p nós dá um epimorfismo contínuo canônico de grupos pro-p :

$$\tilde{\rho}_\epsilon : A_\epsilon \longrightarrow \langle m \rangle \cong C_{p^n}$$

que aplica $x \longmapsto m$ e $z_\epsilon \longmapsto m^{p^{n-t_\epsilon}}$. Escreva o núcleo de $\tilde{\rho}_\epsilon$ como sendo K_ϵ.
Note que $K_\epsilon \lhd_c A_\epsilon$ e além disso é livre de torção, pois caso contrário um de seus elementos de ordem finita deveria ser conjugado a um elemento de C_{p^n} ou $C_{p^{t_\epsilon}}$ (veja Ribes-Zalesskii [25], Teorema 4.2, item b). Mas pela definição de $\tilde{\rho}_\epsilon$, isto não pode ocorrer.
Seja

$$A_\epsilon^{\mathrm{abs}} = \langle x \rangle *_{\left\langle x^{p^{n-t_i}} = y_{t_i} = z_\epsilon{}^{p^{t_\epsilon - t_i}} \right\rangle} \langle z_\epsilon \rangle \cong C_{p^n} *_{C_{p^{t_i}}} C_{p^{t_\epsilon}}$$

o produto livre amalgamado dos grupos abstratos. Considere $K_\epsilon \cap A_\epsilon^{\mathrm{abs}}$ como um subgrupo de $A_\epsilon^{\mathrm{abs}}$.
Agora note que $K_\epsilon \cap A_\epsilon^{\mathrm{abs}}$ é um grupo livre de torção já que o mesmo é um subgrupo de K_ϵ. Além disso, $A_\epsilon^{\mathrm{abs}}$ é um grupo abstrato virtualmente livre como podemos ver no Corolário da Proposição 11 do livro de Serre [29]. Portanto segue de Serre [29] (Proposição 11, letra b, página 120) que $K_\epsilon \cap A_\epsilon^{\mathrm{abs}}$ é um subgrupo livre de G^{abs} cujo índice é igual a p^n.
Novamente por Serre [29] (exercício 3 da página 123), segue que o posto de $K_\epsilon \cap A_\epsilon^{\mathrm{abs}}$ é igual:

$$1 + p^n \left(\frac{1}{p^{t_i}} - \frac{1}{p^n} - \frac{1}{p^{t_\epsilon}} \right) = p^{n-t_i} - p^{n-t_\epsilon}.$$

Como $A_\epsilon^{\mathrm{abs}}$ é denso em A_ϵ e $K_\epsilon \lhd_o A_\epsilon$, segue do exercício 3 do Livro de J. Wilson que:

$$\left(K_\epsilon \cap A_\epsilon^{\mathrm{abs}} \right)_{\hat{p}} = \overline{K_\epsilon \cap A_\epsilon^{\mathrm{abs}}} = K_\epsilon.$$

Donde segue que

$$A_\epsilon = K_\epsilon \rtimes \langle x \rangle \cong F_{p^{n-t_i} - p^{n-t_\epsilon}} \rtimes C_{p^n}.$$

Defina $F^\epsilon = F_{p^{n-t_i} - p^{n-t_\epsilon}}$, para cada $\epsilon = i_0, i_1, \ldots, i_u$.
Considere a partir de agora os subgrupos pro-p de G da forma:

$$A_\delta = \langle x \rangle \coprod_{\left\langle x^{p^{n-t_i}} = y_{t_i} = r_{t_i} \right\rangle} (\langle r_{t_i} \rangle \times F_{h_\delta}) \cong C_{p^n} \coprod_{C_{p^{t_i}}} \left(C_{p^{t_i}} \times F_{h_\delta} \right)$$

onde os $\langle r_{t_i} \rangle \cong C_{p^{t_i}}$ não são conjugados de $C_{p^{k_i}} = \langle n_{k_i} \rangle$ no $N_G(\langle x_i \rangle)$; os F_{h_δ} são subgrupos pro-p livres de posto finito em F_{x_i}, $\delta = s_{i_0}, s_{i_1}, \ldots, s_{i_v}$ e $\langle r_{t_i} \rangle < N_G(\langle x_i \rangle)$.

