# UNIDADES DE ANÉIS DE GRUPO E O PROBLEMA DO ISOMORFISMO

Fernando Quadros Gouvêa

Dissertação apresentada ao Instituto de Matemática e Estatística da Universidade de São Paulo para obtenção do grau de mestre em matemática.

Orientador:
Prof. Dr. Francisco César Polcino Milies.

Agosto, 1981

Durante a elaboração deste trabalho o autor recebeu apoio financeiro da FAPESP e da FINEP.

"... τι ποιεῖτε, πάντα εἰς δόξαν
Θεοῦ ποιεῖτε."

SOLI DEO GLORIA

MEU DEUS E MEU PAI:

Explorar qualquer aspecto da Tua multiforme criação é apenas "pensar Teus pensamentos após Ti". Nada tenho de mim mesmo, e assim te agradeço por aquilo que me permitiste pensar, descobrir e entender, pela Tua presença e direção, pela dádiva da salvação em Jesus Cristo. Ao te apresentar e te consagrar este esforço e este trabalho, faço minhas as palavras do salmista:

> "Seja sobre nós a graça do Senhor nosso Deus; confirma sobre nós as obras de nossas mãos, sim, confirma a obra das nossas mãos."

# INTRODUÇÃO

O estudo da estrutura algébrica dos anéis de grupo, e especificamente o estudo do problema do isomorfismo e da estrutura do grupo das unidades, tem atraído a atenção de muitos matemáticos durante as últimas décadas. Parece-nos haver muitas razões para isto. Os anéis de grupo nasceram ligados à teoria de representações de grupos, e há certa razão para crer que seu estudo prove ser relevante nesta área, e até na própria teoria dos grupos. Além disso, há inúmeros problemas abertos em relação à estrutura algébrica dos anéis de grupo, e sua resolução parece que envolverá técnicas da teoria dos grupos e das representações, da teoria de anéis e da teoria algébrica dos números. Esta amplitude de técnicas aumenta a atração deste estudo. Finalmente, os argumentos usados muitas vezes envolvem cálculos explícitos, o que dá à teoria um caráter concreto e uma aparência enganosamente "simples".

É o interesse deste estudo que explica a extensão desta dissertação. Planejada originariamente como estudo do problema do isomorfismo, seu aspecto foi totalmente modificado pelo surgimento, primeiro, do trabalho de D.S.Passman e P.F.Smith, e, depois, do trabalho de G.H.Cliff, S.K.Sehgal e A.R.Weiss. Diante do interesse e da importância destes trabalhos, era imperativo incluí-los.

À parte o capítulo de preliminares, este trabalho se

divide em três partes quase independentes. O capítulo II discute o problema do isomorfismo para anéis de grupo de grupos metabelianos sobre anéis de integridade, obtendo um resultado parcial. O capítulo III contém vários resultados sobre anéis de grupo de grupos diedrais sobre os inteiros, incluindo uma descrição explícita do grupo de unidades em um caso particular. O capítulo IV trata da existência de complementos normais livres de torção para G em $V(\mathbb{Z}G)$, um problema que tem atraído muito interesse nos últimos anos.

Nenhuma dissertação deste tipo pode ser feita em isolamento; é grande o número de pessoas que nos ajudaram, incentivaram e que de algum forma participaram do trabalho. Dentre eles, cumpre lembrar a ajuda e o estímulo de nosso orientador, Prof. César Polcino, as conversas interessadas de nossa colega Heloísa Borsari, a paciência e o trabalho de Marcia Fani Franco Perez, responsável pela datilografia, e, acima de tudo, o amor de minha esposa. A estes, e a todos os que ajudaram, agradecemos de coração.

Passados grande trabalho e quase dois anos, é-nos extremamente gratificante encerrar esta etapa. Com gratidão a Deus, citamos a exclamação de um desconhecido escriba medieval, ao concluir um trabalho especialmente trabalhoso e delicado:

FINIS, FINIS, FINIS,

LUDENDO DICIT!

Fernando Quadros Gouvêa

Agosto de 1981

ÍNDICE

I. PRELIMINARES .....1

§1 - Definições e Resultados Básicos .....1

§2 - Resultados Básicos sobre o Grupo das Unidades... 8

§3 - O Cálculo de Ideais de Aumento.....24

II. ISOMORFISMOS DE ANÉIS DE GRUPO DE GRUPOS METABELIANOS FINITOS.....44

§1 - O Problema do Isomorfismo.....44

§2 - O Exemplo de E.C.Dade.....48

§3 - A Correspondência entre Subgrupos Normais.....65

§4 - Um Resultado Parcial.....66

III. ANÉIS DE GRUPO DE GRUPOS DIEDRAIS SOBRE OS INTEIROS..82

§1 - Grupos Cíclicos.....82

§2 - Grupos Diedrais.....98

IV. COMPLEMENTOS NORMAIS.....115

§1 - Grupos Círculo Nilpotentes.....117

§2 - Grupos Metabelianos: Existência de Complemento.121

§3 - Lemas de Redução.....138

§4 - Ação Fiel e Irredutível de G/A em A.....148

§5 - Caso Geral.....171

Bibliografia.....189

# I. PRELIMINARES

Apresentamos neste capítulo alguns resultados básicos sobre os anéis de grupo, seus ideais de aumento e seus grupos de unidades, dando, em alguns casos, enunciados mais gerais do que os que são normalmente citados. As referências básicas para este capítulo são [Polcino Milies 1976], [Sehgal 1978] e [Passman 1977]. Quando os resultados mencionados ou as demonstrações dadas não constarem destas, serão dadas referências específicas.

## § 1. DEFINIÇÕES E RESULTADOS BÁSICOS

No que segue, R denotará um anel comutativo com 1, G um grupo finito e RG o anel de grupo de G sobre R, definido como o conjunto das combinações R-lineares formais do tipo

$$\alpha = \sum_{g \in G} \alpha(g) g \ , \text{ com } \alpha(g) \in R \ \forall g \in G,$$

munido de soma e multiplicação definidos por

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

e

$$\left(\sum_{g\in G}\alpha(g)g\right)\cdot\left(\sum_{g\in G}\beta(g)g\right) = \sum_{g\in G}\gamma(g)g,$$

$$\text{onde } \gamma(g) = \sum_{h\in G}\alpha(h)\ \beta(h^{-1}g).$$

É imediato verificar que RG, com estas definições, é um anel com 1. Dados $r\in R$ e $\alpha\in RG$, definimos ainda

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

Com esta definição, e identificando $g\in G$ com $1\cdot g\in RG$, vemos que RG possui estrutura de R-módulo livre com base G. Definimos o <u>suporte</u> de $\alpha=\Sigma\alpha(g)g$ como $\mathrm{supp}(\alpha)=\{g\in G \mid \alpha(g)\neq 0\}$.

Se H é um subgrupo de G, é sempre possível considerar RH como subanel de RG. Desta forma, podemos dar a RG uma estrutura de RH-módulo.

<u>Definição</u> - Uma <u>transversal</u> para H em G é um sistema completo de representantes das classes laterais à esquerda de H em G. Suporemos sempre que o representante da classe H é $1\in G$.

<u>Prop. 1.1</u> - Seja $T=\{t_0, t_1,\ldots, t_n\}$ uma transversal para H em G. Então RG é um RH-módulo livre de base T.

<u>Demonstração</u> - Se T é uma transversal para H em G, podemos escrever

$$G = Ht_0 \dot{\cup} Ht_1 \dot{\cup} \ldots \dot{\cup} Ht_n.$$

Pondo $\alpha_i = \sum_{g \in Ht_i} \alpha(g)g$, obtemos imediatamente que

$$\alpha = \alpha_0 + \alpha_1 + \ldots + \alpha_n$$

e que os suportes de $\alpha_0, \alpha_1, \ldots, \alpha_n$ são dois-a-dois disjuntos.

Se $g \in Ht_i$, posso pôr $g = h_g t_i$, com $h_g \in H$. Logo, temos que

$$\alpha_i = \sum_{g \in Ht_i} \alpha(g)g = \sum_{g \in Ht_i} \alpha(g)hgt_i = (\sum_{g \in Ht_i} \alpha(g)hg)t_i = \beta_i t_i$$

onde é claro que $\beta_i = \sum_{g \in Ht_i} \alpha(g)h_g \in RH$. Logo, podemos escrever

$$\alpha = \beta_0 t_0 + \ldots + \beta_n t_n, \text{ com } \beta_i \in RH.$$

Resta provar que $\{t_0, t_1, \ldots, t_n\}$ é livre sobre RH. Suponhamos que

$$\gamma = \gamma_0 t_0 + \gamma_1 t_1 + \ldots + \gamma_n t_n = 0, \text{ com } \gamma_i \in RH, i = 0, 1, \ldots, n.$$

Então $\mathrm{supp}(\gamma) = \phi$, isto é, o coeficiente de todo $g \in G$ é zero. Como os suportes de $\gamma_0 t_0, \gamma_1 t_1, \ldots, \gamma_n t_n$ são dois-a-dois disjuntos (porque $\mathrm{supp}\,(\gamma_i t_i) \subset Ht_i$), segue que devemos ter $\mathrm{supp}\,(\gamma_i t_i) = \phi$, para todo $i = 0, 1, \ldots, n$. Logo, $\gamma_i t_i = 0$, $i = 0, 1, \ldots, n$, donde $\gamma_i = 0$, $i = 0, 1, \ldots, n$.

Logo T é uma base RG sobre RH, como queríamos provar.

Uma propriedade importante dos anéis de grupo é o fato de ser possível definir neles uma <u>involução</u>, isto é, um anti-automorfismo de ordem 2.

<u>Definição</u> - Definimos $*: RG \to RG$ por

$$\left(\sum_{g \in G} \alpha(g) g\right)^* = \sum_{g \in G} \alpha(g) g^{-1}.$$

Resumimos as propriedades fundamentais desta aplicação na proposição seguinte, cuja demonstração é imediata.

<u>Proposição 1.2</u> - Sejam $\alpha, \beta \in RG$ e $g \in G$. Então

i) $g^* = g^{-1}$

ii) $(\alpha+\beta)^* = \alpha^* + \beta^*$

iii) $(\alpha\beta)^* = \beta^* \alpha^*$

iv) $(\alpha^*)^* = \alpha$.

Um instrumento essencial para o estudo da estrutura algébrica dos anéis de grupo é a função de aumento, bem como, e especialmente, seu núcleo, o ideal de aumento.

<u>Definição</u> - A <u>função de aumento</u> de RG é a aplicação $\varepsilon: RG \to R$ dada por

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

É imediato verificar que a função de aumento é um homomorfismo de R-álgebras; seu núcleo é o <u>ideal de aumento</u> de RG, e será denotado por $I(G)$ (ou $I_R(G)$, se necessário). Deve-se notar que o ideal de aumento é também costumeiramente denotado por $\Delta(G)$ [Sehgal, 1978] e $\omega(RG)$ [Passman, 1977]. O ideal de aumento desempenhará um papel fundamental em tudo o que segue.

Dado N um subgrupo normal de G, podemos estender a projeção natural de G em G/N para RG, obtendo um homomorfismo $\pi_N : RG \to R\,G/N$, dado por

$$\pi_N\Big(\sum_{g\in G} \alpha(g)g\Big) = \sum_{g\in G} \alpha(g)\bar{g},$$

onde $\bar{g}$ denota a classe de g em G/N. Se denotarmos por $I(N)$ o ideal de aumento de RN, é imediato verificar que $\ker \pi_N = RG.I(N)$ (este ideal é, às vezes, denotado por $\Delta(G,N)$).

Os elementos inversíveis de RG são chamados <u>unidades</u> de RG, e formam um grupo multiplicativo, que será chamado <u>grupo das unidades</u> de RG, e denotado por $U(RG)$. Uma unidade $\alpha \in U(RG)$ será dita <u>normalizada</u> se $\varepsilon(\alpha)=1$; as unidades normalizadas de RG formam um subgrupo de $U(RG)$, que será denotado por $V(RG)$ (este grupo é, às vezes, denotado por $U_1(RG)$). Observe-se que

$$V(RG) = U(RG) \cap (1 + I(G)),$$

$$G \subset V(RG) \subset U(RG)$$

e

$$U(RG) = U(R) \times V(RG).$$

Dados u um elemento inversível de R e $g \in G$ qualquer, é imediato que ug é uma unidade de RG. As unidades desta forma serão chamadas <u>triviais</u>.

Sejam G e H dois grupos. Um isomorfismo de R-álgebras $\psi: RH \to RG$ será dito <u>normalizado</u> se, para todo $\alpha \in RH$, $\varepsilon(\psi(\alpha)) = \varepsilon(\alpha)$. Para tanto, é suficiente que $\forall h \in H, \varepsilon(\psi(h)) = 1$. Dado um isomorfismo de R-álgebras $\psi: RH \to RG$, podemos definir:

$$\psi_1 : RH \to RG \text{ por}$$

$$\psi_1\left(\sum_{g \in G} \alpha(g) g\right) = \sum_{g \in G} \alpha(g) (\varepsilon(\psi(g)))^{-1} \psi(g).$$

É imediato, então, verificar que $\psi_1$ é um isomorfismo normalizado. Desta forma, quando $RG \cong RH$, podemos sempre supor que o isomorfismo entre eles é normalizado.

Dado $\psi: RH \to RG$ um isomorfismo normalizado, temos que $\psi(H)$ é um subgrupo de $V(RG)$ que é uma base de RG sobre R. Como $H \cong \psi(H)$, notamos que estudar isomorfismos entre anéis de grupos é, em certo sentido, equivalente a estudar subgrupos de $V(RG)$ que são bases de RG.

<u>Definição</u> - Uma <u>base grupal</u> de RG é um subgrupo de $U(RG)$

que é base de RG sobre R. Uma base grupal se diz normalizada se está contida em V(RG). Escrevemos RG=RH para indicar que H é uma base grupal normalizada de RG.

É claro que, se H é base grupal de RG, G é base grupal de RH. Desta forma, se RG=RH, podemos definir duas funções de aumento $\varepsilon_G: RG \to R$ e $\varepsilon_H: RH \to R$, e, através delas, dois ideais de aumento. É importante, então, notar que vale a seguinte proposição, cuja demonstração é evidente.

Proposição 1.3 - Seja RG=RH. Então:

i) $\varepsilon_H(\alpha) = \varepsilon_G(\alpha), \quad \forall \alpha \in RG.$

ii) $I(H) = I(G)$

iii) $V(RG) = V(RH)$

Finalmente, o conceito de produto tensorial nos permite relacionar $R(G_1 \times G_2)$ com $RG_1$ e $RG_2$, e também, quando $R \subset S$, RG com SG. Dessa forma, obtemos:

Proposição 1.4 - Seja R um anel comutativo com 1, e seja S um anel comutativo com $R \subset S$. Então, para todo grupo finito G, temos $SG \cong S \otimes_R RG$.

Proposição 1.5 - Sejam G e H grupos finitos e R um anel comutativo com 1. Então $RG \otimes_R RH \cong R(G \times H)$.

Passamos, agora, ao estudo das propriedades fundamentais do grupo das unidades de um anel de grupo.

## § 2. RESULTADOS BÁSICOS SOBRE O GRUPO DAS UNIDADES

A estrutura do grupo U(RG) das unidades de um anel de grupo tem sido bastante estudada. Os primeiros resultados foram obtidos por G. Higman em 1940 e por S.D. Berman numa série de artigos publicados de 1952 a 1955. Estes resultados dizem respeito às unidades de ordem finita de RG e à determinação dos grupos G tais que RG só possui unidades triviais. Em ambos os casos, os resultados foram obtidos inicialmente para o caso em que R é um anel de inteiros algébricos.

Apresentaremos, em primeiro lugar, sem demonstração, o resultado de G. Higman que determina os grupos G tais que $\mathbb{Z}G$ só possui unidades triviais.

Proposição 2.1 - Seja G um grupo finito. Então temos que $U(\mathbb{Z}G) = \pm G$ se e sómente se vale uma das seguintes afirmações:

i) G é abeliano e $G^4=\{1\}$.

ii) G é abeliano e $G^6=\{1\}$.

iii) G é um 2-grupo hamiltoniano.

Demonstração - Veja-se [Sehgal, 1978, Theorem II.4.1].

O Teorema de Higman-Berman sobre unidades de ordem finita de RG, para G um grupo finito e R um anel de inteiros algébricos, vale em situações bem mais gerais. Damos, a seguir, uma demonstração, devida a Saksonov ([Saksonov, 1971], [Karpilovsky, 1980]), que generaliza o resultado de Higman-Berman para domínios de integridade de característica zero satisfazendo certas condições de inversibilidade. Começamos por um Lema devido a Saksonov.

Lema 2.2 - [Saksonov, 1971] Sejam $\alpha$ um número algébrico e $n \in \mathbb{N}$ tal que $n\alpha$ seja um inteiro algébrico. Se $\{\alpha_1=\alpha,\ldots,\alpha_t\}$ é o conjunto dos $\mathbb{Q}$-conjugados de $\alpha$, então ou $\alpha$ é um inteiro algébrico ou pelo menos um divisor primo racional de $n$ é inversível em $\mathbb{Z}[\alpha_1,\alpha_2,\ldots,\alpha_t]$.

Demonstração - Suponhamos que $\alpha$ não é um inteiro algébrico. Como $\alpha$ é um número algébrico, segue que pelo menos um dos coeficientes de seu polinômio irredutível sobre $\mathbb{Q}$ não pertence a $\mathbb{Z}$.

Logo, existe uma função simétrica elementar $f$ em $t$ variáveis tal que $f(\alpha_1,\alpha_2,\ldots,\alpha_t)\notin \mathbb{Z}$. Então, podemos pôr

$$f(\alpha_1,\alpha_2,\ldots,\alpha_t)=\frac{a}{b}, \quad a,b\in\mathbb{Z},\ (a,b)=1,\ b>1.$$

Como $n\alpha$ é inteiro algébrico e como os conjugados de $n\alpha$ são $n\alpha_2,\ldots, n\alpha_t$ (já que $n\in Q$), segue que

$$f(n\alpha_1,n\alpha_2,\ldots,n\alpha_t) \in \mathbb{Z},$$

pois todos os coeficientes do polinômio irredutível de $n\alpha$ sobre Q são inteiros.

Mas é claro que, para algum $s\in\{1,2,\ldots,t\}$, tem-se que:

$$f(n\alpha_1,\ldots, n\alpha_t)= n^s\, f(\alpha_1,\ldots,\alpha_t)=n^s\,\frac{a}{b},$$

pois f é função simétrica elementar.

Logo $n^s\,\frac{a}{b} \in \mathbb{Z}$, donde, para qualquer primo $p\in\mathbb{Z}$ tal que $p\mid b$, temos que $p\mid n^s$, e portanto que $p\mid n$.

Ainda, se $p\mid b$, como $(a,b)=1$, temos que $(a,p)=1$, donde, pelo Teorema de Bézout, existem $c,d\in\mathbb{Z}$ que $ac+pd=1$.

Agora, é claro que $f(\alpha_1,\ldots,\alpha_t) \in \mathbb{Z}[\alpha_1,\ldots,\alpha_t]$. Logo, $\frac{a}{b} \in \mathbb{Z}[\alpha_1,\ldots,\alpha_t]$, donde, multiplicando por $b/p$, obtemos que

$$\frac{a}{p} \in \mathbb{Z}[\alpha_1,\ldots,\alpha_t] \text{ para todo } p \text{ primo t.q. } p\mid b.$$

Mas então, como c e d são inteiros temos:

$$\frac{1}{p} = \frac{ac+pd}{p} = \frac{a}{p}\cdot c + d \in \mathbb{Z}[\alpha_1,\ldots,\alpha_t].$$

Logo, obtemos que se $p\mid b$, p é inversível em

$\mathbb{Z}[\alpha_1,\ldots,\alpha_t]$.

Assim, como $b>1$, e como todo divisor primo de $b$ é divisor de $n$, segue que existe pelo menos um divisor primo de $n$ que é inversível em $\mathbb{Z}[\alpha_1,\ldots,\alpha_t]$, provando o lema.

A demonstração da generalização de Saksonov do resultado de Berman-Higman depende essencialmente do Lema 2.2 e da noção de <u>representação regular</u> de $RG$ sobre $K$, onde $K$ é um corpo algebricamente fechado que contém $R$.

<u>Definição</u> - Sejam $G$ um grupo de ordem $n$, $R$ um domínio de integridade de característica zero em que nenhum divisor primo de $n$ é inversível e $K$ um corpo algebricamente fechado contendo $R$. Sejam $g_1=1, g_2,\ldots, g_n$ os elementos de $G$ e seja $\{v_1,\ldots,v_n\}$ uma base do espaço vetorial $K^n$ sobre $K$. Definimos

$$T: G \longrightarrow \mathrm{End}(K^n)$$
$$g \longrightarrow T_g \quad ,$$

onde $T_g(v_i)=v_j$ se e só se $gg_i=g_j$. Estendemos $T$ a $RG$ pondo

$$T\left(\sum_{g\in G}\alpha(g)g\right) = \sum_{g\in G}\alpha(g)\,T_g.$$

O homomorfismo de álgebras assim definido chama-se <u>representação regular</u> de RG sobre K.

Considerando T como representação matricial, $T:RG \to M_n(K)$, é fácil ver que

$$T_g=(\alpha_{ij})_{\substack{1\le i\le n\\ 1\le j\le n}}, \text{ onde } \begin{cases} \alpha_{ij}=1, \text{ se } gg_j=g_i \\ \text{e} \\ \alpha_{ij}=0, \text{ caso contrário} \end{cases}$$

O Lema 2.3 resume as propriedades da representação regular de que necessitaremos.

<u>Lema 2.3</u> - Seja $T:RG \to M_n(K)$ a representação regular de RG sobre K (considerada como representação matricial). Então:

i) T é um monomorfismo;

ii) $tr\ (T_1) = |G|$ e $tr(T_g)=0$ se $g\neq 1$.

<u>Demonstração</u>.

i) É imediato que T é um homomorfismo de R-álgebras. Para ver que T é injetora, observemos que as matrizes $T_g$ têm os coeficientes iguais a 1 em posições diferentes, isto é, se

$$T_g=(\alpha_{ij}) \ , \quad T_h=(b_{ij}) \quad \text{e} \quad g\neq h,$$

temos que, para um dado par de índices (i,j), se $a_{ij}=1$, en

tão $b_{ij}=0$. Isto segue imediatamente de que $a_{ij}=1$ só se $gg_j=g_i$, o que implica, para $g\neq h$, em que $hg_j\neq g_i$, donde $b_{ij}=0$.

Logo, se $\sum_{g\in G} u(g)T_g=0$, teremos imediatamente que $u(g)=0$ $\forall g$ G. Portanto, ker $T=\{0\}$ e T é injetora.

ii) Como $T_1=I_n$, a matriz identidade em $M_n(K)$, temos claramente que $tr(T_1)= n = |G|$.

Se, por outro lado, $g\neq 1$, temos que $gg_i\neq g_i$ $\forall i=1,\ldots,n$, donde $\alpha_{ii}=0$, $i=1,\ldots,n$. Logo

$$tr(T_g) = \alpha_{11}+\ldots+\alpha_{nn}=0.$$

Estamos, agora, em condições de demonstrar o teorema principal.

<u>Teorema 2.4</u> - ([Higman, 1940],[Berman, 1955],[Saksonov, 1971]). Sejam G um grupo finito e R um domínio de integridade de característica zero tal que nenhum divisor primo de $|G|$ é inversível em R. Seja ainda $u= \sum_{g\in G} u(g)g$ uma unidade de ordem finita de RG. Se $u(1)\neq 0$, então $u=u(1)$.

<u>Demonstração</u> - Escrevemos $u=\sum_{g\in G} u(g)g$, e suponhamos que

$u^m=1$. Fixemos ainda $|G|=n$.

Seja K um corpo algebricamente fechado que contém R, e consideremos $T:RG \to M_n(K)$ a representação regular de RG sobre K. Dado $x \in RG$, $tr(x)$ denotará o traço da imagem de x por T, isto é,

$$tr(x) = tr(T_x).$$

Como $u^m=1$, temos que $T_u^m=1$, isto é, $T_u$ satisfaz o polinômio $X^m-1$, que é separável. Logo, o polinômio minimal de $T_u$ ( que é um divisor de $X^m-1$) é separável, donde segue que $T_u$ é diagonalizável. Assim, obtemos que

$$T_u \sim \begin{bmatrix} \varepsilon_1 & & & & & 0 \\ & \varepsilon_2 & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & & \cdot \\ 0 & & & & & \varepsilon_n \end{bmatrix}$$

onde $\sim$ indica semelhança de matrizes, e $\varepsilon_1,\ldots,\varepsilon_n$ são raízes m-ésimas da unidade.

Logo, obtemos $tr(u)=\varepsilon_1+\varepsilon_2+\ldots+\varepsilon_n$.

Por outro lado, como $u=\sum_{g\in G} u(g)g$, temos que $T_u=\sum_{g\in G} u(g)T_g$, donde

$$tr(u)=\sum_{g\in G} u(g)\ tr(T_g)$$

Lembrando que $tr(T_1)=|G|=n$ e $tr(T_g)=0$ se $g\neq 1$, obtemos

$$tr(u)=n\ u(1).$$

Logo,

(I) $$tr(u)=n\ u(1)=\varepsilon_1+\varepsilon_2+\ldots+\varepsilon_n.$$

Observemos, agora, que, dado $r\in N$, $(r,m)=1$, temos que

$$T_{u^r}=(T_u)^r \sim \begin{bmatrix} \varepsilon_1^r & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n^r \end{bmatrix},$$

donde segue que

$$tr(u^r)=\varepsilon_1^r+\ldots+\varepsilon_n^r.$$

Por outro lado, escrevendo $u^r=\sum_{g\in G} u^r(g)g$, obtemos, como antes, $tr(u^r)=n\ u^r(1)$. Logo:

(II) $$tr(u^r)=n\ u^r(1) = \varepsilon_1^r+\ldots+\varepsilon_n^r.$$

Observamos, agora, que, como $n\in N$ e raízes da unidade são inteiros algébricos, temos que $u(1)$ e $u^r(1)$ são números algébricos e $nu(1)$ é um inteiro algébrico. Desejamos determinar os Q-conjugados de $u(1)$. Para tanto, observamos que, se $\varepsilon$ é uma raiz m-ésima primitiva da unidade, os Q-automorfismos de $Q(\varepsilon)$ são dados por

$$\sigma_r : Q(\varepsilon) \to Q(\varepsilon)$$
$$\varepsilon \longrightarrow \varepsilon^r \quad , \text{ onde } r\in N,\ (r,m)=1.$$

Calculemos $\sigma_r(n\ u(1))$. De (I) e (II), obtemos

(III) $$\sigma_r(n\ u(1))=\sigma_r(\varepsilon_1+\ldots+\varepsilon_n)=\varepsilon_1^r+\ldots+\varepsilon_n^r=n\ u^r(1).$$

Como $\sigma_r$ é Q-automorfismo e $n\in N$, temos que

(IV) $$\sigma_r(n\ u(1))=\sigma_r(n).\sigma_r(u(1)=n\ \sigma_r(u(1)).$$

De (III) e (IV), obtemos

$$n.\sigma_r(u(1))=n.u^r(1),$$

donde $\sigma_r(u(1))=u^r(1)\in R$. Desta forma, os conjugados de $u(1)$ são $u^r(1)$, $r\in N$, $(r,m)=1$. Pondo $\beta_1=u(1)$ e sendo $\beta_2,\ldots,\beta_t$ os seus Q-conjugados, concluímos que $\{\beta_1,\beta_2,\ldots,\beta_t\}\subset R$. Logo,

$$\mathbb{Z}[\beta_1,\beta_2,\ldots,\beta_t]\subset R.$$

Como $\beta_1=u(1)$ é um número algébrico e $n\beta_1=n\ u(1)$ é um inteiro algébrico, temos, pelo Lema 2.2, duas possibilidades:

a) algum divisor primo de $n$ é inversível em $\mathbb{Z}[\beta_1,\ldots,\beta_t]$,

ou

b) $u(1)$ é inteiro algébrico.

Afirmamos que (a) é impossível. De fato, como $n=|G|$ e $\mathbb{Z}[\beta_1,\ldots,\beta_t]\subset R$, e como, por hipótese, nenhum divisor primo de $|G|$ é inversível em $R$, nenhum divisor primo de $n$ pode ser inversível em $\mathbb{Z}[\beta_1,\ldots,\beta_t]$. Logo $u(1)$ é um inteiro algébrico, donde $u^r(1)$ é inteiro algébrico, para

todo $r \in N$ satisfazendo $(r,m)=1$.

Como $u(1)$, $u^r(1)$ são inteiros algébricos, podemos calcular valores absolutos nas equações (I) e (II), obtendo

$$0 \neq n|u(1)| = |\varepsilon_1 + \ldots + \varepsilon_n| \leq |\varepsilon_1| + \ldots + |\varepsilon_n| = n$$

$$0 \neq n|u^r(1)| = |\varepsilon_1^r + \ldots + \varepsilon_n^r| \leq |\varepsilon_1^r| + \ldots + |\varepsilon_n^r| = n,$$

e a igualdade vale se e só se $\varepsilon_1 = \ldots = \varepsilon_n$. Assim, obtemos que $0 \neq |u(1)| \leq 1$ e $0 \neq |u^r(1)| \leq 1$, com igualdade se e só se $\varepsilon_1 = \ldots = \varepsilon_n$. Mas então, tomando normas sobre $Q$, obtemos que

$$0 \neq |N(u(1)| \leq 1.$$

Por outro lado, como $u(1)$ é inteiro algébrico, temos que $N(u(1)) \in \mathbb{Z}$. Assim, devemos ter $|N(u(1))| = 1$, e isto ocorre só se $|u^r(1)| = 1$, para todo $r \in N$ com $(r,m)=1$. Portanto $\varepsilon_1 = \ldots = \varepsilon_n = \varepsilon$, e

$$u(1) = \frac{n\varepsilon}{n} = \varepsilon,$$

e, além disso,

$$T_u \sim \begin{bmatrix} \varepsilon & & 0 \\ & \ddots & \\ 0 & & \varepsilon \end{bmatrix} = \varepsilon I_n,$$

Mas como $\varepsilon I_n$ é <u>central</u> em $M_n(K)$, segue que $T_u = \varepsilon I_n$. Então, como $T_\varepsilon = \varepsilon I_n$ e $T$ é injetora, obtemos imediatamente que

$$u = \varepsilon = u(1),$$

provando o teorema.

O teorema de Higman-Berman-Saksonov é, sem dúvida, um dos resultados mais importantes que se têm a respeito do grupo das unidades de um anel de grupo. Damos, a seguir, vários corolários importantes. Nestes enunciados, G denota sempre um grupo finito e R é sempre um domínio de integridade de característica zero em que nenhum divisor primo de $|G|$ é inversível.

Corolário 2.5 - Seja $u=\sum_{g\in G} u(g)g$ uma unidade de ordem finita de RG, e seja $g\in Z(G)$. Então, se $u(g)\neq 0$, $u=u(g)g$ e u é uma unidade trivial.

Demonstração - Suponhamos $u(g)\neq 0$, e consideremos $\alpha=ug^{-1}$. É claro que $\alpha(1)=u(g)\neq 0$. Como u é unidade de ordem finita e g é central (e de ordem finita porque G é finito), $\alpha$ é uma unidade de ordem finita.

Pelo Teorema 2.4, $\alpha=\alpha(1)$, isto é,

$$ug^{-1}=u(g).$$

Logo, temos $u=u(g)g$ e u é uma unidade trivial.

Corolário 2.6 - ([Passman-Smith, 1981]). Seja W um subgrupo central de G. Se u é uma unidade de ordem finita de RG tal que

$$u\in 1+I(W)RG,$$

então $u=x$ para algum $x\in W$.

Demonstração - Escrevamos $u=\alpha+\beta$, com $\mathrm{supp}(\alpha)\subset G-W$ e $\mathrm{supp}(\beta)\subset W$. Como $W$ é central, $W\triangleleft G$; logo podemos considerar $\pi_W: RG \to R\,G/W$, cujo núcleo é $I(W)RG$.

Temos que $u\in 1+I(W)RG \iff \pi_W(u)=1$. Logo, devemos ter

$$1=\pi_W(u)=\pi_W(\alpha+\beta)=\pi_W(\alpha)+\pi_W(\beta).$$

Como $\mathrm{supp}(\beta)\subset W$, é claro que $\pi_W(\beta)=\varepsilon(\beta)\in R$.

Como $\mathrm{supp}(\alpha)\subset G-W$, temos que $\mathrm{supp}(\pi_W(\alpha))\subset G/W-\{1\}$. Mas então, como $\mathrm{supp}(\pi_W(\beta))=\{1\}$ e $\pi_W(\beta)+\pi_W(\alpha)=1$, o coeficiente de todo elemento diferente de 1 de $G/W$ deve ser zero em $\pi_W(\alpha)$. Logo, temos $\pi_W(\alpha)=0$.

Então, temos

$$1=\pi_W(\alpha)+\pi_W(\beta)=0+\varepsilon(\beta)=\varepsilon(\beta).$$

Portanto, $\beta\in 1+I(W)$, donde $\beta\neq 0$. Assim, $\exists x\in W$ tal que $x\in \mathrm{supp}\,\beta=W\cap \mathrm{supp}\,u$. Como $W$ é central, pelo Corolário 2.5 segue que $u=u(x)x$.

Finalmente, como $u\in 1+I(W)RG\subset 1+I(G)$, $u$ é unidade normalizada. Logo, devemos ter que $\varepsilon(u)=u(x)=1$, donde $u=x\in W$, como se desejava.

Corolário 2.7 - Seja $\sum_{g\in G} u(g)g$ uma unidade central de

ordem finita de RG. Então u é uma unidade trivial.

Demonstração - Como u é unidade, $u \neq 0$. Logo existe $g \in G$ tal que $u(g) \neq 0$. Como G é finito e u é central, o elemento $\alpha = ug^{-1}$ também é unidade de ordem finita e $\alpha(1) = u(g) \neq 0$. Pelo Teorema 2.4, obtemos imediatamente que $\alpha = \alpha(1)$, donde $u = u(g)g$ é uma unidade trivial.

Definição - Seja G um grupo qualquer. A torção de G é definida por

$$T(G) \doteq \{g \in G \mid \exists\, n \in N^* \text{ tq } g^n = 1\}.$$

Com esta definição, podemos enunciar o Corolário 2.7 de uma forma mais compacta:

Corolário 2.7a - $T(Z(U(RG))) = T(U(R)).Z(G)$

Demonstração - Basta notar que se $u = u(g)g$ é unidade central de ordem finita, então $g \in Z(G)$ e $u(g)$ é unidade de ordem finita de R.

Os próximos dois corolários dizem respeito ao problema do isomorfismo. O primeiro mostra que os grupos abelianos são solução do problema para anéis de grupos sobre domínios de integridade de característica zero em que nenhum divisor primo de $|G|$ é inversível.

Corolário 2.8 - Sejam G um grupo abeliano finito, H um grupo qualquer e R um domínio de integridade de característica zero em que nenhum divisor primo de $|G|$ é inversível. Se $RG \cong RH$, então $G \cong H$.

Demonstração - Como RG é um R-módulo livre de posto $|G|$, RH é livre de posto $|G|$, e portanto H é finito e $|H|=|G|$.

Como G é abeliano, RG é comutativo, donde RH é comutativo e portanto H é abeliano.

Seja, agora $\psi: RG \to RH$ o isomorfismo, que, como já vimos, podemos supor normalizado. Como G é finito, todo elemento $g \in G$ tem ordem finita, donde segue imediatamente que $\psi(g)$ também é unidade de ordem finita. Obtemos, assim, que, para todo $g \in G$, $\psi(g)$ é uma unidade normalizada de ordem finita de RH, isto é,

$$\psi(g) \in T(U(RH)) \cap (1+I(H)) =$$
$$= T(U(R)).H \cap (1+I(H)) = H.$$

Logo $\psi(G) \subset H$. Mas como $\psi$ é isomorfismo e $|G|=|H|$, temos $\psi(G)=H$. Logo $\psi|G: G \to H$ é um isomorfismo, donde $H \cong G$.

Corolário 2.9 - Seja H um grupo de torção de unidades normalizadas de RG. Então H é linearmente independente sobre R, donde H é finito e $|H| \leq |G|$.

Demonstração - Seja $\sum_{i=1}^{n} \alpha_i h_i = 0$, com $\alpha_i \in R$ e $h_i \in H$, e suponhamos que $\alpha_j \neq 0$ para algum j, $1 \leq j \leq u$. Então temos

$$\alpha_j h_j = - \sum_{i \neq j} \alpha_i h_i ,$$

donde,

$$\alpha_j . 1 = - \sum_{i \neq j} \alpha_i h_i h_j^{-1}$$

Como $1 \in supp(\alpha_j . 1) = supp(\sum_{i \neq j} \alpha_i h_i h_j^{-1})$, escrevendo $h_i h_j^{-1}$ em termos dos elementos de G, existe k, $1 \leq k \leq n$, $k \neq j$, tal que $1 \in supp(h_k h_j^{-1})$. Como H é um grupo de torção, $h_k h_j^{-1}$ é uma unidade de ordem finita. Logo, pelo teorema 2.4, $h_k h_j^{-1} = \alpha \in R$, donde segue que $h_k = \alpha h_j$. Como $h_k$ e $h_j$ são ambos unidades normalizadas,

$$\varepsilon(h_k) = \varepsilon(h_j) = 1 ,$$

donde segue que $\alpha = 1$, e portanto $h_k = h_j$, que é absurdo.

Logo, H é linearmente independente sobre R, e como RG é um R-módulo livre de posto $|G|$, segue que H é finito e que $|H| \leq |G|$, provando o teorema.

O último corolário do Teorema 2.4 refere-se a anéis de grupo sobre $\mathbb{Z}$, e é importante porque justifica a espectativa de encontrarmos complementos normais livres de torção para G em $V(\mathbb{Z}G)$, problema de que nos ocuparemos no capítulo IV deste trabalho.

<u>Corolário 2.10</u> - Para todo grupo finito G, $U(\mathbb{Z}G)$ possui um subgrupo normal livre de torção de índice finito.

<u>Demonstração</u> - Seja p um primo ímpar, e consideremos a aplicação natural

$$\rho : \mathbb{Z}G \to \frac{\mathbb{Z}}{p\mathbb{Z}} G$$

dada por $\rho(\sum_{g\in G} \alpha(g)g) = \sum_{g\in G} \overline{\alpha(g)}g$ , onde $\bar{n}$ indica a classe de n em $\mathbb{Z}/_p\mathbb{Z}$. É imediato verificar que $\rho$ é um epimorfismo de anéis.

Seja $N=U(\mathbb{Z}G) \cap (1+\ker\rho)$, que é o núcleo do homomorfismo de grupos (multiplicativos) obtido por restrição,

$$\rho|_{U(\mathbb{Z}G)} : U(\mathbb{Z}G) \to U(\mathbb{Z}/p\mathbb{Z}G).$$

Então $N \triangleleft G$ e $[U:N] < \infty$ pois $\frac{\mathbb{Z}}{p\mathbb{Z}} G$ é finito.

Resta mostrar que N é livre de torção. Dado $\alpha \in N$, temos que $\alpha \in 1+\ker\rho$, donde $\alpha(1) \equiv 1 \pmod{p}$. Logo, como p é primo ímpar, $\alpha(1) \neq 0$ e $\alpha(1) \neq -1$.

Se, agora, $\alpha$ tem ordem finita, segue pelo Teorema 2.4 que $\alpha = \alpha(1)$. Como as unidades de $\mathbb{Z}$ são $\pm 1$ e $\alpha(1) \neq -1$, devemos ter $\alpha(1)=1$, donde $\alpha=1$.

Assim, N é livre de torção.

Finalmente, damos dois exemplos que mostram que as hipóteses sobre R no Teorema 2.4 não podem ser removidas.

Exemplo 2.11 - O teorema falha se char $R \neq 0$. De fato, seja $R=GF(p)$, o corpo de $p$ elementos, e seja $G$ um $p$-grupo abeliano finito. Nesta situação, todo elemento $u \in RG$ que satisfaz $\varepsilon(u)=1$ é unidade central de ordem finita (Veja-se [Polcino Milies, 1976, Corolário 8.2]). Logo, existem unidades centrais de ordem finita não-triviais.

Exemplo 2.12 - [Saksonov, 1971] O teorema falha se algum divisor primo de $|G|$ é inversível em R. De fato, tomemos $G=\langle a\rangle$ o grupo cíclico de ordem quatro e $R=\mathbb{Z}[1/2,i]$. Então, pondo

$$b=\frac{1-i}{2}a+\frac{1+i}{2}a^3,$$

temos que $b$ é central (porque RG é comutativo), mas $b^2=1$. Assim, $b$ é uma unidade central de ordem finita não-trivial.

## § 3. O CÁLCULO DE IDEAIS DE AUMENTO

Neste parágrafo, apresentaremos vários resultados sobre ideais de aumento que serão usados mais tarde. A

maioria destes resultados dizem respeito ao cálculo algébrico com ideais de aumento; quase todos são de demonstração bastante fácil.

Começamos lembrando os resultados fundamentais sobre os ideais $I(G)$ e $RGI(N)$, onde $N$ é um subgrupo de $G$.

<u>Proposição 3.1</u> - Sejam $R$ um anel comutativo com 1, $G$ um grupo e $N$ um subgrupo de $G$. Então temos:

i) $I(G)$ é um ideal bilateral.

ii) $I(G)$ é $R$-livre de base $\{g-1 \mid g \in G,\ g \neq 1\}$.

iii) $I(G)^* = I(G)$.

iv) Se $T$ é uma transversal para $N$ em $G$, $RGI(N)$ é $R$-livre de base $\{t(n-1) \mid n \in N,\ n \neq 1,\ t \in T\}$.

v) Se $N \triangleleft G$, $RGI(N) = I(N)RG$, $RGI(N)$ é ideal bilateral e $(RGI(N))^* = RGI(N)$.

vi) Se $N \triangleleft G$, $I(G)I(N)$ e $I(N)I(G)$ são ideais bilaterais.

Tomemos agora $\alpha \in RG$. Escrevendo $\alpha = \varepsilon(\alpha) + \alpha - \varepsilon(\alpha)$, e notando que $\varepsilon(\alpha - \varepsilon(\alpha)) = 0$, obtemos que

$$RG = R \oplus I(G),$$

como soma direta de $R$-módulos. Multiplicando esta equação por $I(N)$, onde $N$ é um subgrupo de $G$, obtemos:

$$RGI(N) = I(N) + I(G)\ I(N),$$

uma fórmula que será usada várias vezes mais adiante.

Passamos agora à demonstração dos Lemas fundamentais. No que segue, R indica sempre um anel comutativo com 1, G um grupo finito e N um subgrupo de G.

<u>Lema 3.2</u> - $G \cap (1+RGI(N))=N$

<u>Demonstração</u> - Sejam $T=\{t_1,t_2,\ldots,t_k\}$ uma transversal à esquerda para N em G e $N=\{n_1,n_2,\ldots,n_s\}$, onde tomamos sempre $t_1=n_1=1$. Então o conjunto

$$\{t_i(n_j-1) \mid i=1,2,\ldots,k, \quad j=2,\ldots,s\}$$

é uma base de RGI(N) sobre R.

Seja $g \in G \cap (1+RGI(N))$, i.é, $g \in G$ tal que $g-1 \in RGI(N)$. Podemos supor $g \neq 1$.

