SÔBRE AS UNIDADES DE ANÉIS DE GRUPOS

César Polcino Milies

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

SÃO PAULO
1972

INDICE

PREFÁCIO

Segundo Curtis-Reiner 121, a teoría de representações - de grupos foi desenvolvida, em forma surpreendentemente completa e útil por G. Frobenius nas últimas duas décadas do século - dezenove. O primeiro tratamento sistemático se encontra no livro de W. Burnside "The theory of Groups of Finite Order" publicado pela Cambridge University Press em 1911.

Um segundo estágio de desenvolvimento da teoría teve - início em 1929 com os trabalhos de E. Noether, quando a teoría - foi absorvida no estudo de módulos e álgebras. Tal coisa é possível utilizando a noção de anel ou álgebra de grupo; associando a cada representação de um grupo G sobre um corpo K um certo módulo sobre a álgebra KG. Damos algumas indicações a esse respeito na seção I.3.

Este fato, por si só, é suficiente para dar uma idéia - da importância do estudo dos anéis de grupos. Trata-se de uma - área da matemática em que a investigação é particularmente in - tensa - uma consulta ao Mathematical Reviews, por exemplo, mostrará a frequência com que aparecem artigos sobre o assunto e a bibliografía incluída em Curtis-Reiner |2| e I. Reiner |30| dará uma idéia da abundância de tais trabalhos .

Em relação aos anéis de grupos existem várias direções- em que vem se desenvolvendo a pesquisa. O objetivo deste trabalho é apresentar de forma metódica os resultados até agora co - nhecidos sobre os grupos de unidades de tais anéis . O interesse do assunto foi assinalado por I.Reiner em |30|.

Mesmo nesta área nos impusemos certas restrições para manter o trabalho dentro de limites razoáveis. Trabalhamos sempre com anéis de grupos finitos e, na maioria dos casos, limitamo-nos a considerar coeficientes num corpo.

O primeiro artigo sobre unidades de anéis de grupos é devido a G. Higman |22| quem utiliza a teoría de caracteres para obter resultados no caso em que os coeficientes pertencem a um anel de inteiros algébricos. Nossa intenção original era começar expondo estes resultados, mas os trabalhos mais recentes nos levaram a adotar as limitações a que fizemos referência no parágrafo anterior, e deixar de lado o conteúdo desse artigo.

O presente trabalho pretende ser acessível a um leitor com os conhecimentos básicos de álgebra normalmente contidos nos cursos básicos de Pós-Graduação. Com esse objetivo em mente, fizemos uso livremente dos fatos básicos da teoria de grupos, mas incluímos no Capítulo 0 um apanhado geral de resultados sobre anéis e módulos, que serão de uso constante no que segue.

Existem muito poucos textos que tratam sistematicamente dos anéis de grupos, e nenhum deles em português. Por causa disso no Capítulo I apresentamos vários resultados básicos que poderão ser úteis a eventuais interessados, mesmo em relação a outros problemas na área. Alguns destes se encontram, até agora, unicamente em artigos de pesquisa; outros são tratados em textos tais como Curtis-Reiner |2| e P. Ribemboim |11|. Apenas as definições iniciais da seção I.4 serão utilizados na exposição; porém, sua inclusão se justifica pelas aplicações em outra direção, como brevemente se indica nos resultados finais.

No Capítulo II iniciamos o estudo do grupo das unidades de um anel de grupo. Na primeira seção expomos os fatos básicos e na segunda estudamos a estrutura deste grupo em uma situação particular. O resto do capítulo é dedicado ao estudo de certos subgrupos do grupo das unidades.

Finalmente, no Capítulo III estudamos condições para - que o grupo das unidades de um anel de grupo seja nilpotente.

Em toda a dissertação fizemos um especial esforço para indicar, em cada seção, as fontes utilizadas visando oferecer - um guia à literatura sobre o assunto.

Embora a maior parte do trabalho seja expositivo, al - guns resultados isolados são nossos. O teorema II.1.3 foi o primeiro resultado e o teorema II.3.1 representa uma leve generalização de um teorema de D. B. Coleman e foi obtido adaptando ligeiramente a sua demonstração. A seção II.4 é o resultado de - nosso intento para obter informações sobre a estrutura do grupo das unidades no caso não comutativo. Não obtivemos resultados - fortes; porém, foi possível dar uma condição necessária e suficiente para que certos subgrupos, obtidos de forma natural, sejam somandos diretos.

Finalmente, conseguimos estender um resultado de J.M. - Bateman e D. B. Coleman sobre nilpotência, a anéis de grupo com coeficientes num domínio de integridade. Na seção III.2 trans - crevemos a demonstração original e a seção III.3 reúne o nosso trabalho nesse sentido.

Recentemente J.M. Bateman [12] e K. Motose e M. Tominaga [25] obtiveram novos resultados sobre a solubilidade do grupo

das unidades de um anel de grupo, que não foram incluídos neste trabalho para não estendê-lo em demasía e representam a sua - principal omissão.

Durante os nossos estudos de mestrado no Instituto de - Matemática e Estatística de Universidade de São Paulo foram tantas as pessoas que de uma forma ou de outra colaboraram na nossa formação que agradecimentos detalhados seríam impossíveis - sem se cometer injustas omissões . Muito particularmente queremos agradecer as seguintes pessoas:

Aos Profs. Renzo Piccinini e Waldyr M. Oliva, pela sua orientação e estímulo durante os nossos estudos no I.M.E.U.S.P.

Ao Prof. Carlos B. de Lyra, pela paciência e amabilidade com que nos ouviu falar sobre a nossa dissertação e pelas - suas valiosas sugestões.