Como fizemos para os grupos A_ϵ podemos mostrar de maneira análoga que cada

$$A_\delta = F^\delta \rtimes \langle x \rangle \cong F^\delta \rtimes C_{p^n},$$

onde F^δ é um grupo pro-p livre de posto finito em F_{x_i}.
Considere

$$G^{\text{abs}} = \left(*_{i=1}^{k} \ [\mathrm{N}_G\left(\langle x_i \rangle\right)] \right) * F_m^{\text{abs}}$$

onde F_m^{abs} é um grupo livre abstrato sobre o mesmo conjunto de geradores topológicos livres para F_m. Tome $F \cap G^{\text{abs}}$ como um subgrupo de G^{abs}. Aplicando o Teorema do Subgrupo de Kurosch para grupos abstratos (veja Kurosh [13] ou Serre [29]) ao subgrupo $F \cap G^{\text{abs}}$ de G^{abs}, obtemos um subgrupo pro-p livre

$$F_{x_i}^{\text{abs}} = *_{d_{x_i} \in \Xi_i} \left[F \cap \mathrm{N}_G\left(\langle x_i \rangle\right)^{d_{x_i}} \right]$$

tal que

$$F_{x_i} = \left(F_{x_i}^{\text{abs}} \right)_{\hat{p}} \tag{4.1}$$

e além disso

$$F_{x_i}^{\text{abs}} = \left(F^{i_0}\right)^{\text{abs}} * \left(F^{i_1}\right)^{\text{abs}} * \cdots * \left(F^{i_u}\right)^{\text{abs}} * \left(F^{s_{i_0}}\right)^{\text{abs}} * \cdots * \left(F^{s_{i_v}}\right)^{\text{abs}}$$

onde os $(F^\epsilon)^{\text{abs}}$ são os grupos livres abstratos sobre os conjuntos de geradores topológicos livres para F^ϵ e os $\left(F^\delta\right)^{\text{abs}}$ são os grupos livres abstratos sobre os conjuntos de geradores topológicos livres para F^δ, onde $\epsilon = i_0, i_1, \ldots, i_u$, $\delta = s_{i_0}, s_{i_1}, \ldots, s_{i_v}$ e o conjunto $\Xi_i \subseteq \langle x \rangle$ é um conjunto completo de representantes de classes laterais duplas para $F \backslash G / \mathrm{N}_G\left(\langle x_i \rangle\right)$.
Portanto por (4.1), temos que:

$$F_{x_i} = \left(F_{x_i}^{\text{abs}} \right)_{\hat{p}} = F^{i_0} \coprod F^{i_1} \coprod \cdots \coprod F^{i_u} \coprod F^{s_{i_0}} \coprod \cdots \coprod F^{s_{i_v}},$$

onde $0 \leq u < \infty$; $0 \leq v < \infty$; além disso, u e v não são zero simultaneamente e para algum F^{i_t} ou $F^{s_{i_j}}$ o seu posto é maior ou igual a 1. ∎

4.2 Quem é o $\overline{F_{x_i}}$?

Nessa seção vamos provar que para cada $i = 1, \ldots, k$; se o $F_{x_i} \neq \{1\}$, então o $\overline{F_{x_i}}$ é uma soma-direta finita de $\mathbb{Z}_p C_{p^n}$-módulos indecomponíveis que se levantam para algum grupo pro-p virtualmente livre. Temos a seguinte Proposição:

Proposição 93. *Para cada $i = 1, 2, \ldots, k$, temos uma das seguintes afirmações:*

- $\overline{F_{x_i}} = \{0\}$;
- $\overline{F_{x_i}}$ *é uma soma-direta finita de $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p da forma $F_k \rtimes C_{p^n}$, com ação não fiel do C_{p^n}.*

Demonstração. Se o $N_G(\langle x_i \rangle)$ é finito, temos que $\overline{F_{x_i}} = \{0\}$. Vamos considerar a partir de agora somente o último caso pois o outro não a nada a fazer.