Então podemos escrever

$$g-1 = \sum_{\substack{i,j \\ j\neq 1}} r_{ij}t_i(n_j-1) \quad , \; r_{ij} \in R.$$

Logo:

$$g-1 = \sum_{\substack{i,j \\ j\neq 1}} r_{ij}t_in_j - \sum_{\substack{i,j \\ j\neq 1}} r_{ij}t_i.$$

Como $t_in_j \neq 1$, porque $j \neq 1$ e T é transversal, devemos ter que

$$\sum_{j\neq 1} r_{1j}=1.$$

Logo, existe $j_0 \in \{2,\ldots,s\}$ tal que $r_{1j_0} \neq 0$ (pois, se não, teríamos $\sum_{j\neq 1} r_{1j}=0$).

Mas então $r_{1j_0} t_1 n_{j_0} = r_{1j_0} n_{j_0} \neq 0$, e temos que $n_{j_0} \in \mathrm{supp}(g-1)=\{g,1\}$. Como $n_{j_0} \neq 1$, segue que $g=n_{j_0}$ e portanto $g \in N$. Assim,

$$G \cap (1+RGI(N)) \subset N.$$

Como a inclusão recíproca é evidente, o Lema está provado.

<u>Lema 3.3</u> - [Karpilovsky, 1979 b] Sejam M e N subgrupos de G e T uma transversal para $M \cap N$ em M. Então:

i) $I(M)\ I(N) = I(M \cap N)\ I(N) + \sum_{1\neq t\in T} (t-1)\ I(N)$

ii) $I(M)\ I(N) \cap I(N) = I(M \cap N)\ I(N)$

iii) $I(G)\ I(N) \cap I(N) = I(N)^2$

iv) $G \cap (1+I(G)\ I(N)) = N \cap (1+I(N)^2)$

<u>Demonstração</u> - i) Tomemos $m \in M$, e suponhamos que $m=t.n$, com $t \in T$ e $n \in M \cap N$. Então, dado $n' \in N$, temos:

$$(m-1)(n'-1) = (tn-1)(n'-1) =$$
$$= (t-1)(n-1)(n'-1) + (t-1)(n'-1) + (n-1)(n'-1).$$

Como o primeiro e o segundo somando pertencem a $(t-1)\ I(N)$, e o terceiro pertence a $I(M \cap N)\ I(N)$, segue que

$$(m-1)(n'-1) \in I(M \cap N)\ I(N) + (t-1)\ I(N).$$

Como os elementos $(m-1)(n'-1)$, $m\in M$ e $n'\in N$ <u>geram</u> $I(M)\ I(N)$, temos que

$$I(M)\ I(N) \subset I(M\cap N)\ I(N) + \sum_{1\neq t\in T} (t-1)\ I(N)$$

Como a inclusão recíproca é evidente, isto prova (i).

ii) Seja $x\in I(M)\ I(N)\cap I(N)$. Como $x\in I(M)\ I(N)$, pelo ítem (i) podemos escrever:

$$x=y+(t_1-1)[\alpha_{11}(n_1-1)+\ldots+\alpha_{1s}(n_s-1)]+\ldots+$$
$$+\ (t_k-1)\ [\alpha_{k1}(n_1-1)+\ldots+\alpha_{ks}(n_s-1)], \qquad (I)$$

onde $y\in I(M\cap N)\ I(N)$, $1\neq t_j\in T$, $j=1,\ldots,k$, $1\neq n_i\in N$, $i=1,2,\ldots,s$ e $\alpha_{ji}\in R$.

Então:

$$x=y-[\alpha_{11}(n_1-1)+\ldots+\alpha_{1s}(n_s-1)]-\ldots-$$
$$-\ [\alpha_{k1}(n_1-1)+\ldots+\alpha_{ks}(n_s-1)]+$$
$$+\ t_1[\alpha_{11}(n_1-1)+\ldots+\alpha_{1s}(u_s-1)]+\ldots+$$
$$+\ t_k[\alpha_{k1}(n_1-1)+\ldots+\alpha_{ks}(u_s-1)],$$

e como $y\in I(M\cap N)\ I(N)\subset I(N)$ e $n_i-1\in I(N)$, $i=1,\ldots,s$, segue que, como $x\in I(M)\ I(N)\cap I(N)$, pondo $z=t_1[\alpha_{11}(n_1-1)+\ldots+\alpha_{1s}(n_s-1)]+\ldots+t_k[\alpha_{k1}(n_1-1)+\ldots]$, temos $z\in I(N)$. Mas

$$z=\alpha_{11}t_1(n_1-1)+\ldots+\alpha_{1s}t_1(n_s-1)+\ldots+\alpha_{ks}t_k(n_s-1),$$

e, como $t_jn_i\notin N$ (pois $T$ é transversal e $t_j\neq 1$), temos $z\in I(N)$ e $\mathrm{supp}(z)\cap N=\emptyset$, donde segue imediatamente que $z=0$.

Logo $\alpha_{11}=\ldots=\alpha_{1s}=\ldots=\alpha_{ks}=0$, pois o conjunto $\{t_j(n_i-1) \mid 1\neq t_j\in T,\ 1\neq n_i\in N\}$ é linearmente independente sobre R. De (I), então, segue que $x=y$, donde $x\in I(M\cap N)I(N)$.

Logo $I(M)\ I(N)\cap I(N)\subset I(M\cap N)\ I(N)$, e, como a inclusão recíproca é evidente, (ii) está provado.

iii) Por (ii), $I(G)\ I(N)\cap I(N)=I(G\cap N)I(N)$. Como $N\subset G$, $I(G\cap N)=I(N)$ e (iii) está provado.

iv) Como $I(G)\ I(N)\subset RGI(N)$, temos que $G\cap(1+I(G)\ I(N))=G\cap(1+RGI(N))\cap(1+I(G)\ I(N))=$ $=N\cap(1+I(G)\ I(N))$ porque $G\cap(1+RGI(N))=N$.

Se $n\in N$, $n-1\in I(N)$, e segue que $N\cap(1+I(G)\ I(N))=N\cap(1+I(G)\ I(N)\cap I(N))$.

Por (iii) $I(G)\ I(N)\cap I(N)=I(N)^2$, donde $G\cap(1+I(G)\ I(N))=N\cap(1+I(N)^2)$ e o Lema está provado.

O subgrupo de N definido por $N\cap(1+I(N)^2)$ é um caso particular de uma classe de subgrupos que têm um papel importante no estudo de anéis de grupo, especialmente em relação ao problema do isomorfismo.

<u>Definição</u> - Seja R um anel com 1 e G um grupo finito. Sendo $I_R(G)$ o ideal de aumento do anel de grupo RG, o k-ésimo <u>subgrupo de dimensão</u> G sobre R é definido por

$$D_{k,R}(G)=G\cap(1+I_R(G)^k).$$

O problema da determinação dos subgrupos de dimensão de um grupo em relação a um anel arbitrário já foi bastante estudado. Citamos, a seguir, uma descrição de $D_{k,R}(G)$, para R um domínio de integridade, em função de $D_{k,\mathbb{Z}}(G)$, que é um caso particular de resultados de Parmenter e Sandling ([Parmenter, 1972],[Sandling, 1972]).

<u>Teorema 3.4</u> - Seja R um domínio de integridade de característica e G um grupo. Então vale que

$$D_{k,R}(G) = \prod_{p \in \pi(R)} T_p(G \bmod D_{k,\mathbb{Z}}(G)),$$

onde $\pi(R)$ é o conjunto dos primos racionais inversíveis em R e

$$T_p(G \bmod D_{k,\mathbb{Z}}(G)) = \{g \in G \mid (\exists n \in N^*)\, g^{p^n} \in D_{k,\mathbb{Z}}(G)\}$$

<u>Demonstração</u> - Veja-se [Sehgal, 1978, Theorem 1.9] ou [Parmenter, 1972, Theorem 1.2].

Para determinar $D_{2,\mathbb{Z}}(G)$, recorremos ao próximo Lema, após o qual estaremos em condições de calcular $D_{2,R}(G)$ para qualquer domínio de integridade R de característica zero.

<u>Lema 3.5</u> - Sejam G um grupo, n o expoente de $G/G'$ e $R=\mathbb{Z}/m\mathbb{Z}$, onde $m \equiv 0 \pmod{n}$. Para cada elemento $g \in G$, denota

mos por $\bar{\alpha}$ a sua classe em $\mathbb{Z}/m\mathbb{Z}$. Então a função $f: I(G) \to G/G'$ definida por

$$f\left(\sum_{g\in G} \bar{\alpha}_g (g-1)\right) = \prod_{g\in G} \bar{g}^{\alpha_g}$$

é um homomorfismo do grupo aditivo $I(G)$ sobre $G/G'$ cujo núcleo é $I(G)^2$.

<u>Demonstração</u> - Como $m \equiv 0 \pmod{n}$, $f$ está bem definida.

a) Observamos, em primeiro lugar, que $f$ é claramente um homomorfismo, pois

$$f\left(\sum_{g\in G} \bar{\alpha}_g (g-1) + \sum_{g\in G} \bar{\beta}_g (g-1)\right) =$$

$$= f\left(\sum_{g\in G} (\bar{\alpha}_g + \bar{\beta}_g)(g-1)\right) = \prod_{g\in G} \bar{g}^{\alpha_g+\beta_g} =$$

$$= \prod_{g\in G} \bar{g}^{\alpha_g} \cdot \prod_{g\in G} \bar{g}^{\beta_g},$$ já que $G/G'$ é abeliano.

b) Em segundo lugar, notamos que, para $g_1, g_2 \in G$,

$$f((g_1-1)(g_2-1)) = f(g_1g_2 - g_1 - g_2 - 1) =$$

$$= f((g_1g_2-1)-(g_1-1)-(g_2-1)) = \bar{g}_1\bar{g}_2\bar{g}_1^{-1}\bar{g}_2^{-1} = 1.$$

Logo, $I(G)^2 \subset \ker f$.

c) Resta provar que $\ker(f) \subset I(G)^2$. Para tanto, notamos que:

$$(a-1)+(b-1) = (ab-1)-(a-1)(b-1),$$

donde

$$(a-1)+(b-1) \equiv ab-1 \pmod{I(G)^2},$$

e, como ainda

$$-(a-1)=(a^{-1}-1)+(a^{-1}-1)(a-1)\equiv a^{-1}-1 \pmod{I(G)^2},$$

segue, por indução, que

$$\sum_{g\in G}\bar{\alpha}_g(g-1)\equiv \prod_{g\in G} g^{\alpha_g}-1 \pmod{I(G)^2}. \qquad (I)$$

Além disso, observamos que

$$[a,b]-1=ab\,a^{-1}b^{-1}-1=(ab-ba)a^{-1}b^{-1}=$$

$$=[(a-1)(b-1)-(b-1)(a-1)]a^{-1}b^{-1}\in I(G)^2 \qquad (II)$$

Seja agora $\sum_{g\in G}\bar{\alpha}_g(g-1)\in \ker f$. Então, como $I(G)^2\subset\ker f$, segue, por (I), que

$$\prod_{g\in G} g^{\alpha_g}-1\in \ker f.$$

Mas então

$$1=f\Big(\prod_{g\in G} g^{\alpha_g}-1\Big)=\overline{\prod_{g\in G} g^{\alpha_g}}$$

Logo, $\prod_{g\in G} g^{\alpha_g}\in G'$, donde, por (II), $\prod_{g\in G} g^{\alpha_g}-1\in I(G)^2$.

Mas então, por (I), segue imediatamente que

$$\sum_{g\in G}\bar{\alpha}_g(g-1)\in I(G)^2,$$

donde $\ker f= I(G)^2$.

Logo, $f:I(G)\to \frac{G}{G'}$ é um epimorfismo de núcleo $\ker f = I(G)^2$.

<u>Corolário 3.6</u> - Se $G$ é um grupo, $n$ é o expoente de $G/G'$ e $R=\mathbb{Z}/m\mathbb{Z}$, onde $m\equiv 0 \pmod{n}$, então:

i) $\sum_{g\in G} \bar{\alpha}_g (g-1) \equiv \prod_{g\in G} g^{\alpha_g} -1 \pmod{I(G)^2}$.

ii) $\dfrac{I(G)}{I(G)^2} \cong \dfrac{G}{G'}$

iii) $D_{2,R}(G)=G\cap(1+I(G)^2)=G'$

<u>Demonstração</u> -

(i) Já foi provado, no ítem (c) da demonstração do Lema 3.5.

(ii) Temos que $f:I(G)\to \dfrac{G}{G'}$ é um epimorfismo, com $\ker f=I(G)^2$. Pelo teorema do homomorfismo, temos um isomorfismo $\bar{f}: \dfrac{I(G)}{I(G)^2} \to \dfrac{G}{G'}$.

(iii) Dado $g\in G$ tal que $g-1\in I(G)^2$, temos que $f(g-1)=1$, donde $\bar{g}=1$, e portanto $g\in G'$. Por outro lado, a relação (II) do ítem (c) da demonstração do Lema 3.5 dá que, se $g\in G'$, então $g-1\in I(G)^2$.

Logo $D_{2,R}(G)=G'$.

Observamos que, no Lema anterior, podemos tomar $m=0$, obtendo então $D_{2,\mathbb{Z}}(G)=G'$. Com isto, podemos determinar $D_{2,R}(G)$ em alguns casos.

<u>Corolário 3.7</u> - Sejam G um grupo finito e $n=\exp(G/G')$. Se R é um domínio de integridade de característica zero tal que nenhum divisor primo de $|G|$ é inversível em R ou $R=\mathbb{Z}/m\mathbb{Z}$, onde $m\equiv 0 \pmod n$, temos que

$$D_{2,R}(G)=G'.$$

<u>Demonstração</u> - No caso em que $R=\mathbb{Z}/m\mathbb{Z}$, a afirmação é a mesma do ítem (iii) do Corolário anterior. Seja, então, R um domínio de integridade de característica zero em que nenhum divisor primo de $|G|$ é inversível. Como $D_{2,\mathbb{Z}}(G)=G'$ (pondo $R=\mathbb{Z}/m\mathbb{Z}$, com $m=0$), obtemos do Teorema 3.4, que $D_{2,R}(G)=\prod_{p\in\pi(R)} T_p(G \bmod G')$.

Mas $g\in T_p(G \bmod G')$ se e sómente se $\bar{g}^{p^n}=1$ em $G/G'$ para algum $n\in N$. Como $p\in\pi(R)$, $p\nmid|G|$, donde $p\nmid|G/G'|$, e portanto, se $\bar{g}^{p^n}=1$, segue que $\bar{g}=1$, e então que $g\in G'$.

Portanto, $T_p(G \bmod G')=G'$, $\forall p\in\pi(R)$.

Assim, $D_{2,R}(G)=G'$.

<u>Corolário 3.8</u> - Sejam G um grupo, $n=\exp(G/G')$ e $R=\mathbb{Z}/m\mathbb{Z}$, onde $m\equiv 0 \pmod n$. Então, para todo $t\in I(G)$, existe $g\in G$ tal que $t\equiv g-1 \pmod{I(G)^2}$.

<u>Demonstração</u> - Este corolário é uma reformulação do ítem

(i) do Corolário 3.6.

Vale observar que o Corolário 3.8 pode ser generalizado para o caso em que R é um anel comutativo com 1 satisfazendo $R/nR \cong \mathbb{Z}/n\mathbb{Z}$; veja-se [Karpilovsky, 1980].

O próximo resultado nos será bastante útil no capítulo final deste trabalho.

<u>Lema 3.9</u> - Seja A um subgrupo normal abeliano de um grupo finito G. Se $\delta \in \mathbb{Z}G\, I(A)$ e T é uma transversal para A em G, então $\delta$ pode ser escrito, de modo único, na forma

$$\delta = \sum_{x \in T} x(a_x - 1) + \alpha,$$

onde $a_x \in A$ e $\alpha \in \mathbb{Z}G\, I(A)^2$.

<u>Demonstração</u> - Pela Proposição 1.1, podemos escrever

$$\delta = \sum_{x \in T} x\alpha_x, \quad \text{com } \alpha_x \in \mathbb{Z}A.$$

Como $\delta \in \mathbb{Z}G\, I(A)$, é imediato que $\alpha_x \in I(A)$, de modo que, pelo Corolário 3.8, existe $a_x \in A$ tal que $\alpha_x \equiv a_x - 1 \pmod{I(A)^2}$.

Então:

$$\delta = \sum_{x \in T} x(a_x - 1) + \sum_{x \in T} x(\alpha_x - (a_x - 1)).$$

Como $\alpha_x - (a_x - 1) \in I(A)^2$, podemos pôr

$$\alpha = \sum_{x \in T} x(\alpha_x - (a_x - 1)) \in \mathbb{Z}G\, I(A)^2,$$

e $\delta$ tem a forma pedida.

Para provar a unicidade, suponhamos que

$$\delta = \sum_{x \in T} x(a_x - 1) + \alpha = \sum_{x \in T} x(b_x - 1) + \beta$$

Então segue que

$$\sum_{x \in T} x(a_x - b_x) \in \mathbb{Z}G\, I(A)^2,$$

donde segue imediatamente que, para todo $x \in T$, tem-se que $a_x - b_x \in I(A)^2$, donde $a_x b_x^{-1} - 1 \in I(A)^2$; logo,

$$a_x b_x^{-1} \in A \cap (1 + I(A)^2) = A' = 1.$$

Assim $a_x b_x^{-1} = 1$, e $a_x = b_x$, para todo $x \in T$, provando a unicidade.

Damos, a seguir, dois Lemas que procuram relacionar os ideais de aumento, sobre $\mathbb{Z}$, de dois subgrupos de um grupo G.

<u>Lema 3.10</u> -Sejam G um grupo finito, $A \triangleleft G$ um subgrupo normal abeliano e B um subgrupo normal de G contido em A. Então:

i) $I(A)^2 \cap \mathbb{Z}A\, I(B) = I(A)\ I(B)$

ii) $\mathbb{Z}G\, I(A)^2 \cap \mathbb{Z}G\, I(B) = \mathbb{Z}G\, I(A)\ I(B)$

iii) $I(G)\ I(A) \cap \mathbb{Z}G\, I(B) = I(A)\ I(B) +$

$+ \sum_{i>0} (t_i - 1)\ \mathbb{Z}A\, I(B)$,

onde $T=\{t_0=1,\ t_1,\ldots,\ t_r\}$ é uma transversal para A em G.

Demonstração -

i) É imediato que $I(A)I(B) \subset I(A)^2 \cap \mathbb{Z}A\, I(B)$. Seja, então, $\alpha \in I(A)^2 \cap \mathbb{Z}A\, I(B)$ e tomemos uma transversal $\{y_0=1,\ y_1,\ldots,y_m\}$ de B em A.

Escrevendo $\alpha = \sum_{j=0}^{m} y_j \gamma_j$, com $\gamma_j \in \mathbb{Z}B$, temos que, como $\alpha \in \mathbb{Z}A\, I(B)$, então $\gamma_j \in I(B)$, $j=0,\ldots,\ m$.

Logo:

$$\alpha = \sum_{j=0}^{m} (y_j - 1)\gamma_j + \sum_{j=0}^{m} \gamma_j .$$

Ponhamos $\sum_{j=0}^{m} \gamma_j = \beta$.

Como $(y_j - 1)\gamma_j \in I(A)\ I(B)$ para cada $j=0,1,\ldots,m$, temos que $\alpha \equiv \beta \pmod{I(A)\ I(B)}$. Pelo Corolário 3.8, existe $b \in B$ tal que $\beta \equiv b-1 \pmod{I(B)^2}$, de modo que

$$\alpha \equiv b-1 \pmod{I(A)^2},$$

já que $I(B)^2 \subset I(A)^2$ e $I(B)\ I(A) \subset I(A)^2$. Mas $\alpha \in I(A)^2$, donde $b \in A \cap (1+I(A)^2) = 1$; logo, $b=1$, e

$$\beta \equiv 0 \pmod{I(B)^2},$$

donde

$$\beta \equiv 0 \pmod{I(A)\ I(B)},$$

e, como $\alpha \equiv \beta \pmod{I(A)\ I(B)}$, segue que $\alpha \in I(A)\ I(B)$. Logo, $I(A)^2 \cap \mathbb{Z}A\, I(B) = I(A)\ I(B)$.

ii) Por (i), $I(A)^2 \cap \mathbb{Z}A\, I(B) = I(A)\ I(B)$. Novamente, uma das inclusões é evidente, e basta provar que $\mathbb{Z}G\, I(A)^2 \cap \mathbb{Z}G\, I(B) \subset \mathbb{Z}G\, I(A)\ I(B)$.

Seja, então, $\delta \in \mathbb{Z}G\, I(A)^2 \cap \mathbb{Z}G\, I(B)$. Tomemos uma transversal $\{t_0=1,\ t_1,\ldots,t_r\}$ de A em G. Pela Proposição 1.1, podemos escrever $\delta$, de modo único, na forma

$$\delta = \sum_{i=0}^{r} t_i \alpha_i,\quad \alpha_i \in \mathbb{Z}A,\quad i=0,\ldots,r,$$

e como $\delta \in \mathbb{Z}G\, I(A)^2$, temos $\alpha_i \in I(A)^2$, $i=0,1,\ldots,r$.

Seja, agora, $\{y_0=1, y_1,\ldots,y_m\}$ uma transversal de B em A, e escrevamos

$$\alpha_i = \sum_{j=0}^{m} y_j \beta_{ij},\ \text{com}\ \beta_{ij} \in \mathbb{Z}B,\quad j=0,1,\ldots,m,$$

e como $\delta \in \mathbb{Z}G\, I(B)$, temos $\beta_{ij} \in I(B)$, $i=0,\ldots,r$, $j=0,\ldots,m$. Logo,

$$\alpha_i \in I(A)^2 \cap \mathbb{Z}G\, I(B) = I(A)\ I(B)\ \text{por (i)}.$$

Assim,

$$\delta \in \mathbb{Z}G\, I(A)\ I(B),\ \text{provando (ii)}.$$

iii) Novamente, uma das inclusões é evidente, e basta provar que

$I(G)\ I(A) \cap \mathbb{Z}G\, I(B) \subset I(A)\ I(B) + \sum_{i>0} (t_i - 1)\mathbb{Z}A\, I(B)$, onde

$T=\{t_0=1, t_1, \ldots, t_r\}$ é uma transversal de A em G.

Seja, então, $\alpha \in I(G)\ I(A) \cap \mathbb{Z}G\, I(B)$. Pelo Lema 3.3(i), como $\alpha \in I(G)\ I(A)$, temos que

$$\alpha \in I(A)^2 + \sum_{i>0} (t_i - 1)\ I(A).$$

Logo, podemos pôr

$$\alpha = \alpha_0 + \sum_{i>0} (t_i - 1)\alpha_i, \text{ com } \alpha_i \in I(A) \text{ se } i>0 \quad \text{e}$$

$$\alpha_0 \in I(A)^2.$$

Então temos

$$\alpha = (\alpha_0 - \sum_{i>0} \alpha_i) + \Sigma t_i \alpha_i.$$

Como $\alpha \in \mathbb{Z}G\, I(B)$ e $B \triangleleft G$, podemos considerar a aplicação $\pi_B : \mathbb{Z}G \longrightarrow \mathbb{Z}\, G/B$. É claro que $\pi_B(\alpha)=0$.

Logo,

$$\pi((\alpha_0 - \sum_{i>0} \alpha_i) + \sum_{i>0} t_i \alpha_i) = 0, \text{ donde}$$

$$\pi(\alpha_0 - \sum_{i>0} \alpha_i) = -\sum_{i>0} \pi(t_i)\pi(\alpha_i) = -\sum_{i>0} \bar{t}_i \pi(\alpha_i)$$

Mas, como $\alpha_0 - \sum_{i>0} \alpha_i \in \mathbb{Z}A$, temos que $\mathrm{supp}(\pi(\alpha_0 - \sum_{i>0} \alpha_i)) \subset A/B$,

e $\operatorname{supp}\left(\sum_{i>0} \bar{t}_i \pi(\alpha_i)\right) \subset \dot{\bigcup}_{i>0} \bar{t}_i\, A/B$. Como T é transversal, segue que $\operatorname{supp}\left(\sum_{i>0} \bar{t}_i \pi(\alpha_i)\right) \cap \operatorname{supp}\left(\pi\left(\alpha_0 - \sum_{i>0} \alpha_i\right)\right) = \emptyset$, donde

$$\pi\left(\alpha_0 - \sum_{i>0} \alpha_i\right) = 0 = \sum_{i>0} \bar{t}_i \pi(\alpha_i).$$

Logo $\alpha_0 - \sum_{i>0} \alpha_i \in I(A) \cap \mathbb{Z}G\, I(B) \subset \mathbb{Z}A\, I(B)$, e, como $\{\bar{t}_i \mid i>0\}$ é livre sobre $\mathbb{Z}\, A/B$, $\pi(\alpha_i)=0$ se $i>0$. Logo, $\alpha_i \in I(A) \cap \mathbb{Z}G\, I(B) \subset \mathbb{Z}A\, I(B)$ e, como $\alpha_0 - \sum_{i>0} \alpha_i \in \mathbb{Z}A\, I(B)$, segue que $\alpha_0 \in \mathbb{Z}A\, I(B)$. Logo, $\alpha_0 \in I(A)^2 \cap \mathbb{Z}A\, I(B) = I(A)\, I(B)$ por i), donde

$$\alpha = \alpha_0 + \sum_{i>0} (t_i - 1)\alpha_i \quad \text{com } \alpha_0 \in I(A)\, I(B) \text{ e } \alpha_i \in \mathbb{Z}A\, I(B) \text{ se } i>0.$$

Logo,

$$I(G)\, I(A) \cap \mathbb{Z}G\, I(B) \subset I(A)\, I(B) + \sum_{i>0} (t_i - 1)\, \mathbb{Z}A\, I(B),$$

provando (iii).

<u>Lema 3.11</u> - Sejam H e K subgrupos normais de G, com $H \cap K = 1$. Então

$$\mathbb{Z}G\, I(H) \cap \mathbb{Z}G\, I(K) = \mathbb{Z}G\, I(H)\, I(K).$$

<u>Demonstração</u> - Seja $\{x_1 = 1, x_2, \ldots, x_n\}$ uma transversal de $HK = H \times K$ em G. Tomemos $\alpha \in \mathbb{Z}G\, I(H) \cap \mathbb{Z}G\, I(K)$. Podemos escrever

$$\alpha=\sum_i \sum_{h\in H} x_i h\ \beta_{ih}, \text{ com } \beta_{ih}\in I(K).$$

Pondo $h=(h-1)+1$, obtemos que

$$\alpha=\sum_i \sum_{h\in H} x_i(h-1)\beta_{ih} + \sum_i \sum_{h\in H} x_i\ \beta_{ih},$$

donde, como $x_i(h-1)\beta_{ih} \in \mathbb{Z}G\, I(H)\ I(K)$, para todo $i$, $h$, vem que

$$\alpha\equiv\sum_i \sum_{h\in H} x_i\ \beta_{ih} (\text{mod } \mathbb{Z}G\, I(H)\ I(K)).$$

Mas, como $\alpha\in \mathbb{Z}G\, I(H)$ e $\mathbb{Z}G\, I(H)\ I(K)\subset\mathbb{Z}G\, I(H)$, temos que

$$\sum_i \sum_{h\in H} x_i\ \beta_{ih} \in \mathbb{Z}G\, I(H),$$

isto é:

$$\sum_i x_i\Big(\sum_{h\in H} \beta_{ih}\Big)\in \mathbb{Z}G\, I(H).$$

Como $\{x_0,x_1,\ldots,x_n\}$ é transversal, segue que $\sum_{h\in H} \beta_{ih} \in \mathbb{Z}G\, I(H)$, $i=0,1,\ldots,n$. Mas, como $\beta_{ih}\in I(K)$, vem que

$$\sum_{h\in H} \beta_{ih} \in \mathbb{Z}G\, I(H)\cap I(K)=\{0\} \text{porque } H\cap K=1.$$

Logo, $\sum_{h\in H} \beta_{ih}=0$, $i=0,1,\ldots,n$, donde

$$\sum_i \sum_{h\in H} x_i\beta_{ih}=0$$

Logo

$$\alpha \equiv 0 \pmod{\mathbb{Z}G\, I(H)\ I(K)}, \text{ isto é,}$$

$$\alpha \in \mathbb{Z}G\, I(H)\ I(K).$$

Assim, $\mathbb{Z}G\, I(H) \cap \mathbb{Z}G\, I(K) \subset \mathbb{Z}G\, I(H)\ I(K)$. Como a inclusão recíproca é evidente, isto prova o Lema.

Finalmente, damos um Lema que calcula o anulador à esquerda (e à direita) do ideal $RG\, I(H)$. Para tanto, serão necessárias algumas definições.

<u>Definição</u> - Seja A um anel e $J \subset A$ um subconjunto qualquer. Definimos o anulador à direita de J por

$$r(J) = \{ a \in A \mid Ja = \{0\} \}.$$

Analogamente, definimos o anulador à esquerda $\ell(J)$.

<u>Definição</u> - Seja G um grupo e R um anel comutativo 1. Dado H um subgrupo finito de G, definimos o elemento $\hat{H} \in RG$ por

$$\hat{H} = \sum_{h \in H} h.$$

<u>Lema 3.12</u> - Sejam R um anel comutativo com 1 e G um grupo finito. Para todo subgrupo H de G, temos:

i) $\ell(I(H))=RG\ \hat{H}$

$r(I(H))=\hat{H}\ RG$

ii) $\ell(\hat{H})=RG\ I(H)$

$r(\hat{H})=I(H)\ RG$

Demonstração - Veja-se [Passman, 1977, Lemma 3.1.2].

# II. ISOMORFISMOS DE ANÉIS DE GRUPO DE GRUPOS METABELIANOS FINITOS

Neste segundo capítulo, apresentaremos alguns resultados recentes que dão uma solução parcial do problema do isomorfismo para anéis de grupo de grupos metabelianos finitos. O primeiro parágrafo define o problema do isomorfismo e apresenta um panorama histórico restrito. O segundo parágrafo apresenta um exemplo surpreendente, devido a E.C.Dade, enquanto que os dois parágrafos finais apresentam um resultado recente nesta área, devido a G. Karpilovsky, que dá uma solução parcial do problema do isomorfismo no caso em questão.

## § 1. O PROBLEMA DO ISOMORFISMO

É bastante natural perguntar sob que condições o anel de grupo RG, de um grupo arbitrário, G, sobre um anel comutativo com 1, R, determina G. Esta pergunta é conhecida como "problema do isomorfismo", que pode ser enunciado da seguinte forma:

Problema 1.1 - Para que classes de anéis R e de grupos G é verdade que

se $RG \cong RH$, então $G \cong H$?

Duas observações devem ser feitas quanto a este enunciado. Em primeiro lugar, quando se escreve $RG \cong RH$, R é suposto conhecido, de modo que se supõe que RG e RH são isomorfos como álgebras sobre R. Em segundo lugar, vale observar que, como vimos, pode-se sempre supor que o isomorfismo $\psi: RG \to RH$ é normalizado. Neste caso, $G \cong \psi(G)$ e $\psi(G)$ é uma base grupal normalizada de RH. Logo, o problema do isomorfismo pode também ser enunciado da forma seguinte:

Problema 1.2 - Para que classes de anéis R e de grupos G é verdade que, se H é uma base grupal normalizada de RG, então $G \cong H$?

A história do Problema do Isomorfismo já é bastante antiga; ele parece ter sido formulado pela primeira vez por R.M.Thrall, em 1947, sob a seguinte forma: "Dados um grupo G e um corpo K, determinar todos os grupos H tais que $KG \cong KH$." De fato, o primeiro resultado de interesse foi obtido quando R é um corpo: em 1950, Perlis e Walker provaram que se G é abeliano finito e $R=Q$, então, se $RG \cong RH$, tem-se $G \cong H$.

Desde o princípio, havia indicações de que não

se obteriam resultados melhores sobre corpos, exceto no caso em que $R=GF(p)$ e $G$ é um p-grupo. Em 1955, S.D.Berman mostrou que se $G$ e $H$ são os dois grupos não-abelianos não-isomorfos de ordem $p^3$, então $QG \cong QH$. O mais surpreendente dos resultados já obtidos neste sentido é o exemplo, descoberto por E.C.Dade, de dois grupos $G$ e $H$ metabelianos finitos cujos anéis de grupo $RG$ e $RH$ são isomorfos para uma classe muito ampla de anéis $R$, que inclui, em particular, todos os corpos. Este exemplo é apresentado na próxima seção.

Os resultados mais interessantes parece, então, que devem surgir para outras classes de anéis. Em particular, o resultado importantíssimo de G. Higman e S.D. Berman sobre as unidades centrais de ordem finita de um anel de grupo sobre $\mathbb{Z}$ mostrou que:

<u>Teorema 1.3</u> - Se $G$ é um grupo abeliano finito, e $\mathbb{Z}G \cong \mathbb{Z}H$, então $G \cong H$.

Como já vimos, este resultado foi generalizado por Saksonov para um domínio de integridade $R$ de característica zero em que nenhum divisor primo racional de $|G|$ é inversível (veja-se o Corolário I.2.8). Em 1968, A. Whitcomb, em sua tese de doutoramento, mostrou que:

<u>Teorema 1.4</u> - Se $G$ é um grupo metabeliano finito, e

$\mathbb{Z}G \cong \mathbb{Z}H$, então $G \cong H$.

Este resultado, que se apóia na correspondência entre subgrupos normais que será exposta no parágrafo 3, adiante, foi posteriormente tornado mais preciso por Obayashi, usando métodos de cohomologia de grupos. No parágrafo 4, apresentamos uma generalização do resultado de Obayashi para uma classe mais ampla de anéis, devida a G. Karpilovsky.

Deve-se observar que a hipótese de que G e H têm anéis de grupo isomorfos sobre $\mathbb{Z}$ é bastante forte. De fato, temos:

<u>Proposição 1.5</u> - Seja G um grupo finito. Se $\mathbb{Z}G \cong \mathbb{Z}H$, então

(i) G e H têm a mesma tábua de caracteres;

(ii) $RG \cong RH$ para todo anel comutativo com 1.

<u>Demonstração</u> -

(i) Veja-se [Isaacs, 1976, Corollary 3.20].

(ii) Seja R um anel comutativo com 1. Distinguimos dois casos:

i) <u>Char R=0</u> : Neste caso, $\mathbb{Z} \subset R$, e temos:

$$RG \cong R \otimes_{\mathbb{Z}} \mathbb{Z}G \cong R \otimes_{\mathbb{Z}} \cong RH.$$

ii) <u>Char R=m</u> : Neste caso, observamos que

$$\frac{\mathbb{Z}}{m\mathbb{Z}} G \cong \frac{\mathbb{Z}G}{m\mathbb{Z}G} \cong \frac{\mathbb{Z}H}{m\mathbb{Z}H} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} H;$$

como char R=m, temos que $\mathbb{Z}/m\mathbb{Z} \subset R$, e uma repetição do argumento de (i) dá

$$RG \cong RH.$$

Os Teoremas 1.3 e 1.4 e a proposição 1.5 nos levam imediatamente à conjectura de que $\mathbb{Z}G$ determina G, para todo grupo finito G. Muito pouco progresso tem sido feito nesta direção; entretanto, é possível que o estudo da estrutura do grupo das unidades de $\mathbb{Z}G$ leve a bons resultados. Este estudo é retomado em profundidade a partir do capítulo III.

## § 2. O EXEMPLO DE E.C.DADE

Este parágrafo é dedicado à apresentação de dois grupos metabelianos finitos não-isomorfos cujos anéis de grupo, sobre uma grande classe de anéis, são isomorfos. Os enunciados apresentados são um pouco mais fortes que os dados por [Passman, 1977, Theorem 14.2.2], e remontam ao artigo original ([Dade, 1971]). Começa - mos por vários Lemas úteis, a maioria dos quais serão citados sem demonstração.

Lema 2.1 - Seja G=A.B o produto semi-direto de A por B, e seja $\delta$ um automorfismo de A que comuta com a ação de B em A. Então $\delta$ pode ser estendido a um automorfismo de G, definindo-se $\delta(ab)=\delta(a).b$, para todo $a \in A$, $b \in B$.

Demonstração - Veja-se [Passman, 1977, Lemma 14.2.1].

Lema 2.2 - Seja G um grupo e R um anel comutativo com 1. Dado $\lambda \in Hom(G,U(R))$, onde U(R) indica o grupo das unidades de R, definimos $\lambda^{\#}: RG \to RG$ por

$$\lambda^{\#}(\sum_{g\in G} \alpha(g)g) = \sum_{g\in G} \alpha(g)\lambda(g)g.$$

Então $\lambda^{\#}$ é um automorfismo de RG e a aplicação $\# : Hom(G,U(R)) \to Aut\ (RG)$ é um homomorfismo.

Demonstração - [Passman, 1977, Lemma 4.3.4].

Lema 2.3 - Seja H um subgrupo normal de um grupo finito G e seja R um anel comutativo com 1 em que $|H|$ é inversível. Seja e o idempotente central de RG dado por

$$e = \frac{1}{|H|}\hat{H} = \frac{1}{|H|}\sum_{h\in H} h.$$

Então $eRG \cong R\ G/H$.

Demonstração - O resultado segue imediatamente do Lema I.3.12.

Lema 2.4 - Seja R um anel com 1 e seja $1=e_1+\ldots+e_n$ uma decomposição de 1 em soma de idempotentes ortogonais. Seja G um subgrupo do grupo das unidades de R. Se G permuta o conjunto $\{e_1,\ldots,e_n\}$ transitivamente por conjugação, então $R \cong M_n(S)$, onde $S=e_1Re_1$.

Demonstração - Veja-se [Passman, 1977, Lemma 6.1.6].

Passamos agora à construção dos grupos $G_1$ e $G_2$ de E.C. Dade. Primeiramente, sejam p e q primos racionais diferentes, satisfazendo $q \equiv 1 \pmod{p^2}$; por exemplo, poderíamos tomar p=2, q=5. Note-se que q é necessariamente um primo ímpar. Sejam $Q_1$ e $Q_2$ os dois grupos não-abelianos de ordem $q^3$, isto é,

$$Q_1 = \langle x_1, y_1, z_1 \mid x_1^q = y_1^q = z_1^q = 1,\ [x_1, y_1] = z_1,\ [x_1, z] = [y_1, z_1] = 1 \rangle$$

e (I)

$$Q_2 = \langle x_2, y_2, z_2 \mid x_2^q = z_2^q = 1,\ y_2^q = z_2, [x_2, y_2] = z_2, [x_2, z_2] = [y_2, z_2] = 1 \rangle.$$

Sejam ainda $\langle u_1 \rangle$ um grupo cíclico de ordem $p^2$ e $\langle u_2 \rangle$ um grupo cíclico de ordem p.

Como $q \equiv 1 \pmod{p^2}$, $p \mid q-1$, e, como o grupo de unidades de $\mathbb{Z}/q^2\mathbb{Z}$ tem ordem $q(q-1)$, este grupo tem certamente um elemento de ordem p. Logo, existe $n \in \mathbb{N}$ tal que $n \not\equiv 1 \pmod{q^2}$ mas $n^p \equiv 1 \pmod{q^2}$, donde temos também que $n \not\equiv 1 \pmod{q}$.

Sendo i=1,2, j=1,2, definimos uma ação de $u_i$ em $Q_j$ por

$$x_j^{u_i} = x_j,\ y_j^{u_i} = y_j^n,\ z_j^{u_i} = z_j^n. \qquad \text{(II)}$$

Para verificar que (II) define um automorfismo de $Q_j$, basta notar que $\langle y_j, z_j \rangle$ é um subgrupo normal abeliano de $Q_j$, e que $Q_j = \langle y_j, z_j \rangle \langle x_j \rangle$, produto semi-direto, onde a ação de $x_j$ é dada por

$$x_j^{-1}\, y_j\, x_j = y_j^{-1}\, z_j^{-1}$$

Notando, então, que $g \to g^n$ define um automorfismo de $\langle y_j, z_j \rangle$, já que este grupo é abeliano e $q \nmid n$ (pois $n^p \equiv 1 \pmod{q^2}$), e que

$$x_j \, y_j^n \, x_j^{-1} = (x_j \, y_j \, x_j^{-1})^n,$$

segue, pelo Lema 2.1, que (II) define um automorfismo de $Q_j$. Como $n^p \equiv 1 \pmod{q^2}$, este automorfismo tem ordem p, e faz sentido definir o produto semi-direto $Q_j \langle u_i \rangle$.

Com isto, podemos definir os grupos de Dade, pondo

$$\begin{aligned} G_1 &= Q_1 \langle u_1 \rangle \times Q_2 \langle u_2 \rangle \\ G_2 &= Q_1 \langle u_2 \rangle \times Q_2 \langle u_1 \rangle \end{aligned} \qquad \text{(III)}$$

É imediato verificar que $|G_1| = |G_2| = p^3 q^6$ e que $G_1$ e $G_2$ são metabelianos, já que

$$G_1' = \langle y_1, z_1 \rangle \times \langle y_2, z_2 \rangle = G_2'$$

e os grupos $\langle y_j, z_j \rangle$ são abelianos.

<u>Proposição 2.5</u> - Os grupos $G_1$ e $G_2$ definidos em (III) não são isomorfos.

<u>Demonstração</u> - Como já vimos, temos que

$G_i' = \langle y_1, z_1 \rangle \times \langle y_2, z_2 \rangle$, que é abeliano. Por (I), é imediato que $\langle y_1, z_1 \rangle$ é q-abeliano elementar e que $\langle y_2, z_2 \rangle = \langle y_2 \rangle$ é cíclico de ordem $q^2$.

Consideremos a aplicação $\psi_q : G_i' \to G_i'$ dada por

$\psi_q(g)=g^q$. Como $G_i'$ é abeliano, $\psi_q$ é um homomorfismo, e temos que $\psi_q(G_i')=\langle y_2^q\rangle = \langle z_2\rangle$.

Suponhamos, então, que $G_1 \cong G_2$. Então teríamos que

$$C_{G_1}(z_2)=C_{G_1}(\psi_q(G_1'))\cong C_{G_2}(\psi_q(G_2'))=C_{G_2}(z_2).$$

Da definição de $G_1$ e $G_2$ é imediato que

$$C_{G_1}(z_2)=Q_1\langle u_1\rangle \times Q_2$$

$$C_{G_2}(z_2)=Q_1\langle u_2\rangle \times Q_2\langle u_1^p\rangle.$$

O p-subgrupo de Sylow de $Q_1\langle u_1\rangle \times Q_2$ é $\langle u_1\rangle$, que portanto é cíclico de ordem $p^2$; o p-subgrupo de Sylow de $Q_1\langle u_2\rangle\times Q_2\langle u_1^p\rangle$ é $\langle u_2\rangle\times\langle u_1^p\rangle$, que é p-abeliano elementar de ordem $p^2$. Logo

$$Q_1\langle u_1\rangle \times Q_2 \not\cong Q_1\langle u_2\rangle \times Q_2\langle u_1^p\rangle, \text{ donde}$$

$$C_{G_1}(z_2) \not\cong C_{G_2}(z_2), \text{ absurdo.}$$

Logo, $G_1 \not\cong G_2$.

Os resultados centrais desta seção, que dão o isomorfismo de $RG_1$ e $RG_2$ para certos anéis R, são os próximos dois teoremas.

<u>Teorema 2.6</u> - Seja R um anel comutativo com 1 no qual o primo q é inversível. Então

$$RG_1 \cong RG_2.$$

Demonstração.