Ao Prof. Alfredo Jones, por ter sugerido o assunto desta dissertação, pelo apoio e dedicação muito além do que podíamos merecer e por razões ainda mais importantes: a ele devemos ter nos interessado pelo estudo da álgebra e, em boa medida, a própria decisão de estudar Matemática.

São Paulo, dezembro de 1972

C.P.M.

Durante a realização deste trabalho o autor teve o auxílio financeiro do Programa Multinacional de Matemática da Organização de Estados Americanos e da Fundação de Amparo à Pesquisa do Estado de São Paulo .

ÍNDICE DE SÍMBOLOS

$_AA$ = anel A considerado como módulo à esquerda sobre si mesmo.

$x \oplus y$ = soma direta, quando usado x e y forem anéis, módulos, - ideais, álgebras e produto direto, quando x e y forem - grupos escritos multiplicativamente .

$\otimes$ = produto tensorial

$M_n(D)$ = anel de matrizes de nxn com coeficientes em D.

$GL(n,D)$ = grupo das matrizes inversíveis de $M_n(D)$

$Hom_A(B, C)$ = conjunto dos A-homomorfismos de B em C

$J(A)$ = radical de Jacobson de A. (pág. 6)

AG = anel de grupo de G com coeficientes em A. (pág. 8)

ε = função índice (pág. 11)

$dim_K V$ = dimensão de V como espaço vetorial sobre K

$I(KG)$ = conjunto dos ideais de KG

$S(G)$ = conjunto dos subgrupos do grupo G

$L(H)$ = ideal associado ao subgrupo H (pág. 34)

$U(A)$ = grupo das unidades do anel A

T_{p^i} = grupo cíclico de ordem p^i

$K^* = K - \{0\}$

$U^*(KH)$, $U_1^*(KH)$ = ver pág. 59 .

$U_1(KG)$ = subgrupo das unidades normalizadas de KG (pág. 46)

$U_1(K, H)$ = ver pág. 62 .

CAPÍTULO 0

Reuniremos aqui vários resultados clássicos sobre a teoria de anéis e módulos a que faremos referência muito frequentemente.

A maioria delas encontra-se demonstrada com certo cuidado em nossas notas |10| com vários exemplos. Excelentes exposições destes resultados podem ser achadas em Curtis-Reiner |2| ou em Ribemboim |11|. Também poder-se-a consultar com proveito Bourbaki |1|.

Apenas enunciaremos - sem demonstração - os fatos básicos, que serão usados livremente no resto da dissertação sem fazer referência explícita.

Neste capítulo, A indicará sempre um anel com unidade.

0.1. MÓDULOS SEMISIMPLES

Definição 0.1.1.- Seja M um A-módulo . Um submódulo N diz-se um somando direto de M se existe um submódulo $N' \subset M$ tal que $M = N \oplus N'$ i.e. $M = N + N'$ e $N \cap N' = \{0\}$.

Definição 0.1.2.- Um elemento $a \in A$ diz-se um elemento idempotente se $a^2 = a$.

Proposição 0.1.1.- i) Seja M um A-módulo e $p: M \to M$ um endomorfismo de M tal que $p^2 = p$ (p diz-se uma projeção) .

Então: $M = Im(p) \oplus Ker(p)$. Reciprocamente, se $M = N \oplus N'$ existe uma projeção $p: M \to M$ tal que $Im(p) = N$ e $Ker(p) = N'$.

ii) Se a é um elemento idempotente de A, então, $A.a = \{x.a \mid x \in A\}$ é um submódulo de A^A (o anel considerado como módulo à esquerda sobre si mesmo) e :

$$ {}_AA = A.a \oplus A(1-a) $$

Reciprocamente se ${}_AA = A_1 \oplus A_2$, existe um idempotente $a \in A$ tal que $A_1 = A.a$ e $A_2 = A.(1-a)$

Teorema 0.1.1. - Seja M um A-módulo. As seguintes afirmações são equivalentes:

i) M é soma direta de A-módulos simples (i.e. de A-módulos que não contém submódulos próprios)

ii) M é gerado por uma família de A-módulos simples.

iii) Todo submódulo de M é somado direto

iv) Todo quociente de M é fator direto

v) Toda sequência exata do tipo $0 \to N \to M \to M/N \to 0$ cinde

Definição 0.1.3.- Um A-módulo M diz-se semisimples se verifica alguma(e, portanto, todas) das condições equivalentes do teorema acima. Às vêzes M diz-se também, completamente redutível .

Proposição 0.1.2. - Seja $\{N_i\}_{i \in I}$ uma família de A-módulos simples. Então, todo submódulo de $M = \bigoplus_{i \in I} N_i$ é isomorfo a um módulo da forma $\bigoplus_{i \in J} N_i$, onde $J \subset I$.

Corolário.- Todo submódulo simples de M é isomorfo a algum N_i, $i \in I$.

Proposição 0.1.3. - i) Todo submódulo de um A-módulo semisimples é semisimples.

ii) Todo quociente de um A-módulo semisimples é semisimples.

iii) Soma direta de semisimples é semisimples .

Proposição 0.1.4.- Um A-módulo semisimples M tem comprimento finito, se e somente se, é finitamente gerado.

0.2. ANÉIS SEMISIMPLES

Definição 0.2.1.- Um anel com unidade A diz-se semisimples artiniano se o A-módulo ${}_AA$ é semisimples .