Pelo Lema 92 temos

$$F_{x_i} = F^{i_0} \coprod F^{i_1} \coprod \cdots \coprod F^{i_u} \coprod F^{s_{i_0}} \coprod \cdots \coprod F^{s_{i_v}},$$

donde segue que

$$\overline{F_{x_i}} = \overline{F^{i_0}} \oplus \overline{F^{i_1}} \oplus \cdots \oplus \overline{F^{i_u}} \oplus \overline{F^{s_{i_0}}} \oplus \cdots \oplus \overline{F^{s_{i_v}}}$$

como um $\mathbb{Z}_p$-módulo livre.

Agora pelo Teorema 81, temos que os $\overline{F^{\epsilon}}$ são $\mathbb{Z}_p \langle x \rangle$-módulos indecomponíveis, com ação trivial do $\left\langle x^{p^{n-t_i}} \right\rangle$, de maneira mais precisa, temos que

$$\overline{F^{\epsilon}} \cong \operatorname{Ker}\left(\mathbb{Z}_p\left[\frac{C_{p^n}}{C_{p^{t_i}}}\right] \twoheadrightarrow \mathbb{Z}_p\left[\frac{C_{p^{t_\epsilon}}}{C_{p^{t_i}}}\right]\right) \cong \operatorname{Ker}\left(\mathbb{Z}_p[C_{p^{n-t_i}}] \twoheadrightarrow \mathbb{Z}_p[C_{p^{(t_\epsilon - t_i)}}]\right)$$

como $\mathbb{Z}_p \langle x \rangle$-módulos, onde $\epsilon = i_0, \ldots, i_u$ e os mesmos se levantam para os grupos:

$$F^{i_0} \rtimes \langle x \rangle, \ldots, F^{i_v} \rtimes \langle x \rangle$$

respectivamente.

Precisamos estudar a partir de agora, somente o que ocorre com os $\mathbb{Z}_p$-módulos $\overline{F^{\delta}}$, onde $\delta = s_{i_0}, \ldots, s_{i_v}$.

Considere o grupo pro-p livre F_{h_δ} que aparece na prova do Lema 92 e página 77. Suponha que $F_{h_\delta} = \overline{\left\langle \alpha_{h_{\delta_1}}, \ldots, \alpha_{h_{\delta_q}} \right\rangle}$.
Novamente como vimos no Lema 92, a aplicação do Teorema do Subgrupo de Kurosh (Teorema 11) sobre o subgrupo F de G, nos garante que:

$$F^{\delta} = F_{\{\langle x \rangle, \delta_1\}} \coprod F_{\{\langle x \rangle, \delta_2\}} \coprod \cdots \coprod F_{\{\langle x \rangle, \delta_q\}},$$

onde os grupos $F_{\{\langle x \rangle, \delta_l\}}$, para $l = 1, \ldots, q$, são dados a partir dos subgrupos pro-p de G dados por:

$$\langle x \rangle \coprod_{C_{p^{t_\delta}}} \left(C_{p^{t_\delta}} \times \overline{\left\langle \alpha_{h_{\delta_l}} \right\rangle}\right) = F_{\{\langle x \rangle, \delta_l\}} \rtimes \langle x \rangle,$$

onde $\overline{\left\langle \alpha_{h_{\delta_l}} \right\rangle} \cong \mathbb{Z}_p$.

Agora pelo Teorema 81, temos que:

$$\overline{F_{\{\langle x \rangle, \delta_l\}}} \cong \mathbb{Z}_p\left[\frac{C_{p^n}}{C_{p^{t_\delta}}}\right] \cong \mathbb{Z}_p[C_{p^{n-t_\delta}}]$$

como um $\mathbb{Z}_p \langle x \rangle$-módulo indecomponível, cuja ação de $C_{p^{t_\delta}}$ é trivial.

Portanto, por esta última observação juntamente com o Lema 67, temos que:

$$\overline{F^{\delta}} \cong \overline{F_{\{\langle x\rangle,\delta_l\}}} \oplus \overline{F_{\{\langle x\rangle,\delta_2\}}} \oplus \cdots \oplus \overline{F_{\{\langle x\rangle,\delta_q\}}} \cong \underbrace{\mathbb{Z}_p[C_{p^{n-t_\delta}}] \oplus \cdots \oplus \mathbb{Z}_p[C_{p^{n-t_\delta}}]}_{q \text{ vezes}}$$

como um $\mathbb{Z}_pC_{p^n}$-módulo.

