SOBRE O TEOREMA
DE KRULL-SCHMIDT

Aron Taitelbaum

DISSERTAÇÃO
~~TESE~~ APRESENTADA AO INSTITUTO DE MATEMÁTICA E ESTATÍSTICA DA UNIVERSIDADE DE SÃO PAULO, PARA OBTENÇÃO DO GRAU DE MESTRE EM MATEMÁTICA

ORIENTADOR: Prof. Dr. ALFREDO ROSALIO JONES RODRIGUEZ.

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

SÃO PAULO, 1976.

AGRADECIMENTOS

Agradeço:

aos amigos que comigo conviveram no C.R.U.S.P.;

aos participantes dos seminários de Álgebra do IME-USP;

ao Professor Alfredo R. Jones pela paciente e constante orientação bem como pelo estímulo e compreensão durante a elaboração deste trabalho.

Aron Taitelbaum

ÍNDICE

INTRODUÇÃO 1

CAPÍTULO I 12

CAPÍTULO II 23

CAPÍTULO III 36

CAPÍTULO IV 46

CAPÍTULO V 64

BIBLIOGRAFIA 74

INTRODUÇÃO

Todos os anéis considerados serão providos de unidade e, quase sempre, serão domínios de integridade.

Uma representação de grau n de um grupo G sobre um anel R é um homomorfismo de G no grupo multiplicativo das matrizes $n \times n$ inversíveis com coeficientes em R. Duas representações T e T' de um grupo G sobre R são ditas equivalentes quando existe uma matriz P tal que, para todo elemento g de G, se tem $T(g) = PT'(g)P^{-1}$.

Uma representação T de um grupo finito $G=\{g_1,\dots,g_m\}$ sobre um anel R pode ser estendida a uma representação $\bar{T}$ do anel de grupo RG, isto é, a um homomorfismo $\bar{T}$ de RG no anel das matrizes $n \times n$ com coeficientes em R, tal que $\bar{T}(1) = I$, fazendo $\bar{T}\left(\sum_{i=1}^{m} r_i g_i\right) = \sum_{i=1}^{m} r_i T(g_i)$, com $r_i \in R$.

Dado um R-módulo M livre de posto n, como o anel das matrizes $n \times n$ com coeficientes em R é isomorfo ao anel dos endomorfismos de M, podemos, fixando uma base de M, considerar $\bar{T}$ como um homomorfismo de RG no anel dos endomorfismos de M.

Por outro lado, pode-se dar a M uma estrutura de RG-módulo, definindo a ação de G sobre M por: $gm=T(g)(m)$ para $g \in G$ e $m \in M$.

Dessa maneira, obtém-se uma correspondência bijetora entre as classes de equivalência das representações de grau n de um grupo G (ou do anel RG) sobre um anel R e as classes de isomorfismo dos RG-módulos, que, como R-módulos, são livres e de posto igual a n.

Se A é um anel, um A-módulo M é dito decomponível se é possível expressá-lo como soma direta de dois módulos não nulos. Em caso contrário, M é chamado indecomponível. A correspondência acima descrita associa módulos indecomponíveis com representações indecomponíveis.

Esses fatos nos sugerem que podemos generalizar o conceito de representação, considerando a qualquer A-módulo como uma representação do anel A.

Dado, então, um anel A, surgem, de imediato, as seguintes questões:

(i) Se qualquer A-módulo pode ou não ser expresso como soma direta de A-módulos indecomponíveis.

(ii) Determinar o número de A-módulos indecomponíveis não isomorfos.

(iii) Descrever os A-módulos indecomponíveis.

(iv) Determinar se a decomposição de um A-módulo em A-módulos indecomponíveis é única a menos de isomorfismos e da ordem dos somandos.

No presente estudo, trataremos do último problema citado, no caso em que A é um anel de grupo de um grupo finito.

Diz-se que um A-módulo M satisfaz a propriedade de Krull-Schmidt se, sempre que tivermos duas decomposições $M = M_1 \oplus \ldots \oplus M_r \cong N_1 \oplus \ldots \oplus N_s$ desse A-módulo em A-módulos indecomponíveis, seguir-se que r é igual a s e M_i é isomorfo a N_i, para todo i, depois de convenientemente reenumerados os N_j.

Diz-se que o teorema de Krull-Schmidt vale para um anel A ou que A satisfaz a propriedade de Krull-Schmidt quando todo A-módulo finitamente gerado satisfaz ao teorema de Krull-Schmidt.

Quando o anel A satisfaz ao teorema de Krull-Schmidt e todo A-módulo finitamente gerado é soma direta finita de A-módulos indecomponíveis, valem as seguintes propriedades:

1) Se M e N são A-módulos finitamente gerados, N um somando direto de M e $M = M_1 \oplus \ldots \oplus M_r$ é uma decomposição de M em submódulos indecomponíveis, então N é isomorfo à soma direta de um subconjunto do conjunto dos M_i.

2) Se L, M e N são A-módulos finitamente gerados, $L \oplus M \cong L \oplus N$ implica $M \cong N$. Esta propriedade é conhecida como a propriedade do cancelamento.

3) Se M e N são A-módulos finitamente gerados e $M^r \cong N^r$ para algum inteiro positivo r, então $M \cong N$.

As demonstrações dessas propriedades consistem simplesmente em decompor os módulos envolvidos em indecomponíveis e aplicar o teorema de Krull-Schmidt.

Como veremos no capítulo V, nenhuma dessas propriedades é suficiente para assegurar a validade do teorema de Krull-Schmidt.

No capítulo I, demonstraremos o teorema de Krull Schmidt para anéis artinianos, resultado obtido por Ajumaya.

No capítulo II, apresentamos um exemplo construído por Reiner da não validade do teorema no caso em que A=RG, sendo R o anel dos inteiros algébricos de um corpo de números algébricos.

No capítulo III, veremos a demonstração do teorema de Krull-Schmidt para álgebras finitamente geradas sobre anéis locais noetherianos completos, conforme o caminho adotado por R. G. Swan.

No capítulo IV, estudamos o caso em que A = RG, com R um anel de valorização discreta de característica zero. Apresentamos um resultado de Jones, que dá uma condição necessária e suficiente para a validade do teorema quando o grupo G é comutativo e o anel R é o dos racionais p-inteiros, onde p é um primo, e uma generalização de Jacobinski para a suficiência no caso de p-grupos não comutativos com p um primo ímpar.

Finalmente, no capítulo V, estendemos alguns desses resultados para R-ordens.

A seguir, apresentaremos algumas definições e resultados que se constituem em pré-requisitos para o material contido nesta dissertação.

Se A é um anel e M e N são A-módulos, define-se comumente $\mathrm{Ext}_A(M, N)$ por $\mathrm{Ext}_A(M, N) = H_1(\mathrm{Hom}_A(P_M, N))$, onde P_M é uma resolução projetiva contraída de M e H_1 é o primeiro grupo de homologia. Para nós, serão mais convenientes duas outras caracterizações de $Ext_A(M, N)$ que descreveremos abaixo:

1) Dado um domínio de Dedekind R cujo corpo de quocientes é K e um grupo finito G, sejam M e N RG-módulos que, como R-módulos, são livres de posto finito.

Uma função de ligação do par M, N é um R-homomorfismo definido em RG com valores em $Hom_R(N, M)$ tal que: $F(xy)(m) = xF(y)(m) + F(x)(ym)$, para $x,y \in RG$ e $m \in N$.

O conjunto $B(M, N)$ cujos elementos são todas as funções de ligação do par M, N é um grupo comutativo com a soma de funções e um R-módulo finitamente gerado sem torção.

Uma função de ligação F do par M, N é dita uma função de ligação interna se puder ser calculada por uma fórmula do tipo: $F(x)(m) = xD(m) - Dxm$, para $x \in RG$ e $m \in N$, onde D é um R-homomorfismo fixo de N em M.

O conjunto $B'(M, N)$ formado pelas funções de ligação interna do par M, N é um R-submódulo de $B(M, N)$ e define-se $Ext_{RG}(M, N) = \dfrac{B(M,N)}{B'(M, N)}$.

Sejam T e U as representações matriciais de M e N respectivamente. Em linguagem matricial, a uma função de ligação $F \in B(M, N)$ corresponde uma função L que a cada elemento g de G associa a matriz $L(g)$ tal que a função que leva g na matriz

$$\begin{pmatrix} T(g) & L(g) \\ 0 & U(g) \end{pmatrix}$$

é uma representação matricial de G.

Se F é uma função de ligação interna do par M, N então existe uma matriz D com coeficientes em R tal que $L(g) = T(g)D - DU(g)$ para todo g de G.

Seja P um ideal primo de R que contém o ideal gerado em R pela ordem do grupo G e seja $|G|R = P^{\alpha}P_1^{\alpha_1} \ldots P_r^{\alpha_r}$ a expressão de $|G|R$ como produto de ideais primos.

A parte P-primária de $\mathrm{Ext}_{RG}(M, N)$ é definida como sendo o conjunto dos elementos $F \in \mathrm{Ext}_{RG}(M, N)$ tais que $P^{\alpha}F = 0$.

Valem os seguintes teoremas:

TEOREMA 0.1. A parte P-primária de $\mathrm{Ext}_{RG}(M, N)$ é igual a $R_P\ \mathrm{Ext}_{RG}(M, N)$, onde R_P é a localização de R em P.

TEOREMA 0.2. $R_P\ \mathrm{Ext}_{RG}(M, N) = \mathrm{Ext}_{RG}(R_PM, R_PN)$.

TEOREMA 0.3. $|G|\ \mathrm{Ext}_{RG}(M, N) = 0$.

As demonstrações destes teoremas, bem como os detalhes desta caracterização podem ser encontradas em (3, Seção 75).

2) Sejam M e N RG-módulos. Uma extensão de M por N é uma sequência exata de RG-módulos do tipo:

$$0 \longrightarrow M \longrightarrow X \longrightarrow N \longrightarrow 0.$$

Duas extensões ε e ε' de M por N são ditas equivalentes se existe um homomorfismo $\phi:E \longrightarrow E'$ que torna comutativo o diagrama:

$$\begin{array}{ccccccccc} \varepsilon = 0 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & N & \longrightarrow & 0 \\ & & 1_M\downarrow & & \downarrow\phi & & \downarrow 1_N & & \\ \varepsilon' = 0 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & N & \longrightarrow & 0. \end{array}$$

Pode-se definir $\mathrm{Ext}_{RG}(N, M)$ como o conjunto das classes de equivalência das extensões de M por N e definir uma soma de classes que torna $\mathrm{Ext}_{RG}(N, M)$ um grupo no qual o elemento neutro é a classe de equivalência da extensão

$$0 \longrightarrow M \longrightarrow M \oplus N \longrightarrow N \longrightarrow 0.$$

Resulta que se $\mathrm{Ext}_{RG}(N,M)=0$, toda extensão de M por N cinde.

Os detalhes desta caracterização podem ser encontrados em (16, II 49).

Um RG-módulo M é denominado R-redutível se contém um RG-submódulo não nulo cujo posto sobre R seja menor que o de M. Em caso contrário, M diz-se R-irredutível.

Uma cadeia $M = M_h \supset M_{h-1} \supset \ldots \supset M_0 = 0$ de RG-submódulos de M é chamada uma série de R-composição de M, quando:

(i) Como R-módulo, M_{i-1} é um somando direto de M_i, para $i = 1, 2, \ldots h$.

(ii) $\dfrac{M_i}{M_{i-1}}$ é um RG-módulo R-irredutível, para $i=1,2,\ldots,h$.

Os fatores $\dfrac{M_i}{M_{i-1}}$ são chamados fatores de R-composição de M. Nem sempre os fatores de R-composição são unicamente determinados a menos de RG-isomorfismo e ordem de ocorrência. Vale, no entanto, o seguinte teorema:

TEOREMA 0.4. Seja R um anel de valorização discreta e G um grupo finito. Se $|G|R = R$, então os fatores de R-composição de um RG-módulo M, que como R-módulo seja livre de posto finito, são únicos a menos de RG-isomorfismo e ordem de ocorrência (3, 76.19).

Dado um anel R, definimos o radical de Jacobson de R como sendo a interseção de todos os ideais maximais de R e o representaremos por $\text{rad } R$. O $\text{rad } R$ é um ideal bilateral de R. Vamos precisar do seguinte resultado:

LEMA 0.5. (Nakayama). Seja M um R-módulo finitamente gerado e N um submódulo de M.

Se $M = N + (\text{rad } R)M$ então $N = M$.

Um R-módulo simples (ou irredutível) é um R-módulo que não admite submódulos não triviais. Um R-módulo M é dito semisimples quando todo submódulo de M é somando direto de M. Isto equivale a afirmar que M é soma direta de submódulos simples. Um anel R é semisimples quando for semisimples como R-módulo. Isto ocorre se e só se todo R-módulo é semisimples. Valem ainda os seguintes resultados:

LEMA 0.6. Se M é um R-módulo simples, $\text{Hom}_R(M, M)$ é um anel com divisão.

LEMA 0.7. Se R é semisimples, $\operatorname{rad} R = 0$.

LEMA 0.8. Se R é artiniano e $\operatorname{rad} R = 0$, então R é semisimples.

LEMA 0.9. $\operatorname{rad}\left(\dfrac{R}{\operatorname{rad} R}\right) = 0$.

Necessitaremos também alguns resultados sobre extensões ciclotômicas, cujas demonstrações estão em (20).

TEOREMA 0.10. Sejam m um inteiro positivo e p um número primo. Se $\hat{Q}$ é o completamento p-ádico de Q e f o polinômio ciclotômico de ordem m em $Q[x]$, então o número de extensões do ideal gerado em Z por p à $Q(\sqrt[m]{1})$ é igual ao número de fatores irredutíveis distintos de f em $\hat{Q}[x]$ (20, 2-4-5 e 2-4-6).

Seja $\mathcal{O}$ o anel dos inteiros de $Q(\sqrt[m]{1})$.

TEOREMA 0.11. Se p não divide m, $p\mathcal{O} = P_1P_2 \dots P_r$ onde os P_i são ideais primos distintos de $\mathcal{O}$ e $r = \dfrac{\Phi(m)}{d}$, onde Φ é a função de Euler e d é a ordem de p no grupo dos inversíveis do anel $\dfrac{Z}{mZ}$ (20, 7-2-4).

TEOREMA 0.12. Se m é uma potência de p, então p tem uma única extensão a $Q(\sqrt[m]{1})$ a qual é dada por: $p\mathcal{O}=(1-\zeta)^{\Phi(p^s)}$, onde $p^s = m$ e ζ é uma raiz m-ésima primitiva da unidade (20, 7-4-1).

TEOREMA 0.13. Se $m = p^s m'$, onde p não divide m', então: $p\mathcal{O} = (P_1 \dots P_r)^{\Phi(p^s)}$ onde $r = \frac{\Phi(m')}{d'}$ e d' é a ordem de p no grupo dos inversíveis de $\frac{Z}{m'Z}$ (20, 7-4-3).

<u>TEOREMA 0.14.</u> Seja P o ideal maximal do anel de valorização de um corpo valorizado F e seja E uma extensão finita de F, tal que $\hat{F} \otimes_F E$ é semisimples, onde $\hat{F}$ é o completamento P-ádico de F. Se $Q_1, Q_2, \dots, Q_r$ são as extensões de P a E e $\hat{E}_i$ é o completamento Q_i-ádico de E para $i = 1, 2, \dots, r$, tem-se: $\hat{F} \otimes_F E \cong \hat{E}_1 \oplus \dots \oplus \hat{E}_r$ (20, 2-5-11).

Seja G um grupo finito e K um corpo cuja característica não divide a ordem de G. Suponhamos que KG seja isomorfo a $\bigoplus_{j=1}^{r} A_j$, onde A_j é o anel de matrizes $M_{n_j}(D_j)$ com D_j anel com divisão. Seja F uma extensão de K que seja um corpo de decomposição de G e M um FG-módulo simples ao qual corresponde a representação Ψ de G.

Seja λ o caráter de Ψ, isto é, a função de G em F que a cada elemento g de G associa o traço da matriz $\Psi(g)$.

<u>LEMA 0.15.</u> Existe um único j tal que $A_jM \neq 0$, e o centro de A_j é isomorfo a $K(\lambda)$, onde $K(\lambda)$ é a extensão de K obtida pela adjunção dos elementos $\lambda(g)$, com g percorrendo G. (4, 24.7).

Define-se o índice de Schur de Ψ sobre K como sendo a raiz quadrada da dimensão de D_j sobre $K(\lambda)$.

TEOREMA 0.16. (Roquette). Se G é um grupo nilpotente de ordem ímpar, o índice de Schur de uma representação irredutível de G sobre K é igual a 1 (18).