Em primeiro lugar, observamos que, diante da Proposição I.1.5, é suficiente mostrar que

$$R\,Q_1 < u_i > \cong R\,Q_2 < u_i > \;,\; i=1,2,$$

pois então teremos

$$R\,G_1 = R(Q_1 < u_1 > \times Q_2 < u_2 >) \cong R\,Q_1 < u_1 > \otimes_R R\,Q_2 < u_2 > \cong$$
$$\cong R\,Q_1 < u_2 > \otimes_R R\,Q_2 < u_1 > \cong R(Q_1 < u_2 > \times Q_2 < u_1 >) = RG_2 .$$

Passamos agora à demonstração de que $R\,Q_1 < u_i > \cong R\,Q_2 < u_i >$. Como $z_j$ é central em $Q_j$ e $z_j^{u_i} = z_j^n \in < z_j >$, o subgrupo abeliano $< z_j >$ é normal em $Q_j < u_i >$. Logo, se pomos

$$e_j = \frac{1}{q} \widehat{< z_j >} = \frac{1}{q} \sum_{h=0}^{q-1} z_j^h \;,$$

$e_j$ é um idempotente central de $RQ_j < u_i >$, donde segue que

$$R\,Q_j < u_i > \cong e_j\,R\,Q_j < u_i > \oplus (1-e_j)R\,Q_j < u_i >,$$

uma soma direta de R-álgebras.

Pelo Lema 2.3, temos que

$$e_j\,R\,Q_j < u_i > \cong R\,\frac{Q_j < u_i >}{< z_j >} \;.$$

Agora, é claro que

$$\frac{Q_1 < u_i >}{< z_1 >} \cong \frac{Q_2 < u_i >}{< z_2 >},$$

donde segue imediatamente que

$$e_1 R\ Q_1 < u_i > \cong e_2 R\ Q_2 < u_i >.$$

Resta demonstrar que

$$(1-e_1)\ R\ Q_1 < u_i > \cong (1-e_2)\ R\ Q_2 < u_i > .$$

Para tanto, consideramos o subgrupo normal q-abeliano elementar de $Q_j < u_i >$ gerado por $x_j$ e $z_j$. Para cada $k=0,1,\ldots,q-1$, pomos

$$f_{jk} = \frac{1}{q} < \widehat{x_j z_j^k} > = \frac{1}{q} \sum_{h=0}^{q-1} (x_j z_j^k)^h.$$

Como $< x_j z_j^k >$ é um subgrupo, $f_{jk}$ é um idempotente de $R\ Q_j < u_i >$. Observamos, então, que:

i) $(1-e_j)\ f_{jk}\ (1-e_j)\ f_{jk} = (1-e_j)\ f_{jk}$.

De fato, como $e_j$ é central em $R\ Q_j < u_i >$, temos que $(1-e_j)\ f_{jk}\ (1-e_j)\ f_{jk} = (1-e_j)\ f_{jk}\ f_{jk} = (1-e_j)\ f_{jk}$, pois $f_{jk}$ é idempotente.

ii) Se $k \neq s$, $(1-e_j)\ f_{jk}\ (1-e_j)\ f_{js} = 0$.

De fato: $(1-e_j) f_{jk}\ (1-e_j)\ f_{js} = (1-e_j)\ f_{jk}\ f_{js} =$

$= f_{jk}\ f_{js} - e_j\ f_{jk}\ f_{js}$.

Vamos verificar que, quando $k \neq s$, $f_{jk}\ f_{js} = e_j\ f_{jk}\ f_{js}$, o que prova nossa asserção. Temos que

$$f_{jk}\ f_{js} = \frac{1}{q^2}\left(\sum_{\mu=0}^{q-1} (x_j z_j^k)^{\mu}\right).\left(\sum_{\sigma=0}^{q-1} (x_j z_j^s)^{\sigma}\right)$$

$$= \frac{1}{q^2} \sum_{\mu=0}^{q-1} \sum_{\sigma=0}^{q-1} x_j^{\mu+\sigma}\ z_j^{k\mu+s\sigma}\ .$$

Por outro lado,

$$e_j\ f_{jk}\ f_{js} = \frac{1}{q^3}\left(\sum_{\nu=0}^{q-1} z_j^{\nu}\right)\left(\sum_{\sigma=0}^{q-1} (x_j z_j^k)^{\sigma}\right)\left(\sum_{\mu=0}^{q-1} (x_j z_j^s)^{\mu}\right)$$

$$= \frac{1}{q^3} \sum_{\nu=0}^{q-1} \sum_{\mu=0}^{q-1} \sum_{\sigma=0}^{q-1} x_j^{\sigma+\mu}\ z_j^{k\sigma+s\mu+\nu}$$

Fixado $\nu$, consideramos o sistema de equações

$$\begin{cases} \sigma+\mu \equiv \sigma_1+\mu_1 & (\text{mod } q) \\ k\sigma+s\mu \equiv k\sigma_1+s\mu_1 - \nu & (\text{mod } q). \end{cases}$$

Sobre GF(q), a matriz deste sistema é $\begin{bmatrix} 1 & 1 \\ k & s \end{bmatrix}$, cujo determinante é $s-k$. Como $s \neq k$ e $0 \leq s \leq q-1$, $0 \leq k \leq q-1$, temos $s-k \not\equiv 0 \pmod q$, e o sistema tem soluções mod q. Como $0 \leq \sigma \leq q-1$ e $0 \leq \mu \leq q-1$, a solução é única em $\mathbb{Z}$. Logo, fixado $\nu$, para cada par $(\sigma_1, \mu_1)$ existe um único par $(\sigma, \mu)$ tal que

$$x_j^{\sigma_1+\mu_1}\ z_j^{k\sigma_1+s\mu_1} = x_j^{\sigma+\mu}\ z_j^{k\sigma+s\mu+\nu}.$$

Portanto,

$$e_j\ f_{jk}\ f_{js} = \frac{1}{q^3} \sum_{\sigma=0}^{q-1} \sum_{\mu=0}^{q-1} \left( \sum_{\nu=0}^{q-1} x_j^{\sigma+\mu}\ z_j^{k\sigma+s\mu+\nu} \right)$$

$$= \frac{1}{q^3} \sum_{\sigma_1=0}^{q-1} \sum_{\mu_1=0}^{q-1} q\ x_j^{\sigma_1+\mu_1}\ z_j^{k\sigma_1+s\mu_1} =$$

$$= \frac{1}{q^2} \sum_{\sigma_1=0}^{q-1} \sum_{\mu_1=0}^{q-1} x_j^{\sigma_1+\mu_1}\ z_j^{k\sigma_1+s\mu_1} = f_{jk}\ f_{js}.$$

iii) $1-e_j = \sum_{k=0}^{q-1} (1-e_j)\ f_{jk}$ .

De fato, observamos que $1-e_j = \frac{1}{q} \sum_{\sigma=0}^{q-1} (1-z_j^{\sigma})$.

Logo, temos que

$$\sum_{k=0}^{q-1} (1-e_j) f_{jk} = \frac{1}{q^2} \sum_{k=0}^{q-1} \sum_{\sigma=0}^{q-1} \sum_{\mu=0}^{q-1} (1-z_j^{\sigma})\ (x_j z_j^k)^{\mu} =$$

$$= \frac{1}{q^2} \sum_{k=0}^{q-1} \sum_{\sigma=0}^{q-1} \sum_{\mu=0}^{q-1} (x_j^{\mu} z_j^{k\mu} - x_j^{\mu} z_j^{k\mu+\sigma}) =$$

$$= \frac{1}{q^2} \sum_{k=0}^{q-1} \sum_{\sigma=0}^{q-1} (1-z_j^{\sigma}) + \frac{1}{q^2} \sum_{k=0}^{q-1} \sum_{\sigma=0}^{q-1} \sum_{\mu=1}^{q-1} (x_j^{\mu} z_j^{k\mu} - x_j^{\mu} z_j^{k\mu+\sigma})$$

$$= (1-e_j) + \frac{1}{q^2} \sum_{k=0}^{q-1} \sum_{\mu=1}^{q-1} q\ x_j^{\mu} z_j^{k\mu} - \frac{1}{q^2} \sum_{k=0}^{q-1} \sum_{\mu=1}^{q-1} \sum_{\sigma=0}^{q-1} x_j^{\mu} z_j^{k\mu+\sigma}$$

Observando, então, que fixados $k_1, \mu \neq 0$ e $\sigma$, existe um único $k$, $0 \leq k \leq q-1$, tal que $k_1\mu \equiv k\mu+\nu \pmod q$ (pois basta tomar $k \equiv (\frac{1}{\mu})_q (k_1\mu-\sigma) \pmod q$, onde $(\frac{1}{\mu})_q$ indica o inverso de

$\mu$ mod q), obtemos que

$$\sum_{k=0}^{q-1} \sum_{\mu=1}^{q-1} \sum_{\sigma=0}^{q-1} x_j^{\mu} z_j^{k\mu+\sigma} = \sum_{k_1=0}^{q-1} \sum_{\mu=0}^{q-1} q\, x_j^{\mu} z_j^{k_1\mu} ,$$

donde

$$\sum_{k=0}^{q-1} (1-e_j) f_{jk} = 1-e_j, \text{ como se afirmou.}$$

iv) $y_j^{-k} [ (1-e_j) f_{j_0} ] y_j^k = (1-e_j) f_{jk}$

De fato, observamos que, como $[x_j, y_j] = z_j$, temos $y_j^{-1} x_j y_j = x_j z_j$, donde, por indução, $y_j^{-k} x_j y_j^k = x_j z_j^k$ e $y_j^{-k} x_j^{\sigma} y_j^k = (x_j z_j^k)^{\sigma}$. Logo,

$$y_j^{-k} [ (1-e_j) f_{j_0} ] y_j^k = (1-e_j)\, y_j^{-k} f_{j_0} y_j^k =$$

$$= (1-e_j) \frac{1}{q} \sum_{\sigma=0}^{q-1} y_j^{-k} x_j^{\sigma} y_j^k = (1-e_j) \frac{1}{q} \sum_{\sigma=0}^{q-1} (x_j z_j^k)^{\sigma} =$$

$$= (1-e_j)\, f_{jk}.$$

Observando, agora, que $(1-e_j)$ é a identidade multiplicativa de $(1-e_j)\, R\, Q_j \langle u_i \rangle$, temos que $(1-e_j)\, f_{jk}$ é uma família de idempotentes (por (i)) ortogonais (por (ii)) cuja soma é $1-e_j$ (por (iii)). Além disso, (iv) mostra que estes idempotentes são permutados transitivamente pelo grupo cíclico de unidades $(1-e_j) \langle y_j \rangle$, e notemos que $y_j^q$ centraliza todos estes elementos. Logo, pelo Lema 2.4,

$$(1-e_j)\ R\ Q_j\ <u_i> \cong M_q\ (S_j),$$

onde $$S_j=(1-e_j)\ f_{j0}\ (1-e_j)\ R\ Q_j\ <u_i>\ (1-e_j)\ f_{j0} =$$

$$=(1-e_j)f_{j0}\ R\ Q_j\ <u_i>\ (1-e_j)\ f_{j0}$$

Resta, então, demonstrar que

$$S_1=(1-e_1)f_{10}\ R\ Q_1 < u_i>(1-e_1)f_{10} \cong (1-e_2)f_{20}\ R\ Q_2 < u_i>(1-e_2)f_{20} =S_2$$

Para tanto, observamos que $u_i$ normaliza o grupo q-abeliano elementar $< x_j,z_j>$ e que $H_j= < x_j,z_j,u_i>$ é um subgrupo de $Q_j < u_i>$, de índice q. De fato, os elementos $1,\ y_j,\ y_j^2,\ldots,y_j^{q-1}$ formam uma transversal de $H_j$ em $Q_j < u_i>$. Logo, pela Proposição I.1.1,

$$R\ Q_j\ <u_i> = \sum_{k=0}^{q-1} R\ H_j\ y_j^k\ .$$

Como $u_i$ e $z_j$ centralizam $x_j$, também centralizam $f_{j0}$, e temos

$$S_j=(1-e_j)f_{j0}\ R\ Q_j\ <u_i>\ (1-e_j)f_{j0}$$

$$=\sum_{k=0}^{q-1} R\ H_j(1-e_j)\ f_{j0}\,y_j^k\ (1-e_j)f_{j0}\ .$$

Mas $(1-e_j)f_{j0}\ y_j^k\ (1-e_j)\ f_{j0}= y^k y^{-k}(1-e_j)f_{j0}\,y^k(1-e_j)f_{j0}$

$$=y_j^k(1-e_j)\,f_{jk}(1-e_j)f_{j0} = \begin{cases} (1-e_j)f_{j0}\ , & \text{se } k=0 \\ 0\ , & \text{se } k\neq 0 \end{cases}$$

Logo,

$$S_j = R\ H_j(1-e_j)f_{j0} \subset R\ H_j.$$

Definimos, agora, $\psi: H_1 \to H_2$, pondo

$$\psi(x_1)=x_2,\quad \psi(z_1)=z_2,\quad \psi(u_i)=u_i.$$

É fácil ver que $\psi$ é um isomorfismo de grupos. Estendendo $\psi$ R-linearmente, obtemos um isomorfismo $\psi: RH_1 \to RH_2$, tal que

$$\psi(e_1)=e_2 \quad \text{e} \quad \psi(f_{10})=f_{20}$$

Logo, $\psi(S_1)=S_2$, donde $S_1 \cong S_2$.

Logo, $RQ_1 < u_i > \cong RQ_2 < u_i >$, $i=1,2$, provando o teorema.

<u>Corolário 2.7</u> - Seja K um corpo de característica diferente de q. Então $KG_1 \cong KG_2$.

<u>Demonstração</u> - Basta notar que, como K é corpo, se $q \neq 0$, então q é inversível em K.

O segundo teorema de Dade estende o resultado para outra classe de anéis, que inclui, em particular, os corpos de característica q.

<u>Teorema 2.8</u> - Seja R um domínio de integridade no qual o primo p é inversível. Se R contém uma raiz $p^2$-ésima primitiva da unidade, então $RG_1 \cong RG_2$.

Demonstração - Seja $\varepsilon \in R$ uma raiz $p^2$-ésima primitiva da unidade. Então $\varepsilon^p$ é uma raiz p-ésima da unidade, e temos

$$1 + \varepsilon^p + \varepsilon^{2p} + \ldots + \varepsilon^{(p-1)p} = 0. \qquad (I)$$

Para cada inteiro $k=0,\ldots,p-1$, definimos em $RG_i$ os elementos

$$f_{ik} = \frac{1}{p} \sum_{s=0}^{p-1} (\varepsilon^{pk} u_1^p)^s.$$

Como $(\varepsilon^{pk} u_1^p)^s f_{ik} = f_{ik}$, temos imediatamente que

$$(\varepsilon^{pr} u_1^p)^s f_{ik} = \varepsilon^{p(r-k)s} (\varepsilon^{pk} u_1^p)^s f_{ik} =$$
$$= \varepsilon^{p(r-k)s} f_{ik}.$$

Logo,

$$f_{ir} f_{ik} = \frac{1}{p} \sum_{s=0}^{p-1} (\varepsilon^{pr} u_1^p)^s f_{ik} =$$
$$= \frac{1}{p} \sum_{s=0}^{p-1} \varepsilon^{p(r-k)s} f_{ik},$$

donde segue que $f_{ik} f_{ik} = \frac{1}{p} \sum_{s=0}^{p-1} f_{ik} = \frac{1}{p} p f_{ik} = f_{ik}$ e

que, se $r \neq k$, $f_{ir} f_{ik} = \frac{1}{p} [\sum_{s=0}^{p-1} \varepsilon^{p(r-k)s}] f_{ik} = 0$ por (I).

Assim, $\{f_{ik} | 0 \leq k \leq p-1\}$ é uma família de idempotentes ortogonais. Além disso,

$$\sum_{k=0}^{p-1} f_{ik} = \sum_{k=0}^{p-1} \frac{1}{p} [\sum_{s=0}^{p-1} (\varepsilon^{pk})^s u_1^{ps}] =$$

$$= \frac{1}{p} \sum_{s=0}^{p-1} [\sum_{k=0}^{p-1} (\varepsilon^{pk})^s] \; u_1^{ps}.$$

Observando, agora, que, pondo s=0, temos

$$\sum_{k=0}^{p-1} (\varepsilon^{pk})^0 = p,$$

e que, se $s \neq 0$, então

$$\sum_{k=0}^{p-1} (\varepsilon^{pk})^s = \sum_{t=0}^{p-1} (\varepsilon^{ps})^k = 0, \text{ por (I)},$$

segue que

$$\sum_{k=0}^{p-1} f_{ik} = \frac{1}{p} \sum_{s=0}^{p-1} [\sum_{k=0}^{p-1} (\varepsilon^{pk})^s] u_1^{ps} = \frac{1}{p} \cdot p \; u_1^0 = 1.$$

Assim, os idempotentes $f_{i0}, f_{i1}, \ldots, f_{ip-1}$, dão uma decomposição ortogonal de 1. Além disso, como $n^p \equiv 1 \pmod{q^2}$, $u_1^p$ é central em $G_i$, donde segue que $f_{i0}, f_{i1}, \ldots, f_{ip-1}$ são idempotentes centrais de $RG_i$, $i=1,2$.

Logo, $RG_i$ se escreve como uma soma direta de subálgebras:

$$RG_i = RG_i \; f_{i0} \oplus RG_i \; f_{i1} \oplus \ldots \oplus RG_i \; f_{ip-1}.$$

Seja, agora $H_i \subset G_i$ o subgrupo gerado por $Q_1$, $Q_2$ e $u_2$. É imediato que $u_1$ normaliza $H_i$, donde segue que $H_i \triangleleft G_i$ e $G_i$ é um produto semi-direto $G_i = H_i < u_1 >$.

Consideramos as aplicações naturais

$$\pi_i : G_i \longrightarrow \frac{G_i}{H_i} \cong < u_1 >$$

e os homomorfismos de grupos

$$\begin{aligned} \tau_k : < u_1 > &\longrightarrow U(R) \\ u_1 &\longrightarrow \varepsilon^k, \ k=0,1,\ldots,p-1, \end{aligned}$$

que estão bem definidos porque $\varepsilon$ é, por hipótese, uma raiz $p^2$-ésima primitiva da unidade.

Definimos $\lambda_{ik} : G_i \longrightarrow U(R)$ por $\lambda_{ik} = \tau_k \circ \pi_i$. Como $\pi_i$ e $\tau_k$ são homomorfismos de grupos, temos que $\lambda_{ik} \in Hom(G_i, U(R))$, $i=1,2$, $k=0,1,\ldots,p-1$.

Pelo Lema 2.2, podemos definir os automorfismos $\lambda^{\#}_{ik} : RG_i \longrightarrow RG_i$, onde

$$\lambda^{\#}_{ik}\Big(\sum_{g \in G} \alpha(g) g\Big) = \sum_{g \in G} \alpha(g) \lambda_{ik}(g) g.$$

Então temos que

$$\begin{aligned} \lambda^{\#}_{ik}(f_{i0}) &= \lambda^{\#}_{ik}\Big[\frac{1}{p} \sum_{s=0}^{p-1} u_1^{ps}\Big] = \\ &= \frac{1}{p} \sum_{s=0}^{p-1} \lambda_{ik}(u_1^{ps})\, u_1^{ps} = \\ &= \frac{1}{p} \sum_{s=0}^{p-1} \varepsilon^{kps}\, u_1^{ps} = f_{ik} \end{aligned}$$

Logo,

$$\lambda^{\#}_{ik}(RG_i\ f_{i0}) = RG_i\ f_{ik},\ k=0,1,\ldots,p-1,$$

e, como $\lambda^{\#}_{ik}$ é automorfismo de $RG_i$, segue que

$$RG_i\ f_{ik} \cong RG_i\ f_{i0}\ ,\quad k=0,1,\ldots,p-1,$$

e os p somandos diretos de $RG_i$ são todos isomorfos, donde $RG_i$ é isomorfo a uma soma direta de p cópias de $RG_i\ f_{i0}$.

Entretanto, como $f_{i0} = \frac{1}{p} \widehat{< u_1^p >}$, obtemos pelo Lema 2.3, que

$$RG_i\ f_{i0} \cong R\ \frac{G_i}{< u_1^p >}\ .$$

Agora, é imediato que $< u_1^p > \cong < u_2 >$, donde

$$\frac{G_1}{< u_1^p >} \cong Q_1 < u_1^p > \times Q_2 < u_2 > \cong Q_1 < u_2 > \times Q_2 < u_1^p > \cong \frac{G_2}{< u_1^p >}$$

Logo

$$RG_1 f_{10} \cong R\ \frac{G_1}{<u_1^p>} \cong R\ \frac{G_2}{<u_1^p>} \cong RG_2 f_{20}\ ,$$

donde

$$RG_1 \cong \underbrace{RG_1 f_{10} \oplus \ldots\ldots \oplus RG_1 f_{10}}_{p \text{ vezes}} \cong$$

$$\cong \underbrace{RG_2 f_{20} \oplus \ldots\ldots \oplus RG_2 f_{20}}_{p \text{ vezes}} \cong RG_2 ,$$

e o teorema está demonstrado.

<u>Corolário 2.9</u> - Seja K um corpo de característica q. Então $KG_1 \cong KG_2$.

<u>Demonstração</u> - Como $\mathrm{char}K=q\neq p$, p é inversível em K; além disso, $GF(q)\subset K$.

O grupo multiplicativo $GF(q)^*$ é cíclico, de ordem q-1. Como $q\equiv 1 \pmod{p^2}$, temos que $p^2 \mid q-1$, donde, como $GF(q)^*$ é cíclico, existe um elemento $\varepsilon\in GF(q)^*$, de ordem $p^2$. Logo, K possui uma raiz primitiva $p^2$-ésima da unidade. Pelo Teorema 2.8, segue que $KG_1 \cong KG_2$.

O exemplo de Dade deixa claro que, para que RG determine G, devemos supor que nenhum divisor primo de $|G|$ seja inversível em R. Nos próximos dois parágrafos, procuraremos estudar o problema do isomorfismo sob a hipótese de que R é um domínio de integridade satisfazendo essa condição. Em particular, concluiremos que, para os grupos $G_1$ e $G_2$ de Dade, $\mathbb{Z}G_1$ e $\mathbb{Z}G_2$ não são isomorfos.

É interessante notar que os Teoremas 2.6 e 2.8 nos permitem concluir que, se $\mathbb{Z}_{(p)}$ indica o localizado de $\mathbb{Z}$ em p e $\mathbb{Z}_{\hat{p}}$ o anel de inteiros p-ádicos,

$\mathbb{Z}_{(p)}G_1 \cong \mathbb{Z}_{(p)}G_2$, $\mathbb{Z}_{\hat{q}}G_1 \cong \mathbb{Z}_{\hat{q}}G_2$ e $\mathbb{Z}_{\hat{p}}G_1 \cong \mathbb{Z}_{\hat{p}}G_2$. Por outro lado, como $\mathbb{Z}_{(q)}$ não contém raiz $p^2$-ésima da unidade, fica em aberto decidir se $\mathbb{Z}_{(q)}G_1 \cong \mathbb{Z}_{(q)}G_2$.

## § 3. A CORRESPONDÊNCIA ENTRE SUBGRUPOS NORMAIS

O instrumento básico para o estudo de isomorfismos de anéis de grupo sobre domínios de integridade é a chamada "correspondência entre subgrupos normais". Apresentamos, nesta seção, um resumo dos resultados básicos, cuja demonstração pode ser encontrada em [Sehgal, 1978] e [Karpilovsky, 1981]. No que segue, G e H denotam grupos finitos e R um domínio de integridade de característica zero em que nenhum divisor primo de $|G|$ é inversível.

Teorema 3.1 - Seja RG=RH. Dado $N \triangleleft G$, definimos $\phi N = H \cap (1+RG\ I(N))$. Então:

a) $\phi$ define uma correspondência bijetora entre os subgrupos normais de G e os subgrupos normais de H;

b) se $N_1 \triangleleft G$, $N_2 \triangleleft G$, $N_1 \subset N_2$, então $\phi N_1 \subset \phi N_2$;

c) $RG\ I(N) = RH\ I(\phi N)$;

d) $R\dfrac{G}{N} \cong R\dfrac{H}{\phi N}$;

e) se $I$ é um ideal de $RG$ e $N=G \cap (1+I)$, então $\phi N=H \cap (1+I)$;

f) se $N \triangleleft G$, $M \triangleleft G$, então $\phi [M,N]=[\phi M,\phi N]$;

g) se $N \triangleleft G$, $M \triangleleft G$, então $\phi ((M \cap N)')$ = $= (\phi M \cap \phi N)'$;

h) se $N \triangleleft G$, $M \triangleleft G$ e $N \subset M$, então $M/N$ é abeliano se e somente se $\phi M/\phi N$ é abeliano;

i) dado $N \triangleleft G$, seja $C^n(N)= \langle g^n \mid g \in N \rangle$; então $\phi C^n(N)=C^n(\phi N)$;

j) dado $N \triangleleft G$, seja $C_n(N)= \langle g \mid g \in N \text{ e } g^n=1 \rangle$; então $\phi C_n(N)=C_n(\phi N)$.

Observamos, em particular, que o item (i) deste teorema implica em que os subgrupos $N$ e $\phi N$ têm o mesmo expoente.

## § 4. UM RESULTADO PARCIAL

Demonstraremos, neste parágrafo, um resultado parcial sobre o problema do isomorfismo para anéis de grupo de grupos metabelianos, devido a G. Karpilovsky, que diz que $RG$ determina $G$ para uma certa classe de domínios de integridade $R$. Este resultado generaliza um resultado de Obayashi, obtido em 1970 usando métodos de cohomologia de grupos.

Teorema 4.1 - [Obayashi,1970]. Sejam G um grupo finito e A um subgrupo normal de G. Seja $\mathbb{Z}G=\mathbb{Z}H$ e consideremos $A^*=\phi A=$ $=H\cap(1+\mathbb{Z}G\,I(A))$. Se K/A e L/B são os centros de G/A e H/B, respectivamente, então existe um isomorfismo de K sobre L levando A sobre $A^*$.

Este teorema tem como corolário o Teorema 1.4 (de Whitcomb), que diz que um grupo metabeliano finito é determinado pelo seu anel de grupo sobre $\mathbb{Z}$. No que segue, demonstraremos uma generalização do Teorema 4.1 para uma classe mais ampla de domínios de integridade. Para tanto, serão necessários vários lemas.

Lema 4.2 - Sejam G um grupo finito, A um subgrupo de G e $K=\mathbb{Z}/m\mathbb{Z}$, onde $m\equiv 0 \pmod{n}$ e n é o expoente de A/A'. Então valem:

a) $$\frac{KG\ I(A)}{I(G)\ I(A)} \cong \frac{A}{A'}$$

b) Se A é abeliano e x é um elemento de KG tal que $x\equiv g \pmod{KG\ I(A)}$ para algum $g\in G$, então existe um único $g_x=ga$, com $a\in A$, tal que $x\equiv g_x \pmod{I(G)\ I(A)}$.

Demonstração - a) Como $KG\ I(A)=I(A)+I(G)\ I(A)$, temos que

$$\frac{KG\ I(A)}{I(G)\ I(A)} = \frac{I(A)+I(G)\ I(A)}{I(G)\ I(A)} \cong \frac{I(A)}{I(A)\cap I(G)I(A)},$$

Pelo Lema I.3.3, $I(G)\ I(A) \cap I(A) = I(A)^2$, e pelo Corolário I.3.6(b), sabemos que $\frac{I(A)}{I(A)^2} \cong \frac{A}{A'}$, donde obtemos que

$$\frac{KG\ I(A)}{I(G)\ I(A)} \cong \frac{I(A)}{I(A)^2} \cong \frac{A}{A'}.$$

b) Seja $x \equiv g \pmod{KG\ I(A)}$. Então temos que

$$x - g \in KG\ I(A) = I(A) + I(G)\ I(A).$$

Logo, existe $t \in I(A)$ tal que

$$x - g - t \in I(G)\ I(A), \text{ isto é,}$$

$$x \equiv g + t \pmod{I(G)\ I(A)}.$$

Pelo corolário I.3.8, como $t \in I(A)$, existe $a \in A$ tal que $t \equiv a - 1 \pmod{I(A)^2}$. Como $I(A)^2 \subset I(G)\ I(A)$, segue que

$$x \equiv g + a - 1 = ga - (g-1)(a-1) \equiv ga \pmod{I(G)\,I(A)}.$$

Logo, tomando $g_x = ga$, com $a \in A$, temos que

$$x \equiv g_x \pmod{I(G)\ I(A)}.$$

Finalmente, se $x \equiv g_x \pmod{I(G)\ I(A)}$ e também $x \equiv g'_x \pmod{I(G)\ I(A)}$, segue que

$$g_x \equiv g'_x \pmod{I(G)\ I(A)},$$

donde $g_x - g'_x \in I(G)\ I(A)$. Como $I(G)\ I(A)$ é ideal à esquerda de KG, vem que

$$1-g_x^{-1}\, g'_x \in I(G)\, I(A), \text{ donde}$$

$$g_x^{-1}\, g'_x \in 1+I(G)\, I(A).$$

Logo,

$$g_x^{-1}\, g'_x \in G \cap (1+I(G)I(A))=A \cap (1+I(A)^2)=A',$$

pelo Lema I.3.3 e pelo Corolário I.3.6. Como A é abeliano, temos que $A' = \{1\}$, donde $g_x^{-1}\, g'_x = 1$, isto é, $g_x = g'_x$. Logo, $g_x$ é único, provando (b).

Vale observar que o item (b) deste teorema seria igualmente válido, <u>exceto pela unicidade de</u> $g_x$, se A não fosse abeliano.

Para os próximos resultados ser-nos-á necessário introduzir alguns conceitos.

Seja A um subgrupo de um grupo finito G. Se A é normal em G, já definimos uma aplicação $\pi_A : RG \to R\, G/A$, onde G/A é o subgrupo quociente de G por A. Se A não é normal em G, denotaremos por G/A o conjunto $\{gA \mid g \in G\}$ das classes laterais à esquerda de A (que não é um grupo). Denotando por $R\langle G/A\rangle$ o R-módulo livre de base G/A, podemos definir um homomorfismo de R-módulos $\pi_A : RG \to R\langle G/A\rangle$ por

$$\pi_A\Big(\sum_{g \in G} \alpha(g)\, g\Big) = \sum_{g \in G} \alpha(g)\, gA.$$

É imediato que, para $A \triangleleft G$, esta definição coincide com a anterior. Vale observar, ainda, que é possível dar a $R<G/A>$ uma estrutura de RG-módulo à esquerda, definindo, para $g_1 \in G$ e $g_2A \in G/A$, $g_1.g_2A=(g_1g_2)A$. Com estas definições, $\pi_A : RG \to R<G/A>$ é um epimorfismo de RG-módulos à esquerda, e seu núcleo é o ideal $RG\, I(A)$.

Seja, agora, $\psi : R \to \bar{R}$ um epimorfismo de anéis de núcleo $\Lambda \subset R$. Dado $a \in R$, escreveremos $\bar{a}=\psi(a)$. Seja G um grupo arbitrário. Então, podemos definir um homomorfismo de anéis

$$\Phi : RG \to \bar{R}G$$

$$\sum_{g \in G} \alpha(g)g \longrightarrow \sum_{g \in G} \overline{\alpha(g)}g.$$

É imediato verificar que $\Phi$ é um epimorfismo de anéis de núcleo $\Lambda G$, que $\Phi|_G$=identidade e que $\Phi|_R=\psi$.

Com estas notações, temos o seguinte resultado:

<u>Lema 4.3</u> - Sejam G e H grupos finitos, R e $\bar{R}$ anéis comutativos com 1 e $\psi : R \to \bar{R}$ um epimorfismo de anéis. Definimos um epimorfismo $\Phi : RG \to \bar{R}G$, como acima.

Então temos

(i) Se $RG=RH$, então $\bar{R}G=\bar{R}\ \Phi(H)$,

e, portanto, que, dados subgrupos A e N de G e subgrupos B e T de H, temos:

(ii) Se $RG\ I(A)=RG\ I(B)$ e $\pi_A(N)=\pi_A(T)$, então $\bar{R}G\ I_{\bar{R}}(A) = \bar{R}G\ I_{\bar{R}}(\Phi(B))$ e $\bar{\pi}_A(N)=\bar{\pi}_A(\Phi(T))$, onde $\bar{\pi}_A$ denota a aplicação $\bar{\pi}_A:\bar{R}G \longrightarrow \bar{R}\langle G/A\rangle$, definida acima.

Demonstração.

(i) Suponhamos que $RG=RH$. Para provar que $\bar{R}G=\bar{R}\ \Phi(H)$, basta provar que existe um isomorfismo de $\bar{R}$-álgebras $\lambda:\bar{R}H\to\bar{R}G$, tal que $\lambda(H)=\Phi(H)$.

Como $RG=RH$, é claro que $\Lambda G=\Lambda H$. Usando o epimorfismo $\psi:R \to \bar{R}$, podemos, como acima, construir um epimorfismo de anéis

$$\Phi_1:RH \longrightarrow \bar{R}H, \text{ com núcleo } \Lambda H.$$

Pelo Teorema do homomorfismo, podemos passar esta aplicação ao quociente, obtendo um isomorfismo de anéis

$$\lambda_1 : \frac{RH}{\Lambda H} \to \bar{R}H .$$

Como $\lambda_1$ é isomorfismo, podemos tomar seu inverso, $\lambda_1^{-1}:\bar{R}H \to RH/\Lambda H$, e observamos que

$$\lambda_1^{-1}\Big(\sum_{h\in H} \overline{\alpha(h)}h\Big)= \sum_{h\in H} \alpha(h)h + \Lambda H.$$

Analogamente, temos o epimorfismo $\phi:RG \to \bar{R}G$, e, passando ao quociente, obtemos o isomorfismo de anéis

$$\lambda_2 : \frac{RG}{\Lambda G} \to \bar{R}G,$$

e observamos que $\lambda_2(\sum_{g\in G} \alpha(g)g + \Lambda G) = \sum_{g\in G} \overline{\alpha(g)}\, g$, isto é, $\lambda_2(\alpha+\Lambda G) = \Phi(\alpha)$.

Como $RG=RH$ e $\Lambda G=\Lambda H$, obtemos

$$\bar{R}H \xrightarrow{\lambda_1^{-1}} \frac{RH}{\Lambda H} = \frac{RG}{\Lambda G} \xrightarrow{\lambda_2} \bar{R}G.$$

Logo, $\lambda_2 \circ \lambda_1^{-1} : \bar{R}H \longrightarrow \bar{R}G$ é um isomorfismo de anéis. Além disso,

$$\lambda_2 \circ \lambda_1^{-1} (\bar{\alpha}\, h) = \lambda_2(\alpha h+\Lambda G) = \Phi(\alpha h) = \bar{\alpha}\, \Phi(h)$$

e

$$\lambda_2 \circ \lambda_1^{-1} (h) = \lambda_2(h+\Lambda G) = \Phi(h).$$

Logo $\lambda_2 \circ \lambda_1^{-1} (\bar{\alpha} h) = \bar{\alpha}\, \lambda_2 \circ \lambda_1^{-1}(h)$ e também $\lambda_2 \circ \lambda_1^{-1} (H) = \Phi(H)$. Logo, pondo $\lambda=\lambda_2 \circ \lambda_1^{-1}$, $\lambda$ é um isomorfismo de $\bar{R}$-álgebras tal que $\lambda(H)=\Phi(H)$. Assim, $\bar{R}G=\bar{R}\Phi(H)$, provando (i).

A demonstração de (ii) é agora trivial. Basta notar que $\Phi(a-1)=a-\bar{1}$, para todo $a\in A$, donde $I_{\bar{R}}(A)=\Phi(I(A))$, e que, para $b\in B$, $\Phi(b-1)=\Phi(b)-\bar{1}$, donde $I_{\bar{R}}(\Phi(B))=\Phi(I(B))$. Logo, $RG\ I(A)=RG\ I(B) \Rightarrow \Phi(RG\ I(A))=\Phi(RG\ I(B)) \Rightarrow$
$\Rightarrow \bar{R}G\ \Phi(I(A))=\bar{R}G\ \Phi(I(B)) \Rightarrow \bar{R}G\ I_{\bar{R}}(A)=\bar{R}G\ I_{\bar{R}}(\Phi(B))$.

Analogamente, se $\pi_A(N)=\pi_A(T)$, então, dado $n\in N$,

existe $t \in T$ tal que $n-t \in RG\, I(A)$, donde $n-\Phi(t) \in \bar{R}G\, I_{\bar{R}}(A)$, e portanto $\bar{\pi}_A(N)=\bar{\pi}_A(\Phi(T))$, provando (ii).

<u>Lema 4.4</u> - Sejam G um grupo finito e R um domínio de integridade de característica zero em que nenhum divisor primo de $|G|$ é inversível.

Dado $N \triangleleft G$, considero $\pi_N : RG \longrightarrow R\,G/N$.

Se $RG=RH$, então $R\,G/N = R\,\pi_N(H)$.

<u>Demonstração</u>.

Como H gera RG sobre R, e $\pi_N : RG \longrightarrow R\,G/N$ é um epimorfismo de R-álgebras, temos que $\pi_N(H)$ gera $R\,G/N$ sobre R.

Logo, resta provar que $\pi_N(H)$ é livre sobre R. Entretanto, como H é um grupo finito de unidades normalizadas, e como $\varepsilon(\pi_N(\alpha))=\varepsilon(\alpha)$, $\forall \alpha \in RG$, segue que $\pi_N(H)$ é um grupo finito de unidades normalizadas. Logo, pelo Corolário I.2.9, $\pi_N(H)$ é livre sobre R, donde $RG=R\,\pi_N(H)$.

Nosso primeiro resultado importante é:

<u>Proposição 4.5</u> - Sejam G um grupo finito, A um subgrupo normal abeliano de G e $K=\mathbb{Z}/m\mathbb{Z}$ e $m \equiv 0 \pmod{n}$, onde n é o expoente de A.

Suponhamos que $KG=KH$, e sejam $A^*=H\cap(1+KG\ I(A))$, $N$ um subgrupo de $G$ e $M$ um subgrupo de $H$ tais que $A\subset N$ e $A^*\subset M$.

Se $A^*$ é abeliano, $\exp(A^*)\,|\,n$, $KG\ I(A)=KG\ I(A^*)$ e $\pi_A(N)=\pi_A(M)$, então existe um isomorfismo de $M$ sobre $N$ levando $A^*$ sobre $A$.

Demonstração.

i) O conjunto $\{t(a-1)\,|\,a\in A,\ a\neq 1,\ t\in T\}$, onde $T$ é uma transversal para $A$ em $G$, é uma base $KG\ I(A)$ sobre $K$. Logo

$$\dim_K(KG\ I(A)) = \frac{|G|}{|A|}(|A|-1) = |G| - \frac{|G|}{|A|}.$$

Analogamente, $\dim_K(KG\ I(A^*))=|H|-\dfrac{|H|}{|A^*|}$.

Como $|G|=|H|$ e $KG\ I(A)=KG\ I(A^*)$, segue que $|A|=|A^*|$.

ii) Observamos que, como $A^*$ é abeliano, $m\equiv 0 \pmod n$ e $\exp(A^*)\,|\,n$, temos, pelo Lema I.3.3 e pelo Corolário I.3.6, que

$$H\cap(1+I(H)\ I(A^*)) = A^*\cap(1+I(A^*)^2)=1.$$

iii) Observamos, agora, que $\pi_A(N)=\pi_A(M)$. Ora, $\pi_A|_G$ é o epimorfismo canônico $G\to G/A$; logo, como $A\subset N$, temos que $\pi_A(N)=N/A$.

Consideramos agora $\pi_A|_H$. É claro que

$$\ker \pi_{A|_H} = H \cap (1+KG\ I(A)) = A^*.$$

Portanto, segue do Teorema do Homomorfismo que $\pi_A(M) \cong$ $\cong M/A^*$.

Logo, como $\pi_A(N) = \pi_A(M)$, temos $\frac{N}{A} \cong \frac{M}{A^*}$, e como, por (i), $|A| = |A^*|$, segue que $|N| = |M|$.

iv) Observamos, ainda, que de $\pi_A(N) = \pi_A(M)$ segue que, dado $h \in M$, existe $g \in N$ tal que

$$g + KG\ I(A) = h + KG\ I(A),$$

isto é, tal que

$$h \equiv g \pmod{KG\ I(A)}.$$

Pelo Lema 4.2 (b), existe um único $g_h = ga$, com $a \in A \subset N$, tal que $h \equiv g_h \pmod{I(G)\ I(A)}$; como $g \in N$ e $a \in A \subset N$, temos que $g_h = ga \in N$.

Logo, para todo $h \in M$, existe um único $g_h \in N$ tal que $h \equiv g_h \pmod{I(G)\ I(A)}$.

Definimos, então, uma aplicação $f: M \to N$ por $f(h) = g_h$, $\forall h \in M$. É claro que $f$ está bem definida, já que $g_h$ é único.

v) Afirmamos que $f$ é um homomorfismo de grupos. De fato, se $f(h_1) = g_1$, $f(h_2) = g_2$, temos

$$h_1 \equiv g_1 \pmod{I(G)\ I(A)} \text{ e } h_2 \equiv g_2 \pmod{I(G)\ I(A)},$$

isto é, $h_1-g_1 \in I(G)I(A)$

$h_2-g_2 \in I(G)I(A)$.

Então

$$h_1h_2-g_1g_2=h_1(h_2-g_2)+(h_1-g_1)g_2 \in I(G)I(A),$$

pois $I(G)\ I(A)$ é um ideal bilateral de KG, já que $A \triangleleft G$.

Logo, $h_1h_2 \equiv g_1g_2 \pmod{I(G)\ I(A)}$, donde segue que

$$f(h_1h_2)=g_1g_2=f(h_1)f(h_2).$$

Assim, f é homomorfismo.

vi) Se $h \in \ker f$, temos que $h-1 \in I(G)\ I(A)$. Como $KG\ I(A)=KG\ I(A^*)$, $I(G)\ I(A)=I(H)\ I(A^*)$. Logo,

$\ker f \subset H \cap (1+I(H)\ I(A^*))=\{1\}$, pelo item (ii). Assim, f é injetora. Como ainda temos que $|M|=|N|$, segue que f é um isomorfismo de M sobre N.

vii) Resta provar que $f(A^*)=A$. Seja, então, $b \in A^*$. Como $A^*=H \cap (1+KG\ I(A))$, temos que

$$b-1 \in KG\ I(A),$$

isto é, $b \equiv 1 \pmod{KG\ I(A)}$.

Pelo Lema 4.2, sabemos que existe um único elemento $g_b=1.a$, com $a \in A$, tal que

$$b \equiv g_b \pmod{I(G)\ I(A)},$$

e é claro que $g_b=a\in A$. Mas então $f(b)=g_b\in A$. Logo, $f(A^*)\subset A$; como $|A|=|A^*|$ e f é isomorfismo, segue que $f(A^*)=A$.

Desta forma, mostramos que $f:M\to N$ é um isomorfismo de grupos tal que $f(A^*)=A$.

Esta proposição nos permite demonstrar um teorema ainda mais forte que o de Obayashi; este seguirá imediatamente.

Teorema 4.6 - Sejam G um grupo finito, A um subgrupo normal abeliano de G e R um domínio de integridade de característica zero em que nenhum divisor primo racional de $|G|$ é inversível e tal que existe um ideal $J\subset R$ verificando $R/J\cong\mathbb{Z}/n\mathbb{Z}$, onde n é o expoente de A.

Suponhamos que $RG=RH$, e sejam $A^*=H\cap(1+RGI(A))$, N um subgrupo de G e M um subgrupo de H tais que $A\subset N$ e $A^*\subset M$.