Assim para todo $\delta = s_{i_0}, \ldots, s_{i_v}$; temos que $\overline{F^{\delta}}$ é uma soma direta de $\mathbb{Z}_pC_{p^n}$-reticulados indecomponíveis que se levantam para os grupos $F_{\{\langle x\rangle,\delta_l\}} \rtimes \langle x\rangle$ e a Proposição esta provada. ■

4.3 Os Últimos Teoremas

Nessa seção vamos caracterizar o $\mathbb{Z}_pC_{p^n}$-reticulado $\overline{F}$ quando o mesmo é decomponível.

Começamos com o seguinte Teorema:

Teorema 94. *Seja $G = F \rtimes C_{p^n}$, onde $n \in \mathbb{N}$ e F é um grupo pro-p livre de posto finito. Então $\overline{F}$ é uma soma direta única de $\mathbb{Z}_pC_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p virtualmente livre da forma $F_k \rtimes C_{p^n}$.*

Demonstração. Seja $C_{p^n} = \langle x\rangle$. Pela Proposição 68, temos que

$$\overline{F} \cong \overline{F_{\mathcal{X}}} \oplus \overline{F_M} \oplus \overline{F_s}$$

como um $\mathbb{Z}_pC_{p^n}$-módulo.
Nesta mesma Proposição, vimos que

$$\overline{F_s} \cong \overline{F_{x,t_2}} \oplus \cdots \oplus \overline{F_{x,t_k}}$$

como um $\mathbb{Z}_pC_{p^n}$-módulo decomponível, cujos somandos diretos são indecomponíveis e se levantam para os grupos

$$F_{x,t_i} \rtimes \langle x\rangle = \langle x\rangle \coprod \langle y_i\rangle\,,$$

onde os y_i são elementos de ordem finita e maximal no normalizador de $\langle x_i\rangle$ em G.

Agora note que:

$$F_M = \left(\coprod_{j_1=0}^{p^n-1} \overline{\left\langle (\alpha_1)^{x^{j_1}} \right\rangle}\right) \coprod \cdots \coprod \left(\coprod_{j_m=0}^{p^n-1} \overline{\left\langle (\alpha_m)^{x^{jm}} \right\rangle}\right).$$

Como vimos no Lema 58, temos que:

$$\overline{\langle \alpha_r\rangle} \coprod \langle x\rangle = \left(\coprod_{j_r=0}^{p^n-1} \overline{\left\langle (\alpha_r)^{x^{jr}} \right\rangle}\right) \rtimes \langle x\rangle \cong F_{p^n} \rtimes C_{p^n},$$

para cada $r = 1, \ldots, m$.

Assim segue da Proposição 59 que

$$\overline{\left(\coprod_{j_r=0}^{p^n-1} \underline{\left\langle (\alpha_r)^{x^{j_r}} \right\rangle} \right)} \cong \mathbb{Z}_p C_{p^n} \tag{4.2}$$

como um $\mathbb{Z}_p C_{p^n}$-reticulado indecomponível que se levanta para o grupo pro-p virtualmente livre

$$\overline{\langle \alpha_r \rangle} \coprod \langle x \rangle \cong \mathbb{Z}_p \coprod C_{p^n},$$

além disso observamos que a barra superior em (4.2) significa o quociente módulo o subgrupo derivado e a barra inferior em (4.2) significa o fecho topológico do subgrupo $\left\langle (\alpha_r)^{x^{j_r}} \right\rangle$.

Portanto, temos que

$$\overline{F_M} \cong \underbrace{\mathbb{Z}_p C_{p^n} \oplus \mathbb{Z}_p C_{p^n} \oplus \cdots \oplus \mathbb{Z}_p C_{p^n}}_{m \text{ vezes}}$$

como um $\mathbb{Z}_p C_{p^n}$-reticulado.