CAPÍTULO I

Dado um anel R, um R-módulo M é dito artiniano se ele obedece a uma das seguintes condições equivalentes:

(i) Todo conjunto não vazio de submódulos de M possui pelo menos um elemento minimal.

(ii) Toda cadeia descendente $M_1 \supseteq M_2 \supseteq \ldots \supseteq M_i \supseteq \ldots$ de submódulos de M é estacionária, ou seja, existe m_0 tal que $M_i = M_{m_0}$ para i maior ou igual a m_0.

Um R-módulo M é chamado noetheriano quando obedecer a uma das seguintes condições equivalentes:

(i) Todo conjunto não vazio de submódulos de M contém pelo menos um elenento maximal.

(ii) Toda cadeia ascendente $M \subseteq M \subseteq \ldots \subseteq M_i \subseteq \ldots$ de submódulos de M é estacionária.

<u>LEMA 1.1.</u> Um módulo M é noetheriano se e somente se todo submódulo de M é finitamente gerado.

<u>Demonstração:</u> Seja M noetheriano e N um submódulo de M. O conjunto dos submódulos finitamente gerados de N é não vazio e, portanto, admite um elemento maximal N_0. Se x é um elemento de N, como o submódulo gerado por x e N_0 é finitamente gerado, contém N_0 e está contido em N, resulta que este

submódulo é igual a N_0 e, portanto, x pertence a N_0. Logo, $N = N_0$ e, portanto, N é finitamente gerado. Se, por outro lado, todo submódulo de M for finitamente gerado, dada uma cadeia ascendente $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_i \subseteq \ldots$, a união dos M_i será um submódulo de M e, portanto, finitamente gerado. Assim sendo, a cadeia será estacionária a partir daquele M_i que contiver todos os geradores da união. □

<u>LEMA 1.2.</u> Seja N um submódulo de M. Então:

(i) M é noetheriano se e só se N e $\frac{M}{N}$ são noetherianos.

(ii) M é artiniano se e só se N e $\frac{M}{N}$ são artinianos.

<u>Demonstração</u>: Suponhamos que N e $\frac{M}{N}$ sejam noetherianos e seja $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_i \subseteq \ldots$ uma cadeia de submódulos de M. As cadeias

$$M_1 \cap N \subseteq M_2 \cap N \subseteq \ldots \subseteq M_i \cap N \subseteq \ldots$$

e

$$\frac{M_1+N}{N} \subseteq \frac{M_2+N}{N} \subseteq \ldots \subseteq \frac{M_i+N}{N} \subseteq \ldots$$

são ascendentes e, portanto, estacionárias. Assim, para i maior ou igual a um certo j fixo, teremos: $M_i \cap N = M_j \cap N$ e $\frac{M_i+N}{N} = \frac{M_j+N}{N}$. Dado x em M_i, tem-se $x + N = y + N$, com y em M_j. Então: $x - y \in N \cap M_i = N \cap M_j$, donde $x - y$ está em M_j e, portanto, x pertence a M_j.

Logo: $M_i = M_j$ para $i \geq j$. A recíproca é imediata e a demonstração para o caso artiniano é inteiramente análoga. □

<u>COROLÁRIO 1.3.</u> Uma soma direta finita de módulos é noetheriana (ou artiniana) se e só se cada somando é noetheriano (ou artiniano).

<u>TEOREMA 1.4.</u> Todo R-módulo que satisfaz a uma das condições de cadeia é soma direta finita de R-módulos indecomponíveis.

<u>Demonstração</u>: Suponhamos que M não seja soma direta finita de indecomponíveis. Em particular, $M = M_1 \oplus M_2$ com M_1 e M_2 não triviais e com pelo menos um dos dois, M_1 ou M_2, decomponível. Assim, supondo M_2 decomponível,

$$M = M_1 \oplus M_{21} \oplus M_{22}$$

com M_1, M_{21} e M_{22} não triviais. Pela suposição feita, podemos prosseguir na decomposição de M obtendo, por indução, uma decomposição infinita $M = \bigoplus_{i=1}^{\infty} M_i$ com os M_i não triviais. As cadeias infinitas não estacionárias

$$\bigoplus_{i=1}^{\infty} M_i \supsetneqq \bigoplus_{i=2}^{\infty} M_i \supsetneqq \bigoplus_{i=3}^{\infty} M_i \supsetneqq \cdots$$

e

$$M_1 \subsetneqq M_1 \oplus M_2 \subsetneqq M_1 \oplus M_2 \oplus M_3 \subsetneqq \cdots$$

mostram que M não é noetheriano nem artiniano. □

Se um R-módulo não obedece a nenhuma das condições de cadeia, o resultado acima não se mantém. Na verdade, o exemplo que apresentamos a seguir mostra que um módulo pode até mesmo não admitir decomposição alguma em submódulos indecomponíveis.

<u>EXEMPLO 1.5.</u> Seja A o anel das funções contínuas de $\mathbb{Q}$ em $\mathbb{R}$, no qual as operações de soma e multiplicação são definidas a partir das operações correspondentes de $\mathbb{R}$, e onde consideramos em $\mathbb{Q}$ a topologia induzida da topologia usual da reta $\mathbb{R}$. Consideremos A como A-módulo.

Se f é um idempotente de A, temos que $f(x) = x$, para todo x de $\mathbb{Q}$. Consequentemente, os únicos valores que f pode assumir são 0 e 1.

A função $h:\mathbb{Q} \to \mathbb{R}$ definida por $h(x) = 0$ para $x < \sqrt{2}$ e $h(x) = 1$ para $x > \sqrt{2}$ é um exemplo de um idempotente não trivial de A, o que nos garante a decomponibilidade de A, pois, nesse caso, $A = Ah \oplus A(1-h)$, onde 1 é a função constante de $\mathbb{Q}$ em $\mathbb{R}$ que assume o valor 1 em todos os pontos.

Seja f um idempotente não nulo de A e seja $a \in \mathbb{Q}$ um ponto no qual $f(a) = 1$. Como f é contínua e só assume os valores 0 e 1 existe uma vizinhança de raio r de a em $\mathbb{Q}$ na qual f é sempre igual a 1. Escolhamos $b < c < d$ em $\mathbb{R}$ tais que b, c e d sejam irracionais e o intervalo fechado da reta de extremos b e d esteja contido na vizinhança de raio r de a em $\mathbb{R}$.

Vamos definir duas funções g_1 e g_2 de $\mathbb{Q}$ em $\mathbb{R}$ por:

(i) Se $x < b$ ou $x > d$, $g_1(x) = f(x)$ e $g_2(x) = 0$.

(ii) Se $b < x < c$, $g_1(x) = 1$ e $g_2(x) = 0$.

(iii) Se $c < x < d$, $g_1(x) = 0$ e $g_2(x) = 1$.

Então, g_1 e g_2 pertencem a A, são idempotentes e $g_1 + g_2 = f$. Como vemos, nenhum idempotente de A é primitivo. Assim sendo, todo somando direto de A é um A-módulo decomponível.

Um anel A é chamado um anel local quando se verifica uma das três propriedades equivalentes abaixo:

(i) A tem um único ideal maximal.

(ii) O conjunto dos elementos não inversíveis de A forma um ideal bilateral.

(iii) Dados x e y em A, se x e y são não inversíveis, então $x + y$ é não inversível.

Se A é local, o seu ideal maximal é precisamente aquele cujos elementos são os não inversíveis de A e coincide com o radical de Jacobson de A.

<u>LEMA 1.6.</u> Se M é um A-módulo indecomponível, artiniano e noetheriano, o anel $\mathrm{Hom}_A(M, M)$ é local.

<u>Demonstração:</u> Basta verificar que se $f, g \in \mathrm{Hom}_A(M, M)$ são tais que $f + g = 1_M$ um dos dois é inversível.

Com efeito, nesse caso, se $\phi + \psi$ é inversível, existe θ inversível tal que $(\phi + \psi)\theta = 1_M$, donde, por exemplo, $\phi\theta$ é inversível e existe π inversível com $\phi\theta\pi = 1_M$, do que segue que $\phi = (\theta\pi)^{-1}$.

Sejam

$$f^1 = f \quad \text{e} \quad f^i = f_0 f^{i-1}$$

para $i > 1$.

Como M é artiniano e noetheriano, as cadeias

$$\operatorname{Ker} f \subseteq \operatorname{Ker} f^2 \subseteq \operatorname{Ker} f^3 \subseteq \dots$$

e

$$\operatorname{Im} f \supseteq \operatorname{Im} f^2 \supseteq \operatorname{Im} f^3 \supseteq \dots$$

são estacionárias a partir de um certo índice j.

Seja h a restrição de f^j ao conjunto $\operatorname{Im} f^j$ com valores em $\operatorname{Im} f^{2j} = \operatorname{Im} f^j$. Pela maneira como é definida, h é um epimorfismo. Além disso, se $f^j(f^j(x)) = 0$, x pertence ao $\operatorname{Ker} f^{2j} = \operatorname{Ker} f^j$ e, portanto, $f^j(x) = 0$.

Logo, h é um isomorfismo. Tomando $k = ih^{-1}$, onde i é a inclusão de $\operatorname{Im} f^j$ em M, temos que a sequência exata

$$0 \longrightarrow \operatorname{Ker} f^j \longrightarrow M \underset{k}{\overset{\longrightarrow}{\longleftarrow}} \operatorname{Im} f^j \longrightarrow 0$$

cinde, o que, como M é indecomponível, implica em $\operatorname{Im} f^j = 0$ ou $\operatorname{Im} f^j = M$.

Se $\operatorname{Im} f^j = 0$, tem-se $f^j = 0$ e, nesse caso,

$$1 + f + \dots + f^{j-1} = (1 - f)^{-1} = g^{-1}$$

e, portanto, g é inversível.

Se $\operatorname{Im} f = M$, resulta $\operatorname{Ker} f^j = 0$ e daí se obtém que $\operatorname{Im} f = M$ e $\operatorname{Ker} f = 0$, sendo então f inversível. □

<u>LEMA 1.7.</u> (Lema X). Dado o seguinte diagrama de sequências exatas

$$\begin{tikzcd}
 & M' \arrow[dr, "\phi"] & & N'' & \\
 & & x \arrow[ur, "\tau"] \arrow[dr, "\psi"] & & \\
 & N' \arrow[ur, "\sigma"] & & M'' \arrow[dr] & \\
0 \arrow[ur] & & & & 0
\end{tikzcd}$$

se $\tau\phi$ for isomorfismo, $\psi\sigma$ também o será.

Demonstração: Primeiro, vejamos que se $\tau\phi$ é monomorfismo $\psi\sigma$ também o é. Seja $x \in N'$. Se $\psi(\sigma(x)) = 0$, $\sigma(x)$ está em $\mathrm{Ker}\ \psi = \mathrm{Im}\ \phi$, donde $\sigma(x) = \phi(m')$ com m' em M'. Daí: $\tau(\phi(m')) = \tau(\sigma(x)) = 0$, o que implica $m' = 0$, donde $\sigma(x)=0$ e, consequentemente, $x = 0$.

Suponhamos agora que $\tau\phi$ seja um epimorfismo e tomemos y em M''. Temos $y = \psi(x)$ para algum x de X. Além disso, $\tau(x) = \tau(\phi(m'))$, com m' em M'. Segue daí que $x - \phi(m')$ está em $\mathrm{Ker}\ \tau = \mathrm{Im}\ \sigma$ e, portanto, $x-\phi(m')=\sigma(n')$, com n' em N'. Mas $\psi(\sigma(n')=\psi(x)-\psi(\phi(m')) = \psi(x)=y$. □

TEOREMA 1.8. Seja A um anel tal que $\mathrm{Hom}_A(L, L)$ é um anel local sempre que L for um A-módulo indecomponível.

Se M é um A-módulo noetheriano (ou artiniano), então, M satisfaz ao teorema de Krull-Schmidt.

Demonstração: Sejam $M = \bigoplus_{i=1}^{m} M_i = \bigoplus_{j=1}^{n} N_j$ duas decomposições de M em módulos indecomponíveis. Faremos a demonstração por indução sobre m. Se $m = 1$, M é indecomponível e resulta $m = n = 1$ e $M_1 = M = N_1$

Sejam $\pi_i = M \longrightarrow M_i$, $\pi'_j : M \longrightarrow N_j$ as projeções e $\phi_i : M_i \longrightarrow M$, $\phi'_j : N_j \longrightarrow M$ as inclusões correspondentes às decomposições dadas. Temos que $1_M = \sum_{j=1}^{n} \phi'_j \pi'_j$ e, portanto, $1_{M_1} = \pi_1 \phi_1 = \sum_{j=1}^{n} \pi_1 \phi'_j \pi'_j \phi_1$.

Como $\mathrm{Hom}_A(M, M)$ é um anel local, $\pi_1 \phi'_{j_1} \pi'_{j_1} \phi_1$ é inversível para algum j_1. Aplicando o lema X ao diagrama abaixo

$$\begin{tikzcd}
0 \arrow[dr] & & & & 0 \\
& M_1 \arrow[dr, "\pi'_{j_1}\phi_1"'] & & M_1 \arrow[ur] & \\
& & N_{j_1} \arrow[ur, "\pi_1\phi'_{j_1}"'] \arrow[dr, "\pi"] & & \\
& \mathrm{Ker}\ \pi_1\phi'_{j_1} \arrow[ur, "\phi"'] & & \dfrac{N_{j_1}}{\mathrm{Im}\pi'_{j_1}\phi_1} \arrow[dr] & \\
0 \arrow[ur] & & & & 0
\end{tikzcd}$$

obtemos a cisão da sequência exata.

$$0 \longrightarrow \mathrm{Ker}\ \pi_1\phi'_{j_1} \longrightarrow N_{j_1} \longrightarrow M_1 \longrightarrow 0$$

e, portanto, $N_{j_1} \cong \mathrm{Ker}\ \pi_1\phi'_{j_1} \oplus M_1$.

Como N_{j_1} é indecomponível e $M_1 \neq 0$, tem-se $\mathrm{Ker}\ \pi_1\phi'_{j_1} = 0$ e, portanto, $\pi_1\phi'_{j_1}$ é um isomorfismo entre

N_{j_1} e M_1.

Para concluir, aplicamos o lema X ao diagrama

$$\begin{tikzcd}
0 \arrow[dr] & & & & 0 \\
& N_{j_1} \arrow[dr, "\phi_{j_1}"] & & M_1 \arrow[ur] & \\
& & M \arrow[ur, "\pi_1"] \arrow[dr] & & \\
& \bigoplus\limits_{i=2}^{m} M_i \arrow[ur] & & \bigoplus\limits_{\substack{j=1 \\ j\neq j_1}}^{n} N_j \arrow[dr] & \\
0 \arrow[ur] & & & & 0
\end{tikzcd}$$

obtendo $\bigoplus\limits_{i=2}^{m} M_i \cong \bigoplus\limits_{\substack{j=1 \\ j\neq j_2}}^{n} N_j$, e seguindo-se o teorema pela hipótese de indução. □

<u>COROLÁRIO 1.9.</u> Se M é um A-módulo noetheriano e artiniano, então M satisfaz ao teorema de Krull-Schmidt.

<u>Demonstração:</u> Sejam $M = \bigoplus\limits_{i=1}^{m} M_i = \bigoplus\limits_{j=1}^{n} N_j$ duas decomposições de M em módulos indecomponíveis. Pelo lema 1.2. os M_i e os N_j são noetherianos e artinianos e, pelo lema 1.6, podemos concluir que os anéis $\mathrm{Hom}_A(M_i, M_i)$ e $\mathrm{Hom}_A(N_j, N_j)$ são locais. Daí, a mesma demonstração do teorema anterior nos permite obter o resultado desejado. □

Convém observar que a unicidade obtida pelo teorema de Krull-Schmidt é a menos de isomorfismos e que os somandos indecomponíveis não necessitam ser únicos, quando considerados como conjuntos.

Por exemplo, se V é um espaço vetorial de dimensão finita sobre um corpo K, V satisfaz ao teorema de Krull-Schmidt, mas podemos obter decomposições distintas de V, tomando bases diferentes de V.

Dizemos que um anel A é artiniano ou noetheriano conforme ele seja artiniano ou noetheriano considerado como A-módulo.

LEMA 1.10. Todo módulo finitamente gerado sobre um anel artiniano (ou noetheriano) é artiniano (ou noetheriano).

Demonstração: Seja A um anel artiniano e M um A-módulo finitamente gerado. Então, M é imagem homomórfica de um R-módulo L livre de posto finito.