Se $\pi_A(N)=\pi_A(M)$, então existe um isomorfismo de M sobre N levando $A^*$ sobre A.

Demonstração.

i) Observamos, em primeiro lugar, que, pelo Teorema 3.1, temos:

$$(A^*)'=A'=\{1\},\ \text{(portanto } A^* \text{ é abeliano)}$$

$$RG\ I(A)=RG\ I(A^*),$$

e $n=\exp(A)=\exp(A^*)$.

ii) Sejam $K=\mathbb{Z}/n\mathbb{Z}$ e $\psi: R \to R/J \cong K$ a aplicação natural. Podemos, então, definir

$$\Phi : RG \longrightarrow KG, \text{ como antes.}$$

Temos que $RG=RH$, $RG\ I(A)=RG\ I(A^*)$ e $\pi_A(N)=\pi_A(M)$. Do Lema 4.3 segue que $KG=K\Phi(H)$, $KG\ I_K(A)=KG\ I_K(\Phi(A^*))$ e $\bar{\pi}_A(N)=\bar{\pi}_A(\Phi(M))$.

Observando, ainda, que

$$\Phi(A^*)=\Phi(H \cap (1+RG\ I(A))=\Phi(H) \cap (1+KG\ I_K(A)),$$

e que, como $A^*$ é abeliano de expoente $n$, $\Phi(A^*)$ é abeliano, e $\exp(\Phi(A^*))|n$, vemos que as hipóteses da <u>Proposição 4.5</u> estão todas satisfeitas. Logo, existe um isomorfismo de grupos

$$f: \Phi(M) \to N$$

tal que $f(\Phi(A^*))=A$.

iii) Observamos agora que, como $RG\ I(A)=RG\ I(A^*)$, $|A|=|A^*|$, e que, como $\pi_A(N)=\pi_A(M)$, temos que $|N|=|M|$, da mesma forma que nos ítens (i) e (iii) da demonstração da Proposição 4.5.

Logo, temos

$$A^* \xrightarrow{\Phi} \Phi(A^*) \xrightarrow[\cong]{f} A$$

e

$$M \xrightarrow{\Phi} \Phi(M) \xrightarrow[\cong]{f} N.$$

Como $\Phi : M \to \Phi(M)$ é epimorfismo e $f: \Phi(M) \to N$ é isomorfismo, $f \circ \Phi : M \to N$ é epimorfismo; mas $|M| = |N|$, donde $f \circ \Phi$ é isomorfismo.

Analogamente, $f \circ \Phi$ é um isomorfismo de $A^*$ sobre $A$, e o teorema está demonstrado.

<u>Teorema 4.7</u> - ([Obayashi, 1970], [Karpilovsky, 1979 b]). Sejam $G$ um grupo finito, $A$ um subgrupo normal abeliano de $G$ e $R$ um anel satisfazendo as seguintes condições:

(*) $R$ é um domínio de integridade de característica zero em que nenhum primo que divide $|G|$ é inversível,

e

(**) Existe um epimorfismo $\psi : R \to \mathbb{Z}/n\mathbb{Z}$, onde $n$ é o expoente de $A$.

Suponhamos ainda que $RG = RH$, e seja $A^* = H \cap (1 + RG\, I(A))$. Se

$N/A$ é o centro de $G/A$

$M/A^*$ é o centro de $H/A^*$,

então existe um isomorfismo de $M$ sobre $N$ levando $A^*$ sobre $A$.

<u>Demonstração</u> - É claro que basta provar que $\pi_A(N) = \pi_A(M)$, e aplicar o Teorema 4.6.

Pelo Lema 4.4, temos que $R\,G/A=R\,\pi_A(H)$. Logo, temos que

$$T(Z(V(R\,G/A)))=T(Z(V(R\,\pi_A(H)))).$$

Pelo Corolário I.2.7(a), temos que

$$T(Z(V(R\,G/A)))=Z(G/A)=N/A=\pi_A(N)$$

e

$$T(Z(V(R\,\pi_A(H))))=Z(\pi_A(H))=\pi_A(M),$$ pois $M/A^*$ é o centro de $H/A^*$.

Logo $\pi_A(N)=\pi_A(M)$.

Portanto, o Teorema segue do resultado anterior.

<u>Corolário 4.8</u> - ([Whitcomb, 1968],[Karpilovsky, 1979 b]). Seja G um grupo metabeliano finito e R um anel satisfazendo as condições (*) e (**) do Teorema 4.7. Então

$$RG=RH \Rightarrow G\cong H.$$

<u>Demonstração</u> - Seja RG=RH, e tomemos A=G'. Então é claro que N=G, pois G/A é abeliano.

Pelo Teorema 3.1 (f),temos que $A^*=H'$, donde é claro que M=H.

Assim, pelo Teorema 4.7, existe $f:H\to G$ isomorfismo, tal que $f(H')=G'$, donde $G\cong H$.

<u>Definição</u> - Seja G um grupo finito. Definimos

$$\mathbb{Z}_{(G)} = \{\frac{a}{b} \in Q \mid mdc(b,|G|)=1\}.$$

É imediato que $\mathbb{Z}_{(G)}$ é um domínio de integridade de característica zero em que nenhum divisor primo de $|G|$ é inversível. Temos, então:

<u>Corolário 4.9</u> - Sejam G um grupo metabeliano finito e $R=\mathbb{Z}_{(G)}$. Então

$$RG=RH \Rightarrow G\cong H.$$

<u>Demonstração</u> - Basta verificar que R satisfaz a condição (**) do Teorema 4.7. Seja, então $n=\exp(G')$. É claro que $n \mid |G|$, de modo que se $mdc\,(b,|G|)=1$, então $mdc\,(b,n)=1$ e portanto $\bar{b}$ é inversível em $\mathbb{Z}/n\mathbb{Z}$.

Definimos $\psi: R \to \mathbb{Z}/n\mathbb{Z}$ por $\psi(a/b)=\bar{a}\,\bar{b}^{-1}$. É imediato que $\psi$ é epimorfismo de anéis. Logo, R satisfaz (**), e o Corolário está provado.

# III. ANÉIS DE GRUPO DE GRUPOS DIEDRAIS SOBRE OS INTEIROS

Neste capítulo, apresentamos alguns resultados sobre anéis de grupo de grupos cíclicos e diedrais sobre os inteiros, focalizando especialmente na estrutura do grupo das unidades. O objetivo deste estudo será obter uma descrição do grupo das unidades em um caso particular. Estes resultados são devidos a D.S.Passman e P.F.Smith [Passman e Smith, 1981].

## § 1. GRUPOS CÍCLICOS

Nesta seção obteremos alguns resultados sobre anéis de grupo de grupos cíclicos de ordem $p^n$, onde p é um primo racional. Para tanto, fixamos a seguinte:

Notação. No que segue, p denota um número primo, $A=\langle a\rangle$ um grupo cíclico de ordem $p^n$, $b=a^{p^{n-1}}$, $B=\langle b\rangle$, $\varepsilon$ uma raiz $p^n$-ésima primitiva da unidade e $\delta=\varepsilon^{p^{n-1}}$.

Começamos estabelecendo uma série de lemas.

Lemma 1.1 - Sejam $R_1$, $R_2$ e T anéis com 1, e sejam $\pi_1:R_1\to T$ e $\pi_2:R_2\to T$ homomorfismos. Seja S o subconjunto de $R_1\oplus R_2$ dado por

$$S=\{(r_1,r_2)\in R_1\oplus R_2 \mid \pi_1(r_1)=\pi_2(r_2)\}.$$

Então S é um subanel de $R_1 \oplus R_2$ e seu grupo de unidades é

$$U(S) = \{(r_1, r_2) \in S \mid r_i \in U(R_i),\ i=1,2\}$$

Demonstração - Imediato.

Lema 1.2 - A equação

$$\sigma(a) = \varepsilon$$

define um epimorfismo $\sigma : \mathbb{Z}A \to \mathbb{Z}[\varepsilon]$, cujo núcleo é o ideal de $\mathbb{Z}A$ gerado pelo elemento $\hat{B} = \sum_{i=0}^{p-1} b^i$.

Demonstração - A aplicação $\sigma : A \to \langle \varepsilon \rangle$ dada por $\sigma(a) = \varepsilon$ é um isomorfismo de A sobre o grupo das raízes $p^n$-ésimas da unidade, que é um subgrupo do grupo de unidades de $\mathbb{Z}[\varepsilon]$. Pondo

$$\sigma\Big(\sum_{g \in A} \lambda(g) g\Big) = \sum_{g \in A} \lambda(g) \sigma(g),$$

obtemos um homomorfismo de anéis $\sigma : \mathbb{Z}A \to \mathbb{Z}[\varepsilon]$. Como $\varepsilon$ gera $\mathbb{Z}[\varepsilon]$, $\sigma$ é epimorfismo; como a gera $\mathbb{Z}A$, $\sigma$ está bem definido. Resta, portanto, calcular o núcleo de $\sigma$.

Pondo $m = p^{n-1} - 1$, é claro que, dado $\alpha \in \mathbb{Z}A$, podemos escrever

$$\alpha = \sum_{i=0}^{m} \alpha_i a^i, \text{ com } \alpha_i \in \mathbb{Z}B \text{ (pela Proposição I.1.1,}$$

já que $\{a^i \mid i=0,1,\ldots,m\}$ é uma transversal para B em A.).

Então

$$\sigma(\alpha)=\sum_{i=0}^{m}\sigma(\alpha_i)\varepsilon^i, \text{ e é claro que } \sigma(\alpha_i)\in\mathbb{Z}[\delta]$$

Como $(Q(\varepsilon):Q(\delta))=p^{n-1}$, os elementos $\varepsilon^i$, $0\leq i\leq m$, são linearmente independentes sobre $Q(\delta)$, e portanto sobre $\mathbb{Z}[\delta]$. Assim,

$$\sigma(\alpha)=0 \text{ se e só se } \sigma(\alpha_i)=0,\ i=0,1,\ldots,m.$$

Escrevamos

$$\alpha_i=\sum_{j=0}^{p-1} S_{ij}b^j, \text{ com } S_{ij}\in\mathbb{Z},\ i=0,1,\ldots,m.$$

Então, se $\sigma(\alpha)=0$, temos que

$$0=\sigma(\alpha_i)=\sum_{j=0}^{p-1} S_{ij}\ \delta^i,\quad i=0,1,\ldots,m$$

donde segue que $\delta$ é raiz dos polinômios

$$\sum_{j=0}^{p-1} S_{ij}\ X^j\quad,\ i=0,1,\ldots,m.$$

Entretanto, como $\delta$ é uma raiz p-ésima primitiva da unidade, seu polinômio irredutível sobre $\mathbb{Z}$ é

$$\Phi_p=X^{p-1}+x^{p-2}+\ldots+x+1.$$

Logo,

$$\Phi_p \mid \sum_{j=0}^{p-1} S_{ij}\ X^i\quad,\ i=0,\ldots,m,$$

donde, como ambos os polinômios têm grau p-1,

$$\sum_{j=0}^{p-1} S_{ij}\, X^j = n_i\, \Phi_p \quad , \; n_i \in \mathbb{Z}, \quad i=0,\ldots,m.$$

Logo $S_{ij}=n_i$, $j=0,1,\ldots,p-1$, donde

$$\alpha_i = n_i\, \hat{B}$$

e

$$\alpha = \sum_{i=0}^{m} n_i\, \hat{B}\, a^i \in \mathbb{Z}A\hat{B}.$$

Assim $\ker\delta \subset \mathbb{Z}A.\hat{B}$. Entretanto, como

$$\sigma(\hat{B}) = \sum_{j=0}^{p-1} \delta^j = 0,$$

a inclusão recíproca é imediata. Logo, temos que $\ker\sigma = \mathbb{Z}A.\hat{B}$ e o lema está demonstrado.

<u>Lema 1.3</u> - A equação

$$\pi(\varepsilon) = aB \in A/B$$

define um epimorfismo $\pi : \mathbb{Z}[\varepsilon] \to GF(p)\ A/B$, tal que, se $p \neq 2$, então $\ker\pi = (\delta - \delta^{-1})\mathbb{Z}[\varepsilon]$, e, se $p=2$, então $\ker\pi = 2\mathbb{Z}[\varepsilon]$.

Além disso, $(\varepsilon - \varepsilon^{-1})$ não é uma unidade de $\mathbb{Z}[\varepsilon]$.

<u>Demonstração</u> - Existe um epimorfismo natural

$$\Theta : \mathbb{Z}A \to GF(p)\ A/B,$$

dado por $\Theta(a) = aB \in A/B$ e $\Theta(x) = \bar{x} \in GF(p)$, para $x \in \mathbb{Z}$. É imediato que $\Theta(b) = \bar{1}$, donde

$$\Theta(\hat{B}) = \Theta\left(\sum_{i=0}^{p-1} b^i\right) = \sum_{i=0}^{p-1} \bar{1} = \bar{p} = \bar{0}.$$

Logo $\hat{B} \in \ker \Theta$, donde $\ker\sigma \subset \ker\Theta$, onde $\sigma$ é o homomorfismo do lema anterior.

Assim, o homomorfismo $\Theta$ se fatora por $\mathbb{Z}[\varepsilon]$, isto é, existe um único homomorfismo $\pi:\mathbb{Z}[\varepsilon]\to GF(p)\ A/B$ satisfazendo $\pi\circ\sigma=\Theta$. Em particular, $\pi(\varepsilon)=\pi(\sigma(a))=\Theta(a)=aB$.

$\ker\sigma \subset \ker\Theta$

$$\begin{tikzcd} \mathbb{Z}A \arrow[r, "\Theta"] \arrow[d, "\sigma"'] & GF(p)\ A/B \\ \mathbb{Z}[\varepsilon] \arrow[ur, dashed, "\pi"'] & \end{tikzcd}$$

Como $\Theta$ é epimorfismo, segue imediatamente que $\pi$ é epimorfismo.

Vamos calcular o núcleo de $\pi$. Dado $i\geq 0$ qualquer, podemos pôr

$$i=j+p^{n-1}k, \text{ com } 0\leq j\leq p^{n-1}-1, \text{ donde } \varepsilon^i=\varepsilon^j\ \delta^k$$

Logo, obtemos que

$$\mathbb{Z}[\varepsilon]=\sum_{j=0}^{m} \mathbb{Z}[\delta]\varepsilon^j, \text{ onde } m=p^{n-1}-1.$$

Seja $r \in \mathbb{Z}[\varepsilon]$, e escrevamos $r=\sum_{j=0}^{m} r_j\ \varepsilon^j$, com $r_i \in \mathbb{Z}[\delta]$.

Como $\pi(\delta)=\Theta(b)=\bar{1}$, temos que $\pi(r_j)\in GF(p)$, $j=0,1,\ldots,m$.

Como os elementos $\pi(\varepsilon^j)$, $0\leq j\leq m$, são os elementos distintos de $A/B$, são linearmente independentes sobre $GF(p)$. Logo, $\pi(r)=0$ se e sómente se $\pi(r_j)=0$, $0\leq j\leq m$.

Assim, para obter o núcleo de $\pi$, basta obter o núcleo do homomorfismo $\tilde{\pi}:\mathbb{Z}[\delta] \to GF(p)$ que se obtém por restrição de $\pi$.

É imediato que $1-\delta \in \ker\tilde{\pi}$. Dado $r \in \mathbb{Z}[\delta]$, escrevamos

$$r=\sum_{h=0}^{p-1} a_k\ \delta^k = \sum_{k=0}^{p-1} a_k(\delta^k-1) + \sum_{k=0}^{p-1} a_k, a_k \in \mathbb{Z}, \forall k.$$

$$= (1-\delta)\ s + t,$$

onde $s \in \mathbb{Z}[\delta]$ e $t=\sum_{k=0}^{p-1} a_k \in \mathbb{Z}$. Como $(1-\delta) \in \ker\tilde{\pi}$, é claro que $r \in \ker\tilde{\pi}$ se e sómente se $t \in \ker\tilde{\pi}$ isto é, se e só se $p|t$.

Assim, para mostrar que $\ker\tilde{\pi}=(1-\delta)\mathbb{Z}[\delta]$, resta apenas mostrar que $p \in (1-\delta)\mathbb{Z}[\delta]$. Seja $\Phi_p(x)$ o polinômio ciclotômico de ordem p, i.é:

$$\Phi_p(x)=1+x+\ldots+x^{p-1} = \prod_{i=0}^{p-1} (x-\delta^i),$$

donde

$$p=\Phi_p(1)=\prod_{i=0}^{p-1} (1-\delta^i) \in (1-\delta)\mathbb{Z}[\delta]$$

Logo, concluímos que $\ker\tilde{\pi}=(1-\delta)\mathbb{Z}[\delta]$, e portanto que $\ker\pi=\sum_{j=0}^{m} (1-\delta)\mathbb{Z}[\delta]\varepsilon^j = (1-\delta)\mathbb{Z}[\varepsilon]$.

Se $p=2$, temos $\delta=-1$, donde $\ker\pi=2\mathbb{Z}[\varepsilon]$.

Se $p\neq 2$, observamos que

$$\delta^{p-1} + \delta^{p-2} +\ldots+\delta+1= 0,$$

donde

$$-(\delta^{p-1}+\ldots+\delta)=1,$$

isto é,

$$-(\delta^{p-2} + \delta^{p-4} + \ldots + \delta)\ (\delta+1)=1,$$

donde $1+\delta \in U(\mathbb{Z}[\delta])$.

Como $\delta \in U(\mathbb{Z}[\delta])$ e $(\delta-\delta^{-1}) = -\delta^{-1}(1-\delta^2) = -\delta^{-1}(1+\delta)(1-\delta)$, segue que $(\delta-\delta^{-1})$ é associado a $(1-\delta)$ em $\mathbb{Z}[\delta]$, donde $\ker\pi=(\delta-\delta^{-1})\mathbb{Z}[\varepsilon]$.

Finalmente, observamos que

$$\pi(\varepsilon-\varepsilon^{-1})=aB - a^{-1}B \in I_{GF(p)}\ (A/B), \text{donde}$$

segue que $\varepsilon-\varepsilon^{-1}$ não é uma unidade de $\mathbb{Z}[\varepsilon]$.

No restante desta seção, fixamos os homomorfismos $\sigma:\mathbb{Z}A \to \mathbb{Z}[\varepsilon]$ e $\pi:\mathbb{Z}[\varepsilon] \to GF(p)\ A/B$, definidos nos lemas anteriores. Além disso, sejam

$$\tau:\mathbb{Z}A \to \mathbb{Z}\,A/B$$

$$\rho:\mathbb{Z}\,A/B \to GF(p)\ A/B$$

e epimorfismos naturais. Podemos, então, obter uma descrição parcial do anel de grupo $\mathbb{Z}A$.

<u>Lema 1.4</u> - A aplicação

$$\sigma \oplus \tau:\ \mathbb{Z}A \longrightarrow \mathbb{Z}[\varepsilon] \oplus \mathbb{Z}\,A/B$$

é um isomorfismo de $\mathbb{Z}A$ sobre o subanel $S$ de $\mathbb{Z}[\varepsilon] \oplus \mathbb{Z}\,A/B$ dado por

$$S=\{(x,y) \in \mathbb{Z}[\varepsilon] \oplus \mathbb{Z}\ A/B \mid \pi(x)=\rho(y)\}$$

Demonstração - É evidente que $\sigma \oplus \tau$ é um homomorfismo de $\mathbb{Z}A$ em $\mathbb{Z}[\varepsilon] \oplus \mathbb{Z}A/B$. Assim, devemos provar que $\mathrm{Im}(\sigma \oplus \tau)=S$ e $\ker(\sigma \oplus \tau)=\{0\}$.

i) Seja $\alpha \in \ker(\sigma \oplus \tau)$, de modo que $(\sigma \oplus \tau)(\alpha)=(0,0)$. Então $\sigma(\alpha)=0$, de modo que, pelo Lema 1.2, $\alpha=\beta\hat{B}$, para algum $\beta \in \mathbb{Z}A$. Além disso,

$$0 = \tau(\alpha) = \tau(\beta)\ \tau(\hat{B}) = p\ \tau(\beta),$$

de modo que $\tau(\beta)=0$, donde $\beta \in \ker\tau = \mathbb{Z}A\, I(B)$; segue, então do Lema I.3.12 que $\alpha=\beta\ \hat{B}=0$. Logo, $\ker(\sigma \oplus \tau)=\{0\}$.

ii) Consideramos os homomorfismos

$$\pi \circ \sigma : \mathbb{Z}A \to GF(p)\ A/B$$

e

$$\rho \circ \tau\ \ \mathbb{Z}A \to GF(p)\ A/B,$$

e observamos que $(\pi \circ \sigma)(a) = aB = (\rho \circ \tau)(a)$. Como a gera $\mathbb{Z}A$, segue que $\pi \circ \sigma = \rho \circ \tau$. Em particular, se $\alpha \in \mathbb{Z}A$ e $(\sigma \oplus \tau)(\alpha)=(x,y)$, então

$$\pi(x)=\pi(\sigma(\alpha)) = \rho(\tau(\alpha))=\rho(y),$$

donde $\mathrm{Im}(\sigma \oplus \tau) \subset S$.

iii) Finalmente, tomemos $(x,y) \in S$, isto é, $(x,y) \in \mathbb{Z}[\varepsilon] \oplus \mathbb{Z}A/B$ tal que $\pi(x)=\rho(y)$. Como $\sigma$ é epimorfismo, existe $\beta \in \mathbb{Z}A$ tal que $\sigma(\beta)=x$. Então, como $\pi \circ \sigma = \rho \circ \tau$, temos

$$(\rho \circ \tau)(\beta)=(\pi \circ \sigma)(\beta)=\pi(x)=\rho(y),$$

donde $\tau(\beta)-y \in \ker\rho = p\,\mathbb{Z}A/B$. Como $\tau$ é epimorfismo, existe $\gamma\in\mathbb{Z}A$ tal que $\tau(\beta)-y=p\tau(\gamma)$. Ponhamos $\alpha=\beta-\hat{B}\gamma$.

Observamos que, como $\hat{B}\in\ker\sigma$, $\sigma(\alpha)=\sigma(\beta)=x$. Por outro lado, $\tau(\hat{B})=p$, donde

$$\tau(\alpha)=\tau(\beta)-p\tau(\gamma)=y.$$

Logo, obtivemos $\alpha\in\mathbb{Z}A$ tal que

$$(\sigma\oplus\tau)(\alpha)=(x,y).$$

Assim, $\mathrm{Im}(\sigma\oplus\tau)=S$, provando o lema.

<u>Corolário 1.5</u> - Seja A um grupo cíclico de ordem $p^n$, e seja B um subgrupo de ordem p. Então

$$U(\mathbb{Z}A)\cong S_1,$$

onde

$$S_1=\{(x,y)\in\mathbb{Z}[\varepsilon]\oplus\mathbb{Z}A/B \mid \pi(x)=\rho(y),\ x\in U(\mathbb{Z}[\varepsilon]),\ y\in U(\mathbb{Z}A/B)\},$$

onde $\pi$ e $\rho$ são as aplicações definidas acima.

<u>Demonstração</u>. Imediato.

No restante desta seção, discutimos algumas propriedades adicionais de $\mathbb{Z}[\varepsilon]$ e da aplicação $\pi:\mathbb{Z}[\varepsilon]\longrightarrow GF(p)\,A/B$, definida acima.

<u>Lema 1.6</u> - Se $p>2$ ou $n>1$, então o anel $\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$ é o subanel real de $\mathbb{Z}[\varepsilon]$, e temos que,

$$\mathbb{Z}[\varepsilon]=\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\oplus\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1},$$

como soma direta de $\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$-módulos.

Demonstração - O argumento tem vários passos.

i) É imediato verificar que, para todo $i\geq 1$, vale a identidade:

$$\varepsilon^{i+1}+\varepsilon^{-(i+1)}=(\varepsilon+\varepsilon^{-1})(\varepsilon^{i}+\varepsilon^{-i})-(\varepsilon^{i-1}+\varepsilon^{-(i-1)}).$$

Ainda, como $\varepsilon^0+\varepsilon^0=2\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$ e $\varepsilon+\varepsilon^{-1}\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$, segue imediatamente, por indução em $i\geq 1$, que

$$\varepsilon^{i}+\varepsilon^{-i}\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}],\ \forall i\geq 1.$$

ii) Novamente, é imediato verificar que, para todo $i\geq 1$, temos

$$\varepsilon^{i+1}-\varepsilon^{-(i+1)}=(\varepsilon-\varepsilon^{-1})(\varepsilon^{i}+\varepsilon^{-i})-(\varepsilon^{i-1}-\varepsilon^{-(i-1)}),$$

donde

$$\frac{\varepsilon^{i+1}-\varepsilon^{-(i+1)}}{\varepsilon-\varepsilon^{-1}}=\varepsilon^{i}+\varepsilon^{-i}-\frac{\varepsilon^{i-1}-\varepsilon^{-(i-1)}}{\varepsilon-\varepsilon^{-1}},\ \forall i\geq 1.$$

(Observe-se que, como $p>2$ ou $n>1$, $\varepsilon-\varepsilon^{-1}\neq 0$).

Como $\frac{\varepsilon^0-\varepsilon^0}{\varepsilon-\varepsilon^{-1}}=0$ e $\frac{\varepsilon-\varepsilon^{-1}}{\varepsilon-\varepsilon^{-1}}=1$, segue, por indução, que, para todo $i\geq 1$, tem-se que $\frac{\varepsilon^{i}-\varepsilon^{-i}}{\varepsilon-\varepsilon^{-1}}$ é uma soma de termos da forma $\varepsilon^{j}+\varepsilon^{-j}$; logo $\frac{\varepsilon^{i}-\varepsilon^{-i}}{\varepsilon-\varepsilon^{-1}}\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$ para todo $i\geq 1$.

iii) Dado $c \in \mathbb{Z}[\varepsilon]$, escrevamos $c = \sum_{i \geq 0} a_i \varepsilon^i$. Então temos que seu conjugado em $\mathbb{C}$ é dado por $\bar{c} = \sum_{i \geq 0} a_i \varepsilon^{-i}$, donde segue que

$$\frac{c-\bar{c}}{\varepsilon-\varepsilon^{-1}} = \frac{\sum_{i \geq 1} a_i (\varepsilon^i - \varepsilon^{-i})}{\varepsilon-\varepsilon^{-1}} = \sum_{i \geq 1} a_i \frac{\varepsilon^i - \varepsilon^{-i}}{\varepsilon-\varepsilon^{-1}} \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}].$$

iv) Dado $a \in \mathbb{Z}[\varepsilon]$, definimos

$$x = \frac{a\varepsilon - \overline{a\varepsilon}}{\varepsilon-\varepsilon^{-1}} \quad \text{e} \quad y = \frac{a-\bar{a}}{\varepsilon-\varepsilon^{-1}},$$

de modo que $x, y \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}]$, por (iii) . Observando agora que

$$\begin{aligned} x - y\,\varepsilon^{-1} &= \frac{a\varepsilon - \overline{a\varepsilon} - a\varepsilon^{-1} + \bar{a}\varepsilon^{-1}}{\varepsilon - \varepsilon^{-1}} = \\ &= \frac{a\varepsilon - \bar{a}\varepsilon^{-1} - a\varepsilon^{-1} + \bar{a}\varepsilon^{-1}}{\varepsilon - \varepsilon^{-1}} = \\ &= \frac{a\varepsilon - a\varepsilon^{-1}}{\varepsilon - \varepsilon^{-1}} = a, \end{aligned}$$

segue imediatamente que

$$\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon+\varepsilon^{-1}] + \mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1}.$$

v) Como $\varepsilon+\varepsilon^{-1} = \varepsilon+\bar{\varepsilon} \in \mathbb{R}$, é imediato que

$$\mathbb{Z}[\varepsilon+\varepsilon^{-1}] \subset \mathbb{R} \cap \mathbb{Z}[\varepsilon].$$

Além disso, $\varepsilon^{-1} \notin \mathbb{R}$ (pois $p>2$ ou $n>1$); logo, segue que

$$\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1} \subset C - \mathbb{R}^*,$$

donde é imediato que

$$\mathbb{Z}[\varepsilon+\varepsilon^{-1}] \cap \mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1} = \{0\}.$$

Assim,

$$\mathbb{Z}[\varepsilon]=\mathbb{Z}[\varepsilon+\varepsilon^{-1}] \oplus \mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1}.$$

vi) Finalmente, seja $r \in \mathbb{R} \cap \mathbb{Z}[\varepsilon]$. Como $r \in \mathbb{Z}[\varepsilon]$, podemos pôr $r=a+b$, com $a \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}]$ e $b \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1}$. Como $r \in \mathbb{R}$ e $a \in \mathbb{R}$, segue que $b \in \mathbb{R}$, donde, como $\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1} \subset C-\mathbb{R}^*$, vem que $b=0$. Logo, $r \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}]$, e

$$\mathbb{Z}[\varepsilon+\varepsilon^{-1}]=\mathbb{Z}[\varepsilon] \cap \mathbb{R},$$

isto é, $\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$ é o subanel real de $\mathbb{Z}[\varepsilon]$.

Observamos que, no caso em que $p=2$ e $n=1$, temos $\varepsilon=-1$, donde segue que $\mathbb{Z}[\varepsilon]= \mathbb{Z} \subset \mathbb{R}$, e o lema anterior é falso. É claro, entretanto, que esta situação é extremamente simples.

<u>Lema 1.7</u> - Se $p>2$, o núcleo da restrição

$$\pi : \mathbb{Z}[\varepsilon+\varepsilon^{-1}] \longrightarrow GF(p) \quad A/B$$

é o ideal principal de $\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$ gerado por $(\delta-\delta^{-1})(\varepsilon-\varepsilon^{-1})$.

<u>Demonstração</u>.

i) Como $\delta-\delta^{-1}$ e $\varepsilon-\varepsilon^{-1}$ são imaginários puros, temos que $(\delta-\delta^{-1})(\varepsilon-\varepsilon^{-1}) \in \mathbb{R}$. Do Lema 1.3, vem imediatamente que $(\delta-\delta^{-1})(\varepsilon-\varepsilon^{-1}) \in \ker \pi$.

Logo,

$$(\delta-\delta^{-1})(\varepsilon-\varepsilon^{-1})\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\subset \ker\pi.$$

ii) Reciprocamente, tomemos $a\in\ker\pi$ tal que $a\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$. Pelo Lema 1.3, $a\in(\delta-\delta^{-1})\mathbb{Z}[\varepsilon]$, e pelo Lema 1.6, $\mathbb{Z}[\varepsilon]=\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\oplus\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1}$. Logo, podemos escrever

$$a=(b+c\varepsilon^{-1})(\delta-\delta^{-1}),\ \text{com } b,c\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}].$$

Como $a,b,c\in\mathbb{R}$, obtemos, por conjugação,

$$a=-(b+c\varepsilon)(\delta-\delta^{-1}).$$

Somando estas igualdades, obtemos

$$2a=-c(\varepsilon-\varepsilon^{-1})(\delta-\delta^{-1}),$$

donde segue que

$$a=-\frac{c}{2}(\varepsilon-\varepsilon^{-1})(\delta-\delta^{-1});$$

assim, resta apenas provar que $\frac{c}{2}\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$.

iii) Observamos agora que, pondo $q=p^{n-1}$, temos

$$\delta-\delta^{-1}=\varepsilon^{q}-\varepsilon^{-q}=(\varepsilon-\varepsilon^{-1})(\varepsilon^{q-1}+\varepsilon^{q-3}+\ldots+\varepsilon^{-(q-1)}),$$

donde segue que $(\delta-\delta^{-1})\mathbb{Z}[\varepsilon]\subset(\varepsilon-\varepsilon^{-1})\mathbb{Z}[\varepsilon]$.

Da demonstração do Lema 1.3, temos que $p\in(\delta-\delta^{-1})\mathbb{Z}[\varepsilon]$. Logo, $p\in(\varepsilon-\varepsilon^{-1})\mathbb{Z}[\varepsilon]$, de modo que, podemos pôr

$$p^2=d(\varepsilon-\varepsilon^{-1})(\delta-\delta^{-1}),$$

para algum $d \in \mathbb{Z}[\varepsilon]$. Como $p^2 \in \mathbb{R}$ e $(\varepsilon-\varepsilon^{-1})(\delta-\delta^{-1}) \in \mathbb{R}$, temos que $d \in \mathbb{R}$, donde $d \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}]$.

Agora, como p é ímpar, $mdc(p^2,2)=1$; logo, existem $f,g \in \mathbb{Z}$ tais que

$$fp^2+2g=1.$$

Logo,

$$fd(\varepsilon-\varepsilon^{-1})(\delta-\delta^{-1})+2g=1,$$

donde, multiplicando por $\frac{c}{2}$,

$$\frac{c}{2} = fd\,\frac{c}{2}\,(\varepsilon-\varepsilon^{-1})(\delta-\delta^{-1})+cg$$

$$= -fa + cg,$$

e, como $f,a,c,g \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}]$, segue que $\frac{c}{2} \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}]$, provando o Lema.

<u>Lema 1.8</u> - Se p=2, o núcleo da restrição

$$\pi : \mathbb{Z}[\varepsilon+\varepsilon^{-1}] \longrightarrow GF(p)\ \frac{A}{B}$$

é o ideal $2\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$.

<u>Demonstração</u> - Se n=1, $\mathbb{Z}[\varepsilon+\varepsilon^{-1}]=\mathbb{Z}[\varepsilon]$, e não há nada a demonstrar. Se n>1, observamos que, pelo Lema 1.3, o núcleo da aplicação

$$\pi : \mathbb{Z}[\varepsilon] \longrightarrow GF(p)\ \frac{A}{B}$$

é o ideal $2\mathbb{Z}[\varepsilon]$. Logo,

$$\ker \pi\Big|_{\mathbb{Z}[\varepsilon+\varepsilon^{-1}]} = 2\,\mathbb{Z}[\varepsilon] \cap \mathbb{R}.$$

Entretanto, como $\mathbb{Z}[\varepsilon]=\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\oplus \mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1}$, temos que $2\mathbb{Z}[\varepsilon]=2\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\oplus 2\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1}$, e, como $2\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\subset\mathbb{R}$ e $2\mathbb{Z}[\varepsilon+\varepsilon^{-1}]\varepsilon^{-1} \subset C-\mathbb{R}^*$, segue, como acima, que

$$2\mathbb{Z}[\varepsilon] \cap \mathbb{R} = 2\mathbb{Z}[\varepsilon+\varepsilon^{-1}].$$

Logo,
$$\ker \pi\Big|_{\mathbb{Z}[\varepsilon+\varepsilon^{-1}]} = 2\mathbb{Z}[\varepsilon+\varepsilon^{-1}].$$

<u>Lema 1.9</u> - Seja $p>2$. Dado $a\in\mathbb{Z}[\varepsilon]$, escrevemos $a=x-y\varepsilon^{-1}$, com $x,y\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$. Então $\pi(a)=0$ se e sómente se

$$\pi(x)=\pi(y)=k.(\widehat{A/B}),$$

para algum $k\in GF(p)$.

<u>Demonstração</u>. Seja $h=aB$ o gerador do grupo cíclico $H=A/B$.

i) Suponhamos, primeiramente, que $\pi(x)=\pi(y)=k\hat{H}$. Então

$$\pi(a)=\pi(x)-\pi(y)h^{-1}=k\hat{H}-k\hat{H}h^{-1}=0,$$

já que $\hat{H}h^{-1}=\hat{H}$.

ii) Reciprocamente, suponhamos que $\pi(a)=0$. Então temos que $\pi(x)=\pi(y)h^{-1}$. Seja $*:GF(p)H\longrightarrow GF(p)H$ a involução da Proposição I.1.2.

Como $x,y\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$, $\pi(x)$, $\pi(y)\in GF(p)\langle h+h^{-1}\rangle$, e, como $(h+h^{-1})^*=h+h^{-1}$, segue que $\pi(x)$ e $\pi(y)$ são fixos por *. Além disso, como H é abeliano, aplicando * à equação $\pi(x)=\pi(y)h^{-1}$, obtemos que $\pi(x)=\pi(y)h$.

Logo, $\pi(y)h=\pi(x)=\pi(y)h^{-1}$, de modo que

$$\pi(y)(h^{-1}-h)=0,$$

donde obtemos

$$\pi(y)(1-h^2)=0.$$

Então

$$\pi(y)(1-h^2)(h^{2(n-1)}+\ldots+h^2+1)=0,\ \forall n\geq 0,$$

donde

$$\pi(y)(1-h^{2n})=0,\ \forall n\geq 0.$$

Como p é ímpar, $\langle h^2\rangle=H$, donde segue que

$$\pi(y).I(H)=0.$$

Logo, pelo Lema I.3.12, $\pi(y)=k\hat{H}$, para algum $k\in GF(p)$, donde $\pi(x)=\pi(y)h=k\hat{H}h=k\hat{H}$, e o lema está demonstrado.

<u>Lema 1.10</u> - Seja $p=2$ e $n>1$ e escrevamos $H=A/B=\langle h\rangle$, onde $h=aB$, $H_2=\langle h^2\rangle$. Dado $a\in\mathbb{Z}[\varepsilon]$, escrevamos $a=x-y\,\varepsilon^{-1}$, com $x,y\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$. Então $\pi(a)=0$ se e sómente se

$$\pi(x)=k_2\hat{H}_2+k_1h\hat{H}_2$$

e

$$\pi(y)=k_1\hat{H}_2+k_2h\hat{H}_2$$

para algum par de elementos $k_1,k_2\in GF(2)$.

Demonstração.

i) Suponhamos que $\pi(x)=k_2\hat{H}_2 + k_1 h\,\hat{H}_2$ e que $\pi(y)=k_1\hat{H}_2 + k_2 h\,\hat{H}_2$. Então

$$\pi(a)=\pi(x-y\,\varepsilon^{-1})=\pi(x)-\pi(y)h^{-1}$$
$$=k_2\hat{H}_2+k_1 h\,\hat{H}_2-k_1 h\,\hat{H}_2-k_2\hat{H}_2=0,$$

já que $h^{-1}\hat{H}_2=h\hat{H}_2$ e $h\hat{H}_2h^{-1}=\hat{H}_2$.

ii) Reciprocamente, suponhamos que $\pi(a)=0$. Como no Lema 1.9, obtemos que $\pi(y)(1-h^2)=0$, donde, como antes, segue que $\pi(y)$ anula $I(H_2)$.

Pelo Lema I.3.12, segue que

$$\pi(y)=\alpha\hat{H}_2,$$

para algum $\alpha\in GF(2)H$. Portanto, para algum par de elementos $k_1,k_2\in GF(2)$, tem-se que

$$\pi(y)=k_1\hat{H}_2 + k_2 h\,\hat{H}_2.$$

Finalmente,

$$\pi(x)=\pi(y)h = k_1 h\,\hat{H}_2+ k_2\hat{H}_2,$$

e o lema está demonstrado.

## § 2. GRUPOS DIEDRAIS

Nesta seção passaremos a estudar o anel de grupo $\mathbb{Z}G$, para $G=D_{p^n}$, o grupo diedral de ordem $2p^n$. Em particular, estudaremos certos subgrupos de $U(\mathbb{Z}G)$. No caso

$G=D_p$, obteremos uma descrição completa de grupo das unidades.

No curso de nosso estudo, recorreremos repetidas vezes a um certo anel de matrizes. Assim, por conveniência, introduziremos desde já esta estrutura.

Definição.- Seja R um anel comutativo com uma involução, denotada por $a \to a'$. Definimos

$$M_2^*(R) = \{ \begin{pmatrix} c & d \\ d' & c' \end{pmatrix} \mid c,d \in R \}.$$

É claro que $M_2^*(R)$ é um subconjunto de $M_2(R)$. Mais ainda, vale o seguinte lema, de demonstração muito simples:

Lema 2.1 - i) $M_2^*(R)$ é um subanel de $M_2(R)$;

ii) A aplicação "adjunta", dada por

$$\text{adj} \begin{pmatrix} c & d \\ d' & c' \end{pmatrix} = \begin{pmatrix} c' & -d \\ -d' & c \end{pmatrix}$$

define uma involução em $M_2^*(R)$;

iii) Um elemento $\alpha = \begin{pmatrix} c & d \\ d' & c' \end{pmatrix} \in M_2^*(R)$ é uma unidade de $M_2^*(R)$ e e sómente se $\det \alpha = cc' - dd'$ é uma unidade de R.

O próximo lema mostra a relevância desta construção.

<u>Lema 2.2</u> - Seja $G=A\langle t\rangle$ o produto semi-direto de um grupo abeliano A pelo grupo cíclico $\langle t\rangle$, de ordem 2. Nesta situação, a conjugação por t define uma involução de $\mathbb{Z}A$, e a aplicação $\zeta:\mathbb{Z}G\to M_2^*(\mathbb{Z}A)$, dada por

$$\zeta(\alpha+\beta t) = \begin{pmatrix} \alpha & \beta \\ \beta^t & \alpha^t \end{pmatrix}, \qquad \alpha,\beta\in\mathbb{Z}A,$$

é um isomorfismo.

<u>Demonstração</u> - Este lema pode ser provado diretamente, sem qualquer dificuldade, ou pelo seguinte argumento:

Seja $M=\mathbb{Z}G$; então, M é um $\mathbb{Z}G$-módulo à direita <u>fiel</u> e um $\mathbb{Z}A$-módulo à esquerda <u>livre</u>, com base $\{1,t\}$. Isto permite que consideremos $\mathbb{Z}G$ como um anel de transformações $\mathbb{Z}A$ - lineares em M, pondo, para $m\in M$ e $x\in\mathbb{Z}G$, $mx=m.x$, onde escrevemos as transformações lineares à direita. Logo, existe um isomorfismo $\zeta:\mathbb{Z}G\to M_2(\mathbb{Z}A)$.

Vamos calcular $\zeta$ explicitamente. Para tanto, seja $x\in\mathbb{Z}G$, $x=\alpha+\beta t$, onde $\alpha,\beta\in\mathbb{Z}A$. Então

$$1x=1(\alpha+\beta t)=\alpha+\beta t=\alpha.1+\beta.t$$
$$tx=t(\alpha+\beta t)=t\alpha+t\beta t=\beta^t.1+\alpha^t.t.$$

Logo,

$$\zeta(x)=\zeta(\alpha+\beta t)=\begin{pmatrix} \alpha & \beta \\ \beta^t & \alpha^t \end{pmatrix},$$

donde $\zeta(\mathbb{Z}G)=M_2^*(\mathbb{Z}A)$, provando o lema.

No restante deste parágrafo, G denotará o produto semi-direto $A < t >$, com A abeliano e $t^2=1$ e $\zeta$ denotará a aplicação definida no Lema 2.2. Como consequência imediata, obtemos o seguinte resultado:

<u>Lema 2.3</u> - Seja $\gamma=\alpha+\beta t$, $\alpha,\beta\in\mathbb{Z}A$, uma unidade de ordem finita de $\mathbb{Z}G$. Se $A\cap Z(G)=< 1 >$, então temos que

$$\det\zeta(\gamma)=\alpha\alpha^t-\beta\beta^t=\pm 1.$$

Além disso, se $\gamma\in 1+I(A)\mathbb{Z}G$, então $\det\zeta(\gamma)=1$.

<u>Demonstração</u> - Seja $w=\zeta(\gamma)\in M_2^*(\mathbb{Z}A)$. Como $\gamma$ é unidade de ordem finita, w é unidade de ordem finita de $M_2^*(\mathbb{Z}A)$. No Lema 2.1, mostramos que adj é uma involução em $M_2^*(\mathbb{Z}A)$; logo, adj w é uma unidade de ordem finita.