Por fim, pela Proposição 93, temos que:

$$\overline{F_{\mathcal{X}}} \cong \overline{F_{x_1}} \oplus \overline{F_{x_2}} \oplus \cdots \oplus \overline{F_{x_k}}$$

como um $\mathbb{Z}_p C_{p^n}$-módulo decomponível, cujos somandos diretos são somas diretas de $\mathbb{Z}_p C_{p^n}$-módulos indecomponíveis que se levantam.

Juntando-se todas as informações que obtivemos em tal Teorema com relação a $\overline{F_s}$, $\overline{F_M}$ e $\overline{F_{\mathcal{X}}}$, concluí-mos que $\overline{F}$ é uma soma direta de $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p virtualmente livre.

Unicidade A unicidade segue diretamente do Teorema 39 (Teorema de Krull-Schmidt-Azumaya), já que o mesmo diz que um $\mathbb{Z}_p C_{p^n}$-módulo decomponível e f.g. é escrito de maneira única como uma soma direta de $\mathbb{Z}_p C_{p^n}$-módulos indecomponíveis (em particular, no nosso caso temos indecomponíveis que se levantam). ■

Por fim, vamos provar o último Teorema dessa tese que nos garante que só é preciso conhecer os $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam, para que nós conheçamos quaisquer dos $\mathbb{Z}_p C_{p^n}$-reticulados decomponíveis que se levantam.

Teorema 95. *Seja M um $\mathbb{Z}_p C_{p^n}$-reticulado. Suponhamos que $M = \bigoplus_{j \in J < \infty} M_j$, onde os M_j são $\mathbb{Z}_p C_{p^n}$-reticulados indecomponíveis que se levantam para algum grupo pro-p virtualmente livre $F^j \rtimes C_{p^n}$, onde os F^j são grupos pro-p livres de posto finito. Então existe um grupo pro-p virtualmente livre $\tilde{G} = \tilde{F} \rtimes C_{p^n}$, tal que M se levanta para $\tilde{G}$ e $\tilde{F}$ é um grupo pro-p livre de posto finito.*

Demonstração. Seja o seguinte grupo pro-p livre:

$$\tilde{F} = F^1 \coprod F^2 \coprod \cdots \coprod F^i,$$

onde $J = \{1, 2, \ldots, i\}$.
Fazendo-se o quociente módulo o subgrupo de Frattini de $\tilde{F}$ (veja a página 54 em Ribes-Zalesskii [22] para o subgrupo de Frattini e o Lema 9.1.17.), temos que:

$$\text{posto}(\tilde{F}) = posto(F^1) + posto(F^2) + \cdots + posto(F^i) < \infty.$$

Agora, pela hipótese $C_{p^n} = \langle x \rangle$ age continuamente sobre cada $F^j, j = 1, 2, \ldots, i$. Assim segue que a ação de C_{p^n} se estende para $F^1 \coprod F^2 \coprod \cdots \coprod F^i$. Defina $\tilde{G} = \tilde{F} \rtimes \langle x \rangle$.
Pela definição de $\tilde{F}$, temos que

$$\overline{\tilde{F}} \cong \overline{F^1} \oplus \overline{F^2} \oplus \cdots \oplus \overline{F^i}$$

como um $\mathbb{Z}_p$-módulo livre. Agora, pela hipótese temos que cada $\overline{F^j} \cong M_j$ como um $\mathbb{Z}_p \langle x \rangle$-módulo indecomponível, donde segue que $\overline{\tilde{F}} \cong M$. Em outras palavras, M se levanta para o grupo pro-p $\tilde{G} = \tilde{F} \rtimes C_{p^n}$. ■

Referências Bibliográficas

[1] E.A.Behrens e C. Reis, *Ring Theory*, Academic Press Inc., New York (1972).

[2] F.E.Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendartellungen bei arithmetischer Äquivalenz*, Hamb. Abh, (13) (1940), 357-412.

[3] S.D.Berman e P.M.Gudivok, *Indecomposable representations of finite groups over the ring of p-adic integers*, Izv. Akad. Nauk. SSSR Ser. Mat. 28 (1964), 875-910; English transl., Amer. Math. Soc. Trans. (2) (50) (1966), 77-113, MR. 29 # 3550.