Como $L \cong R^n = R \oplus \ldots \oplus R$ (n vezes) para algum inteiro positivo n, L é um R-módulo artiniano, o que implica que suas imagens homomórficas sejam R-módulos artinianos. □

LEMA 1.11. Se A é anel artiniano, A satisfaz a propriedade de Krull- Schmidt.

Demonstração: Basta observar que todo módulo finitamente gerado sobre A é artiniano e noetheriano (pois, todo anel artiniano é noetheriano).

TEOREMA 1.12. Se R é um anel artiniano e G um grupo finito, o anel de grupo RG satisfaz a propriedade de Krull-Schmidt.

Demonstração: Como R é artiniano, RG é um R-módulo artiniano. Como todo ideal de RG é um R-submódulo de RG, segue-se que RG é um anel artiniano e o teorema é uma consequência do lema anterior. □

CAPÍTULO II

Seja K um corpo de números algébricos e R o anel dos inteiros algébricos de K. Neste capítulo, veremos que nem sempre o anel de grupo RG de um grupo finito G satisfaz a propriedade de Krull-Schmidt.

Convencionaremos chamar de RG-módulo a todo RG-módulo finitamente gerado que, como R-módulo, seja sem torção, o que, como R é um domínio de Dedekind, equivale a considerar apenas os RG-módulos finitamente gerados que sejam R-projetivos.

Inicialmente, veremos que a propriedade de Krull-Schmidt falha trivialmente se R possui ideais que não são principais.

Tomando G como sendo o grupo unitário trivial, temos $RG = R$. Se $J_1, J_2, \ldots J_n$ são ideais de R, sabemos que $J_1 \oplus \ldots \oplus J_n \cong R \oplus \ldots \oplus R \oplus J_1 \ldots J_n$, onde R aparece $n-1$ vezes no lado direito desse isomorfismo. Se J é um ideal não principal de R, temos que, como R-módulos J não pode ser isomorfo a R, apesar de que, como vimos acima, $J \oplus J \cong R \oplus J^2$.

Como os ideais de R são finitamente gerados, sem torção e indecomponíveis, temos aí duas decomposições, essen cialmente diferentes, de um mesmo RG-módulo.

Consideraremos, agora, o caso em que R é um domínio de ideais principais. Nesse caso, todo RG-módulo terá uma base finita sobre R.

Sejam M e N RG-módulos. Dado um elemento F de $\mathrm{Ext}_{RG}(N, M)$, podemos associar a F um RG-módulo, o qual é uma extensão de M por N, cuja classe de extensão é F, e anotaremos este módulo por (M, N; F) ou por

$$\begin{pmatrix} M & F \\ 0 & N \end{pmatrix}$$

notação esta que corresponde à representação matricial associada a esse módulo.

<u>LEMA 2.1.</u> Seja A um anel arbitrário e M e N dois A-módulos. Se $\mathrm{Hom}_A(M, N) = \mathrm{Hom}_A(N, M) = 0$ e L é uma extensão de M por N, dado um A-endomorfismo f de L, tem-se:

(i) $f(M) \subseteq M$

(ii) f induz um homomorfismo $f': N \to N$

(iii) A aplicação de $\mathrm{Hom}_A(L, L)$ em $\mathrm{Hom}_A(M, M) \oplus \mathrm{Hom}_A(N, N)$ que leva f no par $(f|M, f')$ é um monomorfismo.

Demonstração: Na sequência exata

$$0 \longrightarrow M \xrightarrow{i} L \xrightarrow{j} N \longrightarrow 0$$

identificamos M com i(M). Como $jfi \in \mathrm{Hom}_A(M, N)$, tem-se $jfi = 0$ e, portanto, $f(i(M)) \subseteq \mathrm{Ker}\, j = i(M)$.

Ou seja, $f(M) \subseteq M$, donde $f|M \in \mathrm{Hom}_A(M, M)$. □

Para definir f', dado um elemento n de N, escolhemos x_n em L tal que $j(x_n) = n$ e fazemos $f'(n) = j(f(x_n))$.

Se x_n' é outro elemento de L tal que $j(x_n') = n$, como $j(x_n' - x_n) = 0$, tem-se que $x_n' - x_n \in i(M)$ e portanto $f(x_n' - x_n) \in i(M)$, do que segue que $j(f(x_n' - x_n)) = 0$, ou seja, $j(f(x_n')) = j(f(x_n))$, o que mostra estar f' bem definida.

Suponhamos agora que $f|M = f' = 0$.

Se $f|M = 0$, $f(i(M)) = 0$ e a aplicação de N em L que leva n em $f(x_n)$ estará bem definida, pois, se $n = j(x_n) = j(x_n')$ vem que $x_n - x_n' \in \text{Ker } j = i(M)$, do que resulta $f(x_n - x_n') = 0$, ou seja, $f(x_n) = f(x_n')$.

Por outro lado, $f' = 0$ implica que $j(f(x_n)) = 0$, para todo n de N e, portanto, $f(x_n) \in i(M)$, para $m \in N$, o que nos permite considerar a função que leva n em $f(x_n)$ um elemento de $\text{Hom}_A(N, M)$ e, portanto, igual à função constante nula, do que resulta $f = 0$.

<u>LEMA 2.2.</u> Sejam M e N RG-módulos indecomponíveis tais que $\text{Hom}_{KG}(KM, KN) = \text{Hom}_{KG}(KN, KM) = 0$ e seja F um elemento de $\text{Ext}_{RG}(N, M)$. Então: $(M, N; F)$ é decomponível se e só se $F = 0$.

Demonstração: Se $F = 0$, F é a extensão trivial de M por N, ou seja, $(M, N; F) \cong M \oplus N$ e, portanto, $(M, N; F)$ é decomponível.

Suponhamos, então, que $(M, N; F)$ seja decomponível e façamos $(M,N; F) = L = A \oplus B$, com $A \neq 0 \neq B$.

Seja $\pi_1 : L \longrightarrow L$ a projeção de L sobre A.

Se ϕ é um RG-homomorfismo de M em N, podemos associar a ϕ o KG-homomorfismo $1 \otimes \phi$ de KM em KN definido por $(1 \otimes \phi)(k \otimes m) = k \otimes \phi(m)$ para k em K e m em M. Pela hipótese, teremos que $1 \otimes \phi = 0$.

Assim sendo, $1 \otimes \phi(m) = 0$ para todo m em M, o que implica que $\phi(m)$ é um elemento de torção sobre R pois K é o corpo de quocientes de R. Como N é sem torção sobre R, concluímos que $\phi(m) = 0$ para todo m em M.

Portanto, $\mathrm{Hom}_{RG}(M, N) = 0$ e, da mesma forma, obtemos que $\mathrm{Hom}_{RG}(N, M) = 0$. Assim, podemos aplicar o lema anterior para obter que $\pi_1(M) \subseteq M$.

Como $(\pi_1|M)^2 = \pi_1|M$, pois π_1 é uma projeção, vemos que $\pi_1|M$ é uma projeção de M e sua imagem, consequentemente, é um somando direto de M. Como M é indecomponível, resulta que $\pi_1(M) = 0$ ou $\pi_1(M) = M$.

Suponhamos que $\pi_1(M) = 0$. Nesse caso, $M \subseteq B$ e temos: $N \cong \dfrac{A \oplus B}{M} \cong A \oplus \dfrac{B}{M}$. Como N é indecomponível e $A \neq 0$, resulta que $N \cong A$ e $B \cong M$.

Suponhamos que $\pi_1(M) = M$. Nesse caso, $M \subseteq A$ e temos $N \cong \dfrac{A \oplus B}{M} \cong \dfrac{A}{M} \oplus B$. Como N é indecomponível e $B \neq 0$ resulta $A \cong M$ e $N \cong B$.

Portanto, $(M, N; F) = L \cong M \oplus N$, donde $F = 0$. □

<u>TEOREMA 2.3.</u> Sejam A, B e C RG-módulos tais que KA, KB e

KC são KG-módulos irredutíveis não isomorfos dois a dois e tais que existem elementos F em $\mathrm{Ext}_{RG}(B, A)$ e F' em $\mathrm{Ext}_{RG}(C, A)$ cujas ordens são relativamente primas. Então, A, $(A, B; F)$ e $(A, C; F')$ são RG-módulos indecomponíveis e $A \oplus (A, B \oplus C; F + F') \cong (A, B; F) \oplus (A, C; F)$.

Demonstração: Como KA, KB e KC são irredutíveis, A, B e C devem ser indecomponíveis. Como $KA \not\cong KB$, $KB \not\cong KC$ e $KA \not\cong KC$, obtemos que $\mathrm{Hom}_{KG}(KA, KB) = \mathrm{Hom}_{KG}(KB, KA) = \mathrm{Hom}_{KG}(KA, KC) = \mathrm{Hom}_{KG}(KC, KA) = \mathrm{Hom}_{KG}(KB,KC) = \mathrm{Hom}_{KG}(KC,KB) = 0$. Como F e F' são diferentes de zero, o lema anterior nos permite afirmar que os RG-módulos $(A, B; F)$ e $(A, C; F')$ são indecomponíveis.

Seja $M = A \oplus (A, B \oplus C; F + F')$. Em notação matricial:

$$M = \begin{bmatrix} A & 0 & 0 & 0 \\ & A & F & F' \\ & & B & 0 \\ & & & C \end{bmatrix}.$$

Como m e n são relativamente primos, podemos escolher um inteiro k tal que $kn \equiv 1$ módulo m.

Fazendo

$$X_1 = \begin{bmatrix} I & knI & 0 & 0 \\ & I & 0 & 0 \\ & & I & 0 \\ & & & I \end{bmatrix}$$

onde os símbolos I representam as matrizes identidades con venientes, obtemos

$$M_1 = X_1 M X_1^{-1} = \begin{bmatrix} I & knI & 0 & 0 \\ & I & 0 & 0 \\ & & I & 0 \\ & & & I \end{bmatrix} \begin{bmatrix} A & 0 & 0 & 0 \\ & A & F & F' \\ & & B & 0 \\ & & & C \end{bmatrix} \begin{bmatrix} I & -knI & 0 & 0 \\ & I & 0 & 0 \\ & & I & 0 \\ & & & I \end{bmatrix}$$

e resulta

$$M_1 = \begin{bmatrix} A & 0 & knF & knF' \\ & A & F & F' \\ & & B & 0 \\ & & & C \end{bmatrix}.$$

Mas n é a ordem de F' em $Ext_{RG}(C, A)$ e, portanto, $knF' = 0$ e podemos escolher T tal que $knF' = AT - TC$. Fazendo agora

$$X_2 = \begin{bmatrix} I & 0 & 0 & T \\ & I & 0 & 0 \\ & & I & 0 \\ & & & I \end{bmatrix}$$

vamos ter

$$M_2 = X_2 M_1 X_2^{-1} = \begin{bmatrix} I & 0 & 0 & T \\ & I & 0 & 0 \\ & & I & 0 \\ & & & I \end{bmatrix} \begin{bmatrix} A & 0 & knF & knF' \\ & A & F & F' \\ & & B & 0 \\ & & & C \end{bmatrix} \begin{bmatrix} I & 0 & 0 & -T \\ & I & 0 & 0 \\ & & I & 0 \\ & & & I \end{bmatrix}$$

e resulta

$$M_2 = \begin{bmatrix} A & 0 & knF & 0 \\ 0 & A & F & F' \\ 0 & 0 & B & 0 \\ 0 & 0 & 0 & C \end{bmatrix}.$$

Como $knF = F$ em $\mathrm{Ext}_{RG}(B, A)$ pois $kn \equiv 1$ módulo m, e m é a ordem de F em $\mathrm{Ext}_{RG}(B, A)$, fazendo

$$X_3 = \begin{bmatrix} I & 0 & 0 & 0 \\ -I & I & 0 & 0 \\ & & I & 0 \\ & & & I \end{bmatrix}$$

obtemos $M_3 = X_3 M_2 X_3^{-1} =$

$$\begin{bmatrix} I & 0 & 0 & 0 \\ -I & I & 0 & 0 \\ & & I & 0 \\ & & & I \end{bmatrix}\begin{bmatrix} A & 0 & F & 0 \\ & A & F & F' \\ & & B & 0 \\ & & & C \end{bmatrix}\begin{bmatrix} I & 0 & 0 & 0 \\ I & I & 0 & 0 \\ & & I & 0 \\ & & & I \end{bmatrix} = \begin{bmatrix} A & 0 & F & 0 \\ & A & 0 & F' \\ & & B & 0 \\ & & & C \end{bmatrix}.$$

Finalmente, tomando

$$X_4 = \begin{bmatrix} I & 0 & 0 & 0 \\ & & I & 0 \\ & I & 0 & 0 \\ & & & I \end{bmatrix}$$

obtemos

$$M_4 = X_4 M_3 X_4^{-1} = \begin{bmatrix} I & 0 & 0 & 0 \\ & & I & 0 \\ & I & 0 & 0 \\ & & & I \end{bmatrix}\begin{bmatrix} A & 0 & F & 0 \\ & A & 0 & F' \\ & & B & 0 \\ & & & C \end{bmatrix}\begin{bmatrix} I & 0 & 0 & 0 \\ & & I & 0 \\ & I & 0 & 0 \\ & & & I \end{bmatrix}$$

resultando

$$M_4 = \begin{bmatrix} A & F & 0 & 0 \\ & B & 0 & 0 \\ & & A & F' \\ & & & C \end{bmatrix}$$

a qual é a representação matricial correspondente a

$(A, B; F) \oplus (A, C; F')$.

Como $M_4 = (X_4X_3X_2X_1)M(X_4X_3X_2X_1)^{-1}$ resulta que $(A, B; F) \oplus (A, C; F') \cong A \oplus (A, B \oplus C; F + F')$. □

Agora vamos demonstrar que, para certos grupos, existem módulos que satisfazem as hipóteses do teorema acima.

Com isso, ficará comprovada a não validade da unicidade da decomposição em indecomponíveis, pois A não pode ser isomorfo a um módulo da forma $(A, B; F)$ com $B \neq 0$.

LEMA 2.4. Seja p um divisor primo da ordem do grupo G. Vamos chamar por A ao conjunto R considerado como RG-módulo no qual G atua trivialmente, isto é, $gr = r$ para g em G e r em R. Então, existe um RG-módulo B tal que KB é irredutível não isomorfo a KA e $\mathrm{Ext}_{RG}(B, A)$ contém um elemento de ordem p.

Demonstração: Seja $h = \sum_{g\in G} g$. Rh é um RG-submódulo de RG que, como RG-módulo é isomorfo a A. Assim, podemos incluir A em RG como submódulo.

Seja P um ideal primo de R que contenha pR e R_P o anel de valorização P-ádica de K, isto é,

$$R_P = \{\tfrac{\alpha}{\beta} \mid \alpha, \beta \in R \ \text{ e } \ \beta \notin P\}.$$

Fazendo $M = \dfrac{R_PG}{R_PA}$, obtemos uma sequência exata de RG-módulos

$$0 \longrightarrow R_PA \longrightarrow R_PG \longrightarrow M \longrightarrow 0.$$

Se $\mathrm{Ext}_{RG}(M, R_PA) = 0$ esta sequência cinde.

Resultaria que $R_pG \cong R_pA \oplus M$, do que seguiria $PR_pG \cong PR_pA \oplus PM$ e daí que $\frac{R_pG}{PR_pG} \cong \frac{R_pA}{PR_pA} \oplus \frac{M}{PM}$.

Fazendo $\bar{M} = \frac{M}{PM}$ e $\bar{R} = \frac{R}{P}$, teremos:

$$\frac{R_pA}{PR_pA} \cong \frac{A}{PA} = \frac{R}{P} = \bar{R}$$

como $\bar{R}G$-módulos onde a ação de G sobre $\bar{R}$ é definida da maneira trivial e

$$\frac{R_pG}{PR_pG} \cong \frac{R_p}{PR_p}G \cong \bar{R}G$$

e daí vem que $\bar{R}G \cong \bar{R} \oplus \bar{M}$ como $\bar{R}G$-módulos.

Se H é um p-subgrupo de Sylow de G, restringindo a ação de G aos escalares de H, transformamos os $\bar{R}G$-módulos em $\bar{R}H$-módulos, e persiste a decomposição $\bar{R}G \cong \bar{R} \oplus \bar{M}$, agora como $\bar{R}H$-módulos. Como $\bar{R}H$-módulo, porém, temos que $\bar{R}G \cong \bar{R}H \oplus \ldots \oplus \bar{R}H$, onde o número de vezes que aparece $\bar{R}H$ é igual ao índice de H em G, pois se $G = Hg_1 \cup \ldots \cup Hg_r$ onde os g_i são representantes das classes de G módulo H o conjunto $\{g_1, g_2, \ldots, g_r\}$ forma uma base de $\bar{R}G$ sobre $\bar{R}H$.

