REPRESENTAÇÕES INTEIRAS

DE GRUPOS CÍCLICOS

ALFREDO ROSALIO JONES RODRIGUEZ

Apresentado ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para o Concurso de Habilitação à
Livre-Docência no
Departamento de Matemática

Este trabalho foi realizado com o auxílio da FAPESP 77/0787.

- SÃO PAULO, AGOSTO DE 1979 -

INDICE

1. Introdução. 1
2. Noções Básicas e Notações 4
3. Unidades de ZG_n 11
4. Representações Indecomponíveis de G_n 15
5. Somas de Indecomponíveis. 28
   Referências 54

REPRESENTAÇÕES INTEIRAS DE GRUPOS CÍCLICOS

1 - INTRODUÇÃO

Uma representação inteira de um grupo finito G é um homomorfismo de G em um grupo de matrizes inversíveis sobre Z. Duas representações inteiras são equivalentes se uma se obtém da outra por conjugação por uma matriz inversível sobre Z. As classes de equivalência das representações inteiras correspondem assim, às classes de isomorfismo dos módulos sobre ZG, com base finita sobre Z. Estes módulos sobre ZG chamam-se reticulados.

A classificação de todas as representações inteiras de grupos concretos é um dos problemas que interessam na teoria, porque são poucos os grupos para os quais se conhecem completamente suas representações inteiras.

Uma representação inteira é equivalente com uma soma direta de representações inteiras indecomponíveis, mas os somandos quase nunca são únicos. De modo que determinar todas as representações inteiras de um grupo, equivale a determinar todas as indecomponíveis, e a dar invariantes para

as somas de indecomponíveis, que permitam decidir quando são equivalentes duas somas.

Observamos que, no caso particular em que G é cíclico de ordem m, determinar todas as representações inteiras de G nesse sentido, equivale a determinar formas canônicas para todas as matrizes sobre os inteiros que tem ordem divisor de m.

Um dos primeiros trabalhos sobre representações inteiras foi o de Diederichsen, [1], quem classificou as representações indecomponíveis do grupo cíclico de ordem p, primo.

Posteriormente, Heller e Reiner, em [3], introduzindo os métodos de álgebra homológica, e Berman e Gudivok, em [5], com métodos matriciais, mostraram que o grupo cíclico de ordem p^2 tem um número finito de representações inteiras indecomponíveis, no entanto que o grupo cíclico de ordem p^n com $n \geq 3$, assim como os p-grupos não cíclicos possuem indecomponíveis de dimensão arbitrariamente grande. O problema de determinar quais são os grupos que tem um número finito de representações inteiras indecomponíveis, foi resolvido em geral em [4], e também em [5].

A classificação completa das representações inteiras do grupo cíclico de ordem p^2, foi feita recentemente por Reiner em [7]. Neste trabalho estendemos os resultados de [7] no sentido seguinte.

Dado um grupo cíclico G_n de ordem p^n, as componentes simples da álgebra QG_n, são todos os corpos ciclotômicos $Q(\zeta_i)$, sendo ζ_i uma raiz primitiva de 1 de ordem p^i, com $0 \leq i \leq n$. Berman e Gudivok mostraram que o número de reticulados indecomponíveis M sobre ZG_n, tais que entre os somandos simples de QM há no máximo três diferentes, incluindo Q, é finito. Também mostraram que os indecomponíveis M tais que em QM há mais de três componentes simples diferentes, ou três diferentes de Q, é infinito. Aqui classificamos todos os reticulados M sobre ZG_n tais que QM é uma soma de cópias de três componentes simples, Q, $Q(\zeta_i)$ e $Q(\zeta_j)$. Estes M são então soma de um número finito de indecomponíveis.

No caso em que $i = 1$ e $j = n = 2$, os reticulados calculados fornecem todas as representações inteiras do grupo cíclico de ordem p^2, pois

$$QG_2 \simeq Q \oplus Q(\zeta_1) \oplus Q(\zeta_2).$$

Assim nossos resultados se reduzem aos de [7].

Os métodos são os mesmos de [7], de modo que só foi necessário reescrever as demonstrações de [7] para aplicá-las em nosso caso.

A contribuição deste trabalho consiste então, no cálculo de novos exemplos concretos de representações inteiras.

Na próxima seção introduziremos as noções básicas

e notações usadas, e daremos um resumo do método de determinação dos reticulados desenvolvido em [7].

Na seção 3 incluimos uma expressão das unidades de ZG_n, e dos anéis quociente deste anel. Estas expressões não serão usadas nas demais seções, mas os resultados são de interesse por si mesmos, já que são escassas as informações disponíveis sobre cálculo de inversos em anéis de grupo em geral, e estas informação é útil nas aplicações desses anéis.

Na seção 4 apresentamos a lista completa dos reticulados indecomponíveis sobre ZG_n dos tipos mencionados acima. Na última seção determinamos os invariantes das somas desses indecomponíveis.

A principal referência para os resultados que suporemos conhecidos é [6], e as notações usadas serão as de [6] e de [7].

2 - NOÇÕES BÁSICAS E NOTAÇÕES

Sejam $G_n = \langle g \rangle$ o grupo cíclico de ordem p^n, ZG_n o anel do grupo G_n com coeficientes inteiros, ζ_n uma raiz primitiva de 1 de ordem p^n, Φ_n o polinômio ciclotômico com raiz ζ_n, $R_n = Z[\zeta_n]$, o anel dos inteiros do corpo ciclotômico, e $\bar{Z}$ o anel dos inteiros módulo p.

Então:

$$ZG_n \simeq Z[X]/(X^{p^n}-1),\ R_n \simeq Z[X]/(\Phi_n),$$

$$\bar{Z}G_{n-1} \simeq Z[X]/(\Phi_n, X^{p^{n-1}}-1).$$

As inclusões de ideais de $Z[X]$:

$$(X^{p^n}-1) = (X^{p^{n-1}}-1)(\Phi_n) \subset (\Phi_n) \subset (\Phi_n, X^{p^{n-1}}-1),$$

$$(X^{p^n}-1) \subset (X^{p^{n-1}}-1) \subset (\Phi_n, X^{p^{n-1}}-1),$$

determinam os epimorfismos indicados pelas flexas do seguinte diagrama comutativo

$$\begin{array}{ccc} ZG_n & \longrightarrow & R_n \\ \downarrow & & \downarrow \\ ZG_{n-1} & \longrightarrow & \bar{Z}G_{n-1} \end{array}$$

Cada reticulado sobre ZG_{n-1}, ou sobre R_n, pode assim ser considerado um reticulado sobre ZG_n, através desses epimorfismos. Ao mesmo tempo, cada reticulado sobre qualquer destes três anéis, é um reticulado sobre $Z[X]$, e assim será considerado quando for conveniente.

Se M é um reticulado sobre ZG_n, então

$$L = \{m \in M ; (X^{p^{n-1}}-1)m = 0\},$$

é um submódulo de M, que é um reticulado sobre ZG_{n-1}.

É claro que $\Phi_n M \subset L$, logo $N = M/L$ é um módulo sobre

$R_n = Z[X]/(\Phi_n)$. É fácil ver que N é sem torção sobre Z. Além disso, se $\alpha \in R_n$, existe $\beta \in R_n$, tal que $\alpha\beta \in Z$. Daqui se deduz que N é sem torção sobre R_n. Em conseqüência, como R_n é um domínio de Dedekind, N é uma soma de ideais de R_n,

$$N \simeq A_1 \oplus \ldots \oplus A_t \simeq R_n^{t-1} \oplus \prod_1^t A_l,$$

e a classe de isomorfismo de N, está determinada pela classe do ideal ΠA_i, e pelo inteiro t.

Consideremos agora o reticulado M como uma extensão de N por L. Também pode-se expressar M como uma extensão de um módulo L' sobre ZG_{n-1}, por um módulo N' sobre R_n. Não há nenhuma vantagem em considerar um ou outro tipo de extensões.

Para todo L e todo N nessas condições, tem-se:

$$\mathrm{Hom}_{ZG_n}(L,N) = \mathrm{Hom}_{QG_n}(QL,QN) = 0.$$

Com efeito, $QG_n \simeq QG_{n-1} \oplus Q(\zeta_n)$, portanto QL e QN, que são respectivamente módulos sobre QG_{n-1} e sobre $Q(\zeta_n)$, não tem nenhuma componente simples em comum, como módulos sobre QG_n, já que provêm de somandos diferentes da álgebra semi-simples QG.

A partir desse fato demonstra-se facilmente que, dado um isomorfismo $\phi: M_1 \longrightarrow M_2$, entre duas extensões de N por L, existem isomorfismos $\gamma: L \longrightarrow L$ e $\delta: N \longrightarrow N$, tais

que o diagrama seguinte é comutativo.

$$\begin{array}{ccccccccc} \theta_1: & 0 & \longrightarrow & L & \longrightarrow & M_1 & \longrightarrow & N & \longrightarrow & 0 \\ & & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \delta} & & \\ \theta_2: & 0 & \longrightarrow & L & \longrightarrow & M_2 & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

E vale também o recíproco. Considerando os elementos $[\theta_1]$ e $[\theta_2]$ de $\mathrm{Ext}_{ZG_n}(N,L)$, definidos por estas seqüências exatas, isto se traduz em que $M_1 \simeq M_2$, se e só se existem um automorfismo γ de L, e um automorfismo δ de N, tais que $\gamma[\theta_1]=[\theta_2]\delta$, onde γ e δ operam sobre $\mathrm{Ext}(N,L)$ na forma usual (ver [7]).

Em conseqüência, dados um L e um N fixos, as classes de isomorfismo das extensões de N por L estão dadas pelas órbitas determinadas no conjunto $\mathrm{Ext}(N,L)$, sob a ação à esquerda dos automorfismos de L, e à direita dos automorfismos de N. Observamos que o grupo $\mathrm{Ext}(N,L)$ é finito, pois é finitamente gerado, já que N e L o são, e $|G_n|\mathrm{Ext}(N,L) = 0$.

Concluímos que um reticulado M sobre ZG_n se determina dando um reticulado L sobre ZG_{n-1}, um reticulado N sobre R_n, e um elemento de $\mathrm{Ext}(N,L)$ que representa uma órbita em este grupo.

Diz-se que dois reticulados sobre ZG, M_1 e M_2, são localmente isomorfos, se para todo primo p que divide a ordem de G , considerando o anel dos inteiros p-ádicos I_p, se tem $I_pM_1 \simeq I_pM_2$, como módulos sobre I_pG. Para indicar o iso-

morfismo local usa-se a notação $M_1 \vee M_2$. Por exemplo, cada ideal A de R_n é um reticulado sobre ZG_n com g operando por multiplicação por ζ_n. Neste caso $I_p A$ é um ideal de $I_p[\zeta_n]$, que é a ideais principais, logo $I_p A \simeq I_p[\zeta_n]$; portanto $A \vee R_n$.

Anotamos aqui que os métodos de localização permitem demonstrar que se G é um p-grupo, um reticulado M sobre ZG é indecomponível se e só se $I_p M$ é indecomponível sobre $I_p G$ (ver [6]).