É imediato que, para todo $v\in M_2^*(\mathbb{Z}A)$,

$$v.\mathrm{adj}\ v=\mathrm{adj}\ v.v=\det v.1.$$

Como w e adj w são unidades de ordem finita, segue que det w.1 também é unidade de ordem finita em $M_2^*(\mathbb{Z}A)$, donde det w é unidade de ordem finita de $\mathbb{Z}A$.

Pelo fato de que A é abeliano, segue pelo Corolário I.2.7 que $\det w=\pm g$, para algum $g\in A$. Além disso, temos que $(\det w)^t=\det w$, donde segue que $g^t=g$ e portanto $g\in Z(G)$. Lembrando que $A\cap Z(G)=< 1 >$, segue que $g=1$, donde $\det w=\pm 1$.

Finalmente, suponhamos que $\gamma\in 1+I(A)\mathbb{Z}G$, de mo-

do que $\alpha \in 1+I(A)$ e $\beta \in I(A)$, e consideremos a função de aumento $\varepsilon : \mathbb{Z}A \longrightarrow \mathbb{Z}$. Então

$$\varepsilon(\det w) = \varepsilon(\alpha\alpha^t - \beta\beta^t) = 1,$$

de modo que não podemos ter $\det w = -1$. Assim, se $\gamma \in 1+I(A)\mathbb{Z}G$, então $\det w = 1$.

No restante deste parágrafo, $A = \langle a \rangle$ indicará um grupo cíclico de ordem $p^n$, e usamos a notação do parágrafo anterior. Além disso, fixamos $G = A\langle t \rangle$, o grupo diedral de ordem $2p^n$, isto é, pomos $t^2 = 1$ e, $a^t = a^{-1}$. O seguinte lema é imediato:

<u>Lema 2.4</u> - Se R e S são anéis comutativos com involução e $\theta : R \to S$ é um homomorfismo de anéis compatível com as involuções, então $\theta$ se estende naturalmente a um homomorfismo de anéis

$$\theta^* : M_2^*(R) \longrightarrow M_2^*(S).$$

<u>Corolário 2.5</u> - Os homomorfismos $\sigma, \tau, \pi$ e $\rho$, definidos acima, induzem homomorfismos

$$\sigma^* : M_2^*(\mathbb{Z}A) \longrightarrow M_2^*(\mathbb{Z}[\varepsilon])$$

$$\tau^* : M_2^*(\mathbb{Z}A) \longrightarrow M_2^*(\mathbb{Z}\, A/B)$$

$$\pi^* : M_2^*(\mathbb{Z}[\varepsilon]) \longrightarrow M_2^*(GF(p)\ A/B)$$

$$\rho^* : M_2(\mathbb{Z}\, A/B) \longrightarrow M_2^*(GF(p)\ A/B),$$

onde as involuções de $\mathbb{Z}A$, $\mathbb{Z}\, A/B$ e $GF(p)A/B$ são dadas por conjugação por t e a involução de $\mathbb{Z}[\varepsilon]$ é a conjugação complexa.

Como consequência imediata dos Lemas 2.2 e 1.4 e do Corolário 2.5, obtemos uma descrição parcial de $\mathbb{Z}G$ para $G=D_{p^n}$.

<u>Proposição 2.6</u> - A aplicação

$$(\sigma^*\oplus\tau^*)\circ\zeta : \mathbb{Z}G \longrightarrow M_2^*(\mathbb{Z}[\varepsilon])\oplus M_2^*(\mathbb{Z}A/B)$$

define um isomorfismo de $\mathbb{Z}G$ sobre o subanel

$$S=\{(x,y)\in M_2^*(\mathbb{Z}[\varepsilon])\oplus M_2^*(\mathbb{Z}A/B)\mid \pi^*(x)=\rho^*(y)\}.$$

<u>Corolário 2.7</u> - Se $G=D_{p^n}$, então

$$U(\mathbb{Z}G)\cong U(S),$$

$$U(S)=\{(x,y)\in M_2^*(\mathbb{Z}[\varepsilon])\oplus M_2^*(\mathbb{Z}A/B)\mid \det x\in U(\mathbb{Z}[\varepsilon]),\det y\in U(\mathbb{Z}A/B) \text{ e } \pi^*(x)=\rho^*(y)\}.$$

<u>Demonstração</u> - Imediato, a partir dos Lemas 1.1 e 2.1.

Interessa-nos, agora, estudar o subgrupo de $V(\mathbb{Z}G)$ dado por

$$K(B)=V(\mathbb{Z}G)\cap(1+I(B)\mathbb{Z}G)\triangleleft V(\mathbb{Z}G).$$

<u>Lema 2.8</u> - A aplicação

$$\sigma^*\circ\zeta : \mathbb{Z}G \longrightarrow M_2^*(\mathbb{Z}[\varepsilon])$$

define um isomorfismo de $K(B)$ sobre o grupo

$$H=\{h\in M_2^*(\mathbb{Z}[\varepsilon])\,|\,\det h\in U(\mathbb{Z}[\varepsilon])\text{ e }\pi^*(h)=1\}.$$

<u>Demonstração</u> - Seja $\gamma=\alpha+\beta t\in K(B)$, com $\alpha,\beta\in\mathbb{Z}A$, e ponhamos $h=\sigma^*(\zeta(\gamma))$. Seja ainda $\pi_B:\mathbb{Z}G\longrightarrow\mathbb{Z}G/B$ o homomorfismo natural, e observemos que $G/B\cong A/B\langle t\rangle$, o produto semi-direto induzido de modo natural.

Como $\gamma\in 1+I(B)\mathbb{Z}G$, temos que $\pi_B(\gamma)=1$; logo, $\pi_B(\alpha)+\pi_B(\beta)t=1$, donde $\alpha\in 1+I(B)\mathbb{Z}A$ e $\beta\in I(B)\mathbb{Z}A$. Assim, $\tau^*(\zeta(\gamma))=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=1\in M_2^*(\mathbb{Z}A)$, donde segue que $(\sigma^*\oplus\tau^*)(\zeta(\gamma))=$ $=(h,1)$. Obtemos, então, duas conclusões:

1) Pela Proposição 2.6, temos que $(\sigma^*\oplus\tau^*)\circ\zeta$ é injetora. Sejam $\gamma_1,\gamma_2\in K(B)$, e suponhamos que

$$\sigma^*\circ\zeta(\gamma_1)=h_1=h_2=\sigma^*\circ\zeta(\gamma_2).$$

Então $(\sigma^*\oplus\tau^*)\circ\zeta(\gamma_1)=(h_1,1)=(h_2,1)=(\sigma^*\oplus\tau^*)\circ\zeta(\gamma_2)$, donde $\gamma_1=\gamma_2$. Logo, a aplicação $\sigma^*\circ\zeta$, <u>restrita a $K(B)$</u>, é injetora.

2) Como $\gamma\in V(\mathbb{Z}G)$, temos $(h,1)\in U(S)$, donde, pelo Corolário 2.7, $\det h\in U(\mathbb{Z}[\varepsilon])$ e $\pi^*(h)=\rho^*(1)=1$.

Logo, $\sigma^*\circ\zeta$ dá um monomorfismo de $K(B)$ em $H$. Resta mostrar, então, que $(\sigma^*\circ\zeta)(K(B))=H$. Para isso, seja $h\in H$. Como $\pi^*(h)=1=\rho^*(1)$, vemos, pelo Corolário 2.7, que $(h,1)\in U(S)$. Logo, ainda do Corolário 2.7, vem que existe $\gamma=\alpha+\beta t\in U(\mathbb{Z}G)$, com $\alpha,\beta\in\mathbb{Z}A$, tal que $(\sigma^*\oplus\tau^*)\circ\zeta(\gamma)=(h,1)$.

Agora, $\tau^*(\zeta(\gamma))=1$ implica em que $\tau(\alpha)=1$ e $\tau(\beta)=0$, donde $\alpha\in 1+I(B)\mathbb{Z}A$ e $\beta\in I(B)\mathbb{Z}A$ e portanto $\gamma=\alpha+\beta t\in 1+I(B)\mathbb{Z}G$.

Logo, $\gamma\in U(\mathbb{Z}G)\cap(1+I(B)\mathbb{Z}G) = K(B)$ e, como $\sigma^*(\zeta(\gamma))=h$, segue que

$(\sigma^*\circ\zeta)(K(B))=H$, e o lema está demonstrado.

A descrição de $K(B)$ assim obtida pode ser ainda melhorada, desde que se exclua o caso $p=2$. Desta forma, no que segue, supomos sempre que $p>2$, e notamos que isto implica em que $\varepsilon\neq\varepsilon^{-1}$.

Consideramos agora a matriz

$$\ell = \begin{pmatrix} \varepsilon^{-1} & 1 \\ -\varepsilon & -1 \end{pmatrix} \in M_2(\mathbb{Q}[\varepsilon]),$$

e observamos que

$$\ell^{-1} = \frac{1}{\lambda}\begin{pmatrix} -1 & -1 \\ \varepsilon & \varepsilon^{-1} \end{pmatrix} \in M_2(\mathbb{Q}[\varepsilon]),$$

onde $\lambda=\det\ell=\varepsilon-\varepsilon^{-1}\neq 0$.

Sendo $\ell$ e $\ell^{-1}$ as matrizes acima, consideraremos o automorfismo $\eta:M_2(\mathbb{Q}[\varepsilon])\longrightarrow M_2(\mathbb{Q}[\varepsilon])$ dado por $\eta(x)=\ell^{-1}x\,\ell$.

Seja, ainda, $GL_2(\mathbb{Z}[\varepsilon+\varepsilon^{-1}])$ o grupo das matrizes 2x2 inversíveis sobre $\mathbb{Z}[\varepsilon+\varepsilon^{-1}]$. Observamos que a aplicação $\pi:\mathbb{Z}[\varepsilon]\longrightarrow GF(p)\ A/B$ induz, de modo natural, um homomorfismo

$$\tilde{\pi}:GL_2(\mathbb{Z}[\varepsilon+\varepsilon^{-1}])\longrightarrow GL_2(GF(p)\ A/B).$$

Com esta notação, temos:

<u>Teorema 2.9</u> - Se $p > 2$, a aplicação composta

$$\eta \circ \sigma^* \circ \zeta : \mathbb{Z}G \longrightarrow M_2^* \ (Q[\varepsilon])$$

define um isomorfismo de $K(B)$ sobre o grupo

$$W = \{ w \in GL_2(\mathbb{Z}[\varepsilon+\varepsilon^{-1}]) \mid \tilde{\pi}(w) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + k(\widehat{A/B}) \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, k \in GF(p) \}.$$

<u>Demonstração</u> - Pelo Lema 2.8, $\sigma^* \circ \zeta|_{K(B)}$ é um monomorfismo, donde, como $\eta$ é injetora, segue que $\eta \circ \sigma^* \circ \zeta|_{K(B)}$ é injetora. Ainda pelo Lema 2.8, $\sigma^* \circ \zeta \ (K(B)) = H$, onde $H = \{ h \in M_2^*(\mathbb{Z}[\varepsilon]) \mid \det h \in U(\mathbb{Z}[\varepsilon])$ e $\pi^*(h) = 1 \}$. Assim, basta mostrar que $\eta(H) = \ell^{-1} H \ \ell = W$.

i) Seja $h = \begin{pmatrix} c & d \\ \bar{d} & \bar{c} \end{pmatrix} \in H$, de modo que $\det h \in U(\mathbb{Z}[\varepsilon])$ e $\pi^*(h) = 1 \in M_2^*(GF(p) \ A/B)$. É claro que $\pi^*(h) = 1 \in M_2^*(GF(p) \ A/B)$ se e só se $\pi(c) = 1 \in GF(p) \ A/B$ e $\pi(d) = 0 \in GF(p) \ A/B$. Pelo Lema 1.6, podemos escrever $c = C - E\varepsilon^{-1}$ e $d = D - F\varepsilon^{-1}$, com $C$, $D$, $E$, $F \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}]$. Pondo $\lambda = \varepsilon - \varepsilon^{-1}$, um cálculo imediato dá que

$$\frac{c-\bar{c}}{\lambda} = E, \qquad \frac{c\varepsilon - \bar{c}\varepsilon^{-1}}{\lambda} = C$$

$$\frac{c\varepsilon^{-1} - \bar{c}\varepsilon}{\lambda} = -C + E(\varepsilon+\varepsilon^{-1}),$$

$$\frac{d-\bar{d}}{\lambda} = F, \qquad \frac{d\varepsilon - \bar{d}\varepsilon^{-1}}{\lambda} = D,$$

$$\frac{d\varepsilon^2 - \bar{d}\varepsilon^{-2}}{\lambda} = -F + D(\varepsilon+\varepsilon^{-1}).$$

Agora, pondo

$$\ell^{-1}\, h\, \ell = w = \begin{pmatrix} x & y \\ z & v \end{pmatrix}$$

temos que

$$w = \frac{1}{\lambda}\begin{pmatrix} -1 & -1 \\ \varepsilon & \varepsilon^{-1} \end{pmatrix}\begin{pmatrix} c & d \\ \bar{d} & \bar{c} \end{pmatrix}\begin{pmatrix} \varepsilon^{-1} & 1 \\ -\varepsilon & -1 \end{pmatrix} = \begin{pmatrix} C-E(\varepsilon+\varepsilon^{-1})+D & -E+F \\ E-D(\varepsilon+\varepsilon^{-1})+F & C-D \end{pmatrix},$$

donde temos que

$$\begin{cases} x=C-E(\varepsilon+\varepsilon^{-1})+D \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}] \\ y=-E+F \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}] \\ z=E-D(\varepsilon+\varepsilon^{-1})+F \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}] \\ v=C-D \in \mathbb{Z}[\varepsilon+\varepsilon^{-1}]. \end{cases} \qquad (*)$$

Assim, $w \in M_2(\mathbb{Z}[\varepsilon+\varepsilon^{-1}])$. Além disso, notamos que $\det w = \det h \in U(\mathbb{Z}[\varepsilon])$, e que $\det h = c\bar{c} - d\bar{d} \in \mathbb{R}$, donde, pelo Lema 1.6, $\det w \in U(\mathbb{Z}[\varepsilon+\varepsilon^{-1}])$. Logo $w \in GL_2(\mathbb{Z}[\varepsilon+\varepsilon^{-1}])$.

Como $h \in H$, temos $\pi^*(h)=1 \in M_2^*(GF(p)A/B)$, de modo que $\pi(c-1)=\pi(d)=0$. Segue, então, pelo lema 1.10, que existam constantes $r,s \in GF(p)$ tais que

$$\pi(C)-1 = \pi(E) = r(\widehat{A/B}) \quad \text{e}$$
$$\pi(D) = \pi(F) = s(\widehat{A/B}),$$

já que $c-1=(C-1)-E\varepsilon^{-1}$ e $d=D-F\varepsilon^{-1}$. Assim, aplicando $\pi$ às equações (*) acima, obtemos

$$\pi(x)=\pi(C)-\pi(E)\,(\pi(\varepsilon)+\pi(\varepsilon^{-1}))+\pi(D)=1+(s-r)\,(\widehat{A/B})$$

$$\pi(y)=-\pi(E)+\pi(F)=(s-r)\,(\widehat{A/B})$$

$$\pi(v)=\pi(C)-\pi(D)=1+(r-s)\,(\widehat{A/B})$$

$$\pi(z)=\pi(E)-\pi(D)\,(\pi(\varepsilon)+\pi(\varepsilon)^{-1})+\pi(F)=(r-s)\,(\widehat{A/B}),$$

donde, pondo $k=s-r$, obtemos

$$\tilde{\pi}(w) = \begin{pmatrix} 1+k(\widehat{A/B}) & k(\widehat{A/B}) \\ -k(\widehat{A/B}) & 1-k(\widehat{A/B}) \end{pmatrix}$$

isto é,

$$\tilde{\pi}(w) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + k(\widehat{A/B}) \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} , \quad k\in GF(p).$$

Logo, $w\in W$, e portanto $\eta(H)\subset W$.

ii) Reciprocamente, seja $w=\begin{pmatrix} x & y \\ z & v \end{pmatrix}\in W$. Um cálculo imediato mostra que

$$\eta^{-1}(w)=\ell\, w\, \ell^{-1} = \begin{pmatrix} c & d \\ \bar{d} & \bar{c} \end{pmatrix} , \text{ onde}$$

$$c=\frac{1}{\lambda}\,(-x\varepsilon^{-1}-z+y+v\varepsilon)$$

$$d=\frac{1}{\lambda}\,(-x\varepsilon^{-1}-z+y\varepsilon^{-2}+v\varepsilon^{-1}).$$

Agora, como $\tilde{\pi}(w)=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + k(\widehat{A/B})\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$, temos que $\pi(y)=k(A/B)$, $\pi(x)-1-\pi(y)=0$, $\pi(z)+\pi(y)=0$ e $\pi(v)-1+\pi(y)=0$. Pelo lema 1.7, sabemos que

$$\ker(\pi\,|_{\mathbb{Z}[\varepsilon+\varepsilon^{-1}]})=(\varepsilon-\varepsilon^{-1})(\delta-\delta^{-1})\mathbb{Z}[\varepsilon+\varepsilon^{-1}]=\lambda(\delta-\delta^{-1})\mathbb{Z}[\varepsilon+\varepsilon^{-1}];$$

logo, podemos escrever

$$x=\lambda(\delta-\delta^{-1})\tilde{x}+y+1, \text{ com } \tilde{x}\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}],$$
$$z=\lambda(\delta-\delta^{-1})\tilde{z}-y \quad , \text{ com } \tilde{z}\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}],$$
$$v=\lambda(\delta-\delta^{-1})\tilde{v}-y+1, \text{ com } \tilde{v}\in\mathbb{Z}[\varepsilon+\varepsilon^{-1}].$$

Substituindo estas equações nas expressões para c e d acima, obtemos, por um cálculo direto,

$$c=\frac{1}{\lambda}(-x\varepsilon^{-1}-z+y+v\varepsilon)=(\delta-\delta^{-1})\tilde{c}+\frac{y(1-\varepsilon)(1-\varepsilon^{-1})}{\lambda}+1,$$

com $\tilde{c}\in\mathbb{Z}[\varepsilon]$, e também

$$d=\frac{1}{\lambda}(-x\varepsilon^{-1}-z+y\varepsilon^{-2}+v\varepsilon^{-1})=(\delta-\delta^{-1})\tilde{d}+\frac{y(1-\varepsilon^{-1})^2}{\lambda}$$

com $\tilde{d}\in\mathbb{Z}[\varepsilon]$.

Observamos, agora, que $\lambda=(\varepsilon-\varepsilon^{-1})=\varepsilon(1-\varepsilon^{-2})=$ $=\varepsilon(1+\varepsilon^{-1})(1-\varepsilon^{-1})$ é associado de $1-\varepsilon^{-1}$ em $\mathbb{Z}[\varepsilon]$ (já que, para $p>2$, $1+\varepsilon$ é inversível em $\mathbb{Z}[\varepsilon]$). Logo, $\frac{1-\varepsilon^{-1}}{\lambda}\in\mathbb{Z}[\varepsilon]$; analogamente, obtemos que $\frac{1-\varepsilon}{\lambda}\in\mathbb{Z}[\varepsilon]$, donde segue imediatamente que $c, d\in\mathbb{Z}[\varepsilon]$.

Além disso, como $\pi(y)=k(\widehat{A/B})$, temos que

$$\pi(y(1-\varepsilon))=k(\widehat{A/B})(1-aB)=0$$
$$\pi(y(1-\varepsilon^{-1}))=k(\widehat{A/B})(1-a^{-1}B)=0,$$

e como $(\delta-\delta^{-1})\in\ker\pi$, calculando $\pi$ nas expressões obtidas para c e d, segue

$$\pi(c)=1 \qquad \text{e} \qquad \pi(d)=0,$$

donde $\pi^*(h)=1 \in M_2^*(\mathbb{Z}[\varepsilon])$. Finalmente, como $w \in GL_2(\mathbb{Z}[\varepsilon+\varepsilon^{-1}])$, $\det h = \det w \in U(\mathbb{Z}[\varepsilon+\varepsilon^{-1}]) \subset U(\mathbb{Z}[\varepsilon])$. Logo $\eta(H) \supset W$, e o teorema está demonstrado.

Salientamos que esta descrição de $K(B)$ é bastante útil, já que a aplicação $\pi:\mathbb{Z}[\varepsilon+\varepsilon^{-1}] \to GF(p)\ A/B$, com $p>2$, é bem compreendida, devido ao Lema 1.7. Isto nos permitirá obter o resultado mais importante deste capítulo, uma descrição explícita do grupo de unidades $U(\mathbb{Z}G)$ para $G=D_p$, o grupo diedral de 2p elementos, para $p>2$. Este resultado generaliza o trabalho de I.Hughes e K.R.Pearson [Hughes e Pearson,1972], que trata do caso $p=3$, e é complementado pelo resultado de C. Polcino Milies [Polcino Milies, 1973], que estuda $U(\mathbb{Z}D_4)$.

No que segue, p denota um número primo racional, $\delta$ uma raiz p-ésima primitiva da unidade e $\pi:\mathbb{Z}[\delta] \to GF(p)$ o homomorfismo obtido no Lema 1.3, supondo sempre $n=1$. Lembramos que o núcleo deste homomorfismo é o ideal $(\delta-\delta^{-1})\mathbb{Z}[\delta]$. Dados $x, y \in \mathbb{Z}[\delta]$, escrevemos $x \equiv y(\pi)$ se e sómente se $\pi(x)=\pi(y)$.

<u>Teorema 2.10</u> - [Passman e Smith, 1981] Seja $G=D_p$, com $p>2$. Então $U(\mathbb{Z}G)$ é isomorfo ao subgrupo de $GL_2(\mathbb{Z}[\delta+\delta^{-1}])$ formado por todas as matrices $w=\begin{pmatrix} x & y \\ z & v \end{pmatrix}$ que satisfazem as condições

$$\det w \equiv \pm 1\ (\pi) \text{ e } x+z \equiv y+v \equiv \pm 1\ (\pi).$$

<u>Demonstração</u> - i) Tomando $n=1$ no Teorema 2.9, temos $A=B$,

$\widehat{A/B}=1$, e, assim, a aplicação $\eta \circ \sigma^* \circ \zeta$ dá o isomorfismo

$$K(A)=K(B)\cong W=\left\{ w\in GL_2(\mathbb{Z}[\delta+\delta^{-1}]) \;\middle|\; \exists\, k\in GF(p) \;\; tq\; \tilde{\pi}(w)=\begin{pmatrix} 1+k & k \\ -k & 1-k \end{pmatrix} \right\}$$

ii) Consideremos agora o homomorfismo natural $\psi:\mathbb{Z}G \longrightarrow \mathbb{Z}\,G/A$. Por restrição a $U(\mathbb{Z}G)$, obtemos um homomorfismo de grupos $\bar{\psi}:U(\mathbb{Z}G) \longrightarrow U(\mathbb{Z}\,G/A)$, cujo núcleo é, claramente, o subgrupo

$$\ker\bar{\psi}=U(\mathbb{Z}G)\cap(1+\ker\psi)=U(\mathbb{Z}G)\cap(1+I(A)\mathbb{Z}G)=K(A).$$

Além disso, como $G/A\cong\langle t\rangle$ tem ordem 2, o anel de grupo $\mathbb{Z}\,G/A$ só tem unidades triviais; logo, o subgrupo $\{\pm 1, \pm t\}\subset G$ é levado, por $\bar{\psi}$, sobre $U(\mathbb{Z}\,G/A)=\pm G/A$. Segue então imediatamente que $U(\mathbb{Z}G) = K(A).(\pm\langle t\rangle)$ (produto semi-direto) e que $\pm\langle t\rangle$ é uma transversal para $K(A)$ em $U(\mathbb{Z}G)$.

iii) Um cálculo imediato mostra que

$$(\eta\circ\sigma^*\circ\zeta)(-1)=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\in GL_2(\mathbb{Z}[\delta+\delta^{-1}])$$

e

$$(\eta\circ\sigma^*\circ\zeta)(t)=\begin{pmatrix} 1 & 0 \\ -(\delta+\delta^{-1}) & -1 \end{pmatrix}\in GL_2(\mathbb{Z}[\delta+\delta^{-1}]).$$

Desta forma, $(\eta\circ\sigma^*\circ\zeta)(U(\mathbb{Z}G))\subset GL_2(\mathbb{Z}[\delta+\delta^{-1}])$, e obtemos um homomorfismo de grupos

$$\eta\circ\sigma^*\circ\zeta : U(\mathbb{Z}G)\longrightarrow GL_2(\mathbb{Z}[\delta+\delta^{-1}]).$$

Vamos calcular o núcleo e a imagem deste homomorfismo .

Observamos que

$$\tilde{\pi}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \notin W$$

e

$$\tilde{\pi}\begin{pmatrix}1 & 0\\ -(\delta+\delta^{-1}) & -1\end{pmatrix} = \begin{pmatrix}1 & 0\\ -2 & -1\end{pmatrix} \notin W.$$

Segue, então, da decomposição de $U(\mathbb{Z}G)$ em classes laterais módulo $K(A)$, que, se $w \in GL_2(\mathbb{Z}[\delta+\delta^{-1}])$ pertence à imagem de $U(\mathbb{Z}G)$ por $\eta \circ \sigma^* \circ \zeta$, então $\tilde{\pi}(w)$ tem uma das quatro formas seguintes:

$$\tilde{\pi}(w) = \begin{pmatrix}1+k & k\\ -k & 1-k\end{pmatrix}, \quad k \in GF(p)$$

$$\tilde{\pi}(w) = -\begin{pmatrix}1+k & k\\ -k & 1-k\end{pmatrix}, \quad k \in GF(p)$$

$$\tilde{\pi}(w) = \begin{pmatrix}1+k & k\\ -k & 1-k\end{pmatrix}\begin{pmatrix}1 & 0\\ -2 & -1\end{pmatrix} = \begin{pmatrix}1-k & -k\\ k-2 & k-1\end{pmatrix}, k \in GF(p)$$

$$\tilde{\pi}(w) = -\begin{pmatrix}1+k & k\\ -k & 1-k\end{pmatrix}\begin{pmatrix}1 & 0\\ -2 & -1\end{pmatrix} = -\begin{pmatrix}1-k & -k\\ k-2 & k-1\end{pmatrix}, k \in GF(p),$$

formas estas que correspondem às quatro classes laterais de $U(\mathbb{Z}G)$ módulo $K(A)$. Mas então é fácil ver que $\tilde{\pi}(w)=1 \in GL_2(\mathbb{Z}[\delta+\delta^{-1}])$

só pode ocorrer se $\tilde{\pi}(w)$ tem a primeira destas quatro formas, isto é, se w pertence à imagem de K(A), que é W. Como $\eta \circ \sigma^* \circ \zeta$ é um isomorfismo de K(A) sobre W, segue que $\eta \circ \sigma^* \circ \zeta : U(\mathbb{Z}G) \longrightarrow GL_2(\mathbb{Z}[\delta+\delta^{-1}])$ é um monomorfismo, e $\ker(\eta \circ \sigma^* \circ \zeta) = \{1\}$.

Resta, agora, calcular a imagem de $U(\mathbb{Z}G)$ por $\eta \circ \sigma^* \circ \zeta$. Pelo feito acima, é imediato que

$$(\eta \circ \sigma^* \circ \zeta)(U(\mathbb{Z}G) = W. \left( \pm \left\langle \begin{pmatrix} 1 & 0 \\ -(\delta+\delta^{-1}) & -1 \end{pmatrix} \right\rangle \right)$$

(produto semi-direto). Queremos, entretanto, uma descrição melhor desta imagem.

Seja, então, $w \in (\eta \circ \sigma^* \circ \zeta)(U(\mathbb{Z}G))$; neste caso $\tilde{\pi}(w)$ pode ter a forma

$$\tilde{\pi}(w) = \pm \begin{pmatrix} 1+k & k \\ -k & 1-k \end{pmatrix},$$

em que $\det(\tilde{\pi}(w))=1$ e $\pm(1+k-k)=\pm(k+1-k)=\pm 1$, ou a forma

$$\tilde{\pi}(w) = \pm \begin{pmatrix} 1-k & -k \\ k-2 & k-1 \end{pmatrix},$$

em que $\det(\tilde{\pi}(w))=-1$ e $\pm(1-k+k-2)=\pm(-k+k-1)=\mp 1$.

Dessa forma, se $\tilde{\pi}(w) = \begin{pmatrix} r & s \\ e & f \end{pmatrix}$, valem, em qualquer caso, as equações

$$\det(\tilde{\pi}(w))=\pm 1 \quad e \quad r+e=s+f=\pm 1.$$

Observamos, agora, que, tomando todos os valores possíveis para $k \in GF(p)$, obtemos 4p valores diferentes para $\tilde{\pi}(w)$, $w \in \eta \circ \sigma^* \circ \zeta(U(\mathbb{Z}G)$. Por outro lado, é fácil verificar que o sistema de equações

$$\begin{cases} rf-se=\pm 1 \\ r+e=s+f=\pm 1 \end{cases}$$

possui, no máximo, 4p soluções (p soluções para cada escolha de sinais). Assim, para $w \in \eta \circ \sigma^* \circ \zeta\ (U(\mathbb{Z}G))$, $\tilde{\pi}(w)$ atinge <u>todas</u> as possíveis matrizes $\begin{pmatrix} r & s \\ e & f \end{pmatrix}$ que satisfazem $rf-se=\pm 1$ e $r+e=s+f=\pm 1$. Logo, a imagem de $U(\mathbb{Z}G)$ é precisamente o conjunto das matrizes $w=\begin{pmatrix} x & y \\ z & v \end{pmatrix} \in GL_2(\mathbb{Z}[\delta+\delta^{-1}])$ que satisfazem

$$\det(w) \equiv \pm 1\ (\pi) \quad \text{e} \quad x+z \equiv y+v \equiv \pm 1\ (\pi).$$

Isto completa a demonstração.

Gostaríamos de salientar que esta descrição de $U(\mathbb{Z}D_p)$ é um resultado bastante importante, inclusive porque é o primeiro resultado deste tipo com alguma generalidade, uma vez que, afora os casos triviais, só se conheciam descrições explícitas de $U(\mathbb{Z}G)$ para $G=D_3, D_4, A_4, S_4$ ([Hughes e Pearson, 1972], [Polcino Milies, 1973], [Allen e Hogby, 1980],[Sekiguchi, 1980]). Além disso, deve ser possível, a partir deste resultado, obter informações sobre a estrutura das classes de conjugação em $U(\mathbb{Z}D_p)$, um problema de bastante interesse.

## IV - COMPLEMENTOS NORMAIS

Este capítulo estuda um problema difícil e interessante relativo à estrutura do grupo das unidades de um anel de grupo: determinar condições para que exista um complemento normal livre de torção para G em $V(\mathbb{Z}G)$, isto é, para que exista um subgrupo $N \triangleleft V(\mathbb{Z}G)$, livre de torção, tal que $N \cap G = \{1\}$ e $V(\mathbb{Z}G) = N.G$. Este problema foi colocado explicitamente pela primeira vez em [D.L. Johnson, 1978]; os primeiros resultados significativos foram de K. Dennis [Dennis, 1976], [Dennis, 1977]. Este problema não apenas possui interesse intrínseco, mas também representa uma nova possibilidade de ataque ao problema do isomorfismo, como observamos a seguir:

Lema. Seja G um grupo finito. Se G tem um complemento normal livre de torção em $V(\mathbb{Z}G)$ e $\mathbb{Z}G = \mathbb{Z}H$, então $G \cong H$.

Demonstração. Seja N o complemento normal livre de torção para G em $V = V(\mathbb{Z}G)$. Então $N \triangleleft V$ e $[V:N] = |G|$. Como H é de torção, $H \cap N = \langle 1 \rangle$. Além disso, $[NH:N] = |H| = |G| = [V:N]$. Logo, $V = NH$, donde

$$G \cong \frac{V}{N} = \frac{N.H}{N} \cong H.$$

Neste capítulo, apresentamos alguns resultados sobre este problema, dando resposta afirmativa quanto à existência de complementos normais livres de torção em três casos:

1) G é grupo círculo nilpotente;

2) G possui um subgrupo normal abeliano A, tal que G/A é abeliano de expoente 2,3,4 ou 6;

3) G possui um subgrupo normal abeliano A, tal que G/A é abeliano de ordem ímpar.

Observamos que os grupos dos casos 2 e 3 são metabelianos, de modo que já se sabia que são solução do problema do isomorfismo, e que o caso 1 se inclui nos que foram estudados em [Sandling, 1974]. Dessa forma, nossos resultados não representam avanço em relação ao problema do isomorfismo, embora sejam extremamente importantes em relação ao estudo da estrutura do grupo das unidades. Em todos os casos, a obtenção de um complemento normal é bastante fácil, ao passo que a demonstração de que este complemento é livre de torção apresenta grande dificuldade. Trataremos primeiro do caso 1, e depois, simultaneamente, dos casos 2 e 3.

Deve-se mencionar que muitos autores têm estudado este problema em situações específicas. Em particular, P.J.Allen e C.Hogby mostraram que existe um complemento se $G=A_4$, K.Sekiguchi fez o mesmo para $G=S_4$ e T. Miyata estudou os grupos diedrais em geral. Veja-se [Allen e Hogby, 1980 ], [Sekiguchi, 1980] , [Miyata, 1980] e o "survey" [Polcino Milies, 1981] .

## § 1. GRUPOS CÍRCULO NILPOTENTES.

Neste parágrafo, mostraremos, seguindo [Passman e Smith, 1980], que, se G é um grupo círculo nilpotente, então existe complemento normal livre de torção para G em $V(\mathbb{Z}G)$. Começamos com a definição básica.

Definição. Seja R um anel com 1 finito, e seja I um ideal de R tal que todo elemento da forma $1+i$, com $i \in I$ seja inversível em R. Nestas condições, o conjunto $1+I = \{1+i \mid i \in I\}$ é um grupo multiplicativo. Dizemos que G é o grupo círculo do ideal I se e sómente se G é isomorfo ao grupo multiplicativo $1+I$.

É imediato verificar que, nas condições da definição, G é um grupo finito. Observamos ainda que, se definirmos, para $i_1, i_2 \in I$,

$$i_1 \circ i_2 = i_1 + i_2 + i_1 i_2,$$

temos que:

$$(1+i_1)(1+i_2) = 1+i_1+i_2+i_1 i_2 = 1+i_1 \circ i_2$$

de modo que G é também isomorfo ao grupo cujos elementos são os do ideal I e cuja operação é o produto $\circ$. Observamos ainda que, se I é um ideal nilpotente, todo elemento da forma $1+i$ com $i \in I$ é inversível em R, e que, neste caso, se G é grupo círculo de I, então G é um grupo nilpotente (veja-se [Singer, 1978, Corol. I.4.6]). Com isto, já podemos provar nosso resultado sobre este caso.

<u>Teorema 1.1</u> - ([ Passman e Smith, 1981 ]). Seja I um ideal nilpotente de um anel com 1 finito R, e seja $G \cong 1+I$ o seu grupo círculo. Então G possui complemento normal livre de torção em $V(\mathbb{Z}G)$.

<u>Demonstração</u>. Seja $V=V(\mathbb{Z}G)$, e seja $\Theta: G \to 1+I$ o isomorfismo dado.

Como $\Theta$ é um isomorfismo de grupos multiplicativos, podemos estender $\Theta$ a um homomorfismo de anéis

$$\Theta: \mathbb{Z}G \longrightarrow R,$$

e pomos $N = \{\alpha \in V \mid \Theta(\alpha)=1\}$, de modo que N é o núcleo de $\Theta|_V$, donde $N \triangleleft V$. Além disso, como $\Theta|_G$ é, por hipótese, um isomorfismo, temos que $N \cap G = \langle 1 \rangle$.

Para cada $g \in G$, ponhamos $\Theta(g)=1+i_g, i_g \in I$. Suponhamos que $\alpha = \sum_{g \in G} \alpha(g) g \in V$. Como $\alpha \in V$, temos que $\sum_{g \in G} \alpha(g)=1$. Então

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

$$= \sum_{g \in G} \alpha(g)(1+i_g) = \sum_{g \in G} \alpha(g) + \sum_{g \in G} \alpha(g)\ i_g =$$

$$= 1 + \sum_{g \in G} \alpha(g) i_g = 1 + i,$$

onde $i = \sum_{g \in G} \alpha(g) i_g \in I$, já que I é ideal de R. Assim, como $G \cong_{\Theta} 1+I$, existe $x \in G$ tal que $\Theta(\alpha)=\Theta(x)$, donde segue que

$\alpha x^{-1} \in N$, e portanto $\alpha \in NG$.

Assim, mostramos que se $\alpha \in V$, então $\alpha \in NG$. Logo $V=NG$, e já vimos que $N \triangleleft V$ e $N \cap G = \langle 1 \rangle$, isto é, $N$ é um complemento normal para $G$ em $V$.

Resta mostrar que $N$ é livre de torção. Fá-lo-emos por indução em $|G| = |I|$; observamos que o resultado é trivial quando $|I| = 1$, isto é, quando $I=0$.

Suponhamos, então, que $I \neq 0$; como $I$ é, por hipótese, um ideal nilpotente, existe $k \in \mathbb{N}$ tal que $I^k \neq 0$ e $I^{k+1}=0$. Seja $J=I^k \neq 0$, e seja $\sigma: R \to R/J$ o epimorfismo canônico. Consideramos a sequência de homomorfismos de grupos multiplicativos

$$G \underset{\cong}{\xrightarrow{\Theta}} 1+I \xrightarrow{\sigma} 1+\sigma(I),$$

e observamos que o núcleo de $\sigma|_{1+I}$ é $1+J$, e que, como $IJ=JI=0$, $1+J$ é <u>central</u> em $1+I$. Portanto, $W=\ker(\sigma \circ \Theta) = \Theta^{-1}(1+J)$ é <u>central</u> em $G$.

Seja, agora $\tau: G \to G/W$ o epimorfismo natural. Pelo Teorema do Homomorfismo, existe $\psi$ tal que

$$G/W = G/\ker(\sigma \circ \Theta) \underset{\psi}{\cong} \mathrm{Im}(\sigma \circ \Theta) = 1+\sigma(I);$$

logo, existe um isomorfismo $\psi$ fazendo comutativo o diagrama:

$$\begin{tikzcd} G \arrow[r, "\Theta"] \arrow[d, "\tau"'] & 1+I \arrow[d, "\sigma"] \\ G/W \arrow[r, "\psi"'] & 1+\sigma(I). \end{tikzcd}$$

Em particular, como $G/W \cong 1+\sigma(I)$, temos que $G/W$ é o grupo círculo do ideal nilpotente $\sigma(I)$ do anel $\sigma(R)$, e, como $J \neq 0$, temos que $|\sigma(I)| < |I|$. Por hipótese de indução, o teorema vale neste caso.

Além disso, as aplicações acima se estendem para homomorfismos de anéis, dando o diagrama comutativo

$$\begin{tikzcd} \mathbb{Z}G \arrow[r, "\Theta"] \arrow[d, "\tau"'] & R \arrow[d, "\sigma"] \\ \mathbb{Z}\,G/W \arrow[r, "\psi"'] & \sigma(R)=R/J. \end{tikzcd}$$

Vamos, então, mostrar que $N$ é livre de torção. Seja $\alpha \in N$ de ordem finita. Pela definição de $N$, $\Theta(\alpha)=1$, donde $(\psi \circ \tau)(\alpha)=(\sigma \circ \Theta)(\alpha)=1$. Além disso, como $\alpha$ é unidade normalizada de ordem finita de $\mathbb{Z}G$, $\tau(\alpha)$ é unidade normalizada de ordem finita de $\mathbb{Z}\,G/W$. Logo, $\tau(\alpha)$ é um elemento de ordem finita de

$$N' = \{\beta \in V(\mathbb{Z}\,G/W) \mid \psi(\beta)=1\}.$$

Pela hipótese de indução, $N'$ é livre de torção, donde $\tau(\alpha)=1$.

Logo, $\alpha \in 1+\ker\tau = 1+I(W)\mathbb{Z}G$, donde, pelo Corolário I.2.6, segue que $\alpha = x \in W \subset G$. Mas $\alpha \in N$, e já provamos que $N \cap G = \langle 1 \rangle$; logo $\alpha=1$. Assim, $N$ é livre de torção, e o teorema está provado.

É interessante observar que todo p-grupo finito $G$ está contido em um p-grupo círculo nilpotente, já que

$I(\frac{\mathbb{Z}}{p\mathbb{Z}}G)$ é nilpotente [Sehgal, 1978, I.2.21] e $G \subset 1+I(\frac{\mathbb{Z}}{p\mathbb{Z}}G)$.

## § 2. GRUPOS METABELIANOS: EXISTÊNCIA DE COMPLEMENTO.

Passamos, agora, a estudar os casos (2) e (3) da introdução. No caso (2), obteremos explicitamente, com certa facilidade, uma família de complementos normais. No caso (3), provaremos apenas a existência de um complemento normal; este caso é bem mais difícil. Deixaremos para os parágrafos seguintes a prova de que estes complementos são livres de torção. Estes parágrafos seguem o trabalho [Cliff, Sehgal e Weiss, 1980]. No que segue, G denota sempre um grupo finito, A um subgrupo normal abeliano de G, e supomos sempre que G/A é abeliano.

Seja T uma transversal para A em G. Neste caso, $\mathbb{Z}G\,I(A)$, considerado como grupo aditivo, é um grupo abeliano livre, de base $B = \{x(a-1) \mid x \in T,\ a \in A,\ a \neq 1\}$. Logo, dado $k \in \mathbb{Z}$ qualquer, podemos definir um homomorfismo de grupos abelianos $\Phi_k : \mathbb{Z}G\,I(A) \longrightarrow A$ definindo $\Phi_k$ para elementos $x(a-1) \in B$, por $\Phi_k(x(a-1)) = a^{x^k} = x^{-k}\,a\,x^k$.

Definição. Na situação acima, definimos

$$I_k = I_k(G, A) = \ker \Phi_k .$$

Lema 2.1 . Com as definições acima, valem as seguintes afirmações:

a) $\forall g \in G$, $\forall a \in A$, $\Phi_k(g(a-1)) = a^{g^k} = g^{-k}\, a\, g^k$;

b) $I_k$ é um ideal bilateral de $\mathbb{Z}G$, que satisfaz $\mathbb{Z}G\, I(A)^2 \subset I_k \subset \mathbb{Z}G\, I(A)$. Além disso, $I_o = I(G)\ I(A)$;

c) $\forall \delta \in \mathbb{Z}G\, I(A)$, $\exists a \in A$ tal que $\delta \equiv a-1 \pmod{I_k}$;

d) $(1+I_k) \cap G = \{1\}$;

e) $I_k^* = I_{-k-1}$, onde * denota a involução natural de $\mathbb{Z}G$.

<u>Demonstração</u>.

a) Como T é uma transversal, todo elemento $g \in G$ pode ser escrito como $g = xb$, $x \in T$, $b \in A$.

Observando que

$xb(a-1) = x(ba-1) - x(b-1)$, $\forall x \in T$, $\forall a, b \in A$, segue:

$$\Phi_k(xb(a-1)) = (ba)^{x^k}(b^{-1})^{x^k} = (bab^{-1})^{x^k} = a^{x^k} = a^{(xb)^k},$$

já que, como A é normal abeliano, $a^{(xb)^k} = (xb)^{-k}\, a\, (xb)^k = b^{-k}\, x^{-k} a\, x^k\, b^k = x^{-k}\, a\, x^k = a^{x^k}$, provando a afirmação.

b) Vamos provar que, dado $g \in G$ e $\delta \in \mathbb{Z}G\, I(A)$, valem as identidades

$$\Phi_k(g\delta) = \Phi_k(\delta)^{g^k} \quad \text{e} \quad \Phi_k(\delta g) = \Phi_k(\delta)^{g^{k+1}},$$

donde segue imediatamente que $I_k$ é um ideal de $\mathbb{Z}G$.