Como H é um p-grupo, $\frac{\bar{R}H}{\text{rad } \bar{R}H} \cong \bar{R}$ (3, 27.28), o que, como $\bar{R}H$ é artiniano, implica que $\bar{R}H$ não tem idempotentes não triviais. Logo, $\bar{R}H$ é um $\bar{R}H$-módulo indecomponível. Como $\bar{R}H \oplus \ldots \oplus \bar{R}H \cong \bar{R}G \cong \bar{R} \oplus M$ e $\bar{R}H$ satisfaz a propriedade de Krull-Schmidt teríamos que $\bar{R}H \cong \bar{R}$ como $\bar{R}H$-módulos e, consequentemente, como R-módulos, o que constitui um absurdo. Assim sendo, concluímos que

$$\mathrm{Ext}_{RG}(M,\ R_pA) \neq 0.$$

Seja $\{m_i\}$ uma base de M sobre R_pG e M_0 o R_pG-módulo gerado pelos elementos das formas m_i e gm_i com g em G. Temos que $M = R_pM_0$. Assim:

$$R_p\ \mathrm{Ext}_{RG}(M_0,\ A) = \mathrm{Ext}_{RG}(R_pM_0,\ R_pA) = \mathrm{Ext}_{RG}(M,\ R_pA) \neq 0.$$

Como $pR \subseteq P$, a componente p-primária de

$$\mathrm{Ext}_{RG}(M_0,\ A)$$

contém a componente P-primária de $\mathrm{Ext}_{RG}(M_0,\ A)$, a qual é $R_p\ \mathrm{Ext}_{RG}(M_0,\ A)$. Portanto, $\mathrm{Ext}_{RG}(M_0,\ A)$ deve conter pelo menos um elemento de ordem p.

Seja $B = \{\alpha \in KG \mid g\alpha = \alpha$ para todo g de $G\}$.

É claro que se $\alpha = \alpha_1 g_1 + \alpha_2 g_2 + \ldots + \alpha_n g_n$, onde $G = \{g_1, \ldots, g_n\}$, α está em B se e só se $\alpha_1 = \alpha_2 = \ldots = \alpha_n$. Ou seja, $B = K \sum_{i=1}^{n} g_i = K \sum_{g \in G} g$ e, portanto, o posto de B sobre K é igual a 1. Assim, em uma decomposição de KG em soma direta de submódulos, K pode aparecer no máximo uma vez. Em consequência disso, KA não pode ocorrer como fator de composição de $\frac{KG}{KA} = KM$. Em particular, $KA \neq KM = KM_0$.

Se KM for simples, KM_0 também será simples e, pelo que vimos acima, M_0 obedece às condições desejadas para o RG-módulo B do enunciado do lema.

Se KM for redutível e M_1 for um submódulo não trivial de KM, fazendo $N = M_1 \cap M$, teremos que N é um R_pG-submódulo de M, R_p-puro e cujo posto sobre R_p é menor que o de M. Então, teremos $M \cong N \oplus L$ e a exatidão da sequência

$$0 \longrightarrow N \longrightarrow M \longrightarrow L \longrightarrow 0$$

implicará na exatidão da sequência

$$\mathrm{Ext}_{RG}(L,\ R_pA) \longrightarrow \mathrm{Ext}_{RG}(M,\ R_pA) \longrightarrow \mathrm{Ext}_{RG}(N,\ R_pA).$$

Assim, como $\mathrm{Ext}_{RG}(M, R_pA) \neq 0$, é necessário que $\mathrm{Ext}_{RG}(L, R_pA) \neq 0$ ou $\mathrm{Ext}_{RG}(N, R_pA) \neq 0$. Se o RG-módulo assim obtido, tal que $\mathrm{Ext} \neq 0$, novamente corresponder a um KG-módulo redutível, prosseguimos esse processo, o qual, por ser M finitamente gerado, deve parar após um número finito de vezes.

Teremos, então, um RG-módulo B tal que B é um somando direto de M, KB é irredutível e $\mathrm{Ext}_{RG}(B, R_pA) \neq 0$.

Tomando B_0 tal que $B = R_pB_0$ teremos que B_0 será o RG-módulo desejado, □

TEOREMA 2.5. Seja G um grupo cuja ordem possui pelo menos dois divisores primos distintos e que admita um subgrupo normal de índice primo. Então, existem RG-módulos A, B e C tais que os KG-módulos KA, KB e KC são irredutíveis e não isomorfos dois a dois e existem elementos F em $\mathrm{Ext}_{RG}(B, A)$ e F' em $\mathrm{Ext}_{RG}(C, A)$ cujas ordens são relativamente primas.

Demonstração: Seja G_0 um subgrupo normal de G cujo índice é o primo p e seja $H = \frac{G}{G_0}$. Para g em G, seja $\bar{g}$ a imagem de g por meio do epimorfismo natural de G em H.

Dado um RH-módulo M, podemos torná-lo um RG-módulo, definindo a ação de G sobre M mediante a ação de H, isto é, para g em G e m em M definimos $gm = \bar{g}m$.

Dessa forma, RH-módulos indecomponíveis tornam-se RG-módulos indecomponíveis e KH-módulos irredutíveis tornam-se KG-módulos irredutíveis. Se M e N são RH-módulos, tem-se, também, que $\mathrm{Ext}_{RG}(M, N) = \mathrm{Ext}_{RH}(M, N)$.

Seja A o RG-módulo definido no conjunto R no qual a ação de G é a trivial. Como H também atua trivialmente sobre R, A é também o RH-módulo R no qual H atua trivialmente.

Pelo lema anterior, existe um RH-módulo B tal que KB é irredutível, KB não é isomorfo a KA e $\mathrm{Ext}_{RH}(B, A)$ contém um elemento de ordem p. Quando tomamos A e B RG-módulos, da maneira acima descrita, obtemos que KA e KB são KG-módulos irredutíveis, KB não é isomorfo a KA e $\mathrm{Ext}_{RG}(B, A)$ contém elemento de ordem p.

Seja agora q um divisor primo da ordem de G, diferente de p. Pelo lema anterior, existe um RG-módulo C tal que KC é irredutível, KC não é isomorfo a KA e $\mathrm{Ext}_{RG}(C, A)$ contém elementos de ordem q.

Finalmente, se KC e KB fossem isomorfos, como KG-módulos, poderíamos definir uma estrutura de RH-módulo em C, mediante a ação de H sobre C dada por $gc = \bar{g}c$ para $\bar{g}$ em h e c em C e, então, $\mathrm{Ext}_{RG}(C, A) = \mathrm{Ext}_{RH}(C, A)$ não poderia conter elementos de ordem q, pois o expoente de $\mathrm{Ext}_{RH}(C, A)$ é igual à ordem de H, ou seja, igual a p.

Logo, KB não é isomorfo a KC. □

EXEMPLO 2.6. Seja G um grupo solúvel e seja $|G|=p_1^{\alpha_1}\dots p_r^{\alpha_r}$, onde os p_i são primos distintos, com $\alpha_i>0$ e $r\geq 2$. Seja $G = G_0 \rhd G_1 \rhd \dots \rhd G_n = \{1\}$ uma cadeia de subgrupos de G na qual os fatores $\frac{G_i}{G_i+1}$ sejam comutativos. Em particular, $\frac{G}{G_i}$ é comutativo e, assim sendo, dado um divisor primo p da ordem de $\frac{G}{G_i}$ existe um subgrupo H de G que contém G_1 e tal que a ordem de $\frac{H}{G_1}$ é igual ao quociente da ordem de $\frac{G}{G_1}$ por p. Então, o índice de H em G será dado por:

$$[G:H] = \frac{|G|}{|H|} = \frac{|G|}{|G_1|}\,\frac{|G_1|}{|H|} = p.$$

Além disso, como $\frac{G}{G_1}$ é comutativo, $\frac{H}{G_1} \lhd \frac{G}{G_1}$ e, consequentemente, H é um subgrupo normal de G.

Como caso particular, temos o exemplo mais simples de um grupo que obedece as hipóteses do teorema 2.5., qual seja, o grupo simétrico de grau 3.

CAPÍTULO III

Neste capítulo, demonstraremos o teorema de Krull-Schmidt para álgebras finitamente geradas sobre anéis locais completos.

Dados um anel R, um R-módulo M e um ideal I de R podemos definir uma topologia sobre M tomando como base os conjuntos da forma $x + I^r M$, onde x está em M e r é um inteiro não negativo.

É imediata a verificação de que tais conjuntos realmente constituem uma base para uma topologia e que essa topologia é separada se e só se $\bigcap_{r=0}^{\infty} I^r M = 0$.

A topologia assim definida sobre M denomina-se a topologia I-ádica de M. Quando M é separado em relação à topologia I-ádica, está é metrizável e sua métrica pode ser definida, por exemplo por: $d(m,m) = 0$ e $d(m,m') = 2^{-n}$ quando $m - m' \in I^n M$ e $m - m' \notin I^{n+1} M$.

Quando M não é separado em relação à topologia I-ádica, com a definição acima, obtemos apenas uma pseudo-métrica para M.

Vamos introduzir a seguir a noção de limite projetivo dos módulos $\frac{M}{I^r M}$ a qual nos permitirá obter o completamento de M relativamente à topologia I-ádica.

Para $r \geq s$, sejam $\pi_{rs}: \frac{M}{I^rM} \to \frac{M}{I^sM}$ as aplicações que levam $x + I^rM$ em $x + I^sM$.

O limite projetivo dos $\frac{M}{I^rM}$, que se representa por $\varprojlim \frac{M}{I^rM}$, é definido como sendo o submódulo do produto direto $\prod_{r=0}^{\infty} \frac{M}{I^rM}$ formado pelas famílias $(m_r + I^rM)_r$ tais que: para $r \geq s$, $m_s + I^sM = \pi_{rs}(m_r + I^rM)$.

Sejam π_r as restrições ao $\varprojlim \frac{M}{I^rM}$ das projeções canônicas de $\prod_{r=0}^{\infty} \frac{M}{I^rM}$ sobre os $\frac{M}{I^rM}$.

O limite projetivo possui a seguinte propriedade u-niversal: dado um R-módulo N e funções $\lambda_r \in \mathrm{Hom}_R(N, \frac{M}{I^rM})$ tais que os seguintes diagramas comutem para $r \geq s$

$$\begin{tikzcd} N \arrow[rr, "\lambda_s"] \arrow[dr, "\lambda_r"'] & & \frac{M}{I^sM} \\ & \frac{M}{I^rM} \arrow[ur, leftarrow, "\pi_{rs}"'] & \end{tikzcd}$$

existe um único $\lambda \in \mathrm{Hom}_R(N, \varprojlim \frac{M}{I^rM})$ tal que os seguintes diagramas comutam para todo s.

$$\begin{tikzcd} N \arrow[rr, "\lambda"] \arrow[dr, "\lambda_s"'] & & \varprojlim \frac{M}{I^rM} \\ & \frac{M}{I^sM} \arrow[ur, leftarrow, "\pi_s"'] & \end{tikzcd}$$

Anota-se $\lambda = \varprojlim \lambda_s$.

Quando tomamos $N = M$ e $\lambda_s: \frac{M}{I^s M}$ tais que $\lambda_s(m) = m + I^s M$, vamos ter $\lambda = \varprojlim \lambda_s$ dado por: $\lambda(m) = (m+I^s M)_s$.

Sejam $\hat{R} = \varprojlim \frac{R}{I^r R}$ e $\hat{M} = \varprojlim \frac{M}{I^r M}$.

Utilizando a propriedade universal do limite projetivo, verifica-se facilmente que $\hat{R}$ é um anel e $\hat{M}$ um $\hat{R}$-módulo, com as operações que se introduzem naturalmente.

Por exemplo, se $\hat{a}$ e $\hat{b}$ são elementos de $\hat{R}$ com $\hat{a} = (a_r + I^r)_r$ e $\hat{b} = (b_r + I^r)_r$, define-se

$$\hat{a}\,\hat{b} = (a_r b_r + I^r)_r.$$

Demonstra-se que $\hat{M}$ é o completamento topológico de M, relativamente à topologia I-ádica, e denomina-se $\hat{M}$ o completamento I-ádico de M. Quando M é completo, a aplicação $\lambda: M \to \hat{M}$ dada por $\lambda(m) = (m + I^r M)_r$ é um isomorfismo.

Se R é um anel local cujo único ideal maximal é P, consideraremos sempre em R a topologia P-ádica.

Lema 3.1. Seja R um anel e P um ideal bilateral nilpotente de R. Se $\bar{e}$ é um elemento idempotente de $\frac{R}{P}$ então existe um elemento idempotente e em R tal que $e + P = \bar{e}$.

Demonstração: Como P é nilpotente, $P^u = 0$ para algum inteiro positivo u. Basta demonstrarmos a proposição para $u = 2$ pois, se o tivermos feito, ela seguirá por indução so bre u do seguinte modo: tem-se $\frac{R}{P} \cong \frac{\frac{R}{P^2}}{\frac{P}{P^2}}$; mas $(\frac{P}{P^2})^2 = 0$ e, portanto, podemos levantar idempotentes de $\frac{R}{P}$ para $\frac{R}{P^2}$ e, como o grau de nilpotência de P^2 (isto é, o menor m tal que $(P^2)^m = 0$) é menor que o de P, por hipótese de indução, podemos levantar idempotentes de $\frac{R}{P^2}$ para R.

Vejamos então o caso em que $P^2 = 0$. Seja x um elemento de R tal que $x + P = \bar{e}$. Sejam $a = x^2 - x$ e $y = (x-a)^2$.

Teremos: $a + P = x^2 - x + P = (x + P)^2 - (x + P) = \bar{e}^2 - \bar{e} = 0$ e, portanto, que a é um elemento de P. Além disso, $y + P = (x - a)^2 + P = (x - a + P)^2 = (x + P)^2 = \bar{e}^2 = \bar{e}$.

Resta verificar que y é idempotente. Para isso, fazemos $y = (x - a)^2 = x^2 - 2ax + a^2 = x^2 - 2ax = x + a - 2ax$. Daí:

$$y^2 = (x + a - 2ax)^2 = x^2 + ax - 2ax^2 + ax - 2ax^2 =$$

$$x^2 + 2ax - 4ax^2 = x + a + 2ax - 4a(x + a) = x + a - 2ax = y.$$

$\square$

<u>Corolário 3.2.</u> Seja R um anel local completo cujo único ideal maximal é P e A uma R-álgebra finitamente gerada sobre R. Se $\bar{e}$ é um idempotente de $\frac{A}{PA}$ existe um idempotente e de A tal que $e + PA = \bar{e}$.

Demonstração: Como R é completo e A é finitamente gerada sobre R é fácil verificar que A também é completo na topologia P-ádica. Assim, a aplicação ϕ de A no $\varprojlim \frac{A}{P^u A}$ dada por $\phi(a) = (a + P^u A)_u$ é um isomorfismo. Seja $\bar{e} = a_1 + PA$ um idempotente de $\frac{A}{PA}$. Como

$$\frac{A}{PA} \cong \frac{\frac{A}{P^2 A}}{\frac{PA}{P^2 A}}$$

e $\frac{PA}{P^2 A}$ é um ideal nilpotente de $\frac{A}{P^2 A}$ podemos levantar $\bar{e}$ a um idempotente de $\frac{A}{P^2 A}$, digamos, $\bar{e}_2 = a_2 + P^2 A$. Suponhamos que $\bar{e}_u$ seja um idempotente de $\frac{A}{P^u A}$. Tal como acima podemos levantar $\bar{e}_u$ a um idempotente $\bar{e}_{u+1} = a_{u+1} + P^{u+1} A$ de $\frac{A}{P^{u+1} A}$. Mais precisamente $\bar{e}_{u+1}$ levanta a imagem de $\bar{e}_u$ pela função que realiza o isomorfismo entre $\frac{A}{P^u A}$ e

$$\frac{A}{P^{u+1} A} \bigg/ \frac{P^u A}{P^{u+1} A}.$$

Isto significa que $a_{u+1} + P^u A = \bar{e}_u = a_u + P^u A$, o que mostra que $\hat{e} = (\bar{e}_u)_u$ pertence ao $\varprojlim \frac{A}{P^u A}$. Mais ainda, como todos os $\bar{e}_u$ são idempotentes segue que $\hat{e}$ é idempotente. Seja e' o elemento de A tal que $\hat{e} = \phi(e)$. Temos que e' é idempotente, pois ϕ é um isomorfismo.