Em [7] demonstra-se que se L' e N' são reticulados sobre ZG_n, e sobre R_n respectivamente, tais que $L \vee L'$ e $N \vee N'$, então existe um isomorfismo $\mathrm{Ext}(N,L) \simeq \mathrm{Ext}(N',L')$ que leva as órbitas do primeiro grupo definidas acima, nas órbitas do segundo. Em conseqüência, essa bijeção leva as classes de isomorfismo das extensões de N por L, nas classes de isomorfismo das extensões de N' por L'.

Para nossas aplicações interessa o cálculo do grupo Ext no caso seguinte.

Para todo i, $0 \leq i \leq n$, escreveremos $\zeta_i = \zeta_n^{p^{n-i}}$, $R_i = [\zeta_i]$, etc.

O epimorfismo $ZG_i \longrightarrow R_i$, faz de R_i um reticulado sobre ZG_i, e logo também sobre ZG_n, com o gerador de G_n operando por multiplicação por ζ_i. Por outro lado, consideremos um reticulado L sobre ZG_{i-1}, que é portanto um reticulado sobre ZG_n através do epimorfismo $ZG_n \longrightarrow ZG_{i-1}$. Com uma apli-

cação da seqüência exata do funtor Ext, mostra-se facilmente que

$$\mathrm{Ext}_{ZG_n}(R_i, L) \simeq L/\Phi_i(g)L = L/pL = \bar{L}.$$

(Observamos que para todo $m \in L$: $g^{p^{i-1}} m = m$, pois a imagem de $g^{p^{i-1}}$ em G_{i-1} é a identidade).

Precisaremos calcular os automorfismos de alguns reticulados sobre ZG_n. Escreveremos para cada i, $0 \leq i \leq n$. $E_i = Z[X]/((X-1)\phi_i)$. Em particular $E_1 \simeq ZG_1$. O epimorfismo de anéis $ZG_i \longrightarrow E_i$ faz de E_i um reticulado sobre ZG_i, com o gerador de G_i operando sobre E_i por multiplicação pela imagem de X.

Indicaremos com $U(R)$ o grupo dos inversíveis de um anel R.

Observando que os módulos Z, R_i, E_i são cíclicos sobre ZG_n (gerados pelo 1), e achando o anulador do gerador, resulta imediatamente que:

$$\mathrm{Hom}(R_i, Z) = \mathrm{Hom}(Z, R_i) = 0$$

$$\mathrm{Hom}(R_i, E_i) \simeq (X-1)E_i, \quad \mathrm{Hom}(E_i, R_i) \simeq R_i$$

$$\mathrm{Hom}(E_i, Z) \simeq Z, \quad \mathrm{Hom}(Z, E_i) \simeq \Phi_i E_i.$$

Precisaremos dos seguintes grupos de automorfismos: para todo ideal A de R_i,

$$\mathrm{aut}(A) \simeq \mathrm{aut}(R_i) \simeq U(R_i);$$

$$\mathrm{aut}(E_i) \simeq U(E_i);$$

$$\mathrm{aut}(Z \oplus R_i) \simeq U(Z) \oplus U(R_i).$$

Como os módulos Z, E_i e R_i são cíclicos, todo endomorfismo de $Z \oplus E_i \oplus R_i$ se representa por uma matriz com elementos $a_l \in Z$, $e_l \in E_i$, $r_l \in R_i$,

$$\begin{pmatrix} a_1 & a_2 & 0 \\ \Phi_i e_1 & e_2 & (X-1)e_3 \\ 0 & r_2 & r_3 \end{pmatrix}.$$

Para compor dois desses endomorfismos deve lembrar-se que ZG_n opera sobre Z, E_i e R_i através dos epimorfismos $\Pi_1\Pi$, Π e $\Pi_2\Pi$ do diagrama

$$\begin{array}{ccccc} ZG_n & \xrightarrow{\Pi} & E_i & \xrightarrow{\Pi_2} & R_i \simeq E_i/(\Phi_i) \\ & & \downarrow{\scriptstyle \Pi_1} & & \downarrow \\ & & E_i/(X-1) \simeq Z & \longrightarrow & \bar{Z} \simeq R_i/(\zeta_i - 1) \end{array}$$

Daqui sai facilmente que, se o endomorfismo tem inverso, então são inversíveis as matrizes:

$$\begin{pmatrix} a_1 & a_2 \\ p\Pi_1(e_1) & \Pi_1(e_2) \end{pmatrix} \in M_2(Z), \quad \begin{pmatrix} \Pi_2(e_2) & (\zeta_i - 1)\Pi_2(e_3) \\ r_2 & r_3 \end{pmatrix} \in M_2(R_i).$$

O diagrama acima é um produto fibrado de anéis, pois $(\Phi_i) \cap (X-1) = (0)$. Isto significa que se $r \in R_i$ e $a \in Z$ tem a

mesma imagem em Z, existe $e \in E_i$ tal que $r = \Pi_2(e)$ e $a = \Pi_1(e)$. Usando este fato verifica-se que se as duas últimas matrizes são inversíveis, então o endomorfismo inicial tem inverso.

Um endomorfismo de $Z \oplus E_i$ se representa por uma matriz:

$$\begin{pmatrix} a_1 & a_2 \\ \Phi_i e_1 & e_2 \end{pmatrix}.$$

Este endomorfismo tem inverso se e só se é inversível o endomorfismo de $Z \oplus E_i \oplus R_i$ dado por

$$\begin{pmatrix} a_1 & a_2 & 0 \\ \Phi_i e_1 & e_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Daqui, pelas observações anteriores, se deduz que este é um automorfismo de $Z \oplus E_i$, se e só se são inversíveis:

$$\begin{pmatrix} a_1 & a_2 \\ p\Pi_1(e_1) & \Pi_1(e_2) \end{pmatrix} \quad \text{e} \quad \Pi_2(e_2).$$

3 - UNIDADES DE ZG_n

Nesta seção estudaremos as unidades do anel ZG_n. Aplicando a fórmula de interpolação de Lagrange, determinaremos os coeficientes do inverso de uma unidade de ZG_n. Os

resultados desta seção não serão usados nas seções seguintes.

Os mesmos métodos podem aplicar-se para dar uma expressão dos inversos das unidades de anéis que são imagens homomorfas de ZG_n, mas não consideraremos este tipo de anéis.

Para simplificar a notação, escreveremos:

$$E = ZG_n, \quad d = X^{p^n} - 1, \quad \Phi_0 = X - 1,$$

$$J = \{j;\ \Phi_j \mid d\}.$$

Se g é o gerador de G_n, cada elemento de E se escreve de modo único na forma $f(g)$, onde f é um polinômio, $f \in Z[X]$, tal que grau $f < p^n$.

PROPOSIÇÃO A - *Vale $f(g) \in U(E)$ se e somente se $f(\zeta_j) \in U(R_j)$ para todo $j \in J$. Se $f(g) \in U(E)$, então seu inverso é $f(g)^{-1} = \Sigma a_k g^k$, com $a_k \in Z$ dado por:*

$$a_k = p^{-n} \sum_j Tr_j(\zeta_j^{-k} f(\zeta_j)^{-1}),$$

onde Tr_j indica o traço na extensão $Q(\zeta_j)$ de Q.

DEMONSTRAÇÃO - Se $h(g)$ é o inverso de $f(g)$ em E, então $fh = 1 \pmod d$, logo $f(\zeta_j) \cdot h(\zeta_j) = 1$ para todo $j \in J$.

Seja $f(\zeta_j) \in U(R_j)$ para todo $j \in J$. Consideremos $d = \Pi(X - \zeta_j^k)$, onde $j \in J$ e, para cada j, ζ_j^k, percorre as raízes de Φ_j. Definimos

$$h = p^{-n} \sum \zeta_j^k f(\zeta_j^k)^{-1} d/(X - \zeta_j^k),$$

onde a soma estende-se sobre todas as raízes de d. Assim resulta que $p^n h \in Z[X]$, pois $p^n h \in R_n[X]$, e é fixo pelos automorfismos de $Q(\zeta_n)$ sobre Q.

Além disso, $h(\zeta_j^k) = f(\zeta_j^k)^{-1}$ para toda raiz ζ_j^k de d, pois o valor de $d/(X-\zeta_j^k)$ em ζ_j^k é:

$$d'(\zeta_j^k) = p^n \zeta_j^{-k},$$

e em toda outra raiz de d o valor é 0.

Daqui se deduz que d divide $fh-1$, logo $f(g)h(g)=1$.

Mostraremos agora que $h \in Z[X]$, e portanto $h(g) \in E$.

Seja $p^t h = h' \in Z[X]$, onde p não divide h'. Então

$$fh' - p^t = p^t \frac{r}{s} qd,$$

onde r e s são inteiros relativamente primos, e $q \in Z[X]$ é primitivo. Como p não divide fh', sai daqui que podemos supor $p^t = s$, logo

$$fh' - p^t = rqd.$$

Tomando as imagens em $\bar{Z}[X]$ desses polinômios, e supondo que $t > 0$, se obtém uma igualdade da forma

$$\bar{f}\bar{h}' = \bar{r}\bar{q}(X-1)^{p^n},$$

pois $\zeta_j = 1 \pmod{p}$ para todo j. Mas

$$\bar{f}(1) = \overline{f(\zeta_j)} \neq 0,$$

pois $f(\zeta_j)$ é inversível. Ademais $\bar{h}'$ não é o polinômio 0, e grau $\bar{h}' \leq$ grau $h' < p^n$. Temos assim uma contradição, logo $t = 0$ e $h \in Z[X]$.

Se $h = \sum a_k X^k$, então:

$$a_0 = h(0) = p^{-n} \sum_{j,k} f(\zeta_j^k)^{-1} =$$

$$= p^{-n} \sum_j Tr_j f(\zeta_j^k)^{-1}.$$

Da expressão de h é imediato que a_k é o coeficiente de 1 em $g^{-k}h(g)$. Este elemento é o inverso de $g^k f(g)$, logo pode-se calcular o valor de a_k, da expressão de a_0, substituindo f por $X^k f$. Assim concluimos que, neste caso,

$$a_k = p^{-n} \sum_j Tr_j(\zeta_j^{-k} f(\zeta_j)^{-1}). \qquad \square$$

Observamos que, dado um conjunto de unidades $\{f_j \in U(R_j), j \in J\}$, existe $f(g) \in U(E)$ tal que $f(\zeta_j^j) = f_j$ para todo j, se e somente se o polinômio h, calculado na proposição A, tem coeficientes inteiros. Com efeito, se $h \in Z[X]$ então, como $h(\zeta_j) = f_j^{-1}$, $h(g)$ é inversível, pela proposição, e seu inverso $f(g)$ verifica $f(\zeta_j) = f_j$. Reciprocamente, se existe um $f(g)$ nessas condições, já mostramos em A que $h \in Z[X]$.