Teorema 0.2.1.- As seguintes afirmações são equivalentes .

i) Todo A-módulo é semisimples

ii) A é um anel semisimples artiniano

iii) A é a soma direta de uma família finita de idéias à esquerda minimais

NOTA : Um anel semisimples artiniano A, no sentido da definição acima, sendo com unidade é finitamente gerado como A-módulo e, portanto, satisfaz a condição de cadeia descendente. O emprego do adjetivo "artiniano" fica assim justificado. Um anel semisimples artiniano também satisfaz a condição de cadeia ascendente; porém é o fato dele ser artiniano que permite obter as condições equivalentes do teorema acima.

Note-se ainda que os submódulos simples do A-módulo ${}_AA$ são, precisamente, os ideais à esquerda minimais de A. Logo, a condição iii) do teorema 0.2.1. é, em essência, uma decomposição de ${}_AA$ em soma direta de submódulos simples .

Proposição 0.2.1. - Seja $A = \bigoplus_{i=1}^{t} L_i$ uma decomposição de A em soma direta de ideais à esquerda minimais. Então, existem elementos $\{e_i\}_{1\leq i\leq t}$ de A tais que

i) $e_i^2 = e_i$, $1\leq i\leq t$

ii) $i \neq j$ implica $e_i . e_j = 0$

iii) e_i não pode ser expresso na forma $e_i = e_i' + e_i''$ com e_i', e_i'' idempotentes tais que $e_i' . e_i'' = 0$, $1\leq i\leq t$.

iv) $1 = \sum_{i=1}^{t} e_i$

v) $L_i = A.e_i$

Reciprocamente, se $\{e_i\}_{1\leq i\leq t}$ é uma família de elementos de A verificando as condições i), ii), iii), iv) acima, definindo - $L_i = A.e_i$, os L_i são ideais à esquerda minimais de A, $1\leq i\leq t$ e $A = \bigoplus_{i=1}^{t} L_i$.

Proposição 0.2.2. - Sejam $A = \bigoplus_{i=1}^{t} L_i = \bigoplus_{j=1}^{s} L'_j$ duas decomposições de um anel A em soma direta de ideais à esquerda minimais. Então, t=s e existe uma permutação $v\in S_t$ - tal que $L_i \cong L'_{v(i)}$.

Definição 0.2.2.- Um anel diz-se simples se ele é semisimples artiniano e contém exatamente dois ideais - bilaterais : (0) e o proprio anel.

Dada uma decomposição de um anel semisimples artiniano em soma direta de ideais à esquerda minimais $A = \bigoplus_{i=1}^{t} L_i$, a família $F = \{L_i\}_{1\leq i\leq t}$ pode-se escrever como reunião de subfamílias $F = F_1 \cup F_2 \cup \ldots \cup F_t$ de modo tal que dois ideais pertencem à mesma família, se e somente se, são isomorfos.

Definimos, então, $B_j = \bigoplus_{L\in F_j} L$

Os conjuntos B_j não dependem da decomposição de A em soma direta e são ideais bilaterais minimais de A.

Definição 0.2.3.- Os ideais B_j, $1\leq j\leq s$, definidos acima dizem-se as componentes simples de A .

Teorema 0.2.2. - (Wedderburn)- Seja A um anel semisimples artiniano. Então:

i) A é soma direta de suas componentes simples $\{B_i\}_{1\leq i\leq s}$

ii) Todo ideal bilateral de A é soma direta de alguns membros da família $\{B_i\}_{1\leq i\leq s}$

iii) Cada componente simples B_i é isomorfa a um anel de matrizes $M_{n_i}(D_i)$ com coeficientes num anel com divisão D_i. Se A for uma álgebra sobre um corpo K então cada D_i estende K e o isomorfismo

$$A \cong M_{n_1}(D_1) \oplus \ldots \oplus M_{n_s}(D_s)$$

é um isomorfismo de K-álgebras .

iv) Se $A = \bigoplus_{i=1}^{s} B_i = \bigoplus_{j=1}^{s'} B'_j$ são duas decomposições de A em soma direta de ideais bilaterais minimais, então, $s = s'$ e existe uma permutação $\sigma \in S_s$ tal que $B_i = B'_{\sigma(i)}$

v) $M_n(D) \cong M_{n'}(D')$, onde D e D' são anéis com divisão, se e somente se, $n = n'$ e $D \cong D'$

Proposição 0.2.3. - Se L_i é um ideal minimal à esquerda de A contido em $B_i \cong M_{n_i}(D_i)$, então, $D_i^0 \cong \mathrm{Hom}_{B_i}(L_i, L_i)$, onde D_i^0 indica o anel oposto do anel D_i, i.é, o anel definido no conjunto D_i com a mesma soma e o produto definido por $\alpha 0 \beta = \beta.\alpha$, $\alpha, \beta \in D$.

Existe um único B_i-módulo simples, a menos de isomorfismos, e este é fiel (i.e. seu anulador é (0))

Pode-se demonstrar ainda que o número n_i é igual ao número de ideais à esquerda minimais que comparecem na família F_i. Ainda, como B_i-módulo simples (pode-se tomar a soma direta de n_i cópias de D_i onde a multiplicação por elementos de B_i define se da seguinte forma:

Dados $b \in B_i$, $x = (x_1, \ldots, x_{n_i}) \in D_i \oplus \ldots \oplus D_i$, consideramos

$\alpha \in M_{n_i}(D_i)$, a imagem de b pelo isomorfismo, e definimos:

$b.x = \alpha.x$

Proposição 0.2.4. - (Lema de Schur) Seja K um corpo algebricamente fechado e A uma álgebra simples de dimensão finita sobre K. Então, $D = \mathrm{Hom}_A(M, M)$ (onde M indica um A-módulo simples) é isomorfo a K .