Além disso, como $\phi(e') = (e' + P^u A)_u$ e

$\phi(e') = \hat{e} = (\bar{e}_u)_u = (a_u + P^u A)_u$ vem que, para $u = 1$,

$$e' + PA = a_1 + PA = \bar{e}.$$

□

<u>Lema 3.3.</u> Se R é um anel noetheriano, A uma R-álgebra finitamente gerada sobre R e M um A-módulo finitamente gerado o anel $\Lambda = \mathrm{Hom}_A(M,M)$ é um R-módulo finitamente gerado.

Demonstração: Como M é finitamente gerado existe um A-módulo livre L de posto finito tal que a seqüência

$$0 \to N \to L \to M \to 0$$

é exata.

Aplicando o funtor $\mathrm{Hom}_A(\ ,M)$ obtemos a seqüência exata $0 \to \mathrm{Hom}_A(M,M) \to \mathrm{Hom}_A(L,M) \to \mathrm{Hom}_A(N,M)$ o que mostra ser $\Lambda = \mathrm{Hom}_A(M,M)$ um A-submódulo de $\mathrm{Hom}_A(L,M)$. Como Como $L \cong A^u$ para algum inteiro positivo u tem-se

$$\mathrm{Hom}_A(L,M) \cong \mathrm{Hom}_A(A^u,M) \cong [\mathrm{Hom}_A(A,M)]^u \cong M^u,$$

sendo que este último é noetheriano, pois M é finitamente gerado sobre R. Logo, $\Lambda = \mathrm{Hom}_A(M,M)$ é finitamente gerado sobre R, pois é um R-submódulo de um R-módulo noetheriano.

□

<u>Lema 3.4.</u> Se R é um anel local noetheriano completo e A uma R-álgebra finitamente gerada sobre R, dado um A-módulo M finitamente gerado e indecomponível, o seu anel de A-endomorfismos é local.

<u>Demonstração</u>: Sejam $\Lambda = \mathrm{Hom}_A(M,M)$, $P = \mathrm{rad}\, R$ e $\frac{J}{P\Lambda} = \mathrm{rad}\, \frac{\Lambda}{P\Lambda}$.

Temos que $\frac{\Lambda}{J} = \frac{\Lambda}{P\Lambda} / \frac{J}{P\Lambda}$. Assim:

$$\text{rad } \frac{\Lambda}{J} = \text{rad } (\frac{\Lambda}{P\Lambda} / \frac{J}{P\Lambda}) = \text{rad } (\frac{\Lambda}{P\Lambda} / \text{rad } \frac{\Lambda}{P\Lambda}) = 0.$$

Pelo lema anterior, Λ é finitamente gerado sobre R. Assim sendo $\frac{\Lambda}{P\Lambda}$ é um $\frac{R}{P}$ - espaço vetorial de dimensão finita e, portanto, $\frac{\Lambda}{P\Lambda}$ é artiniano e, consequentemente $\frac{J}{P\Lambda}$ é nilpotente e $\frac{\Lambda}{J}$ é artiniano e, como rad $\frac{\Lambda}{J} = 0$, $\frac{\Lambda}{J}$ resulta um anel semisimples.

Pelo lema 3.1., podemos levantar idempotentes de $\frac{\Lambda}{J}$ para $\frac{\Lambda}{P\Lambda}$ e, como Λ é completo relativamente à topologia P-ádica, de $\frac{\Lambda}{P\Lambda}$ para Λ. Se Λ admitisse um idempotente não trivial e teríamos que e: $M \rightarrow M$ é uma projeção de M e que $M = e(M) \oplus (1 - e)(M)$, decomposição esta na qual ambos os somandos são não triviais, o que contraria a indecomponibilidade de M. Logo, Λ não possui idempotentes não triviais e, consequentemente, $\frac{\Lambda}{J}$ também não possui idempotentes não triviais do que segue que $\frac{\Lambda}{J}$ é um anel com divisão.

Para um elemento x de Λ, sejam $\bar{x} = x + P\Lambda$ e $\bar{\bar{x}} = x + J$. Se provarmos que x é inversível em Λ se e somente se $\bar{\bar{x}}$ for inversível em $\frac{\Lambda}{J}$, como $\frac{\Lambda}{J}$ é um anel com divisão, teremos que J é precisamente o conjunto dos elementos não inversíveis de Λ e, portanto, resultará que Λ é local.

É claro que se x é inversível $\bar{x}$ e $\bar{\bar{x}}$ são inversíveis.

Suponhamos que $\bar{x}$ é inversível. Nesse caso, as aplicações $\bar{d}: \frac{\Lambda}{P\Lambda} \to \frac{\Lambda}{P\Lambda}$ e $\bar{\ell}: \frac{\Lambda}{P\Lambda} \to \frac{\Lambda}{P\Lambda}$ definidas respectivamente por $\bar{d}(\bar{a}) = \bar{a}\,\bar{x}$ e $\bar{\ell}(\bar{a}) = \bar{x}\,\bar{a}$ são epimorfismos. Daí segue que $d: \Lambda \to \Lambda$ e $\ell: \Lambda \to \Lambda$ definidas por $d(a) = ax$ e $\ell(a) = xa$ são epimorfismos módulo $P\Lambda$, isto é,

$$\Lambda = \operatorname{Im} d + P\Lambda = \operatorname{Im} \ell + P\Lambda.$$

Pelo lema de Nakayama, segue que $\operatorname{Im} d = \operatorname{Im} \ell = \Lambda$, ou seja, d e ℓ resultam epimorfismos do que resulta a inversibilidade de x em Λ.

Suponhamos agora que $\bar{\bar{x}}$ é inversível. Então $\bar{\bar{x}}\,\bar{\bar{y}} = \bar{\bar{1}}$ para algum y de Λ. Daí $-\bar{\bar{1}} = \bar{\bar{x}}(-\bar{\bar{y}})$, ou seja, $x(-y)+1 \in J$ donde $x(-y) = -1 + j$ com j em J e $\bar{x}(-\bar{y}) = -\bar{1} + \bar{j}$. Mas $\bar{j} \in \frac{J}{P\Lambda} = \operatorname{rad} \frac{\Lambda}{P\Lambda}$ e, portanto, $\bar{j} = \bar{1} - \bar{u}$ onde $\bar{u}$ é um inversível de $\frac{\Lambda}{P\Lambda}$.

Logo, $\bar{x}\,\bar{y} = \bar{u}$ e, portanto; $\bar{x}$ é inversível.

□

<u>Teorema 3.5.</u> Se R é um anel local noetheriano completo e A uma R-álgebra finitamente gerada sobre R, o teorema de Krull-Schmidt vale para A-módulos finitamente gerados.

Demonstração: Pelo lema 3.4. o anel dos A-endomorfismos de qualquer A-módulo indecomponível é local.

Pelo teorema 1.8. basta então verificarmos que todo A-módulo finitamente gerado é noetheriano como R-módulo para que A satisfaça a propriedade de Krull-Schmidt. Se M é um A-módulo finitamente gerado, M é finitamente gerado sobre R e, portanto, é noetheriano como R-módulo. Como todo A-

submódulo de M é também um R-submódulo segue-se que M também é noetheriano como A-módulo. □

<u>Corolário 3.6.</u> Seja R um anel de valorização discreta e A uma R-álgebra finitamente gerada sobre R. Se R é completo o teorema de Krull-Schmidt vale para A-módulos finitamente gerados.

<u>Corolário 3.7.</u> Se R é um anel de valorização discreta completo e G um grupo finito, o anel de grupo RG satisfaz ao teorema de Krull-Schmidt.

Um anel local R é denominado henseliano se toda vez que um polinômio mônico $f(X)$ em $R[X]$ se decompõe módulo $MR[X]$, onde M é o ideal maximal de R, esta decomposição pode ser levantada para $R[X]$ no seguinte sentido: se $f(X) = g_0(X)\, h_0(X)$ módulo $MR[X]$ com $g_0(X)$ e $h_0(X)$ mônicos e tais que $g_0(X)\, R[X] + h_0(X)\, R[X] + MR[X] = R[X]$ então existem polinômios mônicos $g(X)$ e $h(X)$ em $R[X]$ tais que $g(X) = g_0(X)$ módulo $MR[X]$, $h(X) = h_0(X)$ módulo $MR[X]$ e $f(X) = g(X)\, h(X)$.

Um anel local R é henseliano se e somente se dada qualquer R-álgebra finitamente gerada A e qualquer ideal I de A é sempre possível levantar idempotentes de $\frac{A}{I}$ para A.

A demonstração desta caracterização está em (1, teorema 22).

Como no teorema 3.5. o fato do anel R ser completo somente foi utilizado para permitir o levantamento de idempotentes de $\frac{\Lambda}{P\Lambda}$ para Λ ($\Lambda = \mathrm{Hom}_R(M,M)$), podemos afirmar então que o teorema de Krull-Schmidt vale para A-módulos finitamente gerados sempre que A for uma R-álgebra finitamente gerada sobre um anel henseliano.

Em um artigo publicado em 1973 (6), E.G.Evans Jr. apresentou uma recíproca parcial desse resultado, demonstrando que se R é um anel local e toda R-álgebra local finitamente gerada sobre R satisfaz o teorema de Krull-Schmidt então R é henseliano.

CAPÍTULO IV

Neste capítulo, consideraremos como RG-módulos tão somente aqueles que, como R-módulos, sejam livres de posto finito. No caso em que R é um domínio de ideais principais, isso equivale a considerar apenas os RG-módulos que, sobre R, sejam projetivos finitamente gerados.

Seja p um número primo. Por Z_p anotaremos o anel dos elementos p-inteiros de Q, isto é,

$$Z_p = \{a/b \mid a \text{ e } b \text{ são inteiros e } p \text{ não divide } b\}.$$

Z_p é precisamente o anel de valorização do corpo dos números racionais Q correspondente à valorização p-ádica. Assim, Z_p é um domínio de ideais principais local cujo único ideal maximal é $P = pZ_p = \{a/b \in Z_p \mid p$ divide a e p não divide b$\}$.

Representaremos por $\hat{Q}$ o completamento p-ádico de Q e por $\hat{Z}$ o seu anel de valorização. $\hat{Z}$ é também um domínio de ideais principais local e o seu único ideal maximal é $p\hat{Z}$.

Vamos estudar a validade do teorema de Krull-Schmidt para Z_pG-módulos, quando G é um grupo finito.

Inicialmente, consideraremos o caso em que p não divide a ordem do grupo G.

TEOREMA 4.1. Se p não divide a ordem de G o anel de grupo Z_pG satisfaz ao teorema de Krull-Schmidt.

Demonstração: Suponhamos que $M_1 \oplus \ldots \oplus M_r \cong N_1 \oplus \ldots \oplus N_s$ onde os M_i e os N_j são Z_pG-módulos indecomponíveis.

Se p não divide a ordem de G, o ideal gerado por $|G|$ em Z_p é igual a Z_p, pois nesse caso, $|G|$ é inversível em Z_p.

Pelo teorema o.3., como $|G|Z_p = Z_p$, segue-se que toda sequência exata de Z_pG-módulos cinde, pois

$$\operatorname{Ext}_{Z_pG}(M, N) = Z_p \operatorname{Ext}_{Z_pG}(M, N) = |G|Z_p \operatorname{Ext}_{Z_pG}(M, N) = 0.$$

Isso implica que todo Z_pG-módulo indecomponível é um Z_pG-módulo irredutível e, portanto, Z_p-irredutível.

A série de submódulos

$$\bar{M}_r = M_1 \oplus \ldots \oplus M_r \supset \bar{M}_{r-1} = M_2 \oplus \ldots \oplus M_r \supset \ldots \supset \bar{M}_1 = M_r \supset \bar{M}_0 = 0$$

é, então, uma série de Z_p-composição de $M_1 \oplus \ldots \oplus M_r$ cujos fatores de Z_p-composição são justamente os M_i.

Da mesma forma, os N_j serão fatores de Z_p-composição de $N_1 \oplus \ldots \oplus N_s$.

Mas, como $|G|Z_p = Z_p$, pelo teorema 0.4., os fatores de Z_p-composição de um Z_pG-módulo são unicamente determinados a menos de Z_pG-isomorfismo e ordem de ocorrência.

Assim, teremos $r = s$ e M_i isomorfo a N_i para

$1 \leq i \leq r$ depois de convenientemente reenumerados os N_j. □

Vejamos agora o que acontece quando p divide a ordem do grupo G. Nessas condições, Berman e Gudivok em (2) apresentaram um exemplo de um grupo cíclico H para o qual o anel Z_pH não satisfaz a propriedade de Krull-Schmidt.

Para grupos comutativos, os resultados que apresentaremos a seguir, devidos a Jones, dão uma condição necessária e suficiente para que Z_pG satisfaça ao teorema de Krull-Schmidt.

Um fato importante do qual vamos necessitar é o seguinte:

LEMA 4.2. Se, para todo QG-módulo M, a irredutibilidade de M implica na irredutibilidade de $\hat{Q}M$ como $\hat{Q}G$-módulo, o teorema de Krull-Schmidt vale para Z_pG-módulos.

A demonstração desse fato será feita no próximo capítulo, sob condições mais gerais, no teorema 5.11. □

TEOREMA 4.3. Seja G um grupo comutativo cujo expoente é qp^n, onde $q = 1$ ou p é raiz primitiva módulo q.

Então, o teorema de Krull-Schmidt vale para Z_pG-módulos.

Demonstração: Vamos usar o lema anterior. Seja, então, M um QG-módulo simples. Como QG é semisimples, tem-se

$$QG = \bigoplus_{i=1}^{m} M_{n_i}(D_i)$$

onde os D_i são anéis com divisão e $M_{n_i}(D_i)$ o anel das ma trizes $n_i \times n_i$ com elementos de D_i.

Por ser G comutativo, temos que $n_1 = n_2 = \ldots = n_m = 1$ e que os D_i são comutativos, ou seja, são corpos.

Se T é a representação racional de G correspondente a M temos que $T(G) \subseteq D_i$ para algum i e, portanto, $T(G)$ é um grupo cíclico.

Se fazemos $H = G/\text{Ker } T$ M torna-se um QH-módulo irredutível, definindo-se $hm = gm$ para h em H, m em M e g de G tal que $g + \text{Ker } T = h$.

Tomemos um elemento a em H que seja um gerador de H e suponhamos que a ordem de a seja igual a r.

Podemos definir um homomorfismo ϕ de $Q[X]$ em QH, associando ao polinômio $g(X) = a_0 + a_1X + \ldots + a_sX^s$ o elemento $\phi(g) = a_0 + a_1a + \ldots + a_sa^s$ de QH. Essa função ϕ é um epimorfismo cujo kernel é o ideal gerado pelo polinômio $X^r - 1$. Em $Q[X]$, $X^r - 1$ se decompõe como o produto dos polinômios ciclotômicos cujas ordens dividem r. Temos, então:

$$QH \cong \frac{Q[X]}{(X^r - 1)} \cong \frac{Q[X]}{(f_1)} \oplus \ldots \oplus \frac{Q[X]}{(f_t)},$$

onde os f_i são os polinômios ciclotômicos cujas ordens são divisores de r. Como os f_i são irredutíveis, os quocientes $\frac{Q[X]}{(f_i)}$ são corpos e, portanto, a decomposição acima é precisamente a decomposição de QH em ideais simples.

Em particular, obtemos que $M \cong \frac{Q[X]}{(f_i)}$ para algum i.

O epimorfismo ϕ leva o polinômio X em a e, con sequentemente, no isomorfismo $QH \cong \frac{Q[X]}{(f_1)} \oplus \ldots \oplus \frac{Q[X]}{(f_t)}$ a corresponde a $(X + (f_1), \ldots, X + (f_t))$. Assim sendo, os elementos de H e, por conseguinte, os de G atuam sobre $\frac{Q[X]}{(f_i)}$ mediante a multiplicação por X e pelas potências de X.

Seja $f = f_i$ tal que $M \cong \frac{Q[X]}{(f_i)}$. Então, f é um polinômio ciclotômico cuja ordem divide r e, consequentemente, divide o expoente de G. Então, a ordem de f é igual a m_0 onde m_0 divide $m = qp^n$. Pelo teorema 0.10. o número de fatores irredutíveis distintos de f em $\hat{Q}[X]$ é igual ao número de extensões ao anel $Q(\sqrt[m_0]{1})$ do ideal gerado por p em Z.