Este método pode usar-se para achar os inversíveis de E_i. Mostra-se assim que dado $f_i \in U(R_i)$, existe $f(g) \in U(E_i)$ tal que $f(\zeta_i) = f_i$, se e somente se $f_i = \pm 1 \pmod{\zeta_i - 1}$. Esta mes-

ma conclusão pode obter-se observando que o diagrama seguinte é um produto fibrado de anéis.

$$\begin{array}{ccc} E_i & \xrightarrow{\Pi_2} & R_i \\ \Pi_1 \downarrow & & \downarrow \\ Z & \longrightarrow & \bar{Z} \end{array}$$

Isto implica que a seqüência que segue é exata:

$$\{1\} \longrightarrow U(E_i) \longrightarrow U(R_i)\times\{\pm 1\} \longrightarrow U(\bar{Z}),$$

das imagens em $\bar{Z}$

onde a última flecha leva o par no produto da primeira componente pela inversa da segunda. A exatidão implica então que as unidades de R_i que se levantam a unidades de E_i, são as que coincidem com ± 1 módulo $\zeta_i - 1$.

4 - REPRESENTAÇÕES INDECOMPONÍVEIS DE G_n

Indicaremos com i, j dois inteiros fixos tais que $1 \leq i < j \leq n$, e escreveremos $\varepsilon = \zeta_i$, $\xi = \zeta_j$.

Determinaremos os reticulados M sobre ZG_n, tais que o módulo QM sobre QG_n, é uma soma dos módulos simples $Q, Q(\varepsilon), Q(\xi)$.

Estes reticulados induzem reticulados I_pM sobre I_pG, cujos fatores de composição são I_p, $I_p[\varepsilon]$ e $I_p[\xi]$. Com efeito, se por exemplo $QM = Q(\varepsilon)$, então, sobre o corpo dos números p-ádicos Q_p, se tem $Q_pM = Q_p(\varepsilon)$. Daqui se deduz que I_pM

é isomorfo com um ideal de $I_p[\varepsilon]$, que é principal, logo $I_pM \simeq I_p[\varepsilon]$. Da mesma forma procede-se no caso em que M tem vários fatores de composição.

Os reticulados indecomponíveis sobre I_pG_n com os fatores de composição I_p, $I_p[\varepsilon]$, $I_p[\xi]$, foram calculados em [5], estudando as representações matriciais de G_n sobre I_p. Estes módulos também podem ser determinados com os métodos apresentados na seção 2, mas partiremos da lista dada em [5]. Para cada $\hat{M}$ dessa lista escolheremos um reticulado M sobre ZG_n, tal que $I_pM \simeq \hat{M}$, isto é, um representante da classe de isomorfismo local.

Lembramos que um reticulado M sobre ZG_j está determinado dando um submódulo L, que é um reticulado sobre ZG_{j-1}, um módulo N sobre R_j, e um elemento de $\mathrm{Ext}(N,L)$ que representa a extensão de N por L.

Notamos que:

$$\bar{R}_i = R_i/pR_i \simeq R_i/(\varepsilon-1)^{\phi(p^i)} \simeq$$

$$Z[X]/(X-1)^{\phi(p^i)} = \bar{Z}[\lambda]/(\lambda)^{\phi(p^i)},$$

onde $\lambda = X-1$.

$$\bar{E}_i = E_i/pE_i \simeq \bar{Z}[X]/(X-1)^{\phi(p^i)+1} =$$

$$\bar{Z}[\lambda]/(\lambda)^{\phi(p^i)+1},$$

pois em $\bar{Z}[X]$ vale $(X-1)\Phi_i = (X-1)^{\phi(p^i)+1}$.

$\bar{R}_i$ e $\bar{E}_i$ são anéis principais locais, com o único ideal maximal (λ), de modo que todo elemento se escreve como uma potência de λ por um inversível. (Indicamos também com λ a imagem de $X-1$ em $\bar{E}_i$).

Com estas notações obtemos a lista I de reticulados indecomponíveis sobre ZG_n, que contém um módulo para cada classe de isomorfismo local, do conjuntos dos M tais que QM tem componentes Q, $Q(\varepsilon)$ ou $Q(\xi)$.

I - 1. Z;

2. R_i, R_j;

3. E_i, E_j;

4. (R_i, R_j, λ^k), $k=0,\ldots,\phi(p^i)-1$;

5. $(E_i, R_j\ \lambda^k)$, $k=0,\ldots,\phi(p^i)$;

6. $(Z\oplus R_i, R_j, (1,\lambda^k))$, $k=0,\ldots,\phi(p^i)-1$;

7. se $p^i \neq 2$, $(Z\oplus E_i, R_j, (1,\lambda^k))$, $k=1,\ldots,\phi(p^i)-1$.

Para $n=2$, tomando $i=1$ e $j=2$ na lista I, se tem todas as classes de isomorfismo locais dos reticulados indecomponíveis sobre ZG_2, pois $QG_2 \simeq Q \oplus Q(\zeta_1) \oplus Q(\zeta_2)$.

Partindo da lista I, enumeraremos todos os reticulados indecomponíveis M sobre ZG_n, tais que QM é soma de componentes Q, $Q(\varepsilon)$ ou $Q(\xi)$. Como já observamos, para isso basta determinar todos os M que são localmente isomorfos com cada um dos módulos da lista I.

Precisaremos de algumas notações.

Indicaremos com H_i um conjunto completo de representantes das classes de ideais de R_i, e analogamente para R_j. Se $A \in H_i$ e $B \in H_j$, escreveremos:

$$E_i(A) = (Z, A, 1), \quad E_j(B) = (Z, B, 1).$$

Do fato que $I_p A \simeq R_i$, $I_p B \simeq R_j$, se deduz

$$E_i(A) \vee E_i, \quad E_j(B) \vee E_j.$$

Para cada t indicaremos com $\bar{U}_t$ o grupo dos inversíveis de $\bar{Z}[\lambda]/(\lambda)^t$.

O epimorfismo $R_i \longrightarrow \bar{R}_i$, composto com o epimorfismo definido para $0 \leq k \leq \phi(p^i)-1$, por

$$\bar{R}_i \longrightarrow \bar{Z}[\lambda]/(\lambda)^{\phi(p^i)-k},$$

determina um homomorfismo:

$$U(R_i) \longrightarrow \bar{U}_{\phi(p^i)-k}.$$

Indica-se com $U^*(R_i)$ a imagem de $U(R_i)$ nesse homomorfismo.

Para R_j, se tem, analogamente,

$$U(R_j) \longrightarrow \bar{U}_{\phi(p^j)-k},$$

que composto com o epimorfismo:

$$\bar{Z}[\lambda]/(\lambda)^{\phi(p^j)-k} \longrightarrow \bar{Z}[\lambda]/(\lambda)^{\phi(p^i)-k},$$

determina um homomorfismo

$$U(R_j) \longrightarrow \bar{U}_{\phi(p^i)-k}.$$

Indicaremos sua imagem com $U^*(R_j)$.

Ao par R_i, R_j associaremos os grupos quocientes:

$$U_{\phi(p^i)-k} = \bar{U}_{\phi(p^i)-k}/U^*(R_i)U^*(R_j).$$

Demonstra-se elementarmente que todo inversível de $\bar{Z}$ coincide com uma unidade circular de R_i, módulo $1-\zeta_i$. Daqui resulta que se podem escolher representantes $\bar{u}\in\bar{U}_{\phi(p^i)-k}$, desse grupo quociente, tais que sua imagem em $\bar{Z}$ é 1, isto é, tais que $\bar{u} = 1 \pmod{\lambda}$. Através do epimorfismo canônico, esses $\bar{u}$ podem-se levantar a elementos $u\in\bar{U}_{\phi(p^i)}$, tais que $u = 1 \pmod{\lambda}$. Indicaremos com $\tilde{U}_{\phi(p^i)-k}$ o conjunto desses representantes u em $\bar{U}_{\phi(p^i)} = U(\bar{R}_i)$. Como

$$\mathrm{Ext}(B,A) \simeq \mathrm{Ext}(R_j,R_i) \simeq \bar{R}_i ,$$

cada u define uma extensão de B por A.

Consideremos agora E_i. Se $i < j$ então $\phi(p^i)+1 \leq \phi(p^j)$, logo para cada $k = 0,\ldots,\phi(p^i)$ se tem um epimorfismo

$$\bar{Z}[\lambda]/(\lambda^{\phi(p^j)-k}) \longrightarrow \bar{Z}[\lambda]/(\lambda^{\phi(p^i)+1-k}).$$

Daqui resulta que, com notações análogas as anteriores, ao par E_i, R_j podem-se associar os grupos quocientes:

$$U_{\phi(p^i)+1-k} = \bar{U}_{\phi(p^i)+1-k}/U^*(E_i)U^*(R_j).$$

Indicaremos com $\tilde{U}_{\phi(p^i)+1-k}$ um conjunto de representantes $u \in \bar{E}_i$, com $u = 1 \pmod{\lambda}$, desse grupo quociente. Cada um desses u define uma extensão de B por $E_i(A)$, pois

$$\mathrm{Ext}(B, E_i(A)) \simeq \mathrm{Ext}(R_j, E_i) \simeq \bar{E}_i.$$

No seguinte enunciado usam-se notações análogas para as extensões de B por $Z \oplus A$, e de B por $Z \oplus E_i(A)$.

PROPOSIÇÃO B - *Para cada par de inteiros i,j com $1 \leq i < j \leq n$, os reticulados indecomponíveis sobre ZG_n que tem componentes Q, $Q(\varepsilon)$ e $Q(\xi)$ sobre QG_n, são os enumerados em* II, *onde $A \in H_i$ e $B \in H_j$.*

II. 1. Z;

2. A, B;

3. $E_i(A)$, $E_j(B)$;

4. $(A, B, \lambda^k u)$, com $k = 0, \ldots, \phi(p^i)-1$, *e para cada k,* $u \in \tilde{U}_{\phi(p^i)-k}$;

5. $(E_i(A), B, \lambda^k u)$, com $k = 0, \ldots, \phi(p^i)$, $u \in \tilde{U}_{\phi(p^i)+1-k}$;

6. $(Z \oplus A, B, 1+\lambda^k u)$, com $k = 0, \ldots, \phi(p^i)-1$, $u \in \tilde{U}_{\phi(p^i)-k}$;

7. se $p^i \neq 2$, $(Z \oplus E_i(A), B, 1+\lambda^k u)$, com $k = 1, \ldots, \phi(p^i)-1$, e $u \in \tilde{U}_{\phi(p^i)-k}$;

8. se $p = 1 \pmod 4$ *e q é um inteiro fixo que não é quadrado módulo p,* $(Z \oplus E_i(A), B, 1+\lambda^k uq)$ com $k = 1, \ldots, \phi(p^i)-1$, e $u \in \tilde{U}_{\phi(p^i)-k}$.

DEMONSTRAÇÃO - Se M é um reticulado sobre ZG_n tal que $M \vee R_i$, então $M \simeq A \in H_i$, e se $M \vee R_j$, então $M \simeq B \in H_j$.