Corolário .- Se A é uma álgebra semisimples artiniana sobre um corpo K algebricamente fechado, então:

$$A \cong M_{n_1}(K) \oplus \ldots \oplus M_{n_s}(K)$$

Proposição 0.2.5.- Seja $A = \bigoplus_{i=1}^{s} B_i$ a decomposição de A em soma direta de suas componentes simples. Então, existem elementos $\{e_i\}_{1 \leq i \leq s}$ em A tais que :

i) $e_i^2 = e_i$, $1 \leq i \leq s$

ii) $e_i . e_j = 0$ se $i \neq j$

iii) e_i pertence ao centro de A, $1 \leq i \leq s$

iv) e_i não pode ser expresso na forma $e_i = e_i' + e_i''$ com e_i', e_i'' idempotentes do centro de A tais que $e_i' . e_i'' = 0$, $1 \leq i \leq s$.

v) $1 = \sum_{i=1}^{s} e_i$

vi) $B_i = A . e_i$

Proposição 0.2.6.- Seja A um anel semisimples artiniano.e $A = \bigoplus_{i=1}^{t} L_i$ uma decomposição de A em soma de ideais à esquerda minimais. Todo A-módulo simples é isomorfo a algum L_i, $1 \leq i \leq t$.

0.3. RADICAL DE JACOBSON

Definição 0.3.1.- Seja M um A-módulo. Chama-se radical de Jacobson de M ao submódulo intersecção de todos os submódulos maximais de M, que indicaremos por J(M) .

Observação .- $J(M) = M$ se e somente se M não contém submódulos maximais. Se $J(M) = (o)$, M diz-se sem radical

$J(M)$ pode-se caracterizar como o conjunto dos elementos de M que pertencem ao núcleo de todo A-homomorfismo de M em algum A-módulo simples.

Definição 0.3.2.- Chama-se radical de Jacobson de um anel A ao radical do A-módulo ${}_AA$.

Proposição 0.3.1.- As seguintes afirmações são equivalentes:

i) $x \in J(A)$

ii) para todo A-módulo simples M vale $x.M = (0)$

iii) $1-ax$ admite inverso à esquerda, para todo $a \in A$.

Definição 0.3.3.- Um elemento $a \in A$ diz-se um elemento nilpotente se existe um inteiro $n \geq 1$ tal que $a^n = 0$.

Um ideal L de A diz-se um nilideal se para cada elemento $x \in L$ existe um inteiro $n(x) \geq 1$ tal que $x^{n(x)} = 0$.

Um ideal N de A diz-se um ideal nilpoetente se existe um inteiro $n \geq 1$ tal que $N^n = (0)$, onde N^n indica o conjunto de todas as somas finitas de elementos da forma $x_1 \ldots x_n$ com $x_i \in N$, $1 \leq i \leq n$.

Proposição 0.3.2.- Se N é um nilideal de A então $N \subset J(A)$. Se A é artiniano, então, $J(A)$ é um ideal nilpotente, que é o ideal soma de todos os ideais à esquerda nilpotentes de A .

Teorema 0.3.1. - Seja A um anel artiniano. Então, A é sem radical, se e somente se, A é semisimples .

NOTA.- O radical definido aqui deveria chamar-se radical à esquerda, pois temos trabalhado sempre com ideais à esquerda de A. Porém, demonstra-se que $J(A)$ é bilateral e coincide com o radical que obter-se-ia trabalhando com ideais à direita.

CAPÍTULO I

ANÉIS DE GRUPOS

I.1. DEFINIÇÃO E PRIMEIROS EXEMPLOS

Seja A um anel com unidade 1 e G um grupo notado multiplicativamente, cujo elemento neutro indicaremos por 1_G ou também por 1 quando não houver perigo de confusão.

Notaremos por AG o conjunto de todas as funções quase nulas definidas em G com valores em A. Se $\alpha \in AG$ é uma tal função, é usual indicar α pela combinação linear formal $\alpha = \sum_{g \in G} \alpha(g).g$, o que facilita as notações. Às vêzes, indexando $G = \{g_i \mid i \in I\}$ escreveremos os elementos de AG na forma

$\alpha = \sum_{i \in I} a_i.g_i$ com $a_i = \alpha(g_i) \in A$ e $(a_i)_{i \in I}$ quase-nula .

Se G for um grupo finito, indexando $G = \{g_1, \ldots, g_n\}$ entenderemos sempre que $g_1 = 1_G$.

Em AG pode-se definir uma soma, usando a noção usual de soma de funções i.é. dados $\alpha, \beta \in AG$, $\alpha+\beta$ é a função definida por $(\alpha+\beta)(g) = \alpha(g) + \beta(g)$, $g \in G$

Com a notação formal introduzida, podemos escrever:

$$\sum_{i \in I} a_i g_i + \sum_{i \in I} b_i g_i = \sum_{i \in I} (a_i+b_i)\, g_i$$

Pode-se definir também produto de elementos de AG por escalares de A da seguinte forma:

Dado $a \in A$, $\alpha \in AG$ $a\alpha$ será a função definida por:

$$(a\alpha)(g) = a.\alpha(g) \quad , \quad g \in G \ .$$

Uma verificação trivial mostra que AG com as operações definidas é um A-módulo à esquerda; mais precisamente, é o A-módulo livre gerado pelos elementos de G.

Queremos introduzir ainda um produto em AG, de forma tal que, com a soma já definida, se obtenha uma estrutura de

anel. Trabalhando apenas formalmente, se $\alpha = \sum_{i\in I} a_i g_i$ e $\beta = \sum_{j\in I} b_j g_j$ seria natural definir:

$$\alpha.\beta = \sum_{i,j} (a_i.b_j)(g_i.g_j)$$

onde $a_i.b_j$ indica o produto no anel de a_i e b_j e $g_i.g_j$ o produ no grupo G.