Se $q = 1$ o teorema 0.12. nos garante que o ideal pZ tem uma única extensão de pZ a $Q(\sqrt[m]{1})$. Quando $q \neq 1$ o número de extensões de pZ a $Q(\sqrt[m]{1})$ é igual a $\frac{\Phi(q)}{t}$ onde t é o menor inteiro positivo tal que $p^t \equiv 1$ módulo q (Teorema 0.13.). Pela hipótese, se $q \neq 1$, p é raiz primitiva módulo q e, portanto $t = \Phi(q)$. Por conseguinte, pZ tem uma única extensão a $Q(\sqrt[m]{1})$ e, portanto, uma única extensão a $Q(\sqrt[m_0]{1})$.

Então, f é irredutível em $\hat{Q}[X]$ e o quociente $\frac{\hat{Q}[X]}{(f)}$ é um $\hat{Q}G$-módulo irredutível. Como veremos a seguir,

$$\frac{\hat{Q}[X]}{(f)} \cong \hat{Q} \otimes \frac{Q[X]}{(f)} \cong \hat{Q} \otimes M = \hat{Q}M$$

e, portanto, $\hat{Q}M$ é um $\hat{Q}G$-módulo irredutível, o que completa a demonstração do teorema. □

LEMA 4.4. Se $f \in Q[X]$, então $\frac{\hat{Q}[X]}{(f)} \cong \hat{Q} \otimes \frac{Q[X]}{(f)}$.

Demonstração: Seja $B: \hat{Q} \times \frac{Q[X]}{(f)} \longrightarrow \frac{\hat{Q}[X]}{(f)}$ a função que leva o par $(q, g + (f))$ em $qg + (f)$, para q em $\hat{Q}$ e $g \in Q[X]$. B é balanceada e, portanto, existe um único $\hat{Q}$-homomorfismo F de $\hat{Q} \otimes \frac{Q[X]}{(f)}$ em $\frac{\hat{Q}[X]}{(f)}$ tal que

$$F(q \otimes g + (f)) = qg + (f).$$

Dado $g = q_0 + q_1 X + \ldots + q_n X^n$ com $q_i \in \hat{Q}$ tem-se:

$$g + (f) = \sum_{i=0}^{n} q_i X^i + (f) = \sum_{i=0}^{n} q_i (X^i + (f)) =$$

$$= \sum_{i=0}^{n} F(q_i \otimes X^i + (f)) = F(\sum_{i=0}^{n} q_i \otimes X^i + (f))$$

o que mostra ser f um epimorfismo.

Seja agora $\sum_{i=1}^{n} q_i \otimes g_i + (f)$ um elemento de $\hat{Q} \otimes \frac{Q[X]}{(f)}$.

Para cada i, $g_i + (f) = \sum_{j=0}^{m_i} q_{ij} X^j + (f)$ com m_i menor que o grau de f ou então g_i está no ideal gerado por f, caso em que $g_i + (f) = 0$.

Assim

$$\sum_i q_i \otimes g_i + (f) = \sum_i q_i \otimes \sum_j q_{ij} X^j + (f) =$$

$$= \sum_{i,j} q_i q_{ij} \otimes X^j + (f) = \sum_j p_j \otimes X^j + (f)$$

com os p_j em $\hat{Q}$.

Segue daí que

$$F(\sum_i q_i \otimes g_i + (f)) = F(\sum_j p_j \otimes X^j + (f)) =$$

$$= \sum_j F(p_j \otimes X^j + (f)) = \sum_j p_j X^j + (f).$$

Assim sendo, se $F(\sum_i q_i \otimes g_i + (f)) = 0$ então $\sum_j p_j X^j + (f) = 0$ donde $\sum_j p_j X^j$ está no ideal gerado por f, fato este que, como $j \leq m_i <$ grau de f para todo j, implica $p_j = 0$ para todo j e, portanto,

$$\sum_i q_i \otimes g_i + (f) = \sum_j p_j \otimes X^j + (f) = 0.$$

Logo, F é um monomorfismo e, portanto, um isomorfismo. □

Trataremos agora de demonstrar a recíproca do teorema 4.3., ou seja, que, se $q \neq 1$ e p não é uma raiz primitiva módulo q, o anel Z_pG não satisfaz a propriedade de Krull-Schmidt.

Seja, então, G um grupo comutativo finito cujo expoente obedece às condições acima. Pelo teorema fundamental dos grupos comutativos finitos podemos escrever:

$$G = H_n \oplus H_1 \oplus \ldots \oplus H_r \oplus H_{11} \oplus \ldots \oplus H_{1r_1} \oplus \ldots \oplus H_{s_1} \oplus \ldots \oplus H_{sr_s}$$

onde os H_i e H_{ij} são subgrupos cíclicos de H cujas ordens são: $|H_n| = p^n$, $|H_i| = p^{\alpha_i}$, $|H_{ij}| = p_i^{\alpha_{ij}}$ sendo p, $p_1, \ldots, p_s$ os divisores primos da ordem de G, $n \geq \alpha_1 \geq \ldots \geq \alpha_r > 0$ e $\alpha_{i1} \geq \alpha_{i2} \geq \ldots \geq \alpha_{ir_i}$ para todo i. Segue que $q = p_1^{\alpha_{11}} \ldots p_j^{\alpha_{s1}}$.

Seja H_0 uma imagem homomórfica de H_n com ordem p. Temos que $H = H_0 \oplus H_{11} \oplus H_{21} \oplus \ldots \oplus H_{s1}$ é uma imagem homomórfica, cíclica e de ordem pq do grupo G.

Seja $\phi: G \to H$ um epimorfismo. Se M é um Z_pH-módulo podemos torná-lo um Z_pG-módulo definindo a ação de G sobre M por meio da ação de H, isto é, fazendo $gm = \phi(g)m$ para g em G e m em M.

Como G atua sobre M mediante H, resultam, de imediato, as seguintes propriedades:

(i) Dois Z_pH-módulos M e N são isomorfos como Z_pH-módulos se e só se são isomorfos como Z_pG-módulos.

(ii) Um Z_pH-módulo M é decomponível como Z_pH-módulo se e só se M é decomponível como Z_pG-módulo.

Em consequência disso, se tivermos $M_1 \oplus \ldots \oplus M_r \cong N_1 \oplus \ldots \oplus N_s$ com M_i e N_j Z_pH-módulos indecomponíveis, teremos que $M_1 \oplus \ldots \oplus M_r \cong N_1 \oplus \ldots \oplus N_s$ como Z_pG-módulos e com os M_i e N_j Z_pG-módulos indecomponíveis.

Assim, se o teorema de Krull-Schmidt valer para Z_pG-módulos, também deverá valer para Z_pH-módulos.

Como vemos, para verificar que o teorema de Krull-Schmidt falha para Z_pG-módulos, podemos supor que G seja cíclico e de ordem igual a pq.

Para reduzir ainda mais o problema, demonstraremos o seguinte resultado:

<u>TEOREMA 4.5.</u> Seja G um grupo tal que $G = G_1 \oplus G_2$ onde G_1 e G_2 são cíclicos de ordem q e p, respectivamente. Se

ψ é uma raiz da unidade tal que $\psi^q = 1$, existe uma correspondência biunívoca entre as classes de isomorfismo dos Z_pG-módulos indecomponíveis e as classes de isomorfismo dos $Z_p[\psi]G_2$-módulos indecomponíveis.

Demonstração: Seja g_1 um gerador de G_1. Podemos dar a $Z_p[\psi]$ uma estrutura de Z_pG_1-módulo por meio da operação $g_1^i\, X = \psi^i X$ para X em $Z_p[\psi]$ e $0 \leq i \leq q-1$.

Se N é um $Z_p[\psi]G_2$-módulo indecomponível definimos em N uma estrutura de Z_pG-módulo da seguinte maneira: $g_1^i g_2 n = \psi^i g_2 n$ para g_2 em G_2, n em N, $0 \leq i \leq q-1$.

Se N_0 é um subgrupo de N vem, de imediato, que N_0 é fechado em relação à multiplicação por escalares de $Z_p[\psi]G_2$ se e somente se é fechado em relação à multiplicação por escalares de Z_pG, ou seja, N_0 é um $Z_p[\psi]G_2$-submódulo de N se e só se for um Z_pG-submódulo de N.

Segue daí que se N for indecomponível como $Z_p[\psi]G_2$-módulo também o será como Z_pG-módulo.

Da mesma forma, se N' e N'' são $Z_p[\psi]G_2$-módulos indecomponíveis e σ uma função de N' em N'' resulta que σ é um $Z_p[\psi]G_2$-homomorfismo se e só se σ for um Z_pG-homomorfismo e daí vem que N' e N'' são isomorfos como Z_pG-módulos.

Seja agora M um Z_pG-módulo indecomponível. Podemos encarar M como um Z_pG_1-módulo, simplesmente restringindo a operação externa de M aos escalares de Z_pG_1.

Como p não divide a ordem de G_1, M é a soma direta de Z_pG_1-submódulos irredutíveis, digamos $M=L_1 \oplus\ldots\oplus L_r$. Suponhamos que $L_1, L_2,\ldots, L_s$ sejam os componentes não isomorfos de M e seja, para cada i, M_i a soma de todos os Z_pG_1-submódulos de M isomorfos a L_i. Vamos mostrar, por indução sobre s, que a decomposição $M = M_1 + M_2 + \ldots + M_s$ é uma soma direta. Se $M_1 \cap (M_2 + \ldots + M_s) \neq 0$, seja L um submódulo irredutível dessa interseção. L é um Z_pG_1-submódulo simples de M_1 e de $M_2 \oplus\ldots\oplus M_s$, a qual é uma soma direta por hipótese de indução. Consequentemente, L deve ser isomorfo a um componente irredutível de M_1 e a um componente irredutível de um dos M_i com $i > 1$. Segue daí que $L_1 \cong L \cong L_i$ com $i \geq 2$ o que é um absurdo. Logo,

$$M = M_1 \oplus M_2 \oplus \ldots \oplus M_s.$$

Seja $g_2 \in G_2$. Como G é comutativo, constata-se que g_2L_i é um Z_pG_1-submódulo de M e isomorfo a L_i pela aplicação que leva um elemento ℓ_i de L_i em $g_2\ell_i$ a qual é um Z_pG_1-isomorfismo. Assim sendo, M_i é fechado relativamente à multiplicação por elementos de G_2 e, portanto, é um Z_pG-submódulo de M para todo i.

Como M é Z_pG-indecomponível resulta que $s = 1$ e, consequentemente, todos os submódulos L_i são Z_pG_1-isomorfos a L_1. Mas L_1 é um Z_pG_1-submódulo simples e, portanto, isomorfo a $Z_p[\psi]$ onde ψ é uma raiz da unidade cuja ordem divide q. Assim, obtemos:

$$M = L_1 \oplus L_2 \oplus \ldots \oplus L_r \cong L_1 \oplus L_1 \oplus \ldots \oplus L_1 \cong$$

$$\cong Z_p[\psi] \oplus \ldots \oplus Z_p[\psi] \cong (Z_p[\psi] \oplus \ldots \oplus Z_p[\psi]) \otimes_{Z_p} Z_p \cong$$

$$\cong (Z_p[\psi] \otimes_{Z_p} Z_p) \oplus \ldots \oplus (Z_p[\psi] \otimes_{Z_p} Z_p) \cong Z_p[\psi] \otimes_{Z_p} M'$$

onde M' é o Z_p-módulo $Z_p \oplus; \ldots \oplus Z_p$ (r vezes).

$Z_p[\psi] \otimes_{Z_p} M'$ é um Z_pG_1-módulo no qual os elementos de G_1 atuam através da multiplicação por potências de ψ.

Aproveitando o Z_pG_1-isomorfismo existente entre M e $Z_p[\psi] \otimes_{Z_p} M'$ podemos fazer os elementos de G_2 atuarem sobre $Z_p[\psi] \otimes_{Z_p} M'$ transformando-o assim em um $Z_p[\psi]G_2$-módulo.

Se N é um $Z_p[\psi]G_2$-submódulo de $Z_p[\psi] \otimes_{Z_p} M'$, N é estável sob a ação de $Z_p[\psi]$ e de G_2 e, portanto, N corresponde a um Z_pG-submódulo de M. Assim, a indecomponibilidade de M como Z_pG-módulo implica na indecomponibilidade de $Z_p[\psi] \otimes_{Z_p} M'$ como $Z_p[\psi]G_2$-módulo.

Aplicando agora a $Z_p[\psi] \otimes_{Z_p} M'$ o processo anteriormente descrito de transformação de $Z_p[\psi]G_2$-módulos indecomponíveis em Z_pG-módulos indecomponíveis, voltaremos a obter M, o que demonstra o teorema. □

Uma consequência deste teorema é que se Z_pG satisfaz a propriedade de Krull-Schmidt, $Z_p[\psi]G_2$ também satisfaz, pois se $M_1 \oplus \ldots \oplus M_r \cong N_1 \oplus \ldots \oplus N_s$ onde os M_i e N_j são $Z_p[\psi]G_2$-módulos indecomponíveis, podemos tomar os seus Z_pG-módulos correspondentes aos quais chamamos por X_i e Y_j. Se $X = X_1 \oplus \ldots \oplus X_r$ e $Y = Y_1 \oplus \ldots \oplus Y_s$, através do mesmo processo utilizado no teorema, podemos tomar X e Y $Z_p[\psi]G_2$-módulos obtendo $X \cong M \oplus \ldots \oplus M_r$ e $Y \cong N \oplus \ldots \oplus N_s$

como $Z_p[\psi]G_2$-módulos. Segue daí que $X_1 \oplus \ldots \oplus X_r \cong Y_1 \oplus \ldots \oplus Y_s$ como Z_pG-módulos e, portanto, $r = s$ e $X_i \cong Y_i$ para $1 \leq i \leq r$ do que resulta $M_i \cong N_i$ para $i \leq i \leq r$.

Assim sendo, precisamos mostrar apenas que o teorema de Krull-Schmidt não vale para $Z_p[\psi]G_2$-módulos, onde G_2 é um grupo de ordem p e ψ uma raiz da unidade tal que $\psi^q = 1$.

Sejam $S = Z_p[\psi]$, θ uma raiz da unidade de ordem p, $R = S[\theta]$ e g um gerador de G_2. S pode ser considerado um SG_2-módulo definindo-se $gs = s$ para s em S.

Também R torna-se um SG_2-módulo definindo-se $gr = \theta r$ para r de R.

Um novo tipo de SG_2-módulo pode ser construído da forma seguinte. Seja γ um elemento de R, tal que γ divide $\theta - 1$ e $R\gamma \neq R(\theta - 1)$. Consideremos o S-módulo $Sy \oplus R$ obtido pela soma direta do S-módulo livre Sy de posto 1 e do S-módulo R.

Fazendo G_2 atuar sobre $Sy \oplus R$ por meio das definições $gy = y + \gamma$ e $gr = \theta r$ para r em R, obtemos um SG_2-módulo, o qual será denotado por (γ, R).

<u>TEOREMA 4.6.</u> Todo SG_2-módulo M é isomorfo à uma soma direta do tipo

$$(\gamma_1, R) \oplus \ldots \oplus (\gamma_r, R) \oplus S \oplus \ldots \oplus S \oplus R \oplus \ldots \oplus R,$$

onde γ_i divide γ_{i+1} para $1 \leq i < r$, γ_r divide $\theta - 1$ e $R\gamma_r \neq R(\theta - 1)$. O número de vezes que S aparece e o número de vezes que R aparece nessa decomposição de M são determinados unicamente por M bem como o são os γ_i a menos de inversíveis de R (10).

Não demonstraremos este teorema. Apenas esboçaremos a maneira como surgem os γ_i. Seja $\sigma = 1 + g + \dots g^{p-1}$ e seja $M_\sigma = \{m \in M \mid \sigma m = 0\}$. Definindo $\theta m = gm$ para m em M_σ, M_σ torna-se um R-módulo finitamente gerado sem torção do qual $(g-1)M$ é um submódulo.

Pelo teorema dos fatores invariantes para módulos finitamente gerados sobre domínios principais existem elementos $b_1, \dots, b_n$ em M_σ e $\gamma_1, \dots, \gamma_n$ em R tais que γ_i divide γ_{i+1} para $1 \leq i < r$ e $M_\sigma = Rb_1 \oplus \dots \oplus Rb_n$ e $(g-1)M = R\gamma_1 b_1 \oplus \dots \oplus R\gamma_n b_n$. Como $(\theta - 1)M_\sigma \subseteq (g-1)M$ resulta que γ_n divide $\theta - 1$.

Escolhe-se r de forma que $R\gamma_r \neq R(\theta - 1)$ e $R\gamma_{r+1} = R(\theta - 1)$.