O reticulado E_i contém o sub-módulo trivial

$$L = (\Phi_i)/(X-1)(\Phi_i) \simeq Z, \quad \text{e} \quad E_i/L \simeq R_i,$$

logo E_i é uma extensão de R_i por Z. Portanto se $M \vee E_i$ então M contém um sub-módulo trivial L', tal que $N' = M/L' \vee R_i$. Logo $N' \simeq A \in H_i$. Em conseqüência:

$$M = (Z, A, \bar{x}),\ \bar{x} \in \mathrm{Ext}(A, Z) \simeq \mathrm{Ext}(R_i, Z) \simeq \bar{Z}.$$

Para ter as classes de isomorfismo devemos escolher os $\bar{x}$ de modo que sejam representantes das órbitas de $\bar{Z}$ sob a ação dos automorfismos de R_i. Mas $U(R_i)$ opera sobre $\bar{Z}$ através do epimorfismo $R_i \longrightarrow R_i/(1-\varepsilon) \simeq \bar{Z}$, e este leva $U(R_i)$ sobre $U(\bar{Z})$. Daqui se deduz que as únicas órbitas são a do 0, e à do 1. Logo as únicas extensões são:

$$(Z, A, 0) \simeq Z \oplus A, \quad (Z, A, 1) \simeq E_i(A).$$

Em particular resulta $(Z, R_i, 1) \simeq E_i$.

Os módulos obtidos quando A percorre H_i são todos não isomorfos, pois a classe de isomorfismo de M determina a classe de A.

As mesmas condições valem para os $E_j(B)$.

Se $M \vee (R_i, R_j, \lambda^k)$, mostra-se, como no caso anterior, que M é uma extensão de um $B \in H_j$ por um $A \in H_i$. Neste caso:

$$\mathrm{Ext}(B, A) \simeq \mathrm{Ext}(R_j, R_i) \simeq \bar{R}_i.$$

Logo

$$M = (A, B, \lambda^k u),\ u \in U(\bar{R}_i).$$

Da forma de $\bar{R}_i$ resulta que, representando u e u' por polinômios em $\bar{Z}[\lambda]$, se tem $\lambda^k u = \lambda^k u'$ se e só se

$$u = u' \pmod{\lambda^{\phi(p^i)-k}}.$$

Por outro lado, $\lambda^k u$ e $\lambda^k u'$ representam a mesma classe de isomorfismo se e só se coincidem a menos da ação de automorfismos de R_i e de R_j, ou seja a menos de um fator de $U^*(R_i)U^*(R_j)$. Assim se obtém os módulos 4. Observamos que, no caso local, todo inversível de $I_p[\varepsilon]/pI_p[\varepsilon]$ e imagem de uma unidade de $I_p[\varepsilon] = I_p R_i$, de modo que

$$(A, B, \lambda^k u) \vee (R_i, R_j, \lambda^k).$$

Se $M \vee (E_i, R_j, \lambda^k)$ então, como no caso anterior, resulta

$$M \simeq (E_i(A), B, \lambda^k u), \quad u \in U(\bar{E}_i).$$

Assim se obtém os módulos do tipo 5.

Analogamente, se $M \vee (Z \oplus R_i, R_j, (1, \lambda^k))$

$$M \simeq (Z \oplus A, B, (u_1, \lambda^k u_2)),$$

onde $u_1 \in U(\bar{Z})$ e $u_2 \in U(\bar{R}_i)$.

Como $U(R_j) \longrightarrow U(\bar{Z})$ é sobre, existe um automorfismo de B definido por uma unidade de R_j com imagem u_1^{-1} em $\bar{Z}$. Assim se obtém uma extensão isomorfa com esta, dada por um par de forma $(1, \lambda^k u_2)$. Dois pares $(1, u_2)$, $(1, u_2')$ tais que u_2 e u_2' diferem na imagem de uma unidade de R_i, dão exten-

sões isomorfas pois se passa de uma à outra por um automorfismo de A. Se u_2 e u_2' diferem no produto pela imagem de uma unidade u_0 de R_j, então aplicando o automorfismo de B definido por u_0^{-1}, e o automorfismo de A definido por uma unidade de R_i que tem a mesma imagem que u_0 em $\bar{Z}$, se obtem um isomorfismo entre as extensões definidas por $(1,u_2)$ e $(1,u_2')$. Assim resultam os módulo do tipo 6, que são não isomorfos.

Suponhamos agora que $p^i > 2$ e determinemos os módulos $M \vee (Z \oplus E_i, R_j, (1,\lambda^k))$. Como antes mostra-se que

$$M \simeq (Z \oplus E_i(A), B, (u_1, \lambda^k u_2)),\ u_1 \in U(\bar{Z}),\ u_2 \in U(\bar{E}_i).$$

Com a mesma demonstração do caso anterior, prova-se que sempre é possível tomar $u_1 = 1$. Vejamos agora quais pares $(1,u)$ representam módulos isomorfos. Para isto devemos determinar qual é a relação entre dois desses pares se estão na mesma órbita de $\mathrm{Ext}(R_j, Z \oplus E_i)$, sob a ação dos automorfismos de R_j, dados por $U(R_j)$ e os automorfismos de $Z \oplus E_i$ dados pelas matrizes

$$\begin{pmatrix} a_1 & a_2 \\ \Phi_i e_1 & e_2 \end{pmatrix}$$

Lembramos que, como a_2 está no módulo trivial, $\lambda a_2 = 0$, e observamos que em $\bar{E}_i$ vale $\Phi_i \bar{e}_1 = \lambda^{\phi(p^i)} \bar{e}_1$.

Assim resulta que a aplicação dessa matriz ao par $(1,\lambda^k u)$ dá:

$$(\bar{a}_1, \lambda^{\phi(p^i)}\bar{e}_1 + \lambda^k \bar{e}_2 u).$$

Para que a primeira componente seja 1, deverá se aplicar um automorfismo de R_j, dado por um $u_0 \in U(R_j)$ que tenha imagem $\bar{a}_1^{-1}$ em $\bar{Z}$. Assim se terá na mesma órbita:

$$(1, \lambda^k(\lambda^{\phi(p^i)-k}\bar{e}_1 + \bar{e}_2 u)\bar{u}_0).$$

Concluímos que $(1, \lambda^k u)$ e $(1, \lambda^k u')$ estão na mesma órbita, se e só se existem um automorfismo de $Z \oplus E_i$, dado por uma matriz da forma indicada, e uma unidade u_0 de R_j, com imagem $\bar{a}_1^{-1}$ em $\bar{Z}$, tais que

$$u' = \lambda^{\phi(p^i)-k}\bar{e}_1 \bar{u}_0 + \bar{e}_2 u\, \bar{u}_0 (\text{mod } \lambda^{\phi(p^i)+1-k}).$$

Mostraremos agora que os reticulados de cada classe local incluída em 7 e em 8 não são isomorfos. Começaremos com as de 7.

Suponhamos que $(1, \lambda^k u)$ e $(1, \lambda^k u')$ estão na mesma órbita, de modo que temos a relação entre u' e u indicada. Seja N a norma relativa na extensão $Q(\xi)$ de $Q(\varepsilon)$. Então das condições sobre a matriz (ver seção 2), resulta:

$$\Pi_2(e_2) N(u_0)^{-1} \in U(R_i).$$

Tomemos as imagens em $\bar{Z}$ desse elemento. Observando que

$$\Pi_1(e_2) a_1 = \pm 1 \ (\text{mod } p),$$

resulta que a imagem em $\bar{Z}$ de $\Pi_1(e_2) u_0^{-1}$ é ± 1. Daqui se deduz,

usando $N(u_0) = u_0 \pmod{\lambda}$ e a seção 3, que existe $e_2' \in U(E_i)$, tal que

$$\Pi_2(e_2') = \Pi(e_2)N(u_0)^{-1}.$$

Para $k=1,\ldots,\phi(p^i)-1$, valem então as seguintes igualdades módulo $\lambda^{\phi(p^i)-k}$:

$$u' = \bar{e}_2 u \bar{u}_0 = \overline{\Pi_2(e_2)}\ u\ \bar{u}_0 =$$

$$= \overline{\Pi_2(e_2')}\ \overline{N(u_0)}\ u\ \bar{u}_0 \pmod{\lambda^{\phi(p^i)-k}}.$$

Logo u' e u diferem em um fator que é o produto da imagem de um inversível de E_i, pela imagem de um inversível de R_j. Concluímos assim que os reticulados das classes locais de 7, não são isomorfos. Também segue daqui que se $p=1 \pmod 4$, então os reticulados 8 são não isomorfos.

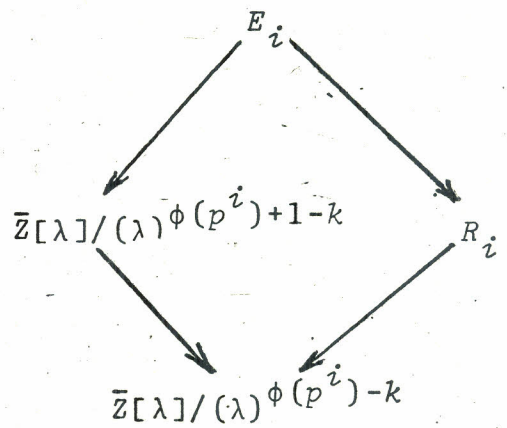
Mostraremos agora que se $p = 1 \pmod 4$ os reticulados de 7 não são isomorfos com os de 8. Para isto tomemos a imagem em $\bar{Z}$ da relação entre u' e u, isto é, consideremos esses elementos módulo λ. Assim

$$u' = \pm\bar{u}_0^2 u = \pm(\bar{a}_1^{-1})^2 u \pmod{\lambda}.$$

Se $p = 1 \pmod 4$, então -1 é um quadrado módulo p, logo u' é um quadrado módulo λ se e só se u o é. Concluímos daqui que se q é um inteiro que não é um quadrado módulo p, então os pares $(1, \lambda^k u q)$, com $u = 1 \pmod{\lambda}$, não estão na órbita de nenhum dos pares que definem os reticulados 7.

Mostraremos agora que em 7 e 8 estão todos os módulos localmente isomorfos com os 7 da lista I.

Primeiramente observamos que tomando uma matriz com $a_1 = 1$, $a_2 = 0$, $e_1 = e_2 = 1$ e $u_0 = 1$, resulta que se u e u' em $U(\bar{E}_i)$ são tais que $u' = u \pmod{\lambda^{\phi(p^i)-k}}$, então $(1-\lambda^k u')$ e $(1-\lambda^k u)$ estão na mesma órbita. De modo que basta tomar um conjunto de unidades u de $\bar{E}_i$ que sejam representantes de $\bar{U}_{\phi(p^i)-k}$. Notamos que os epimorfismos canônicos seguintes formam um diagrama comutativo.



Logo a imagem em $\bar{U}_{\phi(p^i)-k}$ de cada unidade de E_i é também uma imagem de uma unidade de R_i.