Associando para levar à forma inicial, ter-se-ía

$$\alpha.\beta = \sum_{k\in I} c_k.g_k$$

onde c_k é uma soma do tipo $\sum_{i,j} a_i.b_j$ onde os pares i,j de índices são todos aqueles para os quais $g_i.g_j = g_k$

Adotaremos então a seguinte definição para o produto:

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

onde $c(g) = \sum_{m.n=g} a(m).b(n)$

chamado o <u>produto de convolução</u> das funções α e β .

Novamente, é fácil verificar que com a soma e o produto definidos, AG é um anel com unidade. (a unidade sendo o elemento $\sum_g \alpha(g).g$ onde $\alpha(1_G) = 1$ e $\alpha(g) = 0$ para todo outro elemento $g \in G$, que será denotado simplesmente por 1) .

Se A é comutativo, ainda temos:

$$a.(\alpha\beta) = (a\alpha)\ \beta = \alpha(a\beta)\ ,\quad a\in A,\quad \alpha,\ \beta \in AG$$

logo, se A é comutativo <u>AG é uma álgebra sobre A</u> . Tal é o caso quando se tomam os coeficientes num corpo; situação esta a que nos referiremos muito frequentemente neste trabalho.

Definição I.1.1. - Seja A um anel com unidade e G um grupo . O anel AG construído acima diz-se o anel de - grupo de G sobre A. Se A é comutativo, AG diz-se a álgebra de grupo de G sobre A.

A função $i: A \to AG$ definida por $i(a) = a.1_G$, $a \in A$, é um monomorfismo de anéis; portanto, identificaremos frequentemente A com a sua imagem em AG.

Da mesma forma, a função $i:G \to AG$ definida por $i(g)=1.g$ é um monomorfismo (de grupos multiplicativos) e também podemos identificar G com a sua imagem em AG.
Note-se que, com esta identificação, G é uma base do A-módulo - livre AG.

Proposição I.1.1. - i) Sejam G e G' grupos, $f:G \to G'$ um homomorfismo de grupos e A um anel (comutativo) com unidade. Então a função $\overline{f}:AG \to AG'$ definida por

$\overline{f}(\sum_{g \in G} \alpha(g).g) = \sum_{g \in G} \alpha(g).f(g)$ é um homomorfismo de anéis (de álgebras) tal que $\overline{f}|_G = f$. Ainda, se f é epimorfismo ou monomorfismo $\overline{f}$ também o é .

ii) Sejam A, A' anéis (comutativos) com unidade, G um grupo e $f: A \to A'$ um homomorfismo de anéis com unidade. A função $\overline{f}:AG \to A'G$ definida por $\overline{f}(\sum_{g \in G} \alpha(g).g) = \sum_{g \in G} f(\alpha(g)).g$ é um homomorfismo de anéis (de álgebras). Ainda, se f é epimorfismo ou monomorfismo $\overline{f}$ também o é .
A demonstração é imediata .

Alguns homomorfismos importantes, que usaremos frequentemente na exposição podem obter-se como exemplos da proposição acima.

Exemplo I.1.1. - Se H é um subgrupo normal de um grupo G notaremos por $\overline{g}$ a classe do elemento g no quociente G/H . O homomorfismo canônico $G \to G/H$ se extende a um homomorfismo $f:KG \to K(G/H)$ definido por:

$$\sum_i k_i g_i \xmapsto{f} \sum_i k_i \overline{g}_i$$

Exemplo I.1.2.- O homomorfismo trivial $G \to \{1\}$ se extende à função $\varepsilon: KG \to K$ definida por $\varepsilon(\sum_i b_i g_i) = \sum_i k_i$ chamada função índice. O fato da função índice ser um homomorfismo de anéis se traduz nas seguintes propriedades que serão usadas frequentemente:

i) $\varepsilon(\alpha + \beta) = \varepsilon(\alpha) + \varepsilon(\beta)$ ii) $\varepsilon(\alpha.\beta) = \varepsilon(\beta).\varepsilon(\beta)$.

Proposição I.1.2.- Seja $f: G \to H$ um epimorfismo de grupos, K um corpo tal que $carK \nmid |H|$ $\overline{f}: KG \to KH$ o homomorfismo induzido e $N = Ker(f)$. Indicando por $\{c_1 \ldots, c_z\}$ um conjunto completo de representantes de classes módulo N, o conjunto $\{c_i(a_j - 1) \mid a_j \in N, 1 \leq i \leq t\}$ é uma base de $Ker(\overline{f})$ sobre K

Demonstração -

Claramente, os elementos da forma $c_i(a_j - 1)$ pertencem a $Ker(\overline{f})$ e o conjunto é linearmente independente .

Agora, um elemento $\alpha \in AG$ pertence ao núcleo de $\overline{f}$, se e somente se, escrito na forma $\alpha = \sum_{i,j} k_{ij} c_i a_j$ se verifica $\sum_j k_{ij} = 0$, para todo i, $1 \leq i \leq |N|$

Então $\alpha = \sum_{i,j} k_{ij} c_i a_j - \sum_i (\sum_j k_{ij}) c_i = \sum_{i,j} k_{ij} c_i (a_j - 1)$ □

Proposição I.1.3.- Sejam $G_\ell H$ grupos, $f: G \to H$ um epimorfismo de núcleo N, K um corpo tal que $carK \nmid |G|$ e $\overline{f}: KG \to KH$ o homomorfismo induzido. Então $KG \cong KH \oplus Ker(\overline{f})$

Seja $n = \sum_{x \in N} x$

Um cálculo direto mostra que n é um elemento idempotente que pertence ao centro de KG .