De fato, basta verificar as identidades acima para $\delta = h(a-1)$, com $h \in G$ e $a \in A$. Mas então

$$\Phi_k(g.h(a-1))=a^{(gh)^k}=(a^{h^k})^{g^k}=\Phi_k(h(a-1))^{g^k},$$ pois $G/A$ é abeliano. Analogamente,

$$\Phi_k(h(a-1)g)=\Phi_k(hg(a^g-1))=(a^g)^{(hg)^k}=$$

$$=a^{h^k g^{k+1}}=\Phi_k(h(a-1))^{g^{k+1}}.$$

Dessa forma, $I_k$ é um ideal de $\mathbb{Z}G$, e já sabemos, pela definição, que $I_k \subset \mathbb{Z}G\, I(A)$.

Observamos, agora, que, dados $a,b \in A$, temos

$$\Phi_k((a-1)(b-1))=\Phi_k((ab-1)-(a-1)-(b-1))=ab.a^{-1}.b^{-1}=1,$$

donde segue que $I(A)^2 \subset I_k$ e, como $I_k$ é ideal, concluímos que $\mathbb{Z}G\, I(A)^2 \subset I_k \subset \mathbb{Z}G\, I(A)$.

Para provar que $I_o = I(G)\, I(A)$, notemos, em primeiro lugar, que, dados $g \in G$, $a \in A$, temos

$$\Phi_o((g-1)(a-1))=\Phi_o(g(a-1)-(a-1))=a^{g^o}.a^{-1}=1,$$

de modo que $I(G)\ I(A) \subset I_o$. Finalmente, se $\delta \in I_o$, pelo lema I.3.9, podemos escrever $\delta = \sum_{x \in T} x(a_x-1)+\alpha$ , $\alpha \in \mathbb{Z}G\, I(A)^2 \subset I_o$, de modo que $\sum_{x \in T} x(a_x-1) \in I_o$, donde $1=\Phi_o(\sum_{x \in T} x(a_x-1))=\prod_{x \in T} a_x$.

Agora, observamos que

$$\sum_{x \in T} x(a_x-1)=\sum_{x \in T}(x-1)(a_x-1)+\sum_{x \in T}(a_x-1).$$

Pelo Corolário I.3.6,

$$\sum_{x \in T}(a_x-1) \equiv \prod_{x \in T} a_x - 1 \pmod{I(A)^2},$$

mas como $\prod_{x\in T} a_x=1$, segue que $\sum_{x\in T}(a_x-1)\in I(A)^2$, donde

$$\delta\equiv\sum_{x\in T}(x-1)(a_x-1)\pmod{\mathbb{Z}G\,I(A)^2}.$$

Assim, como $\mathbb{Z}G\,I(A)^2\subset I(G)I(A)$ e $\sum_{x\in T}(x-1)(a_x-1)\in I(G)I(A)$, segue que $\delta\in I(G)I(A)$, donde $I_o=I(G)I(A)$, provando a afirmação (b).

c) Dado $\delta\in\mathbb{Z}G\,I(A)$, temos que $\Phi_k(\delta)\in A$. Logo,

$$\Phi_k(\Phi_k(\delta)-1)=\Phi_k(\delta),$$

e, pondo $a=\Phi_k(\delta)\in A$, segue imediatamente que

$$\delta\equiv a-1\pmod{I_k}.$$

d) Seja $\delta\in I_k$ com $1+\delta=g\in G$. Então $g-1=\delta\in\mathbb{Z}G\,I(A)$, donde $g\in G\cap(1+\mathbb{Z}G\,I(A))=A$, isto é, $g=a\in A$. Logo, $\delta=a-1$, e $1=\Phi_k(\delta)=\Phi_k(a-1)=a$. Assim,

$$(1+I_k)\cap G=\{1\}.$$

e) Vamos provar que, para $\delta\in\mathbb{Z}G\,I(A)$,

$$\Phi_k(\delta^*)=\Phi_{-k-1}(\delta)^*,$$

donde segue imediatamente que $I_k^*=I_{-k-1}$. É claro que basta verificar esta equação para $\delta=g(a-1)$, com $g\in G$, $a\in A$.

Como $(g(a-1))^*=(a^{-1}-1)g^{-1}=g^{-1}(a^{-1^{(g^{-1})}}-1)$, temos que

$$\Phi_k((g(a-1))^*)=\Phi_k(g^{-1}(a^{-1^{(g^{-1})}}-1))=(a^{-1})^{g^{-k-1}}=$$

$$=(a^{g^{-k-1}})^*=(\Phi_{-k-1}(g(a-1)))^*,$$

e a afirmação (e) está provada.

Nosso primeiro resultado significativo é agora imediato.

<u>Proposição 2.2</u> - ([Cliff, Sehgal e Weiss, 1980]). Com as notações acima, se $\mathbb{Z}G/A$ só tem unidades triviais, então, para todo inteiro k, o subgrupo $N_k = V(\mathbb{Z}G) \cap (1+I_k)$ é um complemento normal para G em $V(\mathbb{Z}G)$.

<u>Demonstração</u>. Seja $\pi_A : \mathbb{Z}G \longrightarrow \mathbb{Z}G/A$ a aplicação natural; dado $\alpha \in \mathbb{Z}G$, escrevemos $\bar{\alpha} = \pi_A(\alpha)$. Dado $u \in V(\mathbb{Z}G)$, temos $\bar{u} \in V(\mathbb{Z}G/A)$, donde, por hipótese, $\bar{u} = \bar{g}$ para algum $g \in G$. Como o núcleo do homomorfismo de grupos $\pi_A \big|_{V(\mathbb{Z}G)}$ é $V(\mathbb{Z}G) \cap (1+\mathbb{Z}G\, I(A))$, existe $\delta \in \mathbb{Z}G\, I(A)$ tal que $u = g(1+\delta)$.

Pelo Lema 2.1(c), existe $a \in A$ tal que $\delta \equiv a-1 \pmod{I_k}$. Logo, $1+\delta \equiv a \pmod{I_k}$, donde existe $\delta_1 \in I_k$ tal que $1+\delta = a+\delta_1 = a(1+a^{-1}\delta_1)$, e, como $I_k$ é ideal, temos que $\delta' = a^{-1}\delta_1 \in I_k$ e $1+\delta = a(1+\delta')$. Logo, $u = ga(1+\delta')$, donde $V(\mathbb{Z}G) = G.N_k$, já que, como $u \in V(\mathbb{Z}G)$, $1+\delta' \in V(\mathbb{Z}G) \cap (1+I_k) = N_k$.

Finalmente, pelo Lema 2.1 (d),

$$N_k \cap G = V(\mathbb{Z}G) \cap (1+I_k) \cap G = \{1\} ,$$

donde $N_k$ é um complemento normal para G em $V(\mathbb{Z}G)$.

Vale a pena observar que D.S.Passman e P.F. Smith obtiveram um resultado que é um caso particular (para k=0) desta proposição [Passman e Smith, 1981, Lema 1.9].

A seguir, apresentamos dois exemplos; o primeiro mostra que existem grupos para os quais não existe complemento normal N para G em $V(\mathbb{Z}G)$ satisfazendo a equação $N \supset V(\mathbb{Z}G) \cap (1+I_o)$, e o segundo, que existem grupos para os quais não existe N satisfazendo $N \supset V(\mathbb{Z}G) \cap (1+I_k)$, qualquer que seja $k \in \mathbb{Z}$.

<u>Exemplo 2.3</u> - Sejam $G = \langle a,x \mid a^{11} = x^5 = 1,\ x^{-1}a\,x = a^3 \rangle$ e $A = \langle a \rangle$, de modo que A é abeliano e G/A é abeliano de ordem 5. Neste caso, não existe complemento normal N para G em $V(\mathbb{Z}G)$ contendo $V(\mathbb{Z}G) \cap (1+I_o)$.

De fato, seja $u = -1+x+x^{-1}$; então $u \in V(\mathbb{Z}G)$ e $u^{-1} = -1+x^2+x^{-2}$. Suponhamos que exista N nas condições acima. Podemos então escrever $u = ng$, com $n \in N$ e $g \in G$. Segue então que $a^u (a^g)^{-1} = u^{-1} a\, u (g^{-1} a\, g)^{-1} = g^{-1} n^{-1} a\, n\, g\, g^{-1} a^{-1} g = g^{-1}(n.a\,n\,a^{-1}) g \in N$, ou seja, que $a^u \equiv a^g \pmod N$. Um cálculo imediato mostra que $\Phi_o(au - ua^6) = 1$, de modo que $au \equiv ua^6 \pmod{I_o}$. Então $au - ua^6 \in I_o$, donde $u^{-1} a\, u - a^6 \in I_o$; logo $a^u . a^{-6} \in 1+I_o$, e portanto $a^u \equiv a^6 \pmod N$. Como já sabiamos que $a^u \equiv a^g \pmod N$, segue que $a^g \equiv a^6 \pmod N$. Vamos mostrar que isto é impossível.

De fato, se $a^g a^{-6} \in N$, então $a^g a^{-6} \in N \cap G = \{1\}$. Logo, devemos ter $a^g = a^6$, o que contradiz a definição de G. Veremos adiante que existe, neste caso, um complemento normal N satisfazendo $N \supset V(\mathbb{Z}G) \cap (1+I_2)$.

<u>Exemplo 2.4</u> - Sejam $G = \langle a,x \mid a^{41} = x^8 = 1,\ a^x = a^3 \rangle$ e $A = \langle a \rangle$, de

modo que A é um subgrupo abeliano normal e G/A é cíclico de ordem 8. Neste caso, não existe complemento normal N para G em $V(\mathbb{Z}G)$ contendo $V(\mathbb{Z}G)\cap(1+I_k)$ para nenhum $k\in\mathbb{Z}$.

Seja $u=-1-(x+x^{-1})+2x^4+(x^3+x^{-3})\in V(\mathbb{Z}G)$, com $u^{-1}=-1+(x+x^{-1})+2x^4-(x^3+x^{-3})$, e suponhamos que existe um complemento normal N, $N\supset V(\mathbb{Z}G)\cap(1+I_k)$. Novamente, podemos escrever $u=ng$, $n\in N$, $g\in G$, e, como antes, temos que $a^u\equiv a^g \pmod N$.

Vamos calcular $a^u \pmod N$. Para isso, notemos que

$$\begin{aligned} au &= -a-ax-ax^{-1}+2ax^4+ax^3+ax^{-3} \\ &= -a-xa^3-x^{-1}a^{-27}+2x^4a^{-1}+x^3a^{27}+x^3a^{-3}, \end{aligned}$$

de modo que

$$\begin{aligned} au-ua^4 &= a(a^3-1)+xa^3(a-1)+x^{-1}a^{-27}(a^{31}-1)+ \\ &-2x^4a^{-1}(a^5-1)-x^3a^{27}(a^{-23}-1)-x^{-3}a^{-3}(a^7-1), \end{aligned}$$

donde segue, por um cálculo direto, que

$$\Phi_k(au-ua^4)=1 \quad \text{se} \quad k\equiv 0,3,5,6 \pmod 8.$$

Analogamente, obtemos que

$$\Phi_k(au-ua^{-10})=1 \text{ se } k\equiv 1,2,4,7 \pmod 8.$$

Logo, como antes, obtemos que

$$a^u\equiv a^4 \pmod{N_k} \text{ se } k\equiv 0,3,5,6 \pmod 8$$

e

$$a^u\equiv a^{-10} \pmod{N_k} \text{ se } k\equiv 1,2,4,7 \pmod 8,$$

e, como antes, obteríamos que $a^g=a^4$ em um caso e $a^g=a^{-10}$

no outro; entretanto, ambas estas igualdades são impossíveis, dada a estrutura do grupo. Logo, não existe o complemento normal desejado, para nenhum valor de $k \in \mathbb{Z}$.

O Exemplo 2.4 mostra que o problema da obtenção de complemento normais para G em $V(\mathbb{Z}G)$ deve, no caso em que $|G/A|$ é par, ser tratado de forma diferente da exposta aqui, já que todos os complementos normais que obteremos satisfazem $N \supset V \cap (1+I_k)$ para algum $h \in \mathbb{Z}$. Este problema permanece em aberto.

No que segue, suporemos sempre que $[G:A]$ é ímpar, e fixamos $s=\frac{1}{2}([G:A]-1)$. Observamos que isto implica em que $s \equiv -s-1 \pmod{[G:A]}$, donde $\Phi_s=\Phi_{-s-1}$, $I_s=I_{-s-1}$ e, pelo Lema 2.1(e), $I_s^*=I_s$.

<u>Lema 2.5</u> - Dados $g,h \in G$, temos

$$g^{-1}(h+h^{-1})g \equiv h+h^{-1} \pmod{I_s}.$$

<u>Demonstração</u> - Temos que

$$\begin{aligned} g^{-1}(h+h^{-1})g-(h+h^{-1}) &= (h^g-h)+(h^{-1^g}-h^{-1}) = \\ &= h(h^{-1}h^g-1)+h^{-1}(hh^{-1^g}-1) = \\ &= h([h,g]-1)+h^{-1}([h,g]^{-1}-1). \end{aligned}$$

Como G/A é abeliano, segue que $G' \subset A$; logo, podemos aplicar $\Phi_s$ a esta última expressão, obtendo

$$\Phi_s[g^{-1}(h+h^{-1})g-(h+h^{-1})] = [h,g]^{h^s}.[h,g]^{-1^{h^{-s}}} =$$

$$= [h,g]^{h^s}(hh^{-1^g})^{h^{-s}} = h^{-s}[h,g]h^s h^s(hh^{-1^g})h^{-s} =$$

$$= h^{-s}[h,g]h^{2s+1}h^{-1^g}h^{-s}.$$

Como $[h,g] \in A$ e $h^{2s+1} \in A$ (pois $[G:A] = 2s+1$), estes elementos comutam. Logo, obtemos

$$\Phi_s(g^{-1}(h+h^{-1})g-(h+h^{-1}) = h^{-s}h^{2s+1}[h,g]h^{-1}{}^{g}h^{-s} =$$
$$= h^{s+1}(h^{-1}g^{-1}hgg^{-1}h^{-1}g)h^{-s} = h^{s+1}h^{-s-1} = 1,$$

e o lema está provado.

Como $I_s$ é um ideal de $\mathbb{Z}G$, podemos considerar o anel quociente $\frac{\mathbb{Z}G}{I_s}$. O próximo lema resume as propriedades significativas deste anel.

<u>Lema 2.6</u> - Sejam G e A como acima, e seja $\pi_A : \mathbb{Z}G \longrightarrow \mathbb{Z}\,G/A$ o epimorfismo natural. Então:

a) Se $\psi : \mathbb{Z}G \longrightarrow \mathbb{Z}G/I_s$ denota a projeção no quociente, então $\pi_A$ se fatora por $\mathbb{Z}G/I_s$, isto é, existe um epimorfismo $\Psi : \mathbb{Z}G/I_s \longrightarrow \mathbb{Z}\,G/A$ satisfazendo $\Psi \circ \psi = \pi_A$;

b) O anel $\mathbb{Z}G/I_s$ admite uma involução induzida por *;

c) O anel $\mathbb{Z}G/I_s$ admite um homomorfismo (de aumento), induzido pelo homomorfismo de aumento de $\mathbb{Z}G$;

d) A restrição $\psi|_G : G \longrightarrow U(\mathbb{Z}G/I_s)$ é um momomorfismo.

<u>Demonstração</u> - Temos o diagrama abaixo.

$$\begin{tikzcd}
\mathbb{Z}G \arrow[r, "\pi_A"] \arrow[d, "\psi"'] & \mathbb{Z}\,G/A \\
\mathbb{Z}\,G/I_s \arrow[ur, dashed, "\Psi"'] &
\end{tikzcd}$$

Como $\ker \pi_A = \mathbb{Z}G\, I(A) \supset I_s = \ker\psi$, é imediato que existe $\Psi$ tornando comutativo o diagrama (provando (a)).

Para definir uma involução em $\mathbb{Z}G/I_s$, observamos que $I_s^* = I_s$ e, dado $\alpha \in \mathbb{Z}G$, definimos

$$(\alpha + I_s)^* = \alpha^* + I_s.$$

Como $I_s^* = I_s$, esta definição independe do representante, e é imediato que $*: \frac{\mathbb{Z}G}{I_s} \longrightarrow \frac{\mathbb{Z}G}{I_s}$ é involução, provando (b).

Observamos, ainda, que os homomorfismos $\pi_A, \psi$ e $\Psi$ respeitam as involuções de $\mathbb{Z}G$, $\mathbb{Z}G/I_s$ e $\mathbb{Z}G/A$.

Como $I_s \subset \mathbb{Z}G\, I(A) \subset I(G)$, a aplicação de aumento $\varepsilon: \mathbb{Z}G \longrightarrow \mathbb{Z}$, cujo núcleo é $I(G)$, pode ser fatorado por $\mathbb{Z}G/I_s$. Obtemos assim um diagrama comutativo.

$$\begin{tikzcd} \mathbb{Z}G \arrow[r, "\varepsilon"] \arrow[d, "\psi"'] & \mathbb{Z} \\ \mathbb{Z}G/I_s \arrow[ur, dashed, "\bar{\varepsilon}"'] & \end{tikzcd}$$

O homomorfismo $\bar{\varepsilon}: \mathbb{Z}G/I_s \longrightarrow \mathbb{Z}$ é uma função de aumento para $\mathbb{Z}G/I_s$. Chamaremos de $U(\mathbb{Z}G/I_s)$ o grupo de unidades de $\mathbb{Z}G/I_s$, e pomos

$$V\left(\frac{\mathbb{Z}G}{I_s}\right) = U\left(\frac{\mathbb{Z}G}{I_s}\right) \cap (1 + \ker \bar{\varepsilon}),$$

de modo que $V(\mathbb{Z}G/I_s)$ é o grupo de unidades normalizadas de $\mathbb{Z}G/I_s$.

Finalmente, como $G \cap (1 + I_s) = \{1\}$, pelo Lema 2.1(d),

$\psi|G$ é um monomorfismo, e o lema está provado.

No que segue, identificamos G com sua imagem em $\mathbb{Z}G/I_s$. Dado $u \in V(\mathbb{Z}G/I_s)$, pomos $\bar{u}=\Psi(u) \in V(\mathbb{Z}G/A)$. Vamos, agora, obter um complemento normal para G em $V(\mathbb{Z}G/I_s)$, a partir do qual será relativamente fácil obter um complemento normal em $V(\mathbb{Z}G)$. Como G/A é abeliano, começamos com um lema que resume as propriedades básicas dos grupos de unidades de anéis de grupo de grupos abelianos.

<u>Lema 2.7</u> - Seja X um grupo abeliano finito. Então valem:

a) $V(\mathbb{Z}X) = X \times (V(\mathbb{Z}X) \cap (1+I(X)^2))$, produto direto;

b) $V(\mathbb{Z}X)$ é um grupo abeliano finitamente gerado;

c) $V(\mathbb{Z}X) \cap (1+I(X)^2)$ é um grupo abeliano livre;

d) Se $u \in V(\mathbb{Z}X) \cap (1+I(X)^2)$, então $u^*=u$.

<u>Demonstração</u> - Dado $u \in V(\mathbb{Z}X)$, $u-1 \in I(X)$, e, pelo Corolário I.3.6, existe $a \in X$ tal que $u-1 \equiv a-1 \pmod{I(X)^2}$, donde $u \equiv a \pmod{I(X)^2}$. Logo, existe $\alpha \in I(X)^2$ tal que $ua^{-1}=1+\alpha$, e portanto $u=a.(1+\alpha)$. Ainda pelo Corolário I.3.6, $X \cap (1+I(X)^2)=\{1\}$. Logo

$$V(\mathbb{Z}X) = X \times [V(\mathbb{Z}X) \cap (1+I(X)^2)],$$

provando o ítem (a).

Os ítens (b) e (c) seguem imediatamente de[Sehgal, 1978, Theorem II.3.1]. Para provar (d), consideramos

$u \in V(\mathbb{Z}X)$, e $v=u^*u^{-1}$, de modo que $v^*v=(u^{-1})^*u\ u^*\ u^{-1} = 1$, já que X é abeliano. Queremos provar que $v=1$.

Escrevendo $v = \sum_{x \in X} v(x)x$, com $v(x) \in \mathbb{Z}$, observamos que $v^* = \sum_{x \in X} v(x)x^{-1}$, de modo que o coeficiente de 1 em $v^*v$ é $\sum_{x \in X} v(x)^2$. Como $v^*v=1$, obtemos que $\sum_{x \in X} v(x)^2=1$, donde $v=\pm x$ para algum $x \in X$, e, como v é unidade normalizada, obtemos $v=x$, donde $u^*=ux$. Agora, se $u \in 1+I(X)^2$, temos $u \equiv 1 \pmod{I(X)^2}$; logo, $u^* \equiv 1 \pmod{I(X)^2}$. Logo, $u^*u^{-1}=x \equiv 1 \pmod{I(X)^2}$, portanto $x \in X \cap (1+I(X)^2)=\{1\}$. Assim, $x=1$, donde $u=u^*$, e o lema está demonstrado.

Podemos, agora, provar nosso primeiro resultado importante para este caso. Começamos com dois lemas.

<u>Lema 2.8</u> - Seja $\bar{G} = G/A$; dado $\alpha \in \mathbb{Z}\,G/I_s$, escrevemos $\bar{\alpha}=\Psi(\alpha) \in \mathbb{Z}\,G/A=\mathbb{Z}\,\bar{G}$. Definimos

$$V' =\{u \in V(\frac{\mathbb{Z}G}{I_s}) \mid u^*=u \quad e \quad \bar{u} \equiv 1 \pmod{I(\bar{G})^2}\}.$$

Então V' é um subgrupo de $V(\mathbb{Z}G/I_s)$.

<u>Demonstração</u> - Definimos

$$W=\{u \in V(\frac{\mathbb{Z}G}{I_s}) \mid \bar{u} \equiv 1 \pmod{I(\bar{G})^2}\}.$$

É imediato que W é um subgrupo de $V(\mathbb{Z}G/I_s)$ que contém V'.

a) <u>W é abeliano</u>: Dado $u \in W$, temos, pelo Lema 2.7 (d), que $\bar{u}^* = \bar{u}$, de modo que, escrevendo $\bar{u} = \sum_{x \in \bar{G}} u(x)x$, devemos ter $u(x^{-1}) = u(x)$, $\forall x \in \bar{G}$.

Como $[G:A] = |\bar{G}|$ é ímpar, podemos escolher uma transversal T para A em G tal que toda vez que $g \in T$, tem-se também $g^{-1} \in T$.

Definimos $v = \sum_{g \in T} u(\bar{g})g \in \mathbb{Z}G/I_s$. É imediato que v satisfaz $v^* = v$. Como, $\forall x \in \bar{G}$, $u(x) = u(x^{-1})$, v pode ser escrito como uma combinação $\mathbb{Z}$-linear de 1 e termos da forma $g + g^{-1}$. Como G é um conjunto gerador de $\mathbb{Z}G/I_s$, segue, pelo Lema 2.5, que $g + g^{-1}$ é central em $\mathbb{Z}G/I_s$, $\forall g \in G$; logo, v é central em $V(\mathbb{Z}G/I_s)$.

Pela definição de v, temos que $\bar{v} = \bar{u}$, donde existe $\alpha \in \mathbb{Z}G\,I(A)$ satisfazendo $v = u + \alpha$. Pondo, então, $\beta = u^{-1}\alpha \in \mathbb{Z}G\,I(A)$, obtemos $v = u(1+\beta)$, $\beta \in \mathbb{Z}G\,I(A)$. Agora, pelo Lema 2.1(c), existe $b \in A$ tal que $\delta \equiv b - 1 \pmod{I_s}$. Logo, em $\mathbb{Z}G/I_s$, $v = ub$, donde $u = vb^{-1}$.

Assim, todo elemento $u \in W$ pode ser escrito na forma $u = va$, com v <u>central</u> em $\mathbb{Z}G/I_s$ e $a \in A$. Como A é abeliano, segue imediatamente que W é abeliano.

b) <u>V' é subgrupo de W</u>: Basta provar que, se $v_1^* = v_1$ e $v_2^* = v_2$, então $(v_1, v_2)^* = v_1 v_2$. Mas como $V' \subset W$ e W é abeliano, isto é imediato, e o lema está provado.

<u>Lema 2.9</u> - Com as notações do lema anterior, temos que $V' \triangleleft V(\mathbb{Z}G/I_s)$ e $V(\mathbb{Z}G/I_s)=V'.G$.

<u>Demonstração</u> - Tomemos $u' \in V(\mathbb{Z}G/I_s)$ e consideremos sua imagem $\bar{u}' \in V(\mathbb{Z}\bar{G})$. Como $\bar{G}$ é abeliano, podemos, pelo lema 2.7(a), escrever $\bar{u}'=\bar{g}(1+\alpha)$, com $\alpha \in I(\bar{G})^2$, donde $\bar{u}'-\bar{g} = \bar{g}\alpha \in I(\bar{G})^2$; logo, segue que $\bar{u} \equiv \bar{g} \pmod{I(\bar{G})^2}$, para algum $g \in G$. Pondo, então, $u=u'g^{-1}$, temos $\bar{u} \equiv 1 \pmod{I(G)^2}$, donde, com a notação do lema anterior, $u \in W$.

Da demonstração do lema 2.8 vem que $u$ pode ser escrito na forma $u=vb^{-1}$, com $v=v^*$ e $b \in A$. Como $b \in A$ e $v \in V(\mathbb{Z}G/I_s)$, temos que $v \in V(\mathbb{Z}G/I_s)$; logo $v \in V'$. Assim, $u'=vb^{-1}g$, donde $V(\mathbb{Z}G/I_s)=V'.G$. Para provar, então, que $V' \triangleleft V(\mathbb{Z}G/I_s)$, basta conjugar por elementos de G. Mas:

se $\bar{v} \equiv 1 \pmod{I(\bar{G})^2}$, então $\overline{g^{-1}vg} \equiv \overline{g^{-1}g} \equiv 1 \pmod{I(\bar{G})^2}$

e

$(g^{-1}vg)^*=g^{-1}v^*g=g^{-1}vg$, se $v=v^*$.

Logo, se $v \in V'$, $g \in G$, tem-se $g^{-1}vg \in V'$. Assim, $V' \triangleleft V(\mathbb{Z}G/I_s)$, e o lema está provado.

<u>Teorema 2.10</u> - (Cliff, Sehgal, Weiss). O grupo G possui um complemento normal Y em $V(\mathbb{Z}G/I_s)$, e Y é um grupo abeliano livre finitamente gerado.

Demonstração - i) Usando, ainda, as notações dos lemas 2.8 e 2.9, consideramos o subgrupo $G \cap V'$. Então, dado $g \in G$, temos que $g \in G \cap V'$ se e só se $g = g^* = g^{-1}$, isto é, se e só se $g^2 = 1$, o que implica que $g \in A$, já que, por hipótese, $[G:A]$ é ímpar. Assim,

$$G \cap V' = \{a \in A \mid a^2 = 1\} .$$

Denotaremos este subgrupo por $A_2$.

ii) Consideramos, agora, a aplicação $f: V' \to V(\mathbb{Z}\bar{G})$ dada por $f(v) = \bar{v}$, para todo $v \in V'$. Se $v \in \ker f$, então $\bar{v} = 1$ em $\mathbb{Z}\bar{G}$, de modo que existe $\delta \in \mathbb{Z}G\, I(A)$ com $v = 1 + \delta$. Pelo Lema 2.1(c), existe $a \in A$ tal que $\delta \equiv a - 1 \pmod{I_S}$, donde $v = a \in A$ em $\mathbb{Z}G/I_S$. Logo, $\ker f \subset A \cap V = A_2$. Como a inclusão recíproca é evidente, segue que $\ker f = A_2$.

A imagem de f está contida em $V(\mathbb{Z}\bar{G}) \cap (1 + I(\bar{G})^2)$, já que se $u \in V'$, então $\bar{u} \equiv 1 \pmod{I(\bar{G})^2}$. Logo, pelo Lema 2.7 (c), $V'/A^2 \cong \operatorname{Im} f$ é um grupo abeliano livre finitamente gerado. Considerando, então, a sequência exata de $\mathbb{Z}$-módulos

$$0 \longrightarrow A_2 \xhookrightarrow{i} V' \longrightarrow V'/A_2 \longrightarrow 0,$$

temos que, como $V'/A_2$ é livre, a sequência cinde e existe um homomorfismo de grupos abelianos $\sigma: V' \longrightarrow A_2$, satisfazendo $\sigma \circ i = 1_{A_2}$.

iii) Como $V' \triangleleft V(\mathbb{Z}G/I_S)$, podemos definir uma ação de G sobre V' por conjugação, tornando V' um G-módulo. Como $V' \subset W$, $A \subset W$ e W é abeliano (pela demonstração do Lema 2.8), temos que A age trivialmente sobre V', e, passando ao quociente, V' fica sendo um $\bar{G}$-módulo.

Definimos, então, uma aplicação $\tau : V' \longrightarrow A_2$ por

$$\tau(v) = \prod_{x \in \bar{G}} \sigma(v^{x^{-1}})^x, \quad \forall v \in V'.$$

É fácil ver que a aplicação $\tau$ é um homomorfismo de $\bar{G}$-módulos, pois

$$\tau(v^g) = \prod_{x \in \bar{G}} \sigma((v^g)^{x^{-1}})^x = \prod_{x \in \bar{G}} \sigma(v^{g^{x^{-1}}})^x =$$

$$= \prod_{y \in G} \sigma(v^{y^{-1}})^{yg} = (\prod_{y \in G} \sigma(v^{y^{-1}})^y)^g = \tau(v)^g.$$

Além disso, dado $a \in A_2$, temos $\tau(a) = \prod_{x \in \bar{G}} (a^{x^{-1}})^x = a^{[G:A]} = a$, já que $\sigma \circ i = 1_{A_2}$ (por (ii)) e $[G:A]$ é ímpar.

Considerando, então, a sequência exata de G-módulos

$$1 \longrightarrow \ker \tau \hookrightarrow V' \underset{i}{\overset{\tau}{\rightleftarrows}} A_2 \longrightarrow 1,$$

observamos que a inclusão $i : A_2 \longrightarrow V'$ a faz cindir ( pois $\tau \circ i = 1_{A_2}$ ). Logo, pondo $Y = \ker\tau$, temos que $V' = A_2 \times Y$, produto direto de $\bar{G}$-módulos. Agora, como $Y \subset V'$ e A age trivialmente sobre V', temos que, dado $y \in Y$, $y^g = y^{\bar{g}}$, de modo que Y é um G-módulo, e, como $V(\mathbb{Z}G/I_s) = V'.G$, segue que $Y \triangleleft V(\mathbb{Z}G/I_s)$. Além disso, como

$$V(\frac{\mathbb{Z}G}{I_s}) = V'G = (Y \times A_2)G = YA_2G = YG$$

e, já que $Y \cap G \subset V' \cap G = A_2$ e $Y \cap A_2 = \{1\}$, $Y \cap G = \{1\}$,

e temos que Y é complemento normal para G em $V(\mathbb{Z}G/I_s)$.

Finalmente, como $Y \cong V'/A_2$, segue também que Y é abeliano livre finitamente gerado.

O resultado principal segue agora imediatamente:

<u>Teorema 2.11</u> - (Cliff, Sehgal, Weiss) Seja G um grupo finito (metabeliano), e seja A um subgrupo normal abeliano de G, tal que G/A é abeliano de ordem ímpar. Seja ainda $s=\frac{1}{2}([G:A]-1)$. Então G tem um complemento normal N em $V(\mathbb{Z}G)$, e N é uma extensão de $V(\mathbb{Z}G) \cap (1+I_s)$ por um grupo abeliano livre finitamente gerado.

<u>Demonstração</u> - Dado $u \in V(\mathbb{Z}G)$, consideremos a imagem $\tilde{u}=\psi(u) \in \mathbb{Z}G/I_s$. Usando a notação do teorema anterior, podemos escrever $\tilde{u}=y.g$, com $y \in Y$ e $g \in G$. Definimos, então, $\rho: V(\mathbb{Z}G) \longrightarrow G$ por $\rho(u)=g$. Observamos que, se $u_1, u_2 \in V(\mathbb{Z}G)$, $\tilde{u}_1=y_1g_1$, $\tilde{u}_2=y_2g_2$, então $\tilde{u}_1\tilde{u}_2=\tilde{u}_1\tilde{u}_2=y_1g_1y_2g_2=y_1y_2^{g_1^{-1}}g_1g_2$, de modo que $\rho(u_1u_2)=g_1g_2=\rho(u_1)\rho(u_2)$, e $\rho$ é um homomorfismo de grupos. Observamos, ainda, que, para todo $g \in G$, tem-se que $\rho(g)=g$.

Consideramos, então, a sequência exata

$$1 \longrightarrow \ker\rho \longrightarrow V(\mathbb{Z}G) \underset{i}{\overset{\rho}{\rightleftarrows}} G \longrightarrow 1.$$

Como $\rho \circ i = 1_G$, pelo que acabamos de fazer, a sequência

cinde, donde, pondo $N=\ker\rho$, $V(\mathbb{Z}G) = N.G$, e $N$ é um complemento normal para $G$ em $V(\mathbb{Z}G)$.

Finalmente, observamos que, se $v\in V(\mathbb{Z}G)\cap(1+I_s)$, $\tilde{v}=1$, de modo que $V(\mathbb{Z}G)\cap(1+I_s)\subset\ker\rho=N$. Seja $\psi:\mathbb{Z}G\to\mathbb{Z}G/I_s$ a aplicação quociente, e seja $X=\psi(N)$. Como $N=\ker\rho$, dado $u\in N$, temos que $\tilde{u}=y.1\in Y$, de modo que $X=\psi(N)\subset Y$. Logo, $X$ é um grupo abeliano livre finitamente gerado, e temos a sequência exata

$$1\longrightarrow V(\mathbb{Z}G)\cap(1+I_s)\overset{i}{\hookrightarrow} N\xrightarrow{\psi} X\longrightarrow 1,$$

donde $N$ é uma extensão de $V(\mathbb{Z}G)\cap(1+I_s)$ por um grupo abeliano livre finitamente gerado.

Desta forma, a Proposição 2.2 e o Teorema 2.11 mostram a existência de um complemento normal para $G$ em $V(\mathbb{Z}G)$ nos casos em estudo. Resta, então, mostrar que estes complementos são livres de torção. Para tanto, é imediato que basta provar que, para todo $k\in\mathbb{Z}$, se $A\triangleleft G$ com $A$ e $G/A$ abelianos, então $V(\mathbb{Z}G)\cap(1+I_k(G, A))$ é livre de torção. Este resultado não é trivial; para chegar até ele, necessitaremos de uma série de lemas de redução (§3). A seguir, provaremos um caso particular deste resultado (§4), só então passando ao resultado geral (§5).

## § 3. LEMAS DE REDUÇÃO.

Nesta seção, $G$ é um grupo finito e $A$ denota um subgrupo normal abeliano de $G$.

<u>Lema 3.1</u> - Se $\delta \in \mathbb{Z}G\, I(A)$ e $(1+\delta)^p=1$ para algum primo $p$ que não divide a ordem de $A$, então $\delta=0$.

<u>Demonstração</u> - Usamos indução em $|A|$. O caso $|A|=1$ é trivial. Suponhamos, então, que o teorema vale para subgrupos de ordem menor que $|A|$.

Seja $q$ um primo que divida $|A|$. Temos duas possibilidades:

i) <u>A não é um q-grupo</u>. Neste caso, seja $B$ um q-subgrupo de Sylow de $A$. Como $A$ é abeliano, $B$ é característico em $A$, e portanto $B \triangleleft G$. Denotando por $\bar{\delta}$ a imagem de $\delta$ em $\mathbb{Z}G/B$ pelo epimorfismo natural, é claroque $\bar{\delta} \in \mathbb{Z}G/B\, I(A/B)$ e $(1+\bar{\delta})^p=1$, donde, pela hipótese de indução, $\bar{\delta}=0$. Logo, $\delta \in \mathbb{Z}G\, I(B)$ e, como $A$ não é um q-grupo, $|B| < |A|$; consequentemente, $\delta=0$.

ii) <u>A é um q-grupo</u>. Neste caso, por [Sehgal, 1978, Lemma I.2.21], a imagem de $I(A)$ em $\frac{\mathbb{Z}}{q\,\mathbb{Z}}G$ é um ideal nilpotente de $\frac{\mathbb{Z}}{q\,\mathbb{Z}}A$, donde a imagem de $\mathbb{Z}G\, I(A)$ em $\frac{\mathbb{Z}}{q\,\mathbb{Z}}G$ é um idela nilpotente de $\frac{\mathbb{Z}}{q\mathbb{Z}}G$. Logo, existe um inteiro $n$ tal que $\delta^{q^n} \equiv 0 \pmod q$, e portanto $(1+\delta)^{q^n} \equiv 1+\delta^{q^n} \equiv 1 \pmod q$. Mas, além disso, temos que $(1+\delta)^p=1$, e, como $p \neq q$, segue que $(1+\delta) \equiv 1 \pmod q$. Logo, $\delta \in q\mathbb{Z}$.

Suponhamos, então, que $\delta \in q^i\mathbb{Z}$ para algum inteiro $i>0$. Então, como $(1+\delta)^p=1$, temos

$$0=p\delta+\binom{p}{2}\delta^2+\ldots+\delta^p \equiv p\delta \pmod{q^{2i}},$$

já que $\delta \in q^i\mathbb{Z}$. Logo $p\delta \in q^{2i}\mathbb{Z}$, e, como $p \neq q$, seque que $\delta \in q^{2i}\mathbb{Z}$. Assim, para todo $i>0$, se $\delta \in q^i\mathbb{Z}$, então $\delta \in q^{2i}\mathbb{Z}$. Como $\delta \in q\mathbb{Z}$, segue que $\delta \in q^{2^j}\mathbb{Z}$, para todo $j \geq 0$, donde $\delta=0$.

<u>Lema 3.2</u> - Se u é uma unidade de ordem finita de $\mathbb{Z}G$ satisfazendo $u \equiv 1 \pmod{\mathbb{Z}G\, I(A)^2}$, então $u=1$.

<u>Demonstração</u> - Usamos indução em $|A|$, observando que o caso $|A|=1$ é trivial. Supomos, então, que $|A| > 1$ e o resultado vale para subgrupos de ordem menor que $|A|$.

Escrevemos $u=1+\delta$, $\delta \in \mathbb{Z}G\, I(A)^2$. Podemos supor que $u^p=(1+\delta)^p=1$, para algum primo p. Pelo Lema 3.1, se $p \nmid |A|$ então $\delta=0$, donde $u=1$ e o resultado está provado. Podemos, então, supor que $p \mid |A|$. Temos, então, duas possibilidades.

i) Se $|A|$ é divisível por outro primo $q \neq p$, consideramos $A_1$, o q-subgrupo de Sylow de A; é claro que $A_1 \triangleleft G$. Seja $\pi: \mathbb{Z}G \longrightarrow \mathbb{Z}G/A_1$ a projeção natural, e, dado $\alpha \in \mathbb{Z}G$, escrevemos $\bar{\alpha}=\pi(\alpha) \in \mathbb{Z}G/A_1$. Então vale que $\bar{u}=1+\bar{\delta}$, $\bar{\delta} \in \mathbb{Z}\bar{G}\, I(\bar{A})^2$, donde $\bar{u} \equiv 1 \pmod{\mathbb{Z}\bar{G}\, I(\bar{A})^2}$, e, como $\bar{u}$ tem ordem finita, segue, por hipótese de indução, que $\bar{u}=1$. Logo, $u-1 \in \mathbb{Z}G\, I(A_1)$, donde $\delta \in \mathbb{Z}G\, I(A_1)$, e, como $p \nmid |A_1|$, segue, pelo Lema 3.1, que $u=1$, provando o lema.

ii) Se A é um p-grupo, ponhamos $B=\Omega_1(A)=\{a \in A \mid a^p=1\}$. Como antes, temos que $B \triangleleft G$. Seja $\pi: \mathbb{Z}G \longrightarrow \mathbb{Z}G/B$ o epimorfismo natural. Como em (i), segue, por indução, que, se $u=1+\delta$, então $\delta \in \mathbb{Z}G\, I(B)$. Logo, $\delta \in \mathbb{Z}G\, I(B) \cap \mathbb{Z}G\, I(A)^2 = \mathbb{Z}G\, I(A)\, I(B)$ pelo Lema I.3.10 (ii).

Nesta situação, para mostrar que $\delta=0$, mostraremos que $T(\delta)=0$ para toda representação irredutível complexa T de G. Pelo Teorema de Reciprocidade de Frobenius, ([Dornhoff, 1971, Theorem 9.4]), toda representação irredutível complexa T é somanda direta de uma representação S de G induzida por uma representação de grau 1, $\chi:A\to C$. Logo, basta mostrar que $S(\delta)=0$ para todo tal S.

Seja $p^n$ o expoente de A, e seja $\omega$ uma raiz $p^n$-ésima primitiva da unidade, de modo que $\chi(A)\subset\langle\omega\rangle$ e $\chi(\mathbb{Z}A)\subset\mathbb{Z}[\omega]$. Observamos que, se $r=[G:A]$, segue que $S=\chi^G$ leva $\mathbb{Z}G$ em $M_r(\mathbb{Z}[\omega])$. Seja $\nu$ a valorização aditiva de $\mathbb{Z}[\omega]$ em relação ao ideal primo $\langle\omega-1\rangle$. Por [Janusz, 1973, Teor. I.9.1(c)], temos que $\langle p\rangle=\langle\omega-1\rangle^{\phi(p^n)}$, onde $\phi$ é a função de Euler; logo, $\nu(p)=\phi(p^n)=p^{n-1}(p-1)$.

Observamos, ainda, que

$$(\omega-1)^{p^{n-1}}=(\omega^{p^{n-1}}-1)+pr,\ \text{para algum } r\in\mathbb{Z}[\omega].$$

Logo, como $\nu$ é valorização aditiva,

$$p^{n-1}\geq\min\{\nu(\omega^{p^{n-1}}-1),\ \nu(pr)\}.$$

Mas $\nu(pr)\geq p^{n-1}(p-1)>p^{n-1}$, donde segue que devemos ter $p^{n-1}\geq\nu(\omega^{p^{n-1}}-1)$ e $\nu(\omega^{p^{n-1}}-1)\neq\nu(pr)$, donde $\nu(\omega^{p^{n-1}}-1)=p^{n-1}$.

Estendemos $\nu$ ao anel $M_r(\mathbb{Z}[\omega])$ definindo, para cada $X\in M_r(\mathbb{Z}[\omega])$, $\nu(X)=i$ se e só se $X\in(\omega-1)^iM_r(\mathbb{Z}[\omega])$ e $X\notin(\omega-1)^{i+1}M_r(\mathbb{Z}[\omega])$. A aplicação $\nu:M_r(\mathbb{Z}[\omega])\longrightarrow\mathbb{Z}$ satisfaz as seguintes propriedades, de verificação imediata:

(a) $\forall X,Y \in M_r(\mathbb{Z}[\omega])$, $\nu(X\ Y) \geq \nu(X)+\nu(Y)$

(b) $\forall r \in \mathbb{Z}[\omega]$, $\forall X \in M_r(\mathbb{Z}[\omega])$, $\nu(rX) = \nu(r)+\nu(X)$

(c) $\forall X,Y \in M_r(\mathbb{Z}[\omega])$, $\nu(X+Y) \geq \min\{\nu(X),\nu(Y)\}$.