Dado agora $Mv.(Z \oplus E_i, R_j, (1,\lambda^k))$, representado por $(1,\lambda^k u)$, $u \in \bar{E}_i$, devemos mostrar que $(1,\lambda^k u)$ está na órbita de um dos pares que aparecem em 7 e em 8.

Consideremos a imagem de u em $\bar{Z}$; podemos escrever $u = ax^2 \pmod{\lambda}$ com $x \in Z$ e:

$a = 1$ se u é um quadrado módulo λ,

$a = -1$ se $p = 3 \pmod 4$ e u não é um quadrado módulo λ,

$a = q$ se $p = 1 \pmod 4$ e u não é um quadrado módulo λ.

Seja $u_0 \in U(R_j)$ tal que $u_0 = \bar{x}^{-1} \pmod \lambda$ e seja $u_1 = N(u_0)$. Então $u_1 \in U(R_i)$ e $u_1 = \bar{x}^{-1} \pmod \lambda$, pois tomar primeiro a norma relativa e logo considerar a imagem módulo λ, dá o mesmo resultado que tomar diretamente a imagem módulo λ.

Seja agora $e \in E_i$ tal que $\Pi_2(e) = u_1$. Então do diagrama

$$\begin{array}{ccc} E_i & \xrightarrow{\Pi_2} & R_i \\ \Pi_1 \downarrow & & \downarrow \\ Z & \longrightarrow & \bar{Z} \end{array}$$

resulta que, módulo p: $\Pi_1(e) = x^{-1} \neq 0$. Portanto existem inteiros a_i, tais que $a_1 \Pi_1(e) - a_2 p = 1$. Logo são inversíveis:

$$\begin{pmatrix} a_1 & a_2 \\ p & \Pi_1(e) \end{pmatrix} \quad \text{e} \quad \Pi_2(e).$$

Em conseqüência a matriz

$$\begin{pmatrix} a_1 & a_2 \\ \Phi_i & e \end{pmatrix}$$

define um automorfismo de $Z \oplus E_i$. Daqui concluímos que tomando $u' = \bar{e}\, u\, \bar{u}_0$, se tem $(1, \lambda^k u')$ e $(1, \lambda^k u)$ na mesma órbita. Além disso, $u' = x^{-1} a x^2 x^{-1} = a \pmod \lambda$.

Consideraremos agora o par $(1,\lambda^k u')$, e mostraremos que ele representa uma das extensões indicadas em 7 ou em 8.

Primeiramente escolhemos b inteiro tal que $b = a^{-1}$ (mod p). Tomemos agora a imagem de $u'b$ em $U_{\phi(p^i)-k}$, e levantemos essa imagem a um representante em $U(\bar{E}_i)$, dos que definem os reticulados 7 e 8, isto é, um $\tilde{u} \in \tilde{U}_{\phi(p^i)-k}$. Existem então $u_0 \in U(R_j)$ e $u_0' \in U(E_i)$, tais que

$$\tilde{u} = u_0' u' b u_0 \pmod{\lambda^{\phi(p^i)-k}}.$$

Logo

$$a\tilde{u} = u_0' u' u_0 \pmod{\lambda^{\phi(p^i)-k}}.$$

Da definição de $\tilde{U}_{\phi(p^i)-k}$ temos $\tilde{u} = 1 \pmod{\lambda}$, e para todo inversível de E_i vale $u_0' = \pm 1 \pmod{\lambda}$. Por outro lado $u'b = 1 \pmod{\lambda}$. Logo $u_0 = \pm 1 \pmod{\lambda}$.

Em conseqüência temos $(1,\lambda^k u')$ na mesma órbita que $(1,\lambda^k u_0' u' u_0)$ e este na mesma que $(1,\lambda^k a\tilde{u})$. Concluímos daqui que $(1,\lambda^k u)$ está na órbita de $(1,\lambda^k \tilde{u})$, ou na de $(1,\lambda^k q\tilde{u})$.

□

5 - SOMAS DE INDECOMPONÍVEIS

Nesta seção daremos critérios para determinar quando são isomorfas duas somas diretas de reticulados indecomponíveis sobre ZG_n, dos tipos enumerados na proposição B.

Dada uma soma M desses reticulados, denotaremos com $A(M)$ o ideal de R_i produto de todos os ideais $A \in H_i$ dos somandos, e com $B(M)$ o ideal de R_j produto dos $B \in H_j$ dos somandos.

Indicaremos com k_1 o máximo dos expoentes dos λ de somandos do tipo 5, e com k_2, o máximo expoente dos λ de somandos dos tipos 4, 6, 7 e 8. Escreveremos $r(M) = \max(k_1 - 1, k_2)$. Se não há somandos do tipo 5 se escolhe $k_1 = \phi(p^i) + 1$, se não há dos tipos 4, 6, 7, 8, $k_2 = \phi(p^i)$.

Indicaremos com $u(M)$ o produto das imagens no grupo $U_{\phi(p^i)-r(M)}$, dos u dos indecomponíveis dos tipos 4, 5, 6, 7 e 8 presentes na soma, e os q dos somandos de tipo 8.

PROPOSIÇÃO C - *Seja M uma soma direta de reticulados indecomponíveis sobre ZG_n, que tem sobre QG_n os fatores de composição Q, $Q(\varepsilon)$ e $Q(\xi)$. A classe de isomorfismo de M determina os seguintes invariantes.*

I. *As classes de isomorfismo locais dos somandos indecomponíveis.*

II. *A classe do ideal $A(M)$ de R_i, e a classe do ideal $B(M)$ de R_j.*

Se, a) *em M há somandos do tipo* 2 *ou do tipo* 3, *e,* b) $p \neq 1 \pmod 4$ *ou* $p = 1 \pmod 4$ *mas existem somandos de pelo menos um dos tipos* 1, 3, 5, 6, *então a classe de isomorfismo de M está determinada pelos invariantes* I *e* II.

Se M não satisfaz a, *ou se M não satisfaz* b, *para determinar a classe de isomorfismo de M devem acrescentar-se respectivamente os invariantes* III *ou* IV.

III. *O elemento $u(M)$ de $U_{\phi(p^i)-r(M)}$.*

IV. *A paridade do número de somandos do tipo 8 existente na soma.*

DEMONSTRAÇÃO - 1º) Seja M uma soma de indecomponíveis dos tipos 1 a 8. Cada somando indecomponível induz um reticulado indecomponível sobre $I_p G_n$. Como I_p é completo, estes indecomponíveis são únicos, a menos de isomorfismos, pelo teorema de Krull-Schmidt (ver [6]). Em conseqüência o número de somandos da soma M, que são localmente isomorfos com cada um dos indecomponíveis da lista I, é o mesmo para toda decomposição de M em indecomponíveis. Assim, a classe de isomorfismo de M determina I.

2º) M é uma extensão de um módulo N sobre R_j por um módulo L sobre ZG_i, univocamente determinados por M. Este N é a soma dos ideais B de R_j que aparecem em cada somando. Da estrutura dos reticulados sobre um domínio de Dedekind, segue que a classe do ideal $B(M)$, produto desses ideais, está determinada por M. Da mesma forma, considerando L no lugar de M, mostra-se que $A(M)$ está determinado por M.

Por outro lado, observamos que de

$$N = \sum^{t} B_l \simeq R_j^{t-1} \oplus B(M) = N',$$

resulta que

$$(L, N, u) \simeq (L, N', u).$$

De modo que o módulo $B(M)$ pode tomar o lugar de qualquer B_l dos somandos de M, pondo R_j no lugar de todos os outros i-

deais de R_j sem que mude a classe de isomorfismo da soma. Da mesma forma se prova uma afirmação análoga para o ideal $A(M)$ de R_i.

Mostraremos agora que se M satisfaz a) e b), então I e II são suficientes para determinar a classe de isomorfismo de M.

Suponhamos inicialmente que:

3º) há algum somando localmente isomorfo com um dos módulos R_i, R_j, E_i, E_j, e que $p \neq 1 (\mathrm{mod}\ 4)$.

Para cada somando dos tipos 4 a 8, consideremos o u em $\bar{R}_i$ ou $\bar{E}_i$, que determina essa extensão. Então $u = 1 (\mathrm{mod}\ \lambda)$ e pode-se levantar a um $w \in ZG_n$ tal que $w = 1 (\mathrm{mod}\ 1-g)$. Se tem então o seguinte diagrama de seqüências exatas:

$$\begin{array}{ccccccccc}
 & & & & 0 & \longrightarrow & E_i/wE_i & \longrightarrow & R_i/wR_i & \longrightarrow & 0 \\
 & & & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & Z & \longrightarrow & E_i & \longrightarrow & R_i & \longrightarrow & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & Z & \longrightarrow & E_i & \longrightarrow & R_i & \longrightarrow & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & & & \\
 & & 0 & & 0 & & 0 & & & &
\end{array}$$

Também para todo ideal A de R_i vale

$$A/wA \simeq E_i(A)/wE_i(A) \simeq R_i/wR_i \simeq E_i/wE_i.$$

Dado agora um somando de M da forma $(R_i, R_j, \lambda^k u)$,

consideremos o homomorfismo $R_i \longrightarrow R_i$ definido pelo produto por w. Este homomorfismo induz os homomorfismos ϕ e 1 do seguinte diagrama, pois w opera sobre a extensão indicada por multiplicação por u.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & R_i/wR_i & \longrightarrow & \text{Coker} & \longrightarrow & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & R_i & \longrightarrow & (R_i, R_j, \lambda^k u) & \longrightarrow & R_j & \longrightarrow & 0 \\
 & & \uparrow w & & \uparrow \phi & & \uparrow 1 & & \\
0 & \longrightarrow & R_i & \longrightarrow & (R_i, R_j, \lambda^k) & \longrightarrow & R_j & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Assim resulta a seqüência exata:

$$0 \longrightarrow (R_i, R_j, \lambda^k) \longrightarrow (R_i, R_j, \lambda^k u) \longrightarrow R_i/wR_i \longrightarrow 0.$$

Para o caso em que M tem o somando A, consideraremos a seqüência exata:

$$0 \longrightarrow A \longrightarrow A \longrightarrow R_i/wR_i \longrightarrow 0.$$

Do fato que $I_p(R_i/wR_i) = 0$, se deduz, pelo lema de Schanuel na forma demonstrada em [7], que

$$A \oplus (R_i, R_j, \lambda^k u) \simeq A \oplus (R_i, R_j, \lambda^k).$$

Trocando A por $E_i(A)$, se chega ao mesmo resultado. Também pode-se por um ideal B no lugar de R_i.

Da mesma forma se demonstram resultados análogos para os somandos de M dos tipos 5, 6, 7 e 8.

Concluímos daqui que, se na soma há um indecomponível localmente isomorfo com R_i ou com E_i, então podem-se substituir os u por 1 em cada indecomponível dos tipos 4,5, 6, 7 e 8 sem mudar a classe de isomorfismo da soma.

Para demonstrar que este resultado também vale no casi en que existem somandos localmente isomorfos com R_j ou com E_j, se procede na mesma forma, usando as seqüências exatas que indicaremos a continuação.