Chamando $R = KG.n$ e $S = KG.(1-n) = \{\alpha \in KG \mid \alpha.n = 0\}$ tem-se que R e S são ideais bilaterais de KG e $KG = R \oplus S$.

Provaremos inicialmente que R é isomorfo a KH. Seja $\{c_1,\ldots,c_z\}$ um conjunto completo de representantes de classes de G módulo N e $L = \{c_1.n,\ldots, c_z\, n\}$

É fácil provar que o produto de KG é fechado em L e vale a propriedade de cancelativa em L; portanto, L é um subgrupo multiplicativo de KG

Ainda, a aplicação $f:G \to L$ definida por:

$$g \in c_i\, N \xmapsto{f} c_i.n$$

é um epimorfismo de grupos cujo núcleo é, precisamente, N.

Logo $L \cong G/N \cong H$.

Novamente um cálculo direto permite mostrar que L é base de R sobre K; logo:

$$R \cong KL \cong KH$$

Finalmente, provaremos que $S = \mathrm{Ker}(\overline{f})$

Da proposição I.1.2. temos que $\mathrm{Ker}(\overline{f})$ tem base:

$$\{c_i(a_j-1) \mid a_j \in N,\ 1 \leq i \leq t\}$$

Agora: $c_i(a_j-1)\, n = c_i a_j\, n - c_i n$ e $\overline{f}(c_i(a_j-1)n) = 0$. Cada elemento de uma base de $\mathrm{Ker}(\overline{f})$ pertence a S e, portanto. $\mathrm{Ker}(\overline{f}) \subset S$.

Ainda: $\dim [\mathrm{Ker}(\overline{f})] = t(|N|-1)$ e

$$\dim [S] = \dim[KG] - \dim [R] = t|N| - t = \dim [\mathrm{Ker}(\overline{f})]$$

e resulta a igualdade □

Na seção I.2 veremos teoremas mais gerais sobre decomposições - de KG em somas diretas.

Para concluir esta seção estudaremos um caso muito simples em - que é fácil determinar a estrutura do anel de grupo.

Exemplo I.1.3. - Seja G um grupo cíclico de ordem m, a um gerador de G (então $G = \{1, a, a^2, .., a^{m-1}\}$) e R um anel de integridade.

Pode-se definir um epimorfismo $\phi : R[X] \to RG$ por :

$$f \in R[X] \longmapsto f(a) \in RG$$

Do teorema do isomorfismo para anéis temos: $RG \cong \frac{R[X]}{Ker(\phi)}$

onde $Ker(\phi)$ é da forma $Ker(\phi) = (f_0)$ sendo f_0 o polinômio mônico, de grau mínimo, com raíz a .

No isomorfismo $\overline{\phi}: R[X]/Ker(\phi) \to RG$ o elemento a corresponde à classe $X + (f_0)$

Mostraremos inicialmente que $f_0 = X^m - 1$. De fato, como $a^m - 1 = 0$ vem que $f_0 \mid X^m - 1$ mas, se f_0 for da forma $f_0 = \sum_{i=1}^{n} \alpha_i X^i$ com $n<m$ ter-se-ia:

$f_0(a) = \alpha_0 + \alpha_1 a + \ldots + \alpha_n a^n = 0$ e os elementos de G seríam linearmente dependentes em RG, o que é uma contradição.

Seja então $X^m - 1 = f_1^{\alpha_1} \ldots f_t^{\alpha_t}$ a decomposição de $X^m - 1$ em produto de polinômios mônicos irredutíveis de $R[X]$.

Temos então:

$$RG \xrightarrow{\overline{\phi}}_{\sim} \frac{R[X]}{(X^m-1)} \xrightarrow{\overline{\psi}} \frac{R[X]}{(f_1^{\alpha_1})} \oplus \ldots \oplus \frac{R[X]}{(f_t^{\alpha_t})}$$

onde $\overline{\psi}$ leva a classe $X+(X^m-1)$ em $(X+(f_1^{\alpha_1}), \ldots, X+(f_t^{\alpha_t}))$

Agora, se tomamos os coeficientes num corpo K e se $X^m - 1$ se decompõe num produto de polinômios irredutíveis mônicos diferentes dois a dois em $K[X]$, tomando $\xi_1, \ldots, \xi_t$ raízes de $f_1, \ldots, f_t$ num fecho algébrico de K, temos que:

$\frac{K[X]}{(f_i^{\alpha_i})} \cong K(\xi_i)$ onde a classe $X + (f_i^{\alpha_i})$ corresponde ao elemento ξ_i no isomorfismo e resulta:

$$KG \cong K(\xi_1) \oplus \ldots \oplus K(\xi_t)$$

Note-se que os corpos $K(\xi_i)$, $1 \leq i \leq t$, são anéis simples.

Da unicidade no teorema de Wedderburn, vem que a decomposição - obtida é a decomposição de KG em soma direta de anéis simples.

No isomorfismo final $KG \longrightarrow K(\xi_1) \oplus \ldots \oplus K(\xi_t)$ o elemento a vai na t-upla $(\xi_1, \ldots, \xi_t)$. Convém observar que os ξ_i, sendo raízes do polinômio X^m-1, são raízes da unidade.