É claro que S e R são SG_2-módulos indecomponíveis. Vamos usar o teorema 4.5. para mostrar que os SG_2-módulos da forma (γ, R) também são indecomponíveis. Se (γ, R) é igual a $M_1 \oplus M_2$, decompondo M_1 e M_2 pelo teorema obteremos:

$$(\gamma,R) = (\alpha_1,R)\oplus\dots\oplus(\alpha_r,R)\oplus(\beta_1,R)\oplus\dots\oplus(\beta_s,R)\oplus S\dots\oplus S\oplus R\oplus\dots\oplus R$$

onde os (α_i, R) aparecem na decomposição de M_1 e os (β_i,R) na decomposição de M_2. Como o posto de S sobre S é 1 e o posto de R sobre S é $p-1$, o posto sobre S de um SG_2-

módulo da forma (ε, R) é igual a p. Assim, para a decomposição acima de (γ, R) considerando os postos sobre S temos três possibilidades: $(\gamma,R) \cong (\alpha_1,R)$ ou $(\gamma,R) \cong (\beta_1,R)$ y $(\gamma,R) \cong S \oplus R$. No primeiro caso, $M_2 = 0$; no segundo caso, $M_1 = 0$. O terceiro caso não pode ocorrer, pois se A é o SG_2-submódulo de (γ, R) definido por $A = \{m \in (\gamma,R) \mid gm=m\}$ e B é o SG_2-submódulo de $S \oplus R$ dado por

$$B = \{m \in S \oplus R \mid gm = m\}$$

verifica-se que B é igual a S e que

$$A = \left\{-r\left(\frac{\theta - 1}{\gamma}\right)y + r \mid r \in R\right\}$$

e, portanto, o posto de B sobre S é 1 e o posto de A sobre S é maior ou igual ao posto de R sobre S o qual é $p > 1$.

Logo, (γ, R) é indecomponível.

Em $Z_p[\theta]$, p decompõe-se como $p = (1 - \theta)^{\Phi(p)} = (1 - \theta)^{p-1}$, sendo $\theta - 1$ um elemento primo no anel dos inteiros de $Z_p[\theta]$. Por outro lado, em $R = Z_p[\theta, \psi]$, p decompõe-se em $p = (\delta_1 \ldots \delta_h)^{p-1}$ onde os δ_i são primos de R e $h = \frac{\Phi(q)}{d}$, onde d é a ordem de p no grupo dos inversíveis do anel dos inteiros módulo q. Assim, resulta $1 - \theta = \delta_1 \ldots \delta_h$.

Se p não é raiz primitiva módulo q, h é maior do que 1. Façamos, então, $\delta = \delta_1$ e $\gamma = \delta_2 \ldots \delta_h$ e consideremos o SG-módulo $M = (\delta, R) \oplus (\gamma, R)$. Seja x um elemento de (δ, R). Então, $x = sy + r$ com s em S, r em R e y tal que $(\delta, R) = Sy \oplus R$. Temos que:

$$(1 + g + \ldots + g^{p-1})(sy + r) = (sy + r) + g(sy + r) + \ldots$$

$$\ldots + g^{p-1}(sy + r) = (sy + r) + (sy + s\delta + \theta r) + \ldots$$

$$\ldots + (sy + s\delta + s\theta\delta + s\theta^2\delta + \ldots + s\theta^{p-2}y + \theta^{p-1}r) =$$

$$= p(sy) + s[(p-1) + (p-2)\theta + \ldots + \theta^{p-2}]\gamma = 0$$

se e somente se $s = 0$.

Assim se $\sigma = 1 + g + \ldots + g^{p-1}$ e $M_\sigma = \{m \in M | \sigma m = 0\}$ temos $M_\sigma = R \oplus R$ e, portanto, que $\{(1, 0), (0, 1)\}$ é uma base de M_σ sobre R.

Seja x, agora, um elemento de $(\delta, R) \oplus (\gamma, R)$. Tem-se que: $x = (s_1y_1 + r_1, s_2y_2 + r_2)$, com $s_i \in S$, $r_i \in R$, y_i convenientes. Daí:

$$(g - 1)x =$$

$$= (s_1y_1 + s_1\delta + \theta r_1 - s_1y_1 - r_1, s_2y_2 + s_2\gamma + \theta r_2 - s_2y_2 - r_2) =$$

$$= (s_1\delta + (\theta - 1)r_1, s_2\gamma + (\theta - 1)r_2) = ((s_1 + \gamma r_1)\delta, (s_2 + \delta r_2)\gamma).$$

Assim, $\{(\delta, 0), (0, \gamma)\}$ é uma base de $(g - 1)M$ sobre R.

Como δ e γ são relativamente primos em R existem elementos x e y em R tais que $-x\delta + y\gamma = 1$. Obtemos, então:

$$(1,0) = \gamma(y,x) + (-x)(\delta,\gamma) \quad \text{e} \quad (0,1) = -\delta(y,x) + y(\delta,\gamma).$$

Portanto, (y, x) e (δ, γ) geram M_σ sobre R e, como são linearmente independentes, constituem uma base para M_σ sobre R. Além disso,

$$(\delta,0) = -x\delta(\delta,\gamma) + \gamma\delta(y,x) \quad \text{e} \quad (0,\gamma) = y\gamma(\delta,\gamma) + (-1)\gamma\delta(y,x)$$

mostram que (δ, γ) e $\gamma\delta(y, x)$, que são linearmente independentes, formam uma base de $(g - 1)M$ sobre R, a qual provém da base $\{(\delta, \gamma), (y, x)\}$ de M_σ multiplicando (δ,γ) por $1 = \gamma_1$ e (y, x) por $\gamma_2 = \gamma\delta = (1 - \theta)$. Levando em conta, ainda, que o posto de M sobre S é igual a $2p$, chegamos à seguinte decomposição de M dada pelo teorema 4.5.:

$$(S, R) \oplus (\gamma, R) = M \cong (1, R) \oplus S \oplus R.$$

Como todos esses SG_2-módulos são indecomponíveis, resulta, finalmente, que $Z_p[\psi]G_2 = SG_2$ não satisfaz a propriedade de Krull-Schmidt.

Como já vimos, isso implica que o teorema de Krull-Schmidt não vale para Z_pG-módulos sempre que G for um grupo comutativo finito cujo expoente é da forma qp^n com $q\neq 1$ e p não sendo uma raiz primitiva módulo q.

Juntando os resultados apresentados, podemos enunciar o seguinte:

TEOREMA 4.7. Se p é um divisor primo da ordem de um grupo comutativo G, então, o teorema de Krull-Schmidt vale para Z_pG-módulos se e somente se G tem expoente qp^n onde $q = 1$ ou p é uma raiz primitiva módulo q.

Ainda no caso em que p divide a ordem do grupo G, mas sem a hipótese de que o grupo seja comutativo, temos o resultado abaixo, devido a Jacobinski:

TEOREMA 4.8. Seja R um anel de valorização discreta de característica zero, K seu corpo de quocientes e G um p-grupo sendo p um primo ímpar e não inversível em R. Então, o teorema de Krull-Schmidt vale para RG-módulos.

<u>Demonstração</u>: Seja $KG \cong \bigoplus_{i=1}^{m} M_{n_i}(D_i)$ a decomposição de KG em componentes simples. Consideremos uma extensão F de K a qual seja um corpo de decomposição para G. Seja ψ_j uma representação absolutamente irredutível de G sobre K tal que, se M_j é o KG-módulo associado a ψ_j, tenhamos

$$M_{n_j}(D_j)(F \otimes_K M_j)$$

diferente de zero. Se $\bar{\psi}_j$ é a representação associada a $F \otimes_K M_j$, como G é um p-grupo e p é ímpar, aplicando o teorema 0.16., obtemos que o índice de Schur de $\bar{\psi}_j$ sobre K é igual a 1. Pelo lema 0.15., isso significa que D_j é isomorfo ao centro de $M_{n_j}(D_j)$ e, portanto, que D_j é comutativo. Assim, podemos escrever $KG \cong \bigoplus_{i=1}^{m} M_{n_i}(K_i)$, onde os K_i são corpos. Como G é um p-grupo temos $K_i \cong K(w_i)$ onde w_i é uma raiz da unidade cuja ordem é uma potência de p. Se P é o ideal maximal de R, como p pertence a P, pelo teorema 0.12., vem que P se ramifica completamente em K_i.

Assim sendo, o teorema 0.14. nos diz que

$$\hat{K}_i = \hat{K} \otimes K_i \cong \hat{K}_{iQ},$$

onde $\hat{K}_{iQ}$ é o completamento Q-ádico de K_i sendo Q a única extensão de P a K_i. Dessa forma, $\hat{K}G \cong \bigoplus_{i=1}^{m} M_{n_i}(\hat{K}_i)$ é a decomposição de $\hat{K}G$ em componentes simples.

Seja M um KG-módulo simples. Então, M é isomorfo ao KG-módulo constituído pelos vetores coluna $n_i \times 1$

sobre algum dos K_i. Então, $\hat{M}$ será constituído pelos vetores coluna $n_i \times 1$ sobre $\hat{K}_i$ e, portanto, será um $\hat{K}G$-módulo simples.

Como veremos no próximo capítulo, o teorema 5.11. nos permite concluir que o teorema de Krull-Schmidt vale para RG-módulos. □

Se G é um grupo finito qualquer, o mesmo argumento do teorema 4.8. pode ser usado para o caso em que K é um corpo de decomposição de G, ou seja, vale para o seguinte:

TEOREMA 4.9. Se G é um grupo finito e K é um corpo de decomposição para G o teorema de Krull-Schmidt vale para RG-módulos.

Demonstração: Basta observar que, como K é corpo de decomposição de G, tem-se $KG \cong \bigoplus_{i=1}^{m} M_{n_i}(K)$ e, portanto, $\hat{K}G \cong \bigoplus_{i=1}^{m} M_{n_i}(\hat{K})$ é a decomposição de $\hat{K}G$ em componentes simples. Daí, o teorema segue pelo mesmo raciocínio utilizado no teorema anterior. □

CAPÍTULO V

Como já mencionamos, o estudo das representações de um grupo finito G sobre um anel R pode ser efetuado mediante o estudo dos módulos sobre o anel de grupo RG, que, como R-módulos, sejam livres e de posto finito.

Quando R é um domínio e K o seu corpo de quocientes, temos que RG é um subanel de KG.

Essa situação pode ser generalizada pela seguinte definição: Seja R um domínio, K seu corpo de quocientes e A uma K-álgebra de dimensão finita. Um subanel Λ de A é denominado uma R-ordem em A se:

(i) o centro de Λ contém R.

(ii) Λ é um R-submódulo finitamente gerado de A.

(iii) $K\Lambda = A$, ou seja, Λ contém uma base de A sobre K.

Assim, por exemplo, RG é uma R-ordem em KG para todo grupo finito G.

Seja Λ uma R-ordem em uma K-álgebra A.

Um reticulado sobre Λ (ou um Λ-reticulado) é um Λ-módulo finitamente gerado, que, como R-módulo, é livre e sem torção.

Dessa forma, a teoria dos reticulados sobre ordens constitui-se numa generalização da teoria das representações de grupos finitos.

Neste capítulo, estenderemos para reticulados sobre ordens alguns resultados dos capítulos anteriores.

Decorrem imediatamente os seguintes teoremas:

<u>TEOREMA 5.1.</u> Se R é um anel artiniano e Λ uma R-ordem então o teorema de Krull-Schmidt vale para Λ-reticulados.

<u>Demonstração</u>: Se M é um Λ-reticulado, M é um Λ-módulo finitamente gerado, e portanto, artiniano e noetheriano, pois Λ também o é por ser uma R-ordem. Então, pelo corolário 1.9, M satisfaz Krull-Schmidt. □

<u>TEOREMA 5.2.</u> Se R é um anel de valorização discreta completo e Λ uma R-ordem o teorema de Krull-Schmidt vale para Λ-reticulados.

<u>Demonstração</u>: É uma consequência imediata do teorema 3.5. □

Sejam R um anel de valorização discreta, K o seu corpo de quocientes e $P = \pi R$ o seu ideal maximal.

Por $\hat{R}$ e $\hat{K}$ anotaremos os completamentos P-ádicos de R e K. Dado um R-reticulado M, tem-se:

$$\hat{M} = \hat{R} \otimes_R M, \quad \hat{K}M = \hat{K} \otimes_R M \cong \hat{K} \otimes_K (K \otimes_R M) \cong \hat{K} \otimes_R \hat{M} .$$

Se V é um K-módulo que contém M, diz-se que M é pleno em V quando $KM = V$.

Consideremos uma K-álgebra A de dimensão finita e uma R-ordem Λ em A.

<u>LEMA 5.3.</u> Se M é um Λ-reticulado, então $M = KM \cap \hat{M}$, on

de consideramos KM e $\hat{M}$ incluídos em $\hat{K}M \cong \hat{K}\hat{M}$.

Demonstração: Seja $\{x_1, x_2, \ldots, x_m\}$ uma base de M sobre R. Então: $M = \bigoplus_{i=1}^{m} Rx_i$, $KM = \bigoplus_{i=1}^{m} Kx_i$, $\hat{M} = \bigoplus_{i=1}^{m} \hat{R}x_i$. Daí:

$KM \cap \hat{M} = \bigoplus_{i=1}^{m} (K \cap \hat{R})x_i = \bigoplus_{i=1}^{m} Rx_i = M$. □

LEMA 5.4. Seja V um A-módulo finitamente gerado. Então:

(i) Se M é um Λ-reticulado pleno em V, então $\hat{M}$ é um $\hat{\Lambda}$-reticulado pleno em $\hat{V}$.

(ii) Se T é um $\hat{\Lambda}$-reticulado pleno em $\hat{V}$, então $M = V \cap T$ é um Λ-reticulado pleno em V e $\hat{M} = T$.

Demonstração: (i) Se $KM = V$, temos que:

$$\hat{K}\hat{M} = \hat{K} \otimes_{\hat{R}} (\hat{R} \otimes_R M) = \hat{K} \otimes_R M = \hat{K} \otimes_K (K \otimes_R M) = \hat{K} \otimes_K V = \hat{V} .$$

(ii) Sejam $\{x_1, x_2, \ldots, x_n\}$ uma base de T sobre $\hat{R}$ e $\{y_1, \ldots, y_n\}$ uma base de V sobre K (ambos tem o mesmo número de elementos, pois, como $\hat{K}T = \hat{V}$, $\dim_K V = \dim_{\hat{K}} \hat{V} = \dim_{\hat{R}} T$). Então: $T = \sum_{i=1}^{n} \hat{R}x_i$, $\hat{V} = \sum_{i=1}^{n} \hat{K}x_i$, $V = \sum_{i=1}^{n} Ky_i$, $\hat{V} = \sum_{i=1}^{n} \hat{K}y_i$.

Escolhendo em K elementos τ_{ij} suficientemente próximos dos elementos correspondentes de S^{-1}, (onde $S=(\sigma_{jk})$, dada por $y_j = \Sigma\, \sigma_{jk}x_k$), a matriz $(\tau_{ij})(\sigma_{ij})$ será inversível em $M_n(\hat{R})$.

Fazendo $y_i' = \Sigma\, \tau_{ij}y_j = \Sigma\, \tau_{ij}\sigma_{jk}x_k$, teremos:

$V = \sum_{i=1}^{n} Ky_i'$ e $T = \sum_{i=1}^{n} \hat{R}y_i'$, e portanto: $T \cap V = \sum_{i=1}^{n} (K \cap \hat{R}) y_i' =$

$= \sum_{i=1}^{n} Ry_i'$. Assim: $K(T \cap V) = \sum_{i=1}^{n} Ky_i' = V$ e $\hat{R}(T \cap V) = \sum_{i=1}^{n} \hat{R}y_i' =$

$= T$. □

LEMA 5.5. $\hat{R}$ é um R-módulo plano.

Demonstração: $\hat{R}$ é livre de R-torção. Assim, se L é um R-submódulo finitamente gerado de $\hat{R}$, como L também é sem R-torção, L é um R-módulo livre, e, portanto, plano.

Logo, como todo R-submódulo finitamente gerado de $\hat{R}$ é plano, $\hat{R}$ é um R-módulo plano. □

LEMA 5.6. Se M e N são Λ-módulos finitamente gerados, $\hat{R} \otimes_R \mathrm{Hom}_\Lambda (M,N) \cong \mathrm{Hom}_{\hat{\Lambda}} (\hat{M},\hat{N})$ e $\mathrm{Hom}_\Lambda (M,N)$ é denso em $\mathrm{Hom}_{\hat{\Lambda}} (\hat{M},\hat{N})$.