Para cada u em $\bar{R}_i$ ou $\bar{E}_i$, que determina um indecomponível da soma, levantaremos u^{-1} a $w \in ZG_n$, usando os epimorfismos de ZG_n em R_i, e em E_i.

Se tem então:

$$B/wB \simeq E_j(B)/wE_j(B) \simeq R_j/wR_j \simeq E_j/wE_j.$$

Considerando o endomorfismo de R_j definido pelo produto por w, resulta o seguinte diagrama.

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & \text{Coker} & \longrightarrow & R_j/wR_j & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & R_i & \longrightarrow & (R_i, R_j, \lambda^k u) & \longrightarrow & R_j & \longrightarrow & 0 \\
 & & \uparrow 1 & & \uparrow \psi & & \uparrow w & & \\
0 & \longrightarrow & R_i & \longrightarrow & (R_i, R_j, \lambda^k) & \longrightarrow & R_j & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

(w opera à direita sobre $\mathrm{Ext}(R_j, R_i)$ dando $uw = 1$).

Assim se tem a seqüência exata:

$$0 \longrightarrow (R_i, R_j, \lambda^k) \longrightarrow (R_i, R_j, \lambda^k u) \longrightarrow R_j/wR_j \longrightarrow 0,$$

que junto com

$$0 \longrightarrow B \longrightarrow B \longrightarrow R_j/wR_j \longrightarrow 0,$$

permite deduzir:

$$B \oplus (R_i, R_j, \lambda^k u) \simeq B \oplus (R_i, R_j, \lambda^k).$$

O mesmo resultado vale pondo $E_j(B)$ no lugar de B. Também existem isomorfismos análogos para os indecomponíveis dos tipos 5, 6, 7 e 8.

Concluímos daqui que, se vale a hipótese 3º, então a soma M é isomorfa com uma soma M' de indecomponíveis nas seguintes condições. Um dos ideais de R_i da soma M' é $A(M)$, e os demais coincidem com R_i. Um dos ideais de R_j em M' é

$B(M)$, e os demais são iguais com R_j. Todos os u dos indecomponíveis da soma M' são 1. Isto implica que duas somas que verificam as condições 3º, e com os mesmos invariantes I e II, são isomorfas.

Consideremos agora o caso em que:

4º) na soma M não existem somandos dos tipos 2 ou 3, mas $p \neq 1 \pmod 4$, e portanto não há somandos do tipo 8. Aproveitando estas seqüências exatas, mostraremos que duas somas M_1 e M_2 nessas condições, com os mesmos invariantes I, e tais que

$$A(M_1) \simeq A(M_2),\ B(M_1) \simeq B(M_2),\ u(M_1) = u(M_2),$$

são isomorfas.

Sabemos que podemos substituir um dos A da soma M por $A(M)$ e os demais por R_i, e um dos B por $B(M)$ e os demais por R_j. Para demonstrar esta afirmação acima, será então suficiente provar que, em todos os casos, pode-se substituir um dos u da soma M pelo produto de todos, e os demais por 1, sem alterar a classe de isomorfismo da soma.

Para isto consideremos, por exemplo, dois somandos dos tipos 4 e 5:

$$(R_i, R_j, \lambda^k u),\ (E_i, R_j, \lambda^l u').$$

Para poder considerar o produto dos u devemos observar que todo $u \in U(\bar{R}_i)$ se levanta a uma unidade de $\bar{E}_i$. Para sim-

plificar a notação escreveremos nesse caso $u \in U(\bar{E}_i)$.

As seguintes seqüências, obtidas como vimos acima, são exatas:

$$0 \longrightarrow (E_i, R_j, \lambda^l) \longrightarrow (E_i, R_j, \lambda^l u') \longrightarrow E_i/w'E_i \longrightarrow 0,$$

$$0 \longrightarrow (R_i, R_j, \lambda^k u) \longrightarrow (R_i, R_j, \lambda^k uu') \longrightarrow R_i/w'R_i \longrightarrow 0.$$

Logo de $E_i/w'E_i \simeq R_i/w'R_i$,

$$(E_i, R_j, \lambda^l) \oplus (R_i, R_j; \lambda^k uu') \simeq$$

$$(R_i, R_j, \lambda^k u) \oplus (E_i, R_j, \lambda^l u').$$

Os demais casos se tratam em forma semelhante, e daqui segue a conclusão desejada.

Suponhamos agora que:

5º) na soma M há somandos do tipo 2 e 3, e que $p = 1 (\mathrm{mod}\ 4)$, e existem somandos do tipo 8, mas também existem somandos localmente isomorfos com os de 1, 3, 5 ou 6. Como nos casos anteriores, podemos supor todo $A = R_i$ e $B = R_j$.

Se existem somandos Z em M, usaremos a seqüência exata:

$$0 \longrightarrow Z \longrightarrow Z \longrightarrow Z/qZ \longrightarrow 0.$$

Se há somandos do tipo 3, precisaremos das seqüências exatas:

$$0 \longrightarrow E_i \longrightarrow E_i \longrightarrow Z/qZ \longrightarrow 0,$$

$$0 \longrightarrow E_j \longrightarrow E_j \longrightarrow Z/qZ \longrightarrow 0.$$

Por exemplo, a primeira se obtém lembrando que

$$E_i \simeq (Z, R_i, 1) \simeq (Z, R_i, q),$$

e considerando o homomorfismo $E_i \longrightarrow E_i$ induzido pelo homomorfismo $Z \longrightarrow Z$, de multiplicação por q, Um diagrama similar aos anteriores prova o resultado.

Para o caso em que existe algum somando do tipo 5, consideremos este mesmo homomorfismo $E_i \longrightarrow E_i$. Usando o epimorfismo $U(R_j) \longrightarrow U(\bar{Z})$, e achando o "pushout" do diagrama:

$$\begin{array}{ccc} & & E_i \\ & & \uparrow \\ 0 & \longrightarrow & E_i \longrightarrow (E_i, R_j, \lambda^k u), \\ & & \uparrow \\ & & 0. \end{array}$$

se obtém o seguinte diagrama de seqüências exatas, como mostraremos imediatamente:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & Z/qZ & \longrightarrow & \text{Coker} & \longrightarrow & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & E_i & \longrightarrow & (E_i, R_j, \lambda^k u) & \longrightarrow & R_j & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & E_i & \longrightarrow & (E_i, R_j, \lambda^k u) & \longrightarrow & R_j & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Daqui se obtém a seqüência exata:

$$0 \longrightarrow (E_i, R_j, \lambda^k u) \longrightarrow (E_i, R_j, \lambda^k u) \longrightarrow Z/qZ \longrightarrow 0.$$

Para obter o diagrama que precisamos, observa-se que, determinando o "pushout" de,

$$\begin{array}{ccc}
Z & & \\
\uparrow q & & \\
Z & \longrightarrow & E_i
\end{array}$$

resulta que a função χ: $E_i \longrightarrow E_i$ considerada, é a composição de um morfismo ϕ: $E_i \longrightarrow (Z, R_i, q)$ tal que $\phi(1) = (0,1)$, e do isomorfismo $(Z, R_i, q) \simeq E_i$. Este isomorfismo está definido pelo automorfismo de R_i dado pela unidade circular

$$(1-\varepsilon)/(1-\varepsilon^q) = \alpha$$

Logo $\chi(1)$ é a imagem em E_i de $(0,\alpha)$. Indicando com $\bar{\alpha}$ sua imagem em $\bar{E}_i$, obtemos o diagrama seguinte:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_i & \longrightarrow & (E_i, R_j, \lambda^k\bar{\alpha}) & \longrightarrow & R_j & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \chi} & & \uparrow & & \uparrow{\scriptstyle 1} & & \\ 0 & \longrightarrow & E_i & \longrightarrow & (E_i, R_j, \lambda^k) & \longrightarrow & R_j & \longrightarrow & 0 \end{array}$$

Mas em R_j existe uma unidade circular com imagem $\bar{\alpha}$ em $\bar{E}_i$, logo

$$(E_i, R_j, \lambda^k\bar{\alpha}) \simeq (E_i, R_j, \lambda^k).$$

Se existem somandos do tipo 6, usaremos a seqüência que segue, obtida aplicando ao submódulo $Z \oplus R_i$ o endomorfismo de multiplicação por $(q,1)$.

$$0 \longrightarrow (Z\oplus R_i, R_j, (1, \lambda^k u)) \longrightarrow (Z\oplus R_i, R_j, (q, \lambda^k u)$$

$$\longrightarrow Z/qZ \longrightarrow 0.$$

Aplicando o automorfismo de R_j, definido por multiplicação pela unidade que tem imagem q em $\bar{Z}$ (o que não muda a classe de u em $U_{\phi(p^i)-k}$), resulta:

$$(Z\oplus R_i, R_j, (q, \lambda^k u)) \simeq (Z\oplus R_i, R_j, (1, \lambda^k u)).$$

Assim obtemos a seqüência exata:

$$0 \longrightarrow (Z \oplus R_i, R_j, (1, \lambda^k u)) \longrightarrow (Z \oplus R_i, R_j, (1, \lambda^k u))$$

$$\longrightarrow Z/qZ \longrightarrow 0.$$

Observemos agora os somandos do tipo 8. Aplicando a R_j um automorfismo dado por um inversível cuja imagem em $\bar{Z}$ é $q' = q^{-1} \pmod p$, resulta $u' \in \bar{E}_i$ tal que $u' = 1 \pmod \lambda$ e

$$(Z \oplus E_i, R_j, (1, \lambda^k uq)) \simeq (Z \oplus E_i, R_j, (q', \lambda^k u')).$$

Por outro lado, aplicando a multiplicação por q em Z, se obtém a seqüência:

$$0 \longrightarrow (Z \oplus E_i, R_j, (q', \lambda^k u')) \longrightarrow (Z \oplus E_i, R_j, (1, \lambda^k u'))$$

$$\longrightarrow Z/qZ \longrightarrow 0.$$

Por conseguinte é exata:

$$0 \longrightarrow (Z \oplus E_i, R_j, (1, \lambda^k uq)) \longrightarrow$$

$$(Z \oplus E_i, R_j, (1, \lambda^k u')) \longrightarrow Z/qZ \longrightarrow 0.$$

Desta seqüência, e da

$$0 \longrightarrow Z \longrightarrow Z \longrightarrow Z/qZ \longrightarrow 0,$$

resulta:

$$(Z \oplus E_i, R_j, (1, \lambda^k uq)) \oplus Z \simeq (Z \oplus E_i, R_j, (1, \lambda^k u')) \oplus Z.$$

Assim é possível substituir uq por u' em todos os somandos do tipo 8, quando M tem o somando Z.

Se existem somandos localmente isomorfos com os de 3, 5 ou 6, também podem-se eliminar os q dos somandos do tipo 8, usando as seqüências exatas análogas com esta, que indicamos acima.

Concluímos daqui que se na soma M existem indecomponíveis localmente isomorfos com 2 ou 3, e há somandos do tipo 8, mas também há pelo menos um dos tipos 1, 3, 5 ou 6, então duas somas com os mesmos invariantes I e II são isomorfas.