Um caso particularmente interessante é quando $K = \mathbb{Q}$, o corpo dos números racionais. Neste caso, os fatores irredutíveis de X^m-1 são os polinômios ciclotômicos $\Phi_d(X)$ onde d percorre - os divisores de m. O número de componentes simples de $\mathbb{Q}G$, com G cíclico de ordem m, é $\phi(m)$, onde ϕ indica a função de Euler.

Se $K = \mathbb{C}$, o corpo dos números complexos, X^m-1 se decompõe num produto de fatores lineares em $\mathbb{C}[X]$ e $\mathbb{C}G$ é isomorfo a uma soma direta de m copias de $\mathbb{C}$.

Concluiremos estudando dois casos particulares.

Se G é o grupo cíclico de ordem 7, a decomposição de X^7-1 em $\mathbb{Q}[X]$ é $X^7-1 = (X-1)(X^6+X^5+X^4+X^3+X^2+X+1)$.

Logo, chamando ξ a uma raíz primitiva de ordem 7 temos:

$$\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q}(\xi)$$

Se G é o grupo cíclico de ordem 6, a decomposição de X^6-1 em $\mathbb{Q}[X]$ é $X^6-1=(X-1)(X+1)(X^2+X+1)(X^2-X+1)$ e temos:

$$\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}\right) \oplus \mathbb{Q}\left(\frac{1+i\sqrt{3}}{2}\right)$$

onde $\frac{-1+i\sqrt{3}}{2}$ é raiz de X^2+X+1 e $\frac{1+i\sqrt{3}}{2}$ raíz de X^2-X+1.

Note-se que os dois últimos somandos são iguais.

Exemplo I.1.4.- Vamos mostrar aqui que, se G é um grupo abeliano finito e K um corpo tal que $\mathrm{car}K \nmid |G|$, então a álgebra de grupo é da forma:

$$KG \cong K(\xi_1) \oplus \ldots \oplus K(\xi_t)$$

onde $\xi_1, \ldots, \xi_t$ são raízes da unidade num fecho algébrico de K.

A demonstração elementar que daremos é devida a Gulliksen-Viswanathan-Ribemboim |20|

Sendo G comutativo, do teorema de estrutura para grupos abelianos finitos sabemos que G pode-se escrever como um produto direto:

$$G = H_1 x \ldots x H_m$$

onde cada H_i é um grupo cíclico. Faremos a demonstração por indução em m.

Se m = 1, G é cíclico e, do exemplo anterior, podemos escrever : $KG \cong \frac{K[X]}{(X^n-1)}$, onde $n = |G|$ ~

como car$K \nmid n$, X^n-1 é um polinômio separável sobre K a sua decomposição em produto de fatores irredutíveis mônicos em K[X] é da forma $X^m-1 = f_1,\ldots f_t$ onde $i \neq j$ implica $f_i \neq f_j$.

A discussão do exemplo anterior mostra que, neste caso, a tese é verificada

Seja agora $G = H_1 x \ldots x H_m$ com m>1 e suponhamos o resultado válido para todo produto de m-1 grupos cíclicos. Temos então:

$$KG \cong K((H_1 x \ldots x H_{m-1}) \times H_m) = (K(H_1 x \ldots x H_{m-1}))(H_m)$$

Da hipótese de indução podemos supor $K(H_1 x \ldots x H_{m-1}) \cong K_1 \oplus \ldots \oplus K_s$ onde cada K_i , $1 \leq i \leq s$ é uma extensão ciclotômica de K. Agora:

$$KG \cong (K_1 \oplus \ldots \oplus K_s)(H_m) \cong K_1(H_m) \oplus \ldots \oplus K_1(H_m)$$

Finalmente, cada somando $K_i(H_m)$ é soma direta de extensões ciclotômicas F_i de K_i e K_i uma extensão ciclotômica de K, então F_i é uma extensão ciclotômica de K, e resulta a tese.

O recíproco deste resultado também é válido, i.é. se KG é soma direta de extensões ciclotômicas de K, então G é abeliano (o que é trivial pois a própria álgebra KG o será) e car $K \nmid |G|$. Isto último resultará trivialmente do teorema de

Maschke (Teorema I.2.1)

I.2 ALGUNS TEOREMAS DE DECOMPOSIÇÃO .

Começaremos esta seção com um resultado clássico devido a Maschke cuja importância será evidente nas aplicações.

Teorema I.2.1.- Seja K um corpo e G um grupo finito. Então KG é semisimples artiniano, se e somente se, carK $\nmid$ |G|

Demonstração.-

Suponhamos que car K $\nmid$ |G|

Para cada elemento $\alpha \in KG$ definimos uma aplicação K-linear

$T_\alpha : KG \to KG$ por $T_\alpha(x) = \alpha.x$, $x \in KG$.

Se consideramos a matriz associada à função linear T_α na base G, é fácil verificar que:

i) Se $g \neq 1$, $tr(T_g) = 0$ onde $Tr(T_g)$ indica o traço da função T_g

ii) $tr(T_1) = |G|$.

Seja então J = J(KG) o radical de Jacobson de KG. Queremos provar que J ={0}. Como G é finito, KG é de dimensão finita sobre K e, portanto, um anel artiniano.

Logo J é um ideal nilpotente.

Suponhamos que exista $0 \neq \alpha \in J$ da forma $\alpha = \Sigma k_i g_i$ como $k_j \neq 0$ para algum j. Multiplicando por g_j^{-1} temos:

$$g_j^{-1}.\ \alpha = k_j.\ 1_G + \sum_{i \neq 1} k_i'\ g_i \in J$$

Agora, é fácil verificar que $T_\alpha = k_j.T_1 + \sum_{i \neq 1} k_i'\ T_{g_i}$ e

calculando os traços respectivos temos:

$$tr(T_{\alpha'}) = k_j.|G| \neq 0$$

Mas, como $\alpha' \in J$, $T_{\alpha'}$ deve ser uma função linear nilpotente e $tr(T_{\alpha'}) = 0$ e obtemos assim uma contradição

Para provar o recíproco mostraremos que, se car K | |G| então KG não é semisimples .