Seja, então $b \in B$, de modo que $b^p=1$. Como $b \in B \subset A$ e $S$ é induzida por uma representação de grau 1 de $A \triangleleft G$, $S(B)$ é uma matriz diagonal de $M_r(\mathbb{Z}[\omega])$. Logo,

$$S(B) = \begin{bmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_r \end{bmatrix},$$

onde $\varepsilon_i$ é uma raiz p-ésima da unidade, $1 \leq i \leq r$, donde existe um inteiro $k_i$ tal que $\varepsilon_i = (\omega^{p^{n-1}})^{k_i}$. Logo, temos que

$$S(b-1) = S(b)-1 = \begin{bmatrix} \varepsilon_1-1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_r-1 \end{bmatrix}.$$

Para calcular $\nu(S(b)-1)$, observamos que $\nu(\varepsilon_i-1) \geq p^{n-1}$. De fato, basta observar que $\varepsilon_i = (\omega^{p^{n-1}})^{k_i}$ e que $\nu((\omega^{p^{n-1}})^k-1) \geq$ $\geq \nu(\omega^{p^{n-1}}-1)$ para todo $k \in \mathbb{N}$. Como $\nu(\omega^{p^{n-1}}-1) = p^{n-1}$ (vide acima), segue o resultado. Logo, $\nu(S(b)-1) \geq p^{n-1}$.

Agora, se $\beta \in I(B)$, podemos escrever

$$\beta = \sum_i n_i (b_i - 1), \quad n_i \in \mathbb{Z},$$

donde $S(\beta) = \sum_i n_i \; S(b_i - 1)$ e

$$\nu(S(\beta)) \geqslant \min_i \{ \nu(S(b_i) - 1\} \geqslant p^{n-1}.$$

Assim, se $\beta \in I(B)$, temos $\nu(S(\beta)) \geqslant p^{n-1}$.

Analogamente, obtemos que se $a \in A$, então $\nu(S(a)-1) \geqslant 1$, e portanto que $\alpha \in I(A)$ implica em que $\nu(S(\alpha)) \geqslant 1$.

Suponhamos, então, que $S(\delta) \neq 0$. Como já vimos, $\delta \in I(A)I(B)\mathbb{Z}G$. Agora, se $\alpha \in I(A)$, $\beta \in I(B)$, $\gamma \in \mathbb{Z}G$, temos que $\nu(\alpha\beta\gamma) \geqslant \nu(\alpha) + \nu(\beta) + \nu(\gamma) \geqslant p^{n-1} + 1$. Como $\delta$ é soma de elementos desta forma, segue que $\nu(\delta) \geqslant p^{n-1} + 1$. Seja $\nu(\delta) = p^{n-1} + i$, $i > 0$. Como $(1+\delta)^p = 1$, obtemos que

$$p\delta + \binom{p}{2}\delta^2 + \ldots + \delta^p = 0.$$

Agora, é claro que, se $1 < j < p$, vale que $p \mid \binom{p}{j}$, donde $\nu\binom{p}{j} \geqslant \nu(p) = p^{n-1}(p-1)$. Além disso, $\nu(S(\delta^j)) = \nu(S(\delta)^j) \geqslant j\nu(S(\delta))$, donde segue que

$$\begin{aligned} \nu\left(\binom{p}{j} S(\delta^j)\right) &\geqslant \nu\left(\binom{p}{j}\right) + \nu(S(\delta^j)) \geqslant \nu(p) + j\nu S(\delta) \\ &> \nu(p) + \nu(S(\delta)) = \nu(pS(\delta)), \end{aligned}$$

isto é, $\nu\left(\binom{p}{j} S(\delta^j)\right) > \nu(pS(\delta))$, $\forall j$, $1 < j < p$.

Então, como $-p\delta = \binom{p}{2}\delta^2 + \ldots + \delta^p$, temos que

$$\nu(p\,S(\delta)) \geqslant \min\{\,\nu(S(\delta^p)), \nu(\tbinom{p}{j}S(\delta^j),\ 1<j<p\,\}$$

Mas, como já vimos, $\nu(\tbinom{p}{j}S(\delta^j)) > \nu(pS(\delta))$; logo, devemos ter $\nu(pS(\delta)) \geqslant \nu(S(\delta^p))$.

Então, lembrando que $\nu(S(\delta)) = p^{n-1}+i$, $i>0$, temos:

$$\nu(pS(\delta)) = \nu(p)+\nu(S(\delta)) \geqslant \nu(S(\delta^p)) \geqslant p\,\nu(S(\delta)),$$

donde,

$$p^{n-1}(p-1)+p^{n-1}+i \geqslant p(p^{n-1}+i),$$

e portanto $i \geqslant pi$, o que é absurdo, porque $i>0$. Logo, devemos ter $S(\delta)=0$ para todo tal $S$, donde $\delta=0$, como se desejava provar.

<u>Lema 3.3</u> - Seja $B$ um grupo p-abeliano elementar, para algum primo $p$. Então $p\,I(B) \subset I(B)^p$, e vale a igualdade se $|B| = p$.

<u>Demonstração</u> - Tomemos $b \in B$, $b \neq 1$. É claro que $p(b-1) \in I(B)$; suponhamos que $p(b-1) \in I(B)^i$, mas $p(b-1) \notin I(B)^{i+1}$.

Como $B$ é um grupo p-abeliano elementar, temos que:

$$0 = b^p - 1 = (1+(b-1))^p - 1 =$$
$$= p(b-1) + \tbinom{p}{2}(b-1)^2 + \ldots + (b-1)^p.$$

Observando que, se $2 \leqslant j \leqslant p-1$, temos que $p \mid \tbinom{p}{j}$ e

$$\binom{p}{j}(b-1)^j = p(b-1).\ \frac{1}{p}\binom{p}{j}(b-1)^{j-1} \in I(B)^{i+1},$$

já que $p(b-1) \in I(B)^i$, segue então que

$$p(b-1) \equiv -(b-1)^p \pmod{I(B)^{i+1}}.$$

Se, agora, $i \leqslant p-1$, então $p \geqslant i+1$, donde $(b-1)^p \in I(B)^p \subset I(B)^{i+1}$, de modo que $p(b-1) \in I(B)^{i+1}$, contrariando a hipótese inicial. Logo, temos que $i \geqslant p$, donde segue imediatamente que $p(b-1) \in I(B)^p$. Assim, $pI(B) \subset I(B)^p$.

Finalmente, se $|B| = p$, seja $B = \langle b \rangle$. Nestas condições, $I(B) = (b-1)\mathbb{Z}B$, donde $I(B)^p = (b-1)^p\ \mathbb{Z}B$. Agora, $(b-1)^p = b^p - pb^{p-1} + \ldots + pb - 1 = -p(b-1)(b^{p-2} + \ldots + b)$, se $p$ é ímpar, e $(b-1)^2 = b^2 - 2b + 1 = 2(1-b)$, de modo que, em qualquer caso, $(b-1)^p \equiv 0 \pmod{p\ I(B)}$. Logo,

$$(b-1)^p\ \mathbb{Z}B \subset p\ I(B),$$

donde, neste caso, $I(B)^p = p\ I(B)$.

No restante desta seção, $B$ denota sempre um subgrupo normal $p$-abeliano elementar de $G$ contido em $A$.

<u>Lema 3.4</u> - Se $\delta \in \mathbb{Z}G\, I(B)$ e $(1+\delta)^p \equiv 1 \pmod{\mathbb{Z}G\, I(B)^{p+1}}$, então $p\delta + \delta^p \equiv 0 \pmod{\mathbb{Z}G\ I(B)^{p+1}}$.

<u>Demonstração</u> - Como $(1+\delta)^p \equiv 1 \pmod{\mathbb{Z}G\, I(B)^{p+1}}$, temos que

$$p\delta + \binom{p}{2}\delta^2 + \ldots + \delta^p \equiv 0 \pmod{\mathbb{Z}G\, I(B)^{p+1}}.$$

Agora, se $2 \leqslant j \leqslant p-1$, $\binom{p}{j}\delta^j \in p\,\mathbb{Z}G\,I(B)^2$. Como, pelo Lema 3.3, $p\,\mathbb{Z}G\,I(B) \subset \mathbb{Z}G\,I(B)^p$, segue a tese.

<u>Lema 3.5</u> - Se $\alpha \in \mathbb{Z}G\,I(A)\,I(B)$ e $\beta \in \mathbb{Z}G\,I(B)$, então

$$(1+\alpha+\beta)^p \equiv (1+\beta)^p \pmod{\mathbb{Z}G\,I(A)\,I(B)^p}.$$

<u>Demonstração</u> - Temos que

$$(1+\alpha+\beta)^p = 1 + \sum_{i=1}^{p} \binom{p}{i} (\alpha+\beta)^i.$$

Agora, como $\alpha \in \mathbb{Z}G\,I(A)\,I(B)$, temos, para $1 \leqslant i < p$, que

$$\binom{p}{i} (\alpha+\beta)^i \equiv \binom{p}{i} \beta^i \pmod{p\,\mathbb{Z}G\,I(A)\,I(B)}.$$

Pelo Lema 3.4, $p\,\mathbb{Z}G\,I(A)\,I(B) \subset \mathbb{Z}G\,I(A)\,I(B)^p$, donde

$$\binom{p}{i} (\alpha+\beta)^i \equiv \binom{p}{i} \beta^i \pmod{\mathbb{Z}G\,I(A)\,I(B)^p}.$$

Além disso, $(\alpha+\beta)^p = \beta^p + \sum_{j=1}^{p} \binom{p}{j} \alpha^j \beta^{p-j}$, e, se $1 \leqslant j \leqslant p$, temos que

$$\binom{p}{j}\alpha^j \beta^{p-j} \in (\mathbb{Z}G\,I(A)\,I(B))^j (\mathbb{Z}G\,I(B))^{p-j} \subset \mathbb{Z}G\,I(A)\,I(B)^p,$$

donde $(\alpha+\beta)^p \equiv \beta^p \pmod{\mathbb{Z}G\,I(A)\,I(B)^p}$. Logo,

$$(1+\alpha+\beta)^p = 1 + \sum_{i=1}^{p} \binom{p}{i} (\alpha+\beta)^i \equiv 1 + \sum_{i=1}^{p} \beta^i = (1+\beta)^p \pmod{\mathbb{Z}G\,I(A)\,I(B)^p},$$ provando o lema.

<u>Lema 3.6</u> - Seja $G=AX$, com $A \cap X=1$, e seja $G_1=BX$. Então

$$\mathbb{Z}G\, I(A)\ I(B)^n \cap \mathbb{Z}G_1 = \mathbb{Z}G_1\ I(B)^{n+1},\ \forall n \in \mathbb{N}.$$

<u>Demonstração</u> - Tomemos $\alpha \in \mathbb{Z}G\, I(A)\ I(B)^n \cap \mathbb{Z}G_1$. Podemos escrever

$$\alpha = \sum_{x \in X} x\alpha_x,\ \text{com}\ \alpha_x \in I(A)I(B)^n \cap \mathbb{Z}B,\ \forall x \in X.$$

Logo, basta provar que $I(A)\ I(B)^n \cap \mathbb{Z}B = I(B)^{n+1}$.

Seja, então, $\beta \in I(A)\ I(B)^n \cap \mathbb{Z}B$; podemos escrever $\beta$ na forma

$$\beta = \sum_{i,j} n_{i_j}(a_i-1)\beta_j,\ a_i \in A,\ \beta_j \in I(B)^n,\ n_{i_j} \in \mathbb{Z}.$$

Seja $\{1, g_2, \ldots, g_m\}$ uma transversal para $B$ em $A$; definimos uma aplicação $\phi: A \to B$ por $\phi(g_i b)=b$. Estendendo $\phi$ $\mathbb{Z}$ - linearmente a $\mathbb{Z}A$, obtemos um homomorfismo aditivo $\phi: \mathbb{Z}A \to \mathbb{Z}B$ tal que, se $\gamma \in \mathbb{Z}B$, então $\phi(\gamma)=\gamma$. Em particular, $\phi(\beta)=\beta$.

Agora, se $\beta \in I(B)^n$ e $a=g_k b$, temos que $\phi((a-1)\beta_j) = \phi(g_k b\beta_j) - \phi(\beta_j) = b\beta_j - \beta_j = (b-1)\beta_j \in I(B)^{n+1}$. Logo,

$$\beta = \phi(\beta) = \sum_{i,j} n_{i_j}\ \phi((a_i-1)\beta_j) \in I(B)^{n+1},$$

e o lema está provado.

## § 4. AÇÃO FIEL E IRREDUTÍVEL DE G/A EM A.

Nesta seção, provaremos um caso particular do resultado que procuramos. Especificamente, provaremos que, se G=AX, com A p-abeliano elementar e X abeliano, e se X age fiel e irredutivelmente sobre A, então $V(\mathbb{Z}G) \cap (1+I_k(G,A))$ é livre de torção. Para isso, precisamos de alguns resultados preliminares. Começamos por alguns Lemas da Teoria dos Números.

Lema 4.1 - Sejam p um primo, d um inteiro positivo e ponhamos $r=p^d-1$. Sejam ainda $n_1, n_2, \ldots, n_p$, $n \in \mathbb{N}$. Nestas condições, se $p^{n_1} + p^{n_2} + \ldots + p^{n_p} \equiv p^n \pmod{r}$, então $n_1 \equiv n_2 \equiv \ldots \equiv n_p \equiv n-1 \pmod{d}$, e portanto $p^{n_1} \equiv p^{n_2} \equiv \ldots \equiv p^{n_p} \equiv p^{n-1} \pmod{r}$.

Demonstração - Provaremos primeiro um resultado particular. Observamos, antes de tudo, que, como $r=p^d - 1$, $p^d \equiv 1 \pmod{r}$; logo, podemos reduzir os $n_i$ mod d. Assim, podemos sempre supor que $n \leqslant n_i$, $i=1,\ldots,p$.

a) Suponhamos n=0. Então temos

$$p^{n_1}+\ldots+p^{n_p} \equiv 1 \pmod{r}. \qquad (I)$$

É claro que podemos sempre tomar $0 \leqslant n_i < d$, $i=1,2,\ldots,p$, reduzindo módulo d. Temos, então,

$$p \leqslant p^{n_1} + \ldots + p^{n_p} \leqslant p.p^{d-1} = p^d.$$

Mas então (I) só pode ocorrer quando o máximo é atingido, isto é, quando

$$p^{n_1}+\ldots+p^{n_p}=p^d,\quad 0\leqslant n_i<d,$$

donde segue que $n_i = d-1$, $i = 1,2,\ldots,p$. Logo,

$$n_1\equiv n_2\equiv\ldots\equiv n_p\equiv d-1\equiv -1 \pmod{d},$$

provando o lema neste caso.

b) (Caso geral) Suponhamos agora que

$$p^{n_1}+\ldots+p^{n_p}\equiv p^n \pmod{r}.$$

Como $r=p^d-1$, temos que mdc $(p^n,r)=1$. Logo, dividindo por $p^n$, obtemos

$$p^{n_1-n}+\ldots+p^{n_p-n}\equiv 1 \pmod{r},$$

donde, por (a), segue

$$n_1-n\equiv n_2-n\equiv\ldots\equiv n_p-n\equiv -1 \pmod{d},$$

provando o lema.

<u>Lema 4.2</u> - Seja $\omega\in C$ uma raiz p-ésima primitiva da unidade. Então $\omega^n-1\equiv 0 \pmod{(\omega-1)}$, $\forall n\in\mathbb{N}$, mas se $\omega^n-1\equiv 0 \pmod{(\omega-1)^2}$, então $\omega^n=1$.

<u>Demonstração</u> - Observamos, em primeiro lugar, que $\omega^n-1 = (\omega^{n-1}+\omega^{n-2}+\ldots+\omega+1)(\omega-1)$, de modo que $\omega^n-1\equiv 0 \pmod{(\omega-1)}$.

Lembrando que $\omega-1$ é um primo de $\mathbb{Z}[\omega]$, resta

provar que, se $k < p$, então

$$\omega-1 \nmid \omega^{k-1}+\omega^{k-2}+\ldots+\omega+1.$$

Para tanto, observamos que, pelo lema III.1.3, existe uma aplicação $\pi:\mathbb{Z}[\omega] \longrightarrow GF(p)$, cujo núcleo é o ideal de $\mathbb{Z}[\omega]$ gerado por $\omega-1$. Então, como $k < p$, temos $\pi(\omega^{k-1}+\ldots+\omega+1)=k\neq 0$ em $GF(p)$, donde $\omega^{k-1}+\ldots+\omega+1 \notin \ker\pi$, isto é, $\omega-1 \nmid \omega^{k-1}+\ldots+\omega+1$. Logo, se $\omega^n-1\equiv 0 \pmod{(\omega-1)^2}$, então $\omega^n-1=0$, isto é, $\omega^n=1$.

<u>Lema 4.3</u> - Seja $\omega\in C$ uma raiz p-ésima primitiva da unidade. Então, valem:

a) $\sum_{i=0}^{t} \omega^i \equiv t+1 \pmod{\omega-1}$;

b) $(\omega-1)^{p-1} \prod_{i=1}^{p-1} (1+\omega+\ldots+\omega^{i-1}) \equiv (\omega-1)^{p-1}(p-1)! \pmod{(\omega-1)^p}$;

c) $(\omega-1)^{p-1}(p-1)! \equiv -(\omega-1)^{p-1} \pmod{(\omega-1)^p}$;

d) $\dfrac{p}{(\omega-1)^{p-1}} \equiv -1 \pmod{(\omega-1)}$.

<u>Demonstração</u>.

a) Seja $\pi:\mathbb{Z}[\omega] \longrightarrow GF(p)$ a função mencionada na demonstração do lema anterior. Como $\pi$ é sobrejetora e $\ker\pi = \langle \omega-1 \rangle$, temos que $\pi(a)=\pi(b)$ se e só $a\equiv b \pmod{\omega-1}$.

Para provar (a), então, basta notar que $\pi(\omega)=1$, de modo $\pi(\sum_{i=0}^{t} \omega^i) = t+1$.

b) Por (a), temos que $1+\omega+\ldots+\omega^{i-1} \equiv i \pmod{\omega-1}$. Logo,

$$\prod_{i=1}^{p-1} (1+\omega+\ldots+\omega^{i-1}) \equiv (p-1)! \pmod{\omega-1}.$$

Então, multiplicando por $(\omega-1)^{p-1}$, vem que

$$(\omega-1)^{p-1} \prod_{i=1}^{p-1} (1+\omega+\ldots+\omega^{i-1}) \equiv (\omega-1)^{p-1}(p-1)! \pmod{(\omega-1)^p}.$$

c) Como $< p > = < \omega-1 >^{p-1}$, por [Janusz, 1973, Teor.I.9.1(c)], temos que $(\omega-1)^{p-1} \mid p$. Pelo Teorema de Wilson, $(p-1)! \equiv -1 \pmod{p}$. Logo, obtemos

$$(p-1)! \equiv -1 \pmod{(\omega-1)^{p-1}},$$

donde, multiplicando por $(\omega-1)^{p-1}$, segue

$$(\omega-1)^{p-1}(p-1)! \equiv -(\omega-1)^{p-1} \pmod{(\omega-1)^p}.$$

d) Lembrando que

$$X^{p-1}+\ldots+X+1 = \prod_{i=1}^{p-1} (X-\omega^i),$$

pondo $X=1$, obtemos imediatamente que

$$p = \prod_{i=1}^{p-1} (1-\omega^i).$$

Então:

$$p=\prod_{i=1}^{p-1}(1-\omega^i)=(1-\omega)^{p-1}\prod_{i=1}^{p-1}\frac{1-\omega^i}{1-\omega}=$$

$$=(1-\omega)^{p-1}\prod_{i=1}^{p-1}(1+\omega+\ldots+\omega^{i-1})$$

$$\equiv(-1)^{p-1}(\omega-1)^{p-1}(p-1)!\ (\mathrm{mod}\,(\omega-1)^p). \qquad \text{(por (b))}$$

$$\equiv -(\omega-1)^{p-1}(\mathrm{mod}\ (\omega-1)^p) \qquad \text{(por (c))}.$$

Donde, dividindo esta última congruência por $(\omega-1)^{p-1}$, obtemos

$$\frac{p}{(\omega-1)^{p-1}}\equiv -1 \quad (\mathrm{mod}\ \omega-1).$$

<u>Lema 4.4</u> - Seja $K=GF(p^d)$, e ponhamos $r=p^d-1$. Se $1\leqslant k\leqslant r-1$, então $\sum_{x\in K^*} x^k=0$.

<u>Demonstração</u> - Observamos, em primeiro lugar, que, se $K=GF(2)$, temos $r=1$, donde não existe $k\in\mathbb{Z}$ satisfazendo $1\leqslant k\leqslant r-1$. Logo, podemos supor que $p^d>2$.

Seja $G_k=\{x^k\,|\,x\in K^*\}$. Como $K^*$ é cíclico, $G_k$ é um subgrupo de $K^*$, e portanto é cíclico. Seja $G_k=\langle y\rangle$, e supomos $y^\ell=1$. Como $p^d>2$ e $1\leqslant k\leqslant r-1$, temos $\ell>1$. Seja $N_k=\{x\in K^*\mid x^k=1\}$.

É claro que $x_1^k=x_2^k$ se e só se $x_1x_2^{-1}\in N_k$. Logo,

$$\sum_{x\in K^*} x^k = |N_k| \sum_{i=0}^{\ell-1} y^i.$$

Mas, como $y^\ell-1=0$, temos que $y^{\ell-1}+y^{\ell-2}+\ldots+y+1=0$, donde $\sum_{x\in K^*} x^k = 0$.

Passamos agora a alguns resultados preliminares da Teoria dos Grupos.

<u>Proposição 4.5</u> - [Huppert, 1967, Satz II.3.10]. Seja $V=V(n,p^f)$ o espaço vetorial de dimensão $n$ sobre o corpo $K=GF(p^f)$. Seja $X$ um grupo abeliano de transformações lineares de $V$, tal que $V$ é um $X$-módulo irredutível. Então existe um isomorfismo $\gamma$ de $V$ sobre o grupo aditivo de $GF(p^{nf})$ e um monomorfismo $\phi: X \longrightarrow GF(p^{nf})^*$, de modo que, para todo $v\in V$ e $x\in X$, temos

$$\gamma(v^x) = \phi(x)\ \gamma(v).$$

Além disso, $X$ é cíclico, e vale que $|X| \mid p^{nf}-1$.

<u>Demonstração</u> - Temos que $X\subset Hom_K(V,V)$ e, é claro, podemos considerar $K\subset Hom_K(V,V)$. Seja $C$ o subanel comutativo de $Hom_K(V,V)$ gerado por $K$ e $X$.

Como $X\subset C$, temos que $V$ é um $C$-módulo irredutível. Como $C$ é comutativo, podemos considerar $C\subset Hom_C(V,V)$. Observamos, ainda, que, $V$ é um $C$-módulo irredutível, e portanto $Hom_C(V,V)$ é um anel com divisão (pelo lema de Schur).

Afirmamos que $C-\{0\}$ é um subgrupo multiplicativo de $Hom_C(V,V)$. De fato, basta observar que, como $X \subset C$, $C$ é um anel com 1, donde $C-\{0\}$ é um monóide. Agora, é claro que $C \subset Hom_K(V,V) \cong M_n(K)$, que é finito. Assim, $C-\{0\}$ é um monóide finito contido em um anel com divisão, e, portanto, um grupo. Concluímos então que $C$ é um corpo.

Agora, como $V$ é um $C$-módulo irredutível e $C$ é um corpo, segue que $\dim_C V=1$, donde, dado $v \in V$, $v \neq 0$, obtemos $V=Cv$, e portanto $C \cong V$ (isomorfismo de $C$-espaços vetoriais, dado por $c \longmapsto cv$). Logo, $|C| = |V| = p^{nf}$, donde $C \cong GF(p^{nf})$, já que todos os corpos de ordem $p^{nf}$ são isomorfos. Seja $\gamma$ o isomorfismo de $V$ em $GF(p^{nf})$ assim obtido.

Temos então $X \subset C \cong GF(p^{nf})$. Seja $\phi: C \to GF(p^{nf})$ o isomorfismo; é claro que $\phi$ dá, por restrição, um monomorfismo de $X$ em $GF(p^{nf})^*$. Das definições de $\gamma$ e $\phi$, segue imediatamente que

$$\gamma(v^x) = \phi(x)\ \gamma(v)$$

Finalmente, como $C^*$ é cíclico e $X \subset C^*$, segue que $X$ é cíclico e $|X| \mid p^{nf}-1$.

Corolário 4.6 - Seja $G=A.X$, com $A \triangleleft G$, $A$ um grupo $p$-abeliano elementar, finito, e $X$ um grupo abeliano. Suponhamos que $X$ aja fiel e irredutivelmente sobre $A$. Então, se $|A|=p^d$ e $K=GF(p^d)$, existe um isomorfismo $\gamma$ de $A$ sobre o grupo aditivo de $K$ e um monomorfismo $\phi: X \longrightarrow K^*$, tais que

$$\gamma(a^x)=\phi(x)\gamma(a),\ \forall x\in X,\ \forall a\in A.$$

Além disso, X é cíclico e $|X| \mid p^d-1$.

Demonstração - Como A é p-abeliano elementar de ordem $p^d$, temos um isomorfismo de $\mathbb{Z}$-módulos

$$A \cong \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{d \text{ vezes}}.$$

Como $p\in \mathrm{Anl}(A)$, podemos passar ao quociente da ação de $\mathbb{Z}$ por $p\mathbb{Z}$, obtendo um isomorfismo de $\mathbb{Z}_p$ - espaços vetoriais

$$A \cong \underbrace{\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{d \text{ vezes}} \cong V(d,p)$$

Como a ação de X é fiel, X pode ser considerado um grupo de transformações de A. Basta, então aplicar a proposição anterior para V(d,p), e o lema está provado.

Lema 4.7 - Seja X um grupo cíclico de ordem $p^d-1$, seja $K=GF(p^d)$ e seja $\phi: X \longrightarrow K^*$ o isomorfismo natural. Definimos, para cada i, $0\leqslant i\leqslant r-1$, onde $r=p^d-1$,

$$\varepsilon_i = \frac{1}{r} \sum_{x\in X} \phi(x)^{-i} x \in KX.$$

Então $\{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{r-1}\}$ é um sistema de idempotentes ortogonais de KX, e, portanto, uma base de KX sobre K.

Demonstração - É claro que basta mostrar que, para $1 \leqslant i, j \leqslant r-1$, tem-se que $\varepsilon_i \varepsilon_j = \delta_{ij} \varepsilon_i$.

Observamos inicialmente que

$$\varepsilon_i^2 = \frac{1}{r^2} \sum_{x \in X} \sum_{y \in X} \phi(x)^{-i} \phi(y)^{-i} xy = \frac{1}{r^2} \sum_{x,y \in X} \phi(xy)^{-i} xy =$$

$$= \frac{1}{r^2} . r \sum_{z \in X} \phi(z)^{-i} z = \varepsilon_i .$$

Logo, os $\varepsilon_i$ são idempotentes de KX.

Vamos calcular $\varepsilon_i \varepsilon_j$ para $i \neq j$. Podemos supor $i > j$; seja $j = i-k$, $k \neq 0$. Então

$$\varepsilon_i \varepsilon_j = \frac{1}{r^2} \sum_{x \in X} \sum_{y \in Y} \phi(x)^{-i} \phi(y)^{-j} xy =$$

$$= \frac{1}{r^2} \sum_{x \in X} \sum_{y \in Y} \phi(x)^{-i} \phi(y)^{-i+k} xy =$$

$$= \frac{1}{r^2} \sum_{y \in X} (\phi(y)^k \sum_{x \in X} \phi(xy)^{-i} xy)$$

$$=\frac{1}{r}\sum_{y\in X}(\phi(y)^k.\frac{1}{r}\sum_{x\in X}\phi(xy)^{-i}xy)$$

$$=\frac{1}{r}(\sum_{y\in X}\phi(y)^k)\ \varepsilon_i$$

Agora, como $\phi:X\longrightarrow K^*$ é um isomorfismo, temos que $\sum_{y\in X}\phi(y)^k=\sum_{x\in K^*}x^k=0$ pelo lema 4.4, já que $0<k\leqslant r-1$. (Observe-se que, no caso $p^d=2$, $|X|=1$ e o resultado é trivial). Logo, $\varepsilon_i\varepsilon_j=0$ se $i\neq j$, e o lema está provado.

No que segue, G denota um grupo finito, A um subgrupo normal p-abeliano elementar de ordem $p^d$ e X um subgrupo abeliano de G, tais que G=AX e X age fiel e irredutivelmente sobre A. Pelo Corolário 4.6, X deve ser cíclico e $|X|\mid p^d-1$. Temos ainda mais um resultado preliminar.

<u>Lema 4.8</u> - Suponhamos que $|X|=p^d-1$, e seja $\chi:A\longrightarrow C$ uma representação de grau 1 de A, não trivial. Sejam $\omega\in C$ uma raiz p-ésima primitiva da unidade, $R=\mathbb{Z}[\omega]$, e seja $T=\chi^G$ a representação de G induzida por $\chi$. Então podemos tomar o espaço de representação de T como sendo RX, onde

$$T(a)y=\chi(a^y)y \qquad \forall a\in A,\ \forall y\in X$$

$$T(x)y=xy \qquad \forall x,y\in X.$$

Demonstração - Estendendo $\chi$ a $\mathbb{Z}A$, obtemos um homomorfismo $\chi:\mathbb{Z}A \longrightarrow R$. O espaço de representação natural de T é, então, $\mathbb{Z}G \otimes_{\mathbb{Z}A} R$, com a estrutura de $\mathbb{Z}G$-módulo definida por

$$T(x)(y \otimes r)=xy \otimes r$$

$$T(a)(y \otimes r)=ay \otimes r = ya^y \otimes r =$$

$$= y \otimes \chi(a^y)r,$$

para $x,y \in X$, $a \in A$, $r \in R$, já que a estrutura de $\mathbb{Z}A$ - módulo em R é definida por $a.r=\chi(a)r$.

Lembrando que $\mathbb{Z}G$ é um $\mathbb{Z}A$ - módulo livre de base X, definimos uma aplicação $\mathbb{Z}A$-balanceada $f:\mathbb{Z}G \times R \longrightarrow RX$ pondo $f(x,r)=rx$, $\forall r \in R$, $\forall x \in X$, e estendendo $\mathbb{Z}A$-linearmente. Logo, obtemos uma aplicação $f^*:\mathbb{Z}G \otimes_{\mathbb{Z}A} R \longrightarrow RX$, cuja inversa é claramente $g:RX \longrightarrow \mathbb{Z}G \otimes_{\mathbb{Z}A} R$, dada por $g(\sum_i r_i x_i)= \sum_i x_i \otimes r_i$. Logo, $\mathbb{Z}G \otimes_{\mathbb{Z}A} R \cong RX$.

Finalmente, observamos que a ação de $\mathbb{Z}G$ sobre $\mathbb{Z}G \otimes_{\mathbb{Z}A} R$ passa, pelo isomorfismo, a RX, dando

$$T(x)y=T(x)f^*(y \otimes 1)=f^*(T(x)(y \otimes 1)) =$$

$$=f^*(xy \otimes 1) = xy$$

e

$$T(a)y=T(a)f^*(y \otimes 1) = f^*(T(a)(y \otimes 1))=$$

$$=f^*(y \otimes \chi(a^y)) = \chi(a^y)y,$$

e o lema está provado.

<u>Proposição 4.9</u> - Suponhamos que $|X|=p^d-1$, e sejam $\chi$, $\omega$, $R$ e $T$ como no lema anterior. Então:

i) Dado $\alpha\in\mathbb{Z}G\,I(A)$, existe um operador $S(\alpha):RX\to RX$ tal que $T(\alpha)=(\omega-1)S(\alpha)$.

ii) Se $\delta\in\mathbb{Z}G\,I(A)$ e $(1+\delta)^P\equiv 1 \pmod{\mathbb{Z}G\,I(A)^{P+1}}$, então $-S(\delta)+S(\delta^P)\equiv 0 \pmod{\omega-1}$.

<u>Demonstração</u> - i) Dados $a\in A$, $y\in X$, temos, pelo lema 4.8, que $T(a-1)y=(\chi(a^y)-1)y$. Agora, é claro que $\chi(a^y)=\omega^k$, para algum k. Logo, do lema 4.2, vem que $\chi(a^y)-1\equiv 0 \pmod{\omega-1}$.

Dado $\alpha\in\mathbb{Z}G\,I(A)$, podemos escrever $\alpha=\sum_{x\in X}\alpha_x(a_x-1)x$, onde $\alpha_x\in\mathbb{Z}$ e $a_x\in A$. Logo, dado $y\in X$, temos

$$T(\alpha)y=\sum_{x\in X}\alpha_x(\chi(a_x^y)-1)xy\in(\omega-1)RX.$$

Assim podemos definir $S(\alpha):RX\longrightarrow RX$ por

$$S(\alpha)y=\frac{T(\alpha)y}{\omega-1}$$

É claro que $S(\alpha)$ é linear, e $T(\alpha)=(\omega-1)S(\alpha)$, provando (i).

ii) Como $(1+\delta)^P\equiv 1 \pmod{\mathbb{Z}G\,I(A)^{p+1}}$, segue, pelo Lema 3.4, que $p\delta+\delta^P\equiv 0 \pmod{\mathbb{Z}G\,I(A)^{p+1}}$. Calculando T, obtemos

$$p\,T(\delta)+T(\delta)^P\equiv 0 \pmod{(\omega-1)^{p+1}},$$

donde segue que

$$p(\omega-1)S(\alpha)+(\omega-1)^p\, S(\delta)^p \equiv 0 \pmod{(\omega-1)^{p+1}},$$

ou, dividindo por $(\omega-1)^p$,

$$\frac{p}{(\omega-1)^{p-1}}\, S(\delta) + S(\delta)^p \equiv 0 \pmod{\omega-1}.$$

Finalmente, observamos que, pelo Lema 4.3 (d), temos

$$\frac{p}{(\omega-1)^{p-1}} \equiv -1 \pmod{\omega-1};$$

logo, obtemos $-S(\delta) + S(\delta)^p \equiv 0 \pmod{\omega-1}$, provando (ii).

Antes de passarmos ao nosso resultado princi - pal, vamos lembrar uma definição que nos será necessária.

<u>Definição</u> - Seja p um primo e $K=GF(p^d)$. Definimos o <u>traço</u> de um elemento $x \in K$ por

$$tr(x) = \sum_{\sigma \in Gal(K/GF(p))} \sigma(x) \in GF(p).$$

Em relação a esta definição, observamos que, como $K=GF(p^d)$, $Gal(K/GF(p)) = \langle \sigma_p \rangle$, onde $\sigma_p$ é o automorfismo de K dado por $\sigma_p(x)=x^p$. Então, a equação acima se reduz a

$$tr(x) = \sum_{n=0}^{d-1} x^{p^n}.$$

<u>Teorema 4.10</u> - Seja $G=A.X$, produto semi-direto, onde $A \triangleleft G$ é um subgrupo p-abeliano elementar de ordem $p^d$ e $X$ é um grupo abeliano que age fiel e irredutivelmente sobre $A$. Suponhamos que $|X|=p^d-1$, e seja $\delta = \sum_{x \in X} x(a_x-1)$, com $x \in X$ e $a_x \in A$. Nestas condições, valem:

i) Seja $\chi : A \longrightarrow C$ uma representação não-trivial de grau 1, e seja $T=\chi^G$ a representação de $G$ induzida por $\chi$. Se $\omega$ é uma raiz p-ésima primitiva da unidade e $R=\mathbb{Z}[\omega]$, podemos supor que o espaço de representação de $T$ é $RX$. Se $T(\delta) \equiv 0 \pmod{(\omega-1)^2}$, então $\delta=0$.

ii) Se $\delta \in I_K(G,A)$ e $(1+\delta)^p \equiv 1 \pmod{\mathbb{Z}G\, I(A)^{p+1}}$, então $\delta=0$.

<u>Demonstração</u> - i) Pelo Lema 4.8, podemos supor que o espaço de representação de $T$ é $RX$. Suponhamos, então, que $T(\delta) \equiv 0 \pmod{(\omega-1)^2}$. Como $\delta = \sum_{x \in X} x(a_x-1)$, obtemos que, para todo $y \in X$,

$$T\Big(\sum_{x \in X} x(a_x-1)\Big)y \in (\omega-1)^2 RX,$$

isto é,

$$\sum_{x\in X} (\chi(a_x^y)-1)xy \in (\omega-1)^2 RX.$$

Fixamos $x\in X$, e seja $a=a_x$, de modo que vale $\chi(a^y)-1\equiv 0 \pmod{(\omega-1)^2}$. Como $\chi(a^y)$ é uma potência de $\omega$, segue, pelo lema 4.2, que $\chi(a^y)=1$. Logo $\chi(a^y)=1$, $\forall y\in X$. Agora, se $a\neq 1$, o conjunto $\{a^y | y\in X\}$ gera A, porque A é um X-módulo irredutível. Logo, se $a\neq 1$, $\chi$ é a representação trivial de A, o que contraria a hipótese. Logo, temos que $a_x=a=1$.

Assim, para todo $x\in X$, temos que $a_x=1$, donde $\delta=0$.

ii) a) Pelo Corolário 4.6, existe um isomorfismo $\gamma$ de A sobre o grupo aditivo de $K=GF(p^d)$ e um isomorfismo $\phi: X \longrightarrow K^*$, tais que

$$\gamma(a^x) = \phi(x)\ \gamma(a).$$

Definimos uma representação não trivial de grau 1 de A tomando uma raiz p-ésima primitiva da unidade $\omega\in C$ e considerando $\chi(a)=\omega^{tr(\gamma(a))}$, $\forall a\in A$, onde $tr: K \longrightarrow GF(p)$ é o traço, definido acima. É imediato que $\chi: A \longrightarrow C$ é, de fato, uma representação não-trivial de A. Seja $T=\chi^G$ a representação induzida por $\chi$; pelo ítem (i), podemos supor que o espaço de representação de T é RX. Ainda pelo ítem (i), é claro que basta provarmos que $T(\delta)\equiv 0 \pmod{(\omega-1)^2}$.

Como $\delta \in \mathbb{Z}G\,I(A)$, podemos, pela Proposição 4.9 obter um operador $S(\delta):RX \longrightarrow RX$ tal que $T(\delta)=(\omega-1)S(\delta)$. É claro, então, que basta provar que $S(\delta)\equiv 0 \pmod{(\omega-1)}$.

Dado $\alpha \in \mathbb{Z}G\,I(A)$, podemos reduzir $S(\alpha):RX \longrightarrow RX$ módulo $<\omega-1>$, obtendo

$$\bar{S}(\alpha): \frac{R}{<\omega-1>} X \longrightarrow \frac{R}{<\omega-1>} X.$$

Pelo Lema III.1.3, temos que $\frac{R}{<\omega-1>} \cong GF(p)$, donde obtemos que $\bar{S}(\alpha):GF(p)X \longrightarrow GF(p)X$. Finalmente, como $K=GF(p^d)$, podemos, por extensão de escalares, supor que $\bar{S}(\alpha):KX \longrightarrow KX$. Ainda, $S(\alpha)\equiv 0 \pmod{(\omega-1)}$ se e só se $\bar{S}(\alpha)=0$; logo, basta provarmos que $\bar{S}(\delta)=0$.

Analogamente, dado $x \in G$, podemos reduzir $T(x):RX \longrightarrow RX$ módulo $<\omega-1>$, obtendo, como acima, um operador $\bar{T}(x):KX \longrightarrow KX$. Observamos ainda que, como $T(x(a-1))=T(x)\,T(a-1)$, temos que

$$\bar{S}(x(a-1)) = \bar{T}(x)\,\bar{S}(a-1) \quad \forall x \in X \quad \forall a \in A.$$

Além disso, como $(1+\delta)^p \equiv 1 \pmod{\mathbb{Z}G\,I(A)^{p+1}}$, pela Proposição 4.9 segue que $-S(\delta)+S(\delta)^p \equiv 0 \pmod{\omega-1}$.

b) Como $\chi(a)=\omega^{tr(\gamma(a))}$, temos que, pelo lema 4.3(a),

$$\frac{\chi(a)-1}{\omega-1} = 1+\omega+\ldots+\omega^{tr\gamma(a)-1} \equiv tr(\gamma(a)) \pmod{\omega-1}.$$

Como $S(a-1)y = \dfrac{T(a-1)y}{\omega-1} = \dfrac{\chi(a^y)-1}{\omega-1}y \equiv \operatorname{tr}\gamma(a^y)y \pmod{\omega-1}$,

temos que $\bar{S}(a-1)y=(\operatorname{tr}\gamma(a^y))y=\operatorname{tr}(\phi(y)\gamma(a))y$, $\forall a\in A, \forall y\in X$. Seja $\{\varepsilon_0,\ldots,\varepsilon_{r-1}\}$, $r=p^d-1$, a base de $KX$ obtida no lema 4.7; lembramos que $\varepsilon_i\varepsilon_j=\delta_{ij}\varepsilon_i$. Observamos então que, como

$\varepsilon_i=\frac{1}{r}\sum_{x\in X}\phi(x)^{-i}x$, temos que, $\forall y\in X$,

$$\bar{T}(y)\varepsilon_i=y\varepsilon_i=\frac{1}{r}\sum_{x\in X}\phi(x)^{-i}yx=\phi(y)^i\frac{1}{r}\sum_{x\in X}\phi(yx)^{-i}yx=\phi(y)^i\varepsilon_i.$$

Logo, para todo $y\in X$, a matriz de $\bar{T}(y)$ em relação a esta base é diagonal, da forma

$$\begin{pmatrix} \phi(y)^0 & & & 0 \\ & \phi(y)^1 & & \\ & & \ddots & \\ 0 & & & \phi(y)^{r-1} \end{pmatrix}$$

Dado $a\in A$, temos:

$$\bar{S}(a-1)\varepsilon_j=\bar{S}(a-1)\frac{1}{r}\sum_{x\in X}\phi(x)^{-j}x$$

$$=\frac{1}{r}\sum_{x\in X}\phi(x)^{-j}\bar{S}(a-1)x$$

$$=\frac{1}{r}\sum_{x\in X}\phi(x)^{-j}tr(\phi(x)\gamma(a))x$$

$$=\frac{1}{r}\sum_{x\in X}[\phi(x)^{-j}\sum_{n=0}^{d-1}\phi(x)^{p^n}\gamma(a)^{p^n}x]$$

$$=\sum_{n=0}^{d-1}[\gamma(a)^{p^n}\frac{1}{r}\sum_{x\in X}\phi(x)^{-j+p^n}x] .$$

Logo, temos $\bar{S}(a-1)\varepsilon_j=\sum_{n=0}^{d-1}\gamma(a)^{p^n}\varepsilon_{j-p^n}$, $a\in A$, onde $j$ e $j-p^n$ são tomados módulo $r$.