6º) Ao mesmo tempo, deste último resultado e do demonstrado em 4º, deduzimos que para as somas nas quais faltam módulos localmente isomorfos com 2 e com 3, e há do tipo 8, mas também existem de um dos tipos 1, 5 ou 6, então duas somas com os mesmos invariantes I e II, e com o mesmo $u(M)$ são isomorfas.

7º) Consideremos agora o caso em que a soma contém somandos do tipo 2 e do tipo 8, mas faltam somandos dos tipos 1, 3, 5 e 6.

Primeiramente observamos que, sem usar nenhuma hipótese sobre o tipo de somandos, para os reticulados do tipo 8, analogamente com a seqüência do parágrafo 5, se obtém:

$$0 \longrightarrow (Z \oplus E_i, R_j, (1, \lambda^l u' q^2) \longrightarrow$$

$$(Z \oplus E_i, R_j, (1, \lambda^l u' q)) \longrightarrow Z/qZ \longrightarrow 0.$$

Onde, como antes, sai

$$(Z \oplus E_i, R_j, (1, \lambda^k uq)) \oplus (Z \oplus E_i, R_j, (1, \lambda^l u' q)) \simeq$$

$$(Z \oplus E_i, R_j, (1, \lambda^l u' q^2)) \oplus (Z \oplus E_i, R_j, (1, \lambda^k u)).$$

Portanto, em todos os casos, um número par de indecomponíveis do tipo 8 pode substituir-se por uma soma de indecomponíveis do tipo 7.

Concluímos daqui que se na soma existem somandos do tipo 2 e do tipo 8, mas faltam os dos tipos 1, 3, 5 ou 6, então as somas com os mesmos invariantes I e II, e a mesma paridade do número de módulos do tipo 8, são isomorfas.

Finalmente, para as somas de reticulados dos tipos 4, 7 e 8, só podemos afirmar que as somas com os mesmos I, II, $u(M)$, e com a mesma paridade do número de módulos do tipo 8, são isomorfas.

8º) Para terminar a demonstração, precisamos provar que $u(M)$, e a paridade do número de somandos do tipo 8, são efetivamente invariantes sob isomorfismo, em aqueles casos em que determinam a classe de isomorfismo da soma.

Devemos considerar o caso em que faltam tanto os somandos localmente isomorfos com 2, como os localmente isomorfos com 3, e o caso em que faltam dos tipos 1, 3, 5 e 6.

Já vimos que basta considerar as somas em que os ideais $A = R_i$, e os ideais $B = R_j$. Também sabemos que podemos supor que na soma há, no máximo, um indecomponível com $u \neq 1$, e que aparece no máximo um q.

O módulo M pode-se expressar como uma extensão de uma soma de cópias de R_j, R_j^d, por um reticulado sobre ZG_i, da forma $Z^a \oplus E_i^b \oplus R_i^c$. Essa extensão se representa por uma matriz de extensões de R_j por Z, R_j por E_i, e de R_j por R_i. Segundo a notação de [3] e de [7], a matriz tem uma coluna para cada R_j, e uma linha para cada Z, cada E_i, e cada R_i. No lugar dado por uma linha e uma coluna determinadas, coloca-se o elemento de $\bar{Z}$, $\bar{E}_i$ ou $\bar{R}_i$, que define a extensão correspondente. A cada Z, E_i ou R_i que aparece como somando direto, corresponde-lhe uma linha de zeros, e a cada somando direto R_j uma coluna de zeros.

Ordenaremos os somandos de modo de ter primeiro as linhas de zeros que correspondem com os somandos triviais; logo os blocos 0 e I que representam extensões de R_i pelos Z, que aparecem nos somandos dos tipos 7, 8 e 6; depois blocos de matrizes diagonais em $\bar{E}_i$, que representam as extensões de R_j por E_i dos tipos 5, 7 e 8, e finalmente os blo-

cos sobre R_j, que procedem dos tipos 4 e 6.

Suporemos primeiro que não há somandos 2 nem 3.

O caso em que o máximo expoente dos λ aparece em um indecomponível que não é do tipo 5, isto é $k_1 \leq k_2$ e $r(M) = k_2$, é o mais fácil de analisar. Para isto considera-se o módulo M', quociente de M por seu sub-módulo trivial. A classe de isomorfismo de M determina a classe de M'. Agora M' é uma extensão de R_j^d por R_i^f, de modo que a matriz dessa extensão tem elementos no anel principal, local, $\bar{R}_i = \bar{Z}[\lambda]/\lambda^{\phi(p^i)}$.

Dadas duas somas, M_1 e M_2, nessas condições, o isomorfismo $M_1 \simeq M_2$ implica $M_1' \simeq M_2'$. Este isomorfismo se obtém, como sabemos, por um automorfismo de R_j^d e um automorfismo de R_i^f, que se podem representar por uma matriz de $GL(R_j^d)$ e uma matriz de $GL(R_i^f)$, respectivamente. Estas matrizes operam através dos epimorfismos $R_j \longrightarrow \bar{R}_i$, $R_i \longrightarrow \bar{R}_i$

Sejam L_1 e L_2 as matrizes de $\bar{R}_i$ que representam as extensões M_1' e M_2'. As matrizes L_1 e L_2 podem ter algumas linhas 0, e depois blocos diagonais com elementos λ^k na diagonal, com máximo expoente k_2, e possivelmente um fator $u \neq 1$ de R_i e um q. Sejam v_1 e v_2 esses coeficientes de λ^k, diferentes de 1, se existirem, e $v_1 = 1$ ou $v_2 = 2$ no caso contrário. Com um cálculo simples (ver [7]) mostra-se que

$$S_i L_1 = L_2 S_j, \quad S_i \in GL(R_i^d), \quad S_j \in GL(R_j^d),$$

implica que em $\bar{Z}[\lambda]/(\lambda)^{\phi(p^i)}$ vale

$$\det S_i v_1 \lambda^{k_2} = v_2 \lambda^{k_2} \det S_j .$$

Donde segue

$$\det S_i v_1 = v_2 \det S_j \pmod{\lambda^{\phi(p_i)-k_2}} .$$

Agora devemos mostrar que se o expoente máximo provém exclusivamente de um somando do tipo 5, isto é se $k_1 > k_2$ e $r(M) = k_1 - 1$, o invariante em $U_{\phi(p^i)-k_1+1}$ está determinado pela classe de isomorfismo da soma. Neste caso o raciocínio anterior é insuficiente, pois mostraria somente a invariância da imagem desse elemento no grupo $U_{\phi(p^i)-k_1}$.

Precisamos considerar a extensão M_1 de R_j^d por $Z^a \oplus E_i^b \oplus R_i^c$, e todos os automorfismos de $Z^a \oplus E_i^b \oplus R_i^c$ e de R_j^d, operando sobre a matriz que representa a extensão, para provar que o isomorfismo entre duas extensões, implica a igualdade dos invariantes.

Um endomorfismo de $Z^a \oplus E_i^b \oplus R_i^c$ representa-se por uma matriz

$$\begin{pmatrix} a_1 & a_2 & 0 \\ \Phi_1 e_1 & e_2 & (X-1)e_3 \\ 0 & r_2 & r_3 \end{pmatrix},$$

onde as letras indicam blocos de matrizes sobre Z, sobre E_i, e sobre R_i, respectivamente. Como no caso considerado na seção 2, mostra-se que este é um automorfismo se e só se são

inversíveis as matrizes

$$\begin{pmatrix} a_1 & a_2 \\ p\Pi_1(e_1) & \Pi_1(e_2) \end{pmatrix}, \begin{pmatrix} \Pi_2(e_2) & (\varepsilon-1)\Pi_2(e_3) \\ r_2 & r_3 \end{pmatrix}$$

formadas por blocos sobre Z e sobre R_i.

A matriz da extensão M_1 que estamos considerando, é da forma:

$$\begin{array}{c} (1) \\ (7,8) \\ (6) \\ (5) \\ (7,8) \\ (4) \\ (6) \end{array} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & 0 & I \\ D_1 & 0 & 0 & 0 \\ 0 & D_2 & 0 & 0 \\ 0 & 0 & D_3 & 0 \\ 0 & 0 & 0 & D_4 \end{pmatrix}$$

Se $M_1 \simeq M_2$, as matrizes correspondentes estão na mesma órbita, logo operando à esquerda sobre a matriz de M_1 por certo automorfismo de $Z^a \oplus E_i^b \oplus R_i^c$, e à direita sobre a matriz de M_2 por certo automorfismo de R_j^d, se obterá uma mesma matriz. Escreveremos esta matriz deixando de lado as primeiras linhas, que são as que representam somandos triviais, para simplificar a notação. Assim se tem uma igualdade:

$$(*)\qquad \begin{pmatrix} \Phi_i e_1 & e_2 & (X-1)e_3 \\ 0 & r_2 & r_3 \end{pmatrix} \left(\begin{array}{cc:c:c} 0 & 0 & 0 & 0 \\ 0 & I & 0 & I \\ 0 & 0 & 0 & 0 \\ \hdashline D_1 & 0 & 0 & 0 \\ 0 & D_2 & 0 & 0 \\ 0 & 0 & D_3 & 0 \\ 0 & 0 & 0 & D_4 \end{array}\right) = \left(\begin{array}{cc:c:c} D_1' & 0 & 0 & 0 \\ 0 & D_2' & 0 & 0 \\ \hdashline 0 & 0 & D_3' & 0 \\ 0 & 0 & 0 & D_4' \end{array}\right) S,$$

onde S indica uma matriz inversível sobre R_j.

Agora observamos que

$$\Phi_i e_1 = \lambda^{\phi(p^i)} e_1,$$

e que os blocos D_3 e D_4 são diagonais, tendo na diagonal elementos λ^k com

$$k \leq k_2 \leq \phi(p^i) - 1 < \phi(p^i).$$

Consequentemente, das colunas de

$$\Phi_i e_1 \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix},$$

podem-se tirar como fatores os elementos diagonais dos blocos D_3 e D_4, de modo que existe uma matriz e' tal que:

$$= \lambda^{\phi(p^i)-k_2} e' \begin{pmatrix} D_3 & 0 \\ 0 & D_4 \end{pmatrix}.$$

Daqui segue que o lado esquerdo da igualdade (*) pode-se escrever na forma:

$$\begin{pmatrix} e_2 & \lambda^{\phi(p^i)-k_2} e' + \lambda e_3 \\ r_2 & r_3 \end{pmatrix} \left(\begin{array}{cc|c} D_1 & 0 & 0 \\ 0 & D_2 & 0 \\ \hline 0 & 0 & D_3 \end{array}\right) \quad 0 \\ 0 \quad 0 \quad 0 \quad D_4 \Big).$$

Indicaremos com v_1 e v_2 o coeficiente diferente de 1, dos termos λ^k das diagonais das matrizes que representam as extensões M_1 e M_2. (Se todos foram 1 escreveremos $v_1=1$ ou $v_2=1$. Como no caso anterior, verifica-se que se δ é o determinante da (*) primeira das matrizes acima, então em $\bar{Z}[\lambda]/(\lambda)^{\phi(p^i)+1}$:

$$\delta v_1 \lambda^{k_1} = \det S \cdot v_2 \lambda^{k_1}.$$

Donde concluímos que,

$$\delta v_1 = \det S \cdot v_2 (\mathrm{mod}\ \lambda^{\phi(p^i)+1-k_1}).$$

Agora observamos que

$$\phi(p^i) - k_2 \geq \phi(p^i)+1-k_1.$$

Por conseguinte a imagem em $\bar{U}_{\phi(p^i)+1-k_1}$ de δ, coincide com a imagem de

*) matriz sobre R_i associada com

$$\det\begin{pmatrix} \Pi_2(e_2) & (\varepsilon-1)\Pi_2(e_3) \\ r_2 & r_2 \end{pmatrix} \in U(R_i).$$

Como $\det S \in U(R_j)$, obtemos assim, em $U_{\phi(p^i)+1-k_1}$, a igualdade $u(M_1) = u(M_2)$.