[4] S.D.Berman e P.M.Gudivok, *Integral representations of finite groups*, Dokl. Akad. Nauk. SSSR 145 (1962), 1199-1201= Soviet Math. Dokl. 3 (1962), 1172-1174, MR. 25 # 3595.

[5] C.W. Curtis e I. Reiner, *Methods of Representation Theory - whit applications to finite groups and ordes*, Wiley, New York, 1981.

[6] W.N.Herfort e L. Ribes, *Subgroups of free pro-p-products*, Math. Proc. Camb. Phil. Soc. (1987), 101-197.

[7] W.N. Herfort e P.A. Zalesskii, *Cyclic extensions of free pro-p groups*, J. Algebra 216 (1999), 511-547.

[8] W.N. Herfort e P. A. Zalesskii, *Virtually free pro-p groups whose torsion elements have finite centralizer* , Bulletin London Mathematical Society 40, (2008) 929-936.

[9] A. Heller e I. Reiner, *Representations of Cyclic Groups in Ring of Integers, I* , Ann. of Mathematics (2) 76, (1962) 73-92.

[10] A. Heller e I. Reiner, *Representations of Cyclic Groups in Ring of Integers, II* , Ann. of Mathematics (2) 77, (1963) 318-328.

[11] M. Kang, *Integral representations of cyclic groups of order* p^2, Journal of Algebra 207, (1998), 82-126.

[12] F. Kasch, *Modules and Rings*, Academic Press, Inc. London, LTD (1982).

[13] A.G. Kurosh, *The Theory of Groups*, Vol. 2, Translate and edited by K.A.Hirsch, Chelsea Publishing Co, New York, N.Y. (1995).

[14] S. Lang, *Algebra*, Addison-Wesley, Reading (1971).

[15] A. Lubotzky, *Combinatorial group theory for pro-p groups*, J. Pure Appl. Algebra 25 (1982), número 3, 311-325.

[16] R.C. Lyndon e P.E. Schupp, *Combinatorial Group Theory*, Springer, Berlin (1977).

[17] O.V. Mel'nikov, *Subgroups and homology of free products of profinite groups*, Math. USSR Izvestya, 34 (1990), 97-119.

[18] T. Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, New York (1974).

[19] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin Heidelberg, New York (1999).

[20] I. Reiner, *Invariants of Integral Representations*, Pacific Journal of Math. Vol. 78, Number 2 (1978).

[21] L. Ribes, *On amalgamated products of profinite groups*, Mathematische Zeischrift, (123) (1971), 357-364.

[22] L.Ribes e P.A. Zalesskii, *Profinite Groups*, Springer- Verlag, Berlin-Heidelberg , New York (2000).

[23] A.V.Roiter, *Integral representations of cyclic groups of the fourth order*, Proc. Leningrad Univ., (19) (1960), 65-74.

[24] J.J. Rotman, *An Introduction to Homological Algebra*, Academic Press Inc., University Illinois, Urbana, Illinois.

[25] M. du Sautoy, D. Segal, A. Shalev, *New horizons in pro-p groups*, Progress in Mathematics, 184 (2000), Birkhäuser.

[26] C. Scheiderer, *The structure of some virtually free pro-p groups*, Proc. Amer. Math. Soc. 127 (1999), 695-700.

[27] S.K. Sehgal, *Units in integral group rings*, University of Alberta, Alberta, Canada.

[28] S.K. Sehgal and C.P. Milies, *An introduction to group rings*, Algebras and Applications, Volume 1, Kluwer Academic Publishers (2002).

[29] J.P. Serre, *Trees*, Springer, Berlin (1980).

[30] A.Troy, *Integral representations of cyclic groups of order* p^2, Thesis, Univ. of Illinois, 1961.

[31] A.V. Yakolev, *The classification of* 2*-adics representations of the cyclic group of order* 8, Zapiski Nauchn. Seminar. Leningradst OTD, Mat. Inst. AN SSSR 28 (1972), 93-129.

[32] J.S. Wilson, *Profinite Groups*, Claredon Press, Oxford (1998).