Então, como $\delta=\sum_{x\in X}x(a_x-1)$, temos

$$\bar{S}(\delta)\varepsilon_j=\sum_{x\in X}\bar{T}(x)\bar{S}(a_x-1)\varepsilon_j=$$

$$=\sum_{x\in X}\sum_{n=0}^{d-1}\gamma(a_x)^{p^n}\phi(x)^{j-p^n}\varepsilon_{j-p^n}$$

$$=\sum_{n=0}^{d-1}\sum_{x\in X}(\gamma(a_x)\phi(x)^{p^{-n}j-1})^{p^n}\varepsilon_{j-p^n}.$$

Definindo, então, para todo $i$ (tomado módulo $r$),

$$\delta_i=\sum_{x\in X}\phi(x)^i\gamma(a_x),$$

podemos escrever

$$\bar{S}(\delta)\varepsilon_j = \sum_{n=0}^{d-1} (\delta_{p^{-n}j-1})^{p^n} \varepsilon_{j-p^n}. \qquad (*)$$

c) Seja $(S(i,j))$ a matriz de $\bar{S}(\delta)$ em relação à base $\{\varepsilon_0,\ldots,\varepsilon_{r-1}\}$, isto é,

$$\bar{S}(\delta)\varepsilon_j = \sum_{i \bmod r} S(i,j)\varepsilon_i.$$

Então a equação (*) implica em que $S(i,j)=0$ exceto se $j-i\equiv p^n \pmod r$ para algum n.

Tomando n=0 em (*), obtemos que

$$S(j,\ j+1) = \delta_j, \quad \forall j \bmod r.$$

Como já foi observado no ítem (a), temos que $-S(\delta)+S(\delta)^p\equiv 0 \pmod{(\omega-1)}$; logo $\bar{S}(\delta)=\bar{S}(\delta)^p$. Fazendo o produto de matrizes, obtemos que

$$S(i,j)= \sum_{m_1,\ldots,m_{p-1}} S(i,m_1)S(m_1,m_2)\ldots S(m_{p-1},j). \quad (**)$$

Como $S(i,j)=0$ exceto se $j-i\equiv p^n$, vemos que a soma se reduz àqueles $(m_1,\ldots, m_{p-1})$ tais que $m_1-i,\ m_2-m_1,\ldots,j-m_{p-1}$ são todos potências de p módulo r.

Suponhamos, então, que $S(i,j)\neq 0$. Então, para cada termo $(m_1,\ldots,m_{p-1})$ <u>que aparece na soma</u>, temos

$$(m_1-i)+\ldots+(j-m_{p-1})=j-i\equiv p^n \pmod r,$$

donde obtemos

$$p^{n_1}+\ldots+p^{n_p}\equiv p^n \pmod r.$$

Pelo Lema 4.1, segue que $n_1\equiv n_2\equiv\ldots\equiv n_p\equiv n-1 \pmod d$ e $p^{n_i}\equiv p^{n-1} \pmod r$, $i=1,2,\ldots,p$.

Logo, a soma em (**) se reduz a um único termo:

$$S(i,i+p^n) = \prod_{m=0}^{p-1} S(i+mp^{n-1}, i+(m+1)p^{n-1}). \quad (***)$$

Substituindo, então, $n=1$, obtemos

$$S(i,i+p)=\prod_{m_0=0}^{p-1} S(i+m_0,\ i+m_0+1); \quad (****)$$

e, substituindo $n=2$,

$$S(i,i+p^2)=\prod_{m_1=0}^{p-1} S(i+m_1p,\ i+(m_1+1)p).$$

Agora, substituindo (****) nesta última equação, obtemos

$$S(i,i+p^2)=\prod_{m_1}\prod_{m_0} S(i+m_1p+m_0,\ i+m_1p+m_0+1).$$

Prosseguindo dessa forma, obtemos

$$S(i,i+1)=\prod_{m_{d-1}}\cdots\prod_{m_1}\prod_{m_0} S(i+m_{d-1}p^{d-1}+\ldots+m_1p+m_0,\, i+m_{d-1}p^{d-1}+\ldots+m_1p+m_0+1).$$

Agora, como $m_{d-1}p^{d-1}+\ldots+m_1p+m_0$, $0\leqslant m_s\leqslant p-1$ é a expansão dos inteiros de 0 a r na base p, obtemos que

$$S(i,i+1)=S(i,i+1)S(i+1,i+2)\ldots S(i-1,i)S(i,i+1),$$

para todo i (tomado módulo r).

d) Finalmente, como $\delta\in I_k(G,A)$, temos que

$$\prod_x (a_x)^{x^k} = 1,$$

donde, aplicando $\gamma$, vem

$$0 = \sum_x \phi(x)^k \ \gamma(a_x) = \delta_k.$$

Como $S(k,k+1)=\delta_k$, segue que $S(k,k+1)=0$, donde obtemos imediatamente que $S(i,i+1)=0$, para todo i. Como novamente, $S(i,i+1)=\delta_i$, obtemos que $\delta_i=0$, para todo i, donde, por (*), $\bar{S}(\delta)=0$, provando o teorema.

<u>Teorema 4.11</u> - [Cliff, Sehgal, Weiss, 1980]. Seja $G$ um grupo metabeliano finito, e suponhamos que $G=AX$, onde $A \triangleleft G$, $A$ é p-abeliano elementar e que $X$ é abeliano e age fiel e irredutivelmente sobre $A$. Se $\delta \in I_K(G,A)$ e $(1+\delta)^p \equiv 1 \pmod{\mathbb{Z}G\, I(A)^{p+1}}$, então $\delta \in \mathbb{Z}G\, I(A)^2$.

<u>Demonstração</u> - Pelo Corolário 4.6, temos que $|X| \mid p^d-1$, onde $|A|=p^d$. Distinguimos, então, dois casos:

i) $|X|=p^d-1$. Neste caso, pelo Lema I.3.9, como $\delta \in I_K(G,A) \subset \mathbb{Z}G\, I(A)$, podemos escrever $\delta$ na forma

$$\delta = \sum_{x \in X} x(a_x-1) + \alpha ,$$

com $a_x \in A$ e $\alpha \in \mathbb{Z}G\, I(A)^2$. Então, pelo Lema 3.5, temos que

$$(1+\delta)^p = (1+\alpha+\sum_{x \in X} x(a_x-1))^p \equiv (1+\sum_{x \in X} x(a_x-1))^p \pmod{\mathbb{Z}G\, I(A)^{p+1}}.$$

Logo, como $(1+\delta)^p \equiv 1 \pmod{\mathbb{Z}G\, I(A)^{p+1}}$, vem que

$$(1+\sum_{x \in X} x(a_x-1)^p \equiv 1 \pmod{\mathbb{Z}G\, I(A)^{p+1}},$$

e, pelo Teorema 4.10, segue que $\sum_{x \in X} x(a_x-1)=0$, donde $\delta = \alpha \in \mathbb{Z}G\, I(A)^2$, provando o teorema neste caso.

ii) Se $|X| < p^d-1$, seja $X_1$ um grupo cíclico de ordem $p^d-1$ contendo $X$, e seja $\phi_1 : X_1 \longrightarrow K^*$ um isomorfismo que estende o homomorfismo $\phi : X \longrightarrow K^*$ dado pelo Corolário 4.6.

Seja $G_1 = A.X_1$ o produto semi-direto, com a ação de $X_1$ em $A$ definida por

$$a^x = \gamma^{-1}(\phi_1(x)\gamma(a)) \quad \forall a \in A, \ \forall x \in X_1,$$

onde $\gamma$ é o isomorfismo $\gamma : A \longrightarrow K$ do Corolário 4.6. É imediato, então, que $G \subset G_1$, e como $G = AX$, $G_1 = AX_1$ e $X \subset X_1$, temos $I_k(G,A) \subset I_k(G_1,A)$. Logo, $\delta \in I_K(G_1,A)$, e como $|X_1| = p^d-1$, segue, pelo caso (i), que $\delta \in \mathbb{Z}G_1 I(A)^2$. Mas, como $\delta \in \mathbb{Z}G$, obtemos que $\delta \in \mathbb{Z}G\, I(A)^2$, e o teorema está provado.

Podemos, agora, obter o resultado central desta seção.

<u>Corolário 4.12</u> - [Cliff, Sehgal, Weiss, 1980] Se $G = A.X$, onde $A \triangleleft G$, $A$ é p-abeliano elementar finito e $X$ é abeliano e age fiel e irredutivelmente sobre $A$, então o subgrupo

$$V(\mathbb{Z}G) \cap (1 + I_k(G,A)).$$

é livre de torção, para todo $k \in \mathbb{Z}$.

Demonstração - Seja $\alpha \in V(\mathbb{Z}G) \cap (1+I_k(G,A))$, e ponhamos $\alpha=1+\delta$, com $\delta \in I_k(G,A)$. Suponhamos que, para algum primo q, $\alpha^q=(1+\delta)^q=1$. Então:

a) Se $p \neq q$, então $\delta=0$ pelo lema 3.1.

b) Se $p=q$, então, pelo Teorema 4.11, segue que $\delta \in \mathbb{Z}G\, I(A)^2$, donde, pelo lema 3.2, $\delta=0$. Logo, $\alpha=1$, e $V(\mathbb{Z}G) \cap (1+I_k(G,A))$ é livre de torção.

## § 5. CASO GERAL

Já provamos que o subgrupo $V(\mathbb{Z}G) \cap (1+I_k(G,A))$ é livre de torção se $G=AX$ e X age fiel e irredutivelmente sobre A. Nesta seção, provaremos que o mesmo vale para G metabeliano qualquer. Estudaremos, primeiro, o caso em que G cinde sobre A, passando, depois, ao caso metabeliano geral. Para isso, precisaremos de vários resultados preliminares.

Lema 5.1 - Seja G um grupo finito e A um subgrupo normal abeliano de G. Se $H \triangleleft G$ e $\pi_H : \mathbb{Z}G \longrightarrow \mathbb{Z}\, G/H$ é a projeção natural, então, para todo $k \in \mathbb{Z}$, tem-se que

$$\pi_H(I_k(G,A)) \subset I_k(G/H,\ \pi_H(A)).$$

Demonstração - Basta notar que $\delta=\sum_i n_i g_i(a_i-1) \in I_k(G,A)$ im-

plica em que $\prod_i (a_i^{n_i})^{g_i^k} = 1$, donde $\pi_H(\prod_i (a_i^{n_i})^{g_i^k})=1$, e

portanto $\prod_i (\pi_n (a_i)^{n_i})^{\pi_H(g_i)^k} = 1$. Logo, $\pi_H(\delta) =$

$= \sum_i n_i\pi_H(g_i)(\pi_H(a_i)-1) \in I_k(G/H, \pi_H(A))$.

<u>Proposição 5.2</u> - Seja $G=AX$ um grupo finito, com $A \triangleleft G$, $A \cap X=1$, $A$ e $X$ abelianos. Se existe um subgrupo central de $G$ contido em $X$, não trivial, então

$$V(\mathbb{Z}G) \cap (1+I_K(G,A))$$

é livre de torção, para todo $k \in \mathbb{Z}$.

<u>Demonstração</u> - Usamos indução em $|G|$, observando que o caso $|G|=1$ é trivial.

Seja, então, $u \in V(\mathbb{Z}G) \cap (1+I_k(G,A))$, e suponhamos que $u^p=1$, para algum primo $p$. Como $H \leqslant X$, então $G/H$ cinde sobre $A$ (isto é, $G/H \cong A.X/H$). Seja $\pi:\mathbb{Z}G \longrightarrow \mathbb{Z}\,G/H$ a projeção natural; escrevemos $\bar{G}=G/H$, $\bar{A}=\pi(A)$ e, dado $\alpha \in \mathbb{Z}G$, poremos $\bar{\alpha}=\pi(\alpha)$.

Como $\pi(I_k(G,A)) \subset I_k(\bar{G},\bar{A})$, pelo lema 5.1, temos que $\bar{u} \equiv 1 \pmod{I_k(\bar{G},\bar{A})}$ e $\bar{u}^p=1$. Logo, por indução, $\bar{u}=1$ em $\mathbb{Z}\bar{G}$, donde $u \equiv 1 \pmod{\mathbb{Z}G\,I(H)}$.

Seja $\{1,g_2,\ldots,g_n\}$ uma transversal para H em G. Podemos escrever

$$u=1+\alpha+\sum_{i=2}^{n} g_i\alpha_i, \text{ com } \alpha,\alpha_i \in I(H).$$

Nestas condições, como $1\notin \operatorname{supp}\left(\sum_{i=2}^{n} g_i\ \alpha_i\right)$, temos que, se $\alpha=0$, então $1\in\operatorname{supp}(u)$, donde, pelo Teorema I.2.4, $u=1$.

Por outro lado, se $\alpha\neq 0$, então existe $h\in H$ tal que $h\in\operatorname{supp}(u)$, já que $\operatorname{supp}(\alpha)\subset H$ e $\operatorname{supp}\left(\sum_{i=2}^{n} g_i\ \alpha_i\right)\cap H=\phi$. Mas, então, aplicando o Teorema I.2.4 a $uh^{-1}$, obtemos que $u=h$. Mas $G\cap(1+I_k(G,A))=1$, pelo lema 2.1(d), donde $u=1$, provando a proposição.

<u>Proposição 5.3</u> - Seja $G=AX$ um grupo finito, com $A\triangleleft G$, $A\cap X=1$, A e X abelianos, e seja B um subgrupo normal de G contido em A. Se existem $B_1\triangleleft G$, $B_2\triangleleft G$, não triviais, tais que $B=B_1\times B_2$, então

$$V(\mathbb{Z}G)\ \cap\ (1+I_k(G,A))$$

é livre de torção, para todo $k\in\mathbb{Z}$.

<u>Demonstração</u> - Usamos indução em $|G|$, o caso $|G|=1$ sendo trivial.

Seja $\pi_1 : \mathbb{Z}G \longrightarrow \mathbb{Z}G/B_1$ a projeção natural, e tomemos $u \in V(\mathbb{Z}G) \cap (1+I_k(G,A))$ tal que $u^p=1$, para algum primo p. Então, como na demonstração da proposição anterior, segue por indução que $\pi_1(u)=1$, donde $u \equiv 1 \pmod{\mathbb{Z}G\, I(B_1)}$. Da mesma forma, obtemos que $u \equiv 1 \pmod{\mathbb{Z}G\, I(B_2)}$.

Logo,

$$u \equiv 1 (\mathrm{mod}\ \mathbb{Z}G\, I(B_1) \cap \mathbb{Z}G\, I(B_2));$$

e, pelo lema I.3.11, temos que $\mathbb{Z}G\, I(B_1) \cap \mathbb{Z}G\, I(B_2) = \mathbb{Z}G\, I(B_1)\, I(B_2)$, donde $u \equiv 1 \pmod{\mathbb{Z}G\, I(B_1)\, I(B_2)}$. Mas, como $B_1 \subset A$ e $B_2 \subset A$, vem que $\mathbb{Z}G\, I(B_1) I(B_2) \subset \mathbb{Z}G\, I(A)^2$. Logo, $u \equiv 1 (\mathrm{mod}\ \mathbb{Z}G\, I(A)^2)$, donde, pelo lema 3.2, segue que $u=1$. Assim, neste caso,

$$V(\mathbb{Z}G) \cap (1+I_k(G,A))$$

é livre de torção, $\forall k \in \mathbb{Z}$.

<u>Definição</u> - Seja G um grupo finito e $B \triangleleft G$. Dizemos que B é <u>indecomponível em subgrupos normais</u> se $B=B_1 \times B_2$ com com $B_1 \triangleleft G$ e $B_2 \triangleleft G$ implica em que $B_1 = \langle 1 \rangle$ ou $B_2 = \langle 1 \rangle$.

Dessa forma, a Proposição 5.3 nos permite reduzir o problema ao caso em que G=AX e todo subgrupo de G contido em A é indecomponível em subgrupos normais. Em particular, como $A \triangleleft G$, obtemos um corolário importante.

Corolário 5.4 - Seja $G=AX$ um grupo finito, com $A \triangleleft G$, $A \cap X=1$, $A$ e $X$ abelianos. Se $u \in V(\mathbb{Z}G) \cap (1+I_k(G,A))$ satisfaz $u^p=1$ para algum primo $p$ e $A$ não é um $p$-grupo, então $u=1$.

Demonstração - Em primeiro lugar, observamos que, se $A$ não é um $q$-grupo, para algum primo $q$, $A$ pode ser escrito como o produto dos seus subgrupos de Sylow(que são normais em $G$ porque $A$ é abeliano).

Pela Proposição 5.3, $V(\mathbb{Z}G) \cap (1+I_k(G,A))$ é livre de torção, donde $u=1$.

Por outro lado, se $A$ é um $q$-grupo e $q \neq p$, temos que $u \equiv 1 \pmod{\mathbb{Z}G\, I(A)}$ e $u^p=1$, donde, como $p \nmid |A|$, segue pelo lema 3.1, que $u=1$.

Lema 5.5 - Seja $X$ um grupo abeliano finito e $p$ um primo. Então existem subgrupos $X_p \triangleleft X$, $X_0 \triangleleft X$ tais que $X=Xp \times X_0$, $Xp$ é um $p$-grupo e $p \nmid |X_0|$.

Demonstração - imediato.

Definição - Seja $X$ um grupo finito e $p$ um número primo.

i) Um subgrupo $X_0 < X$ diz-se um p'-subgrupo de X se $p \nmid |X_0|$;

ii) Um subgrupo $X_0 \triangleleft X$ diz-se um p'-subgrupo de Hall de X se existe $X_p \triangleleft X$ tal que $X_0$ é um p'-

-subgrupo de X, $X_p$ é um p-subgrupo de X e $X = X_0 \times X_p$.

Antes do nosso próximo resultado significativo, necessitamos ainda de mais um lema.

Lema 5.6 - Seja A um grupo p-abeliano elementar finito. Se $\alpha \in \mathbb{Z}A$ e $p\alpha \in I(A)^{p+1}$, então $\alpha \in I(A)^2$.

Demonstração - Seja $\alpha \in \mathbb{Z}A$, e suponhamos que $p\alpha \in I(A)^{p+1}$. Então é claro que $\alpha \in I(A)$, e, pelo Corolário I.3.6, existe $a \in A$ tal que $\alpha \equiv a-1 \pmod{I(A)^2}$. Logo, basta provar o Teorema para o caso $\alpha = a-1$.

Suponhamos, então $\alpha = a-1$. Queremos provar que $\alpha \in I(A)^2$, o que, pelo Corolário I.3.6, é equivalente a provar que $a=1$.

Se $a \neq 1$, seja $\chi : A \longrightarrow C$ uma representação linear não-trivial de A, com $\chi(a) = \omega$, onde $\omega$ é uma raiz p-ésima primitiva da unidade. Estendendo $\chi$ $\mathbb{Z}$ - linearmente, obtemos um homomorfismo $\chi : \mathbb{Z}A \longrightarrow \mathbb{Z}[\omega]$.

Agora, $\chi(p(a-1)) = p(\omega-1)$ e $\chi(I(A)^{p+1}) = \chi(I(A))^{p+1} = (\omega-1)^{p+1}\mathbb{Z}[\omega]$. Portanto, $p(a-1) \in I(A)^{p+1}$ implica em que $p(\omega-1) \in (\omega-1)^{p+1}\mathbb{Z}[\omega]$, o que é absurdo, pois $(\omega-1)^{p-1} | p$ e $(\omega-1)^p \nmid p$. Logo, devemos ter $a=1$, e o lema está provado.

Teorema 5.7 - Sejam $G = AX$, $A \triangleleft G$, $A \cap X = 1$, A e X abelianos. Suponhamos que A é um p-grupo abeliano elementar para algum primo p, e que um p'-subgrupo de Hall $X_0$

de X age fiel e irredutivelmente sobre A. Nestas condições, se $\delta \in I_k(G,A)$ e $(1+\delta)^p \equiv 1 \pmod{\mathbb{Z}G\, I(A)^{p+1}}$, então $\delta \in \mathbb{Z}G\, I(A)^2$.

Demonstração - Escrevemos $X=X_0 \times X_p$, onde $X_p$ é o p-subgrupo de Sylow de X. Usamos indução em $|X_p|$.

i) O caso $|X_p|=1$ é o Teorema 4.11, de modo que não há nada a demonstrar.

ii) Suponhamos que $|X_p| > 1$, e seja $B=C_A(X_p)$. Como o caso $|A|=1$ é trivial, podemos supor $|A|\neq 1$. Como $AX_p$ é um p-grupo e $A \triangleleft AX_p$, temos que

$$A \cap Z(AX_p) \neq 1,$$

e como $A \cap Z(AX_p) \subset C_A(X_p)$, segue que $|B|\neq 1$. Além disso, é imediato que $B \triangleleft G$, e portanto B é estável pela ação de $X_0$. Como $X_0$ age irredutivelmente sobre A, segue que $B=A$. Logo, $C_A(X_p)=A$, donde segue que $X_p \subset Z(G)$.

Tomemos $x \in X_p$ com $x^p=1$, $x\neq 1$. Como $X_p \subset Z(G)$, temos $\langle x\rangle \triangleleft G$. Seja, então, $-:\mathbb{Z}G \longrightarrow \mathbb{Z}G/\langle x\rangle$ o epimorfismo natural. É imediato que, por indução, devemos ter $\bar{\delta} \in \mathbb{Z}\bar{G}\ I(\bar{A})^2$, de modo que

$$\delta = \alpha + \delta_1, \text{ onde } \alpha \in \mathbb{Z}G\, I(A)^2 \text{ e } \delta_1 \in \mathbb{Z}G\, I(\langle x\rangle).$$

Do lema 3.5, vem que

$$(1+\delta_1)^p=(1+\delta-\alpha)^p\equiv(1+\delta)^p \pmod{\mathbb{Z}G\,I(A)^{p+1}},$$

de modo que temos $(1+\delta_1)^p\equiv 1 \pmod{\mathbb{Z}G\,I(A)^{p+1}}$. Então, pelo lema 3.4, segue que

$$p\delta_1 + \delta_1^p \equiv 0 \pmod{\mathbb{Z}G\,I(A)^{p+1}}.$$

Além disso $\delta_1 \in \mathbb{Z}G\,I(\langle x\rangle) \cap \mathbb{Z}G\,I(A)=\mathbb{Z}G\,I(\langle x\rangle)I(A)$, pelo lema I.3.11. Como $I(\langle x\rangle)=(1-x)\mathbb{Z}\langle x\rangle$, e pelo lema 3.3, temos:

$$I(\langle x\rangle)^p=(1-x)^p\mathbb{Z}\langle x\rangle = p(1-x)\mathbb{Z}\langle x\rangle$$

e

$$p\,\mathbb{Z}G\,I(A) \subset \mathbb{Z}G\,I(A)^p.$$

Logo,

$$\delta_1^p \in (1-x)^p\,\mathbb{Z}G\,I(A)^p = p(1-x)\mathbb{Z}G\,I(A)^p \subset$$
$$\subset (1-x)\,\mathbb{Z}G\,I(A)^{p+1} \subset \mathbb{Z}G\,I(A)^{p+1}.$$

Assim, como $p\delta_1+\delta_1^p\equiv 0 \pmod{\mathbb{Z}G\,I(A)^{p+1}}$ e também $\delta_1^p \in \mathbb{Z}G\,I(A)^{p+1}$, segue que $p\delta_1 \in \mathbb{Z}G\,I(A)^{p+1}$. Escrevendo $\delta_1 = \sum_{x\in X} x\,\alpha_x$, com $\alpha_x \in \mathbb{Z}A$, vem que, como $p\delta_1 \in \mathbb{Z}G\,I(A)^{p+1}$, $p\alpha_x \in I(A)^{p+1}$, para todo $x\in X$. Logo, pelo lema 5.6, $\alpha_x \in I(A)^2$,

para todo $x \in X$, donde $\delta_1 \in \mathbb{Z}G\,I(A)^2$. Como $\delta \equiv \delta_1 \pmod{\mathbb{Z}G\,I(A)^2}$, segue que $\delta \in \mathbb{Z}G\,I(A)^2$, provando o teorema.

Usando este teorema, poderemos estender o Corolário 4.12 para o caso em que G cinde sobre A, sem hipótese sobre a ação de X. Para tanto, necessitaremos de alguns resultados preliminares da teoria de grupos, alguns dos quais serão citados sem demonstração.

Teorema 5.8 - Seja $X_p \times X_0$ um grupo de automorfismos de um p-grupo A, com $X_p$ um p-grupo e $X_0$ um p'-grupo. Se $X_0$ age trivialmente em $C_A(X_p)$, então $X_0=1$.

Demonstração - [Gorenstein, 1968, Theorem 5.3.4].

Teorema 5.9 - Se $X_0$ é um p'-grupo de automorfismos de um p-grupo abeliano G que age trivialmente em $\Omega_1(G)=\{g \in G \mid g^p=1\}$, então $X_0=1$.

Demonstração - [Gorenstein, 1968, Theorem 5.2.4].

Corolário 5.10 - Seja $G=AX$ um grupo finito, com $A \triangleleft G, A \cap X=1$, A um p-grupo abeliano e X um grupo abeliano. Escrevemos $X=X_0 \times X_p$, onde $X_0$ é p'-grupo e $X_p$ é p-grupo. Então $C_A(X_p) \neq 1$ e, se X age fielmente em A, $X_0$ age fielmente em $C_A(X_p)$ e em $B=\Omega_1(C_A(X_p))$.

Demonstração - Como $A \triangleleft AX_p$ e $AX_p$ é p-grupo, temos que $1 \neq A \cap Z(AX_p) \subset C_A(X_p)$. Logo $C_A(X_p) \neq 1$. Suponhamos, então, que X age fielmente em A, de modo que X pode ser olhado como um grupo de automorfismos de A.

i) É claro que $C_A(X_p)$ é estável sob a ação de $X_0$. Queremos provar que esta ação é fiel. Seja, então, $x \in X_0$ tal que $x^{-1}\, a\, x = a$ $\forall a \in C_A(X_p)$, e consideremos o grupo $X_p \times \langle x \rangle$ que é claramente um grupo de automorfismos de A que satisfaz as hipóteses do Teorema 5.8. Logo, $\langle x \rangle = 1$, donde $x=1$. Assim, $X_0$ age fielmente em $C_A(X_p)$.

ii) Como $X_0$ age fielmente em $C_A(X_p)$, posso olhá-lo como um grupo de automorfismos de $C_A(X_p)$, que é um p-grupo abeliano. É claro que $B=\Omega_1(C_A(X_p))$ é estável sob a ação de $X_0$.

Seja $x \in X_0$ tal que $x^{-1}\, b\, x = b$, $\forall b \in B$, e considero $\langle x \rangle < X_0$. Então $\langle x \rangle$ é um p'-grupo de automorfismos de $C_A(X_p)$ que age trivialmente sobre $\Omega_1(C_A(X_p))$, donde, pelo teorema 5.9, temos $\langle x \rangle = 1$, i.é, $x=1$.

Logo $X_0$ age fielmente sobre B.

Teorema 5.11 - (Teorema de Maschke generalizado). Seja G um grupo e R um anel com unidade. Então RG é semisimples se e sômente se as seguintes condições estão verificadas:

(i) G é finito.

(ii) $|G|$ é inversível em R.

(iii) R é um anel semisimples.

Demonstração - [Polcino Milies, 1976, Teorema 7.11].

Proposição 5.12 - Seja G um p'-grupo de automorfismos de um p-grupo abeliano elementar V, e suponha que $V_1$ é um fator direto de V que é G-invariante. Então $V=V_1 \times V_2$, onde $V_2$ é G-invariante.

Demonstração - Escrevendo V aditivamente, é imediato que V possui estrutura de $\mathbb{Z}_p$- espaço vetorial de dimensão finita. Logo, podemos definir em V uma estrutura de $\mathbb{Z}_p$ G-módulo, de forma natural.

Pelo Teorema 5.11, $\mathbb{Z}_p G$ é semisimples; logo V é um $\mathbb{Z}_p$ G-módulo completamente redutível, isto é, todo $\mathbb{Z}_p$ G-submódulo $V_1$ de V é somando direto. Mas é isto que afirma a proposição.

Proposição 5.13 - Seja G=AX um grupo finito, com $A \triangleleft G$, $A \cap X=1$, A um p-grupo abeliano e X um grupo abeliano. Escrevemos $X=X_0 \times X_p$, onde $X_0$ é p'-grupo e $X_p$ é p-grupo, e

seja $B=\Omega_1(C_A(X_p))$. Então, se X age fielmente em A e B é indecomponível em subgrupos normais de G, $X_0$ age fiel e irredutivelmente em B.

Demonstração - Segue do Corolário 5.10 que $B\neq 1$ e que $X_0$ age fielmente em B. Seja $B_1 < B$, e suponhamos que $B_1$ é estável sob $X_0$. Pela proposição 5.12, segue que temos $B=B_1 \times B_2$, onde $B_1$ e $B_2$ são estáveis sob $X_0$. Mas é imediato que, como $B_1, B_2 \subset C_A(X_p)$, $B_1$ e $B_2$ são estáveis sob $AX_p$. Logo $B_1 \triangleleft G$ e $B_2 \triangleleft G$, donde, como B é indecomponível em subgrupos normais de G, $B_1=1$ ou $B_2=1$. Logo $X_0$ age irredutivelmente em B.

Passamos, agora, a nosso segundo resultado importante, nesta seção.

Teorema 5.14 - Seja $G=AX$ um grupo finito, com $A \triangleleft G, A \cap X=1$, A e X abelianos. Então

$$V(\mathbb{Z}G) \cap (1+I_k(G,A))$$

é livre de torção, para todo $k \in \mathbb{Z}$.

Demonstração - i) Observamos, em primeiro lugar, que pela Proposição 5.2, se X contém um subgrupo central de G, então $V(\mathbb{Z}G) \cap (1+I_k(G,A))$ é livre de torção. Da mesma forma, segue da Proposição 5.3 que o teorema vale se existe um subgrupo normal de G contido em A que seja de-

componível num produto de subgrupos normais de G.

Seja $u \in V(\mathbb{Z}G) \cap (1+I_k(G,A))$, e suponhamos que $u^p=1$ para algum primo p. Se A é um q-grupo, para $p \neq q$, temos u=1 pelo Corolário 5.4. Logo, podemos supor que:

a) A é um p-grupo,

b) X não contém nenhum subgrupo central de G,

c) A não contém nenhum subgrupo normal de G decomponível como produto de subgrupos normais de G.

ii) Supondo $u^p=1$ e supondo que G satisfaz (a), (b) e (c), queremos provar que u=1. Fá-lo-emos por indução em $|G|$, observando que o caso $|G|=1$ é trivial.

Escrevamos $X=X_p \times X_0$, onde $X_p$ é um p-grupo e $X_0$ é um p'-grupo. Se existe $x \in X$ tal que $x^{-1} a x = a$, $\forall a \in A$, é claro que $\langle x \rangle \subset X$ é um subgrupo central de G, contra a hipótese (b). Logo X age fielmente em A. Pondo $B=\Omega_1(C_A(X_p))$, temos, por (c), que B é indecomponível em subgrupos normais de G. Logo, pela Preposição 5.13, $X_0$ age fiel e irredutivelmente em $B \neq 1$.

Seja, agora, $u=1+\delta$, com $\delta \in I_k(G,A)$. Como $|B| > 1$, temos, por indução, que $u \equiv 1 \pmod{\mathbb{Z}G\, I(B)}$, de modo que $\delta \in \mathbb{Z}G\, I(B)$. Seja $\{a_1,\ldots,a_n\}$ uma transversal

para B em A. Então, podemos escrever

$$\delta = \sum_{x\in X} \sum_{i=1}^{n} x\, a_i\, \beta_{ix},$$

com $\beta_{ix} \in I(B)$, $\forall x\in X$, $i=1,\ldots,n$. Sejam, então

$$\alpha = \sum_{x\in X} \sum_{i=1}^{n} x(a_i-1)\beta_{ix} \quad e \quad \delta_1 = \sum_{x\in X} \sum_{i=1}^{n} x\, \beta_{ix},$$

de modo que $\delta=\alpha+\delta_1$, e $\alpha\in \mathbb{Z}G\, I(A)\, I(B)$. Além disso, como $\delta\in I_k(G,A)$ e $\alpha\in \mathbb{Z}G\, I(A)^2 \subset I_k(G,A)$, temos também que $\delta_1\in I_k(G,A)$. Se pusermos, então $G_1=BX$, segue que $\delta_1\in I_k(G_1,B)$.

Agora, pelo Lema 3.5, temos que

$$1=(1+\delta)^p=(1+\alpha+\delta_1)^p \equiv (1+\delta_1)^p \pmod{\mathbb{Z}G\, I(A)\, I(B)^p}.$$

Além disso, como $\delta_1\in \mathbb{Z}G_1$, temos

$$1-(1+\delta_1)^p \in \mathbb{Z}G\, I(A)\, I(B)^p \cap \mathbb{Z}G_1 = \mathbb{Z}G_1\, I(B)^{p+1},$$

pelo lema 3.6. Logo, $(1+\delta_1)^p\equiv 1 \pmod{\mathbb{Z}G_1\, I(B)^{p+1}}$. Como B é p-abeliano elementar, $G_1=BX$ e $X_0$ age fiel e irredutivelmente sobre B, segue, pelo Teorema 5.7, que $\delta_1 \in \mathbb{Z}G_1\, I(B)^2 \subset \mathbb{Z}G\, I(A)^2$.

Como $\alpha\in \mathbb{Z}G\, I(A)^2$, segue que $\delta\in \mathbb{Z}G\, I(A)^2$, e, pe

lo lema 3.2, segue que $\delta=0$, donde $u=1$. Logo,

$$V(\mathbb{Z}G) \cap (1+I_k(G,A))$$

é livre de torção, como se desejava demonstrar.

Resta, agora, generalisar este último resultado para grupos metabelianos quaisquer. Para tanto, usaremos uma construção clássica da teoria dos grupos, o produto orlado ("wreath product").

<u>Definição</u> - Sejam A e B grupos finitos. O <u>produto orlado</u> de A e B é o conjunto $A \wr B=\{(f,\alpha) \mid \alpha \in B,\ f:B \to A\}$, munido do produto dado por

$$(f_1,\alpha_1)(f_2,\alpha_2)=(g,\alpha_1\alpha_2),$$

onde, $\forall \beta \in B$, $g(\beta)=f_1(\beta)f_2(\beta\alpha_1)$.

É imediato observar que

$$A \wr B = A^B.B \text{ (produto semi-direto)},$$

onde $A^B=\{f \mid f:B \to A\}$ e a ação de B em $A^B$ é dada por $f^\beta(\alpha)=f(\alpha\beta)$, $\forall \beta \in B$. Dessa forma, segue imediatamente que $A \wr B$ é um grupo. A propriedade fundamental, para nós, desta construção é dada pelo próximo resultado, que não será demonstrado aqui.

<u>Proposição 5.15</u> - [Huppert, 1967, Satz I.15.9]. Sejam $A \triangleleft G$ e $X=G/A$ grupos finitos. Então existe um monomorfismo $\tau: G \to A \wr X$, satisfazendo $\tau(A) \subset A^X$ e também $A \wr X = A^X . \tau(G)$.

Podemos, agora, obter nosso resultado fundamental.

<u>Teorema 5.16</u> - [Cliff, Sehgal, Weiss, 1980]. Seja $G$ um grupo metabeliano finito, com $A \triangleleft G$ e $A$ e $G/A$ abelianos. Então, para todo $k \in \mathbb{Z}$, $V(\mathbb{Z}G) \cap (1+I_k(G,A))$ é livre de torção.

<u>Demonstração</u> - Seja $X=G/A$, e ponhamos $\tilde{G}=A \wr X$, $\tilde{A}=A^X \subset A \wr X$. Pela Proposição 5.15, existe um monomorfismo $\tau: G \to \tilde{G}$, $\tilde{A} \triangleleft \tilde{G}$, $\tilde{G}=\tilde{A}.X$, produto semidireto, $\tilde{G}=\tilde{A}.\tau(G)$ e $\tau(A) \subset \tilde{A}$. Como $A$ é abeliano e $\tilde{A}=A^X$, $\tilde{A}$ é abeliano. Logo, $\tilde{G}$ satisfaz as hipóteses do Teorema 5.14. Estendemos $\tau$ a um monomorfismo $\tau: \mathbb{Z}G \to \mathbb{Z}\tilde{G}$.

Como $\tau(G) \subset \tilde{G}$ e $\tau(A) \subset \tilde{A}$, $\tau(\mathbb{Z}G\, I(A)) \subset \mathbb{Z}\tilde{G}\, I(\tilde{A})$. Queremos provar que $\tau(I_k(G,A)) \subset I_k(\tilde{G},\tilde{A})$. De fato, se $g(a-1) \in \mathbb{Z}G\, I(A)$, temos que

$$\tau(g(a-1))=\tau(g)(\tau(a)-1) \in \mathbb{Z}\tilde{G}\ I(\tilde{A}),$$

e é imediato que

$$\tau(\phi_k(g(a-1))) = \tau(a^{g^k}) = \tau(a)^{\tau(g)^k} =$$
$$=\phi_k(\tau(g(a-1))).$$

Logo $\tau \circ \phi_k = \phi_k \circ \tau$ nos geradores de $\mathbb{Z}G\,I(A)$, donde $\tau \circ \phi_k = \phi_k \circ \tau$. Mas então segue imediatamente que $\tau(I_k(G,A)) \subset I_k(\tilde{G},\tilde{A})$.

Seja, então, $u \in V(\mathbb{Z}G) \cap (1+I_k(G,A))$, e suponhamos que $u^p=1$, para algum primo p. Então temos

$$\tau(u) \in V(\mathbb{Z}\tilde{G}) \cap (1+I_k(\tilde{G},\tilde{A}))$$

e $\tau(u)^p=1$. Pelo Teorema 5.14, $\tau(u)=1$ e, como $\tau$ é monomorfismo, segue que $u=1$. Logo,

$$V(\mathbb{Z}G) \cap (1+I_k(G,A))$$

é livre de torção, como queríamos provar.

Podemos, então, resumir os resultados deste capítulo para grupos metabelianos finitos:

<u>Teorema 5.17</u> - [Cliff, Sehgal, Weiss, 1980]. Seja G um grupo metabeliano finito, e seja $A \triangleleft G$ um subgrupo normal abeliano. Definindo

$$N_k(G,A) = V(\mathbb{Z}G) \cap (1+I_k(G,A)),$$

temos que:

i) Se $G/A$ é abeliano de expoente 2,3,4 ou 6, então $N_k(G,A)$ é um complemento normal livre de torção para $G$ em $V(\mathbb{Z}G)$, para todo $k \in \mathbb{Z}$;

ii) Se $G/A$ é abeliano de ordem ímpar, então $G$ possui um complemento normal livre de torção em $V(\mathbb{Z}G)$, que é uma extensão de $N_s(G,A)$ por um grupo abeliano livre finitamente gerado, onde $S=\frac{1}{2}([G:A]-1)$.

Conseguimos, desta forma, uma solução parcial para o problema da obtenção de complementos normais para $G$ em $V(\mathbb{Z}G)$. Restaria estudar o caso em que $G/A$ é abeliano de ordem par e não se inclui no caso (i); vale observar que o Exemplo 2.4 mostra que os complementos obtidos neste capítulo não são adequados nesse caso, que, parece, exigirá o desenvolvimento de métodos diferentes.

# BIBLIOGRAFIA


P.J.Allen & C.Hobby

1980 - A Characterization of Units in $\mathbb{Z}[A_n]$, J.Alg.66 (1980), 534-543.

S.D.Berman

1955 - On the Equation $x^m=1$ in an Integral Group Ring, Ukrainsk. Mat. Zh. 7 (1955), 253-261.

G.H.Cliff, S.K.Sehgal & A.R.Weiss

1980 - Units of Integral Group Rings of Metabelian Groups, to appear.

C.W.Curtis & I.Reiner

1962 - Representation Theory of Finite Groups and Assosciative Algebras, Interscience, New York.

E.C.Dade

1971 - Deux Groupes Finis Distincts Ayant la Même Algebre de Groupe sur tout Corps, Math. Z. 119 (1971), 345-348.

R.K.Dennis

1976 - Units of Group Rings, J.Alg. 43(1976), 655-664.

1977 - The Structure of the Unit Group of Group Rings, Lect. Notes in Pure and Appl. Math. 26, Marcel Dekker, New York.

L. Dornhoff

1971 - Group Representation Theory, Part A, Marcel Dekker, New York.

D. Gorenstein

1968 - Finite Groups, Harper e Row, New York.

G. Higman

Tese - Units in Group Rings, Thesis for D. Phil., Oxford University, 1940.

1940 - The Units of Group Rings, Proc.London Math. Soc. (2), 46 (1940), 231-248.

I. Hughes & K.R.Pearson

1972 - The Group of Units of the Integral Group Ring $\mathbb{Z}S_3$, Canad. Math. Bull. 15 (1972), 529-534.

B. Huppert

1967 - Endliche Gruppen I, Springer-Verlag, Heidelberg.

D.A.Jackson

1969 - The Groups of Units of the Integral Group Rings of Finite Metabelian and Finite Nilpotent Groups,Quart. J. Math. Oxford (2), 20 (1969), 319-331.

G.J.Janusz

1973 - Algebraic Number Fields, Academic Press, New York.

D.L.Johnson

1978 - The Modular Group Ring of a Finite p-Group, Proc. Amer. Math. Soc. 68 (1978), 1, 19-22.

G. Karpilovsky

1979a- On the Isomorphism Problem for Integral Group Rings, J.Alg. 59 (1979), 1-4.

1979b- On Group Rings of Finite Metabelian Groups, J. Austral. Math. Soc. (Series A) 28 (1979), 378-384.

1980 - On Certain Group Ring Problems, Bull. Austral. Math. Soc. 21 (1980), 329-350.

1981 - Finite Groups with Isomorphic Group Algebras, Ill. J.Math. 25 (1981), 1, 107-111.

T. Miyata

1980 - On the Units of Integral Group Rings of a Dihedral Group, J. Math. Soc. Japan 32 (1980), 4, 703-708.

T. Obayashi

1970 - Integral Group Rings of Finite Groups, Osaka J.Math. 7 (1970), 253-266.

M.M.Parmenter

1972 - Dimension Theory, Isomorphism and Related Problems in Group Rings, Thesis, University of Alberta.

D.S.Passman

1977 - The Algebraic Structure of Group Rings, Interscience, New York.

D.S.Passman & P.F.Smith

1981 - Units in Integral Group Rings, J.Alg. 69 (1981), 213-239.

C. Polcino Milies

1976 - Anéis de Grupos, Escola de Álgebra, São Paulo.

1973 - The Units of the Integral Group Ring $\mathbb{Z}D_4$, Bol.Soc. Brasil. Mat. 4 (1973), 85-92.

1981 - Units of Group Rings: A Short Survey, Trabalhos do Depto. de Mat. nº 26, IME-USP, São Paulo.

J. Ritter & S.K.Sehgal

1980 - Group Rings of Metabelian Groups, Comm. Alg. 8 (1980), 10, 941-951.

A.I.Saksonov

1971 - Group Rings of Finite Groups I, Publ.Mathematicae Debrecen, 18 (1971), 187-209.

R.Sandling

1972 - Dimension Subgroups over Arbitrary Coefficient Rings, J.Alg. 21 (1972), 250-265.

1974 - Group Rings of Circle and Unit Groups, Math.Z. 140 (1974), 195-202.

1977 - Notes on Higman's Thesis, manuscript.

S.K.Sehgal

1978 - Topics in Group Rings, Marcel Dekker, New York.

K. Sekiguchi

1980 - On the Units of Integral Group Rings, Tokyo J.Math. 3 (1980), 149-162.

M.L.S. Singer

1978 - Anéis Radicais e Grupos Círculo, Dissertação de Mestrado, IME-USP, São Paulo.

A. Whitcomb

1968 - The Group Ring Problem, Ph.D. Thesis, University of Chicago.

Pende