Consideremos agora o caso em que $p = 1 \pmod 4$, e faltam na soma os indecomponíveis dos tipos 1, 3, 5 e 6. Um isomorfismo entre duas somas $M_1 \simeq M_2$ se traduz, como nos casos anteriores, em uma ~~igualdade das~~ relação entre as matrizes que representam as extensões.

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ \Phi_i e_1 & e_2 & (X-1)e_3 \\ 0 & r_2 & r_3 \end{pmatrix} \begin{pmatrix} 0 & I & 0 \\ 0 & D_1 & 0 \\ 0 & 0 & D_2 \end{pmatrix} = \begin{pmatrix} 0 & I & 0 \\ 0 & D_1' & 0 \\ 0 & 0 & D_2' \end{pmatrix} S.$$

Esta igualdade implica

$$\Phi_i e_1 + e_2 D_1 = D_1' s_{22},$$

onde s_{22} é um bloco da matriz S. Logo

$$e_2 D_1 = D_1' s_{22} \pmod{\lambda^{\phi(p^i)}}$$

Daqui, como no caso anterior, e com notações análogas, se obtém

$$\det e_2 \cdot v_1 \lambda^k = \det s_{22} \cdot v_2 \lambda^k \pmod{\lambda^{\phi(p^i)}},$$

$$\det e_2 \cdot v_1 = \det s_{22} \cdot v_2 \pmod{\lambda^{\phi(p^i)-k}}.$$

Donde, como o máximo expoente $k < \phi(p^i)$:

$$\det e_2 v_1 = \det s_{22} v_2 (\mathrm{mod}\ \lambda).$$

Por outro lado $a_2 D_1 = 0$, pois os expoentes de λ em D_1 são > 0, desde que provém de módulos do tipo 7 e 8. Em conseqüência da igualdade de matrizes acima se deduz $a_1 = s_{22}$ (mod λ).

Como a matriz

$$\begin{pmatrix} a_1 & a_2 \\ p\Pi_1(e_1) & \Pi_1(e_2) \end{pmatrix}$$

é inversível,

$$\det a_1 \det \Pi_1(e_2) = \pm 1 (\mathrm{mod}\ p).$$

Logo, $v_1 = \pm(\det s_{22})^2 v_2 (\mathrm{mod}\ \lambda)$.

Daqui concluímos que v_1 tem o fator q se e só se v_2 o tem, portanto M_1 tem um somando do tipo 8, se e só se M_2 o tem. □

Finalmente faremos algumas considerações sobre os módulos Σ que são soma direta de indecomponíveis sobre ZG_n, tais que cada um tem no máximo três fatores de composição irredutíveis sobre QG_n, incluindo o trivial. Σ é assim formada pela soma de vários módulos ${}_iM_j$, do tipo estudado na proposição C, para vários pares (i,j), com $1 \leq i < j \leq n$.

É fácil ver que a classe de isomorfismo de Σ está determinada pela informação seguinte:

1º A classe de isomorfismo local dos indecomponíveis.

2º Para cada i, a classe do ideal $A_i(\Sigma)$, produto dos ideais de R_i que aparecem nos somandos de Σ.

3º Para cada par (i,j), os invariantes III e IV de ${}_iM_j$.

Com efeito, a soma Σ é uma extensão de um reticulado N sobre R_n por um reticulado Σ_{n-1} sobre ZG_{n-1}. Este N é uma soma de ideais de R_n, e está determinado pelo posto, e pela classe do ideal $A_n(\Sigma)$, produto desses ideais. Também sabemos que $A_n(\Sigma)$ pode-se colocar no lugar de um R_n qualquer, sem mudar a classe de isomorfismo de N, nem a de Σ. Do mesmo modo, mostra-se que os ideais de $R_{n-1},\ldots,R_1$ podem-se multiplicar e por no lugar de um dos $R_{n-1},\ldots,R_1$, sem alterar a classe de isomorfismo de Σ.

A classe de isomorfismo local dos indecomponíveis determina os tipos dos indecomponíveis. Fixado, para cada i, o ideal $A_i(\Sigma)$ em um somando determinado, fica determinada a classe de isomorfismo dos indecomponíveis dos tipos 1, 2 e 3 em cada ${}_iM_j$. Finalmente, dados os invariantes III e IV para cada par i,j, está determinado ${}_iM_j$.

Sejam agora Σ e Σ' duas somas dessa forma tais que $\Sigma \simeq \Sigma'$. Nessas condições a classe de isomorfismo local dos indecomponíveis de Σ e Σ' é a mesma. O reticulado Σ_{n-1} sobre ZG_{n-1} indicado acima é um submódulo bem determinado de

Σ, que tem por imagem segundo o isomorfismo $\Sigma \simeq \Sigma'$, um submódulo análogo Σ'_{n-1} de Σ'. Daqui resulta que $A_n(\Sigma) \simeq A_n(\Sigma')$. Repetindo isto com Σ_{n-1} e Σ'_{n-1}, se obtém $A_{n-1}(\Sigma) \simeq A_{n-1}(\Sigma')$, e assim sucessivamente.

Mas o isomorfismo $\Sigma \simeq \Sigma'$, em geral não implica que, para cada par (i,j), os invariantes III e IV das somas parciais ${}_iM_j$ e ${}_iM'_j$ de Σ e Σ', sejam iguais. De modo que estes invariantes das somas parciais não são sempre invariantes da soma Σ.

Para verificá-lo basta ver, por exemplo, que as seqüências exatas

$$0 \longrightarrow (R_1, R_2, \lambda^k) \longrightarrow (R_1, R_2, \lambda^k u) \longrightarrow R_1/wR_1 \longrightarrow 0$$

$$0 \longrightarrow (R_1, R_3, \lambda^k) \longrightarrow (R_1, R_3, \lambda^k u) \longrightarrow R_1/wR_1 \longrightarrow 0$$

implicam, como vimos na demonstração da proposição C, que

$$(R_1, R_2, \lambda^k) \oplus (R_1, R_3, \lambda^k u) \simeq (R_1, R_2, \lambda^k u) \oplus (R_1, R_3, \lambda^k).$$

Em geral, dados $i < j_1 < j_2 < \ldots$, relações como estas permitem, para cada k, pôr em um somando o produto de todos os $u \in \bar{R}_i$, dos somandos da forma

$$(R_i, R_{j_1}, \lambda^k u_1), (R_i, R_{j_2}, \lambda^k u_2), \ldots,$$

sem mudar a classe de isomorfismo da soma.

Se $w \in ZG_n$ tem imagem u^{-1} em $\bar{R}_1$ e imagem u' em $\bar{R}_2$, então as seguintes seqüências são exatas, como mostramos em C.

$$0 \longrightarrow (R_1, R_2, \lambda^k) \longrightarrow (R_1, R_2, \lambda^k u) \longrightarrow R_2/\omega R_2 \longrightarrow 0$$

$$0 \longrightarrow (R_2, R_3, \lambda^k) \longrightarrow (R_2, R_3, \lambda^k u') \longrightarrow R_2/\omega R_2 \longrightarrow 0.$$

Isto implica:

$$(R_1, R_2, \lambda^k) \oplus (R_2, R_3, \lambda^k u') \simeq (R_1, R_2, \lambda^k u) \oplus (R_2, R_3, \lambda^k).$$

Assim é possível relacionar os $u \in \bar{R}_i$ com os $u' \in \bar{R}_j$ se há somandos

$$(R_i, R_j, \lambda^k u), (R_j, R_l, \lambda^k u'),$$

com $i < j < l$.

Por outro lado, se u_1, u_1', u_3, u_3' são representantes escolhidos como na proposição B, então

$$(R_1, R_2, \lambda^k u_1) \oplus (R_3, R_4, \lambda^k u_3) \simeq (R_1, R_2, \lambda^k u_1') \oplus (R_3, R_4, \lambda^k u_3')$$

implica $u_1 = u_1'$ e $u_3 = u_3'$.

Com efeito, estas duas somas contêm os seguintes submódulos sobre ZG_2, levado um no outro pelo isomorfismo,

$$(R_1, R_2, \lambda^k u_1) \simeq (R_1, R_2, \lambda^k u_1').$$

Logo, pela proposição B, $u_1 = u_1'$. Tomando os quocientes das somas por estes submódulos; resulta a outra igualdade.

Com estas relações é possível determinar os invariantes de uma soma de indecomponíveis dos tipos 1, 2, 3, 4. Também podemos demonstrar outras relações similares com estas. Mas ainda não temos informação suficiente para dar um conjunto de invariantes de toda soma Σ. Porém, os métodos

que temos aplicado, devem permitir caracterizar qualquer soma de indecomponíveis dos tipos considerados aqui.

REFERENCIAS

[1] - F.E.Diederichsen, Über die Ausreduktion ganzzahliger Gruppendarstellugem bei arithmetischer Äquivalenz, *Abh. Math. Sem. Univ. Hamburg 13* (1940), 347-412.

[2] - C.W.Curtis & I.Reiner, *Representation of finite groups and associative algebras*, Interscience, New York, 1962.

[3] - A.Heller & I,Reiner, Representations of cyclic groups in rings of integers I, II, *Ann.ofMath.76* (1962), 73-92 e *77* (1963),318-328.

[4] - Alfredo Jones, Groups with a finite number of indecomposable integral representations, *Mich. Math. J. 10* (1963), 257-261.

[5] - S.D.Berman & P.M.Gudivok, Indecomposable representations of finite groups over the ring of p-adic integers, *Izv. Akad. Nauk, SSSR, Ser. Mat. 28* (1964), 875-910.

[6] - Irving Reiner, Topics in integral representation theory, IV Escola de Álgebra, São Paulo, 1976, a ser publicado na série *Springer Lecture Notes*.

[7] - Irving Reiner, Invariants of integral representations, *Pacific J. Math. 78* (1978), 467-501.

[8] - Irving Reiner, Integral representations of cyclic p-groups, *Proceedings Canberra SLN 697*, 1978, 70-87.