Demonstração: Como M é finitamente gerado, existe um epimorfismo $\phi: \Lambda^r \longrightarrow M$ para algum r. Como Λ é noetheriano, $\mathrm{Ker}\, \phi$ é um Λ-módulo finitamente gerado, e, da mesma forma, existe um epimorfismo $\theta: \Lambda^s \longrightarrow \mathrm{Ker}\, \phi$ para algum s. Obtemos assim, a sequência exata $\Lambda^s \xrightarrow{\theta} \Lambda^r \xrightarrow{\phi} M \longrightarrow 0$, da qual, segue a exatidão de

$$0 \longrightarrow \mathrm{Hom}_\Lambda (M,N) \longrightarrow \mathrm{Hom}_\Lambda (\Lambda^r,N) \longrightarrow \mathrm{Hom}_\Lambda (\Lambda^s,N) .$$

Como $\hat{R}$ é plano, as sequências

$$0 \longrightarrow \hat{R} \otimes \mathrm{Hom}_\Lambda (M,N) \longrightarrow \hat{R} \otimes \mathrm{Hom}_\Lambda (\Lambda^r,N) \longrightarrow \hat{R} \otimes \mathrm{Hom}_\Lambda (\Lambda^s,N)$$

e $\hat{\Lambda}^s \longrightarrow \hat{\Lambda}^r \longrightarrow \hat{M} \longrightarrow 0$ são exatas, e da última segue a exatidão de $0 \longrightarrow \mathrm{Hom}_{\hat{\Lambda}}(\hat{M},\hat{N}) \longrightarrow \mathrm{Hom}_{\hat{\Lambda}}(\hat{\Lambda}^r,\hat{N}) \longrightarrow \mathrm{Hom}_{\hat{\Lambda}}(\hat{\Lambda}^s,\hat{N})$.

Seja $\alpha: \hat{R} \otimes_R \mathrm{Hom}_\Lambda(M,N) \longrightarrow \mathrm{Hom}_{\hat{\Lambda}}(\hat{M},\hat{N})$ definida por $\alpha(\gamma \otimes f) = \gamma_r \otimes f$, onde $\gamma_r: \hat{M} \longrightarrow \hat{N}$ é dada por $\gamma_r(x) = x\gamma$, para $x,\gamma \in \hat{R}$, $f \in \mathrm{Hom}_\Lambda(M,N)$, e sejam

$$\alpha_1: \hat{R} \otimes_R \mathrm{Hom}_\Lambda(\Lambda^r,N) \longrightarrow \mathrm{Hom}_{\hat{\Lambda}}(\hat{\Lambda}^r,\hat{N}),$$

$$\alpha_2: \hat{R} \otimes_R \mathrm{Hom}_\Lambda(\Lambda^s,N) \longrightarrow \mathrm{Hom}_{\hat{\Lambda}}(\hat{\Lambda}^s,\hat{N})$$

definidas de maneira análoga. α, α_1 e α_2 são R-homomorfismos que tornam comutativo o diagrama seguinte:

$$\begin{array}{ccccccc}
0 \longrightarrow & \hat{R} \otimes_R \mathrm{Hom}_\Lambda(M,N) & \longrightarrow & \hat{R} \otimes_R \mathrm{Hom}\ (\Lambda^r,N) & \longrightarrow & \hat{R} \otimes_R \mathrm{Hom}_\Lambda(\Lambda^s,N) \\
& \alpha \downarrow & & \alpha_1 \downarrow & & \alpha_2 \downarrow \\
0 \longrightarrow & \mathrm{Hom}_{\hat{\Lambda}}(\hat{M},\hat{N}) & \longrightarrow & \mathrm{Hom}_{\hat{\Lambda}}(\hat{\Lambda}^r,\hat{N}) & \longrightarrow & \mathrm{Hom}_{\hat{\Lambda}}(\hat{\Lambda}^s,\hat{N}) & .
\end{array}$$

Como $\hat{R} \otimes_R \mathrm{Hom}_\Lambda(\Lambda^r,N) \cong \hat{R} \otimes_R [\mathrm{Hom}_\Lambda(\Lambda,N)]^r \cong \hat{R} \otimes_R N^r \cong$ $\cong (\hat{R} \otimes_R N)^r = \hat{N}^r \cong [\mathrm{Hom}_{\hat{\Lambda}}(\hat{\Lambda},\hat{N})]^r \cong \mathrm{Hom}_{\hat{\Lambda}}(\hat{\Lambda}^r,\hat{N})$, vem que α_1 é um isomorfismo. Da mesma forma, obtém-se que α_2 é um isomorfismo, e o diagrama implica em que α é um isomorfismo. □

<u>LEMA 5.7.</u> Se M é um R-módulo finitamente gerado, então $M \cap \pi\hat{M} = \pi M$.

<u>Demonstração:</u> R é um anel de valorização discreta e, portanto, um domínio de ideais principais. Assim, M é isomorfo a uma soma direta finita de R-módulos isomorfos a R ou a $\frac{R}{p^n}$ com $n \geq 1$. Assim, é suficiente demonstrar o lema para

módulos dessa forma, pois, se $M = M_1 \oplus \ldots \oplus M_r$, temos:

$$M \cap \pi\hat{M} = M_1 \oplus \ldots \oplus M_r \cap (\pi\hat{M}_1 \oplus \ldots \oplus \pi\hat{M}_r) =$$

$$= (M_1 \cap \pi\hat{M}_1) \oplus \ldots \oplus (M_r \cap \pi\hat{M}_r) = \pi M_1 \oplus \ldots \oplus \pi M_r = \pi M .$$

É claro que $R \cap \pi\hat{R} = R$. Seja então $M = \frac{R}{p^n}$ com $n \geq 1$. Nesse caso, $M = \frac{R}{p^n} \cong \frac{\hat{R}}{p^n\hat{R}} \cong \hat{M}$, e identificando M com $\hat{M}$ temos o resultado desejado. □

<u>LEMA 5.8.</u> Sejam M e N Λ-módulos finitamente gerados. Então: M e N são isomorfos como Λ-módulos se e só se $\hat{M}$ e $\hat{N}$ são isomorfos como $\hat{\Lambda}$-módulos.

<u>Demonstração:</u> Se $M \cong N$, é claro que $\hat{M} \cong \hat{N}$.

Suponhamos então que $\hat{M} \cong \hat{N}$ e seja $f: \hat{M} \longrightarrow \hat{N}$ um isomorfismo, com $g = f^{-1}$. Pelo lema 5.6., existirão $f_1 \in \mathrm{Hom}_\Lambda(M,N)$ e $g_1 \in \mathrm{Hom}_\Lambda(N,M)$ tais que a imagem de M por $f_0 = f_1 - f$ esteja contida em $\pi\hat{N}$ e a imagem de N por $g_0 = g_1 - g$ esteja contida em $\pi\hat{M}$.

Daí, resulta que $g_1(f_1(m)) = g_0(f_0(m)) + g_0(f(m)) + g(f_0(m)) + g(f(m))$. Como as tres primeiras parcelas pertencem a $\pi\hat{M}$ e $g(f(m)) = m$, vem que $g_1(f_1(m)) - m \in \pi\hat{M}$, para todo $m \in M$. Como $M \cap \pi\hat{M} = \pi M$, resulta que $M = (g_1 \circ f_1)(M) + \pi M$. Pelo lema de Nakayama, concluímos que $M = (g_1 \circ f_1)(M)$. Assim, $g_1 \circ f_1$ é um epimorfismo, e, como M é noetheriano, $g_1 f_1$ é um isomorfismo.

Da mesma forma, obtemos que $f_1 g_1$ é um isomorfismo, e daí segue que f_1 e g_1 são isomorfismos, e, portanto, $M \cong N$. □

Uma consequência desse lema é o seguinte:

LEMA 5.9. (i) Se M e N são Λ-módulos finitamente gerados, N um somando direto de M e $M = M_1 \oplus \ldots \oplus M_r$ é uma decomposição de M em submódulos indecomponíveis, então N é isomorfo à soma direta de um subconjunto do conjunto dos M_i.

(ii) Se L, M e N são Λ-módulos finitamente gerados, $L \oplus M \cong L \oplus N$ implica $M \cong N$.

(iii) Se M e N são Λ-módulos finitamente gerados e $M^r \cong N^r$ para algum inteiro positivo r, então $M \cong N$.

Demonstração: Vamos demonstrar apenas a segunda afirmação, pois as outras são inteiramente análogas.

Se $L \oplus M \cong L \oplus N$, tem-se $\hat{L} \oplus \hat{M} \cong \hat{L} \oplus \hat{N}$.

Como Krull-Schmidt vale para $\hat{\Lambda}$-módulos, segue-se que $\hat{M} \cong \hat{N}$, e pelo lema 5.8., que $M \cong N$. □

Como vemos, as tres propriedades do lema acima são consequências do teorema de Krull-Schmidt, porém, não são suficientes para garantir a validade da propriedade de Krull-Schmidt. Para isso, necessitaremos condições mais fortes como as que vem a seguir.

LEMA 5.10. Seja A uma K-álgebra semisimples. Se $\hat{S}$ for um $\hat{A}$-módulo simples sempre que A for um A-módulo simples, então todo $\hat{\Lambda}$-reticulado é isomorfo ao completamento de algum Λ-reticulado.

Demonstração: Como A é semisimples, temos que $A \cong \bigoplus_{i=1}^{n} S_i$ onde os S_i são A-módulos simples.

Daí, $\hat{A} \cong \bigoplus_{i=1}^{n} \hat{S}_i$ com os $\hat{S}_i$ $\hat{A}$-módulos simples, e, portanto, $\hat{A}$ também é semisimples.

Seja T um $\hat{\Lambda}$-reticulado. Temos que $\hat{K}T$ é um $\hat{A}$-módulo finitamente gerado, e, portanto, isomorfo a uma soma direta finita do tipo $\oplus \hat{S}_i^{n_i}$. Então $\hat{K}T \cong \hat{V}$, onde $V = \oplus S_i^{n_i}$. Daí, $\hat{K}T \cong \hat{K}V$. Seja T' a imagem isomórfica de T em $\hat{K}V$. Como $\hat{K}T' = \hat{K}V$, T' é um $\hat{\Lambda}$-reticulado pleno em $\hat{K}V$. Assim, pelo lema 5.4., $T' = \hat{M}$, onde $M = V \cap T'$ é um Λ-reticulado. □

TEOREMA 5.11. Se A é uma K-álgebra semisimples e se $\hat{S}$ é um $\hat{A}$-módulo simples para todo A-módulo simples S, o teorema de Krull-Schmidt vale para Λ-reticulados.

Demonstração: Seja M um Λ-reticulado indecomponível. Se $\hat{M} = T_1 \oplus T_2$, ter-se-ia $T_i \cong \hat{M}_i$ para Λ-reticulados M_i, e, portanto, $\hat{M} \cong \hat{M}_1 \oplus \hat{M}_2$, donde, pelo lema 5.8., seguiria que $M \cong M_1 \oplus M_2$. Portanto, $\hat{M}$ deve ser indecomponível.

Tomemos então $\bigoplus_{i=1}^{r} M_i \cong \bigoplus_{j=1}^{s} N_j$, com M_i, N_j Λ-reticulados indecomponíveis. Então, $\bigoplus_{i=1}^{r} \hat{M}_i \cong \bigoplus_{j=1}^{s} \hat{N}_j$ com os $\hat{M}_i$ e $\hat{N}_j$ $\hat{\Lambda}$-reticulados indecomponíveis, e, como o teorema de Krull-Schmidt vale para $\hat{\Lambda}$-reticulados, vem que $r = s$ e $\hat{M}_i \cong \hat{N}_i$, para $i = 1, 2, \ldots, r$.

Assim, o lema 5.8. nos dá $M_i \cong N_i$, para $i = 1, 2, \ldots, r$. □

<u>LEMA 5.12.</u> Seja $A \cong \bigoplus_{i=1}^{n} M_{n_i}(D_i)$ a decomposição de uma K-álgebra semisimples A em K-álgebras simples. Se $\hat{D}_i$ é um anel com divisão para todo i, então todo $\hat{\Lambda}$-reticulado é isomorfo ao completamento de algum Λ-reticulado.

<u>Demonstração</u>: Como $\hat{A} \cong \bigoplus_{i=1}^{n} M_{n_i}(\hat{D}_i)$ e os $\hat{D}_i$ são anéis com divisão, resulta que $\hat{A}$ também é semisimples e o resultado segue pelo mesmo raciocínio do lema 5.10. . □

Como consequência, temos:

<u>TEOREMA 5.13.</u> Se $A = \oplus M_{n_i}(D_i)$ é a decomposição em K-álgebras simples da K-álgebra semisimples A, e se para todo i, $\hat{D}_i$ é um anel com divisão, então o teorema de Krull-Schmidt vale para Λ-reticulados.

<u>Demonstração</u>: Pelo lema anterior, todo $\hat{\Lambda}$-reticulado provém de um Λ-reticulado via completamento. Assim sendo, podemos utilizar o mesmo argumento do teorema 5.11. . □

<u>TEOREMA 5.14.</u> Se $A = \bigoplus_{i=1}^{n} M_{n_i}(K_i)$, onde os corpos K_i são extensões de K tais que o ideal $\pi R = P$ tem uma única extensão a cada um dos K_i, o teorema de Krull-Schmidt vale para Λ-reticulados.

<u>Demonstração</u>: Pelo teorema 0.14, o completamento P-ádico de K_i é isomorfo ao completamento de K_i relativamente à

única extensão de P a K_i, e portanto, é um corpo. □

COROLÁRIO 5.15. Se K é um corpo de decomposição para A, o teorema de Krull-Schmidt vale para Λ-reticulados.

Demonstração: Nesse caso, $A \cong \bigoplus_{i=1}^{n} M_{n_i}(K)$. □

Finalmente, mencionaremos mais dois resultados concernentes à validade do teorema de Krull-Schmidt para reticulados sobre ordens.

TEOREMA 5.16. Se A é uma álgebra separável comutativa e Λ uma R-ordem, o teorema de Krull-Schmidt vale para os Λ-reticulados projetivos [16] .

Uma R-ordem Λ em A é dita maximal se não está contida propriamente em nenhuma outra R-ordem em A.

TEOREMA 5.17. Seja R_P a localização de R em P e Λ uma R_P-ordem maximal. Então o teorema de Krull-Schmidt vale para Λ-reticulados [15] .

BIBLIOGRAFIA

[1] *Azumaya, G.* - On maximally central algebras, Nagoya Math. I. 2 (1960).

[2] *Berman, S. D. and Gudivok, P. M.* - Integral representations of finite groups, Dolk. Akad. Nank. SSSR 145 (1962).

[3] *Curtis, C. W. and Reiner, I.* - Representation theory of finite groups and associative algebras, Interscience Publishers (1966).

[4] *Dornhoff, L.* - Group representation theory, Part A, Marcel Dekker, Inc., (1971).

[5] *Dress, A.* - On the Krull-Schmidt Theorem for integral group representations of rank 1, Michigan Math. I. 17 (1970).

[6] *Evans, E. G. Jr.* - Krull-Schmidt and cancellation over local rings, Pacific I. of Math. 46 nº 1 (1973).

[7] *Heller, A* - On group representations over a valuation ring, Proc. Nat. Acad. U.S.A. 47 (1961).

[8] *Heller, A. and Reiner, I.* - Representations of cyclic groups in rings of integers II, Anuals of Math. 77 nº2 (1963).

[9] *Jones, A.* - Notas de aula de representações de grupos fi-

nitos, (1974).

[10] *Jones, A.* - On representations of finite groups over valuation rings, Illinois I. of Math. 9 nº (1965).

[11] *Reiner, I.* - The Krull-Schmidt theorem for integral representations, Bull. Am. Math. Soc. 67 (1961).

[12] *Reiner, I* - Failure of the Krull-Schmidt theorem for integral representations, Michigan Math. I. 9 (1962).

[13] *Reiner, I.* - A survey of integral representation theory, Bull. Am. Math. Soc. 76 (1970).

[14] *Reiner, I.* - Maximal Orders, Academic Press (1975).

[15] *Reiner, I.* - Topics in integral representation theory, 4ª Escola de Álgebra, USP (1976).

[16] *Roggenkamp, K. W. and Huber-Dyson, V.* - Lattices over orders I, Lecture Notes in Mathematics 115, Springer (1970).

[17] *Roggenkamp, K. W.* - Lattices over orders II, Lecture Notes in Mathematics 142, Springer (1970).

[18] *Roquette, D.* - Realisierung von Darstellungen endlicher nilpotenten gruppen, Archiv der Math. 9 (1958).

[19] *Irvan, R. G. and Evans, E. G. Jr.* - K-theory of finite groups and orders, Lecture Notes in Math. 149, Springer (1970).

[20] *Weiss, E.* - Algebraic Number Theory, McGraob-Hill (1963).