Seja $\alpha = \sum_{g \in G} g$. Como os elementos de G são linearmente independentes em KG, certamente $\alpha \neq 0$.

Dado $g \in G$ tem-se $g.\alpha = \alpha.g = \alpha$. Agora:

$$\alpha^2 = \alpha. \sum_{g \in G} g = \sum_{g \in G} \alpha.g = |G|.\alpha$$

Como car K | |G| temos assim $\alpha^2 = 0$

O ideal $KG.\alpha$ gerado por α é um ideal nilpotente, não nulo pois $(KG.\alpha)^2 = 0$ e $0 \neq \alpha \in KG.\alpha$ logo $KG.\alpha \subset J(KG) \neq 0$ □

O resultado acima foi generalizado por I.G. Connell - |18|, que provou que o anel RG é semisimples, se e somente se, R é semisimples e G é finito, tal que |G| é inversível em R (Ver também P. Ribemboim |11|)

Traduzindo agora o teorema de Wedderburn no caso que - nos ocupa obtemos:

Teorema I.2.2.-

i) Se G é um grupo finito e K um corpo tal que carK $\nmid$ |G| então KG tem um número finito de componentes simples $I_1, \ldots, I_m$; cada ideal bilateral de KG é da forma $I_{i_1} \oplus \ldots \oplus I_{i_t}$ com $1 \leq i_1 < \ldots < i_t \leq m$ e, em particular $KG = I_1 \oplus \ldots \oplus I_m$

ii) Cada componente simples é soma de ideais à esquerda minimais de KG, todos isomorfos entre si. Ideais minimais à esquerda correspondentes a componentes simples diferentes são não isomorfos.

iii) Cada componente simples tem unidade e, considerada como álgebra é isomorfa a uma álgebra de matrizes $M_{n_i}(D_i)$ onde D_i é

um anel com divisão e n_i é o número de ideais à esquerda mini - mais que comparecem na decomposição de I_i. Ainda, do lema de Schur, se K é algebricamente fechado, $D_i = K$ para $1 \leq i \leq t$.

iv) A cada componente simples I_i corresponde um único I_i-módulo irredutível, fiel, M_i . Se L_i é um ideal à esquerda minimal na decomposição de I_i, pode-se tomar $D_i^0 = \mathrm{Hom}_{I_i}(L_i, L_i)$. Ainda $L_i \cong D_i \oplus \ldots \oplus D_i$ (n_i vezes) com a multiplicação por um elemento $\alpha \in KG$ definida da seguinte forma .

No isomorfismo $KG \xrightarrow{\sim} M_{n_1}(D_1) \oplus \ldots \oplus M_{n_t}(D_t)$ o elemento α corresponde a um elemento da forma $(A_1, \ldots, A_t)$. Define-se então:

$(d_1 \ldots, d_{n_i})$ como sendo o produto de matrizes $A_i \cdot \begin{bmatrix} d_1 \\ \vdots \\ d_{n_i} \end{bmatrix}$.

Para calcular o número de componentes simples de KG no caso semisimples precisamos provar o seguinte:

Lema I.1.1. - Seja A um anel comutativo com unidade e G um grupo finito. O centro da A-álgebra AG, $C(AG) = \{\alpha \in AG \mid \alpha x = x\alpha \ , \ x \in AG\}$ é uma subálgebra de AG; considerada como A-módulo é livre e seu posto é igual ao número de classes - conjugadas de G.

Demonstração.- O fato de que C(AG) é subálgebra resulta imediatamente. Para provar que é livre com o posto indicado vamos exibir uma base de C(AG) sobre A.

Sejam $c_1, \ldots, c_z$ as classes conjugadas de G. Para cada i, $1 \leq i \leq t$, definimos:

$$\gamma_i = \sum_{g \in c_i} g$$

Mostraremos inicialmente que $\gamma_i \in C(AG)$, $1 \leq i \leq t$.

De fato, $\gamma_i \in C(AG)$, se e somente se $c\gamma_i c^{-1} = \gamma_i$, $c \in G$

mas : $c\gamma_i c^{-1} = \sum_{g\in C_i} cgc^{-1} = \sum_{g\in C_i} g = \gamma_i$ pois conjugação por um elemento de G é um automorfismo que conserva as classes conjugadas.

Verificaremos agora que o conjunto $\{\gamma_i\}_{1\leq i\leq t}$ é linearmente independente. Suponhamos $\sum_{i=1}^{t} k_i\gamma_i = 0$ com $k_i \in A$, $1\leq i\leq t$, i.é. $\sum_{i=1}^{t} \left(\sum_{g\in C_i} k_i g \right) = 0$. Da independência linear de G em AG vem imediatamente que $k_i = 0$, $1\leq i\leq t$.

Finalmente, deveremos provar que o conjunto $\{\gamma_i\}_{1\leq i\leq t}$ é gerador. Para isso, bastará provar que um elemento $\alpha \in \bar{A}G$ pertence a C(AG), se e somente se, escrito na forma $\alpha = \sum_i k_i g_i$, elementos de G pertencentes a uma mesma classe conjugada aparecem com iguais coeficientes .

Sejam $g_i, \bar{g}_i \in C_i$ e $h \in G$ tal que $h.g_i h^{-1} = \bar{g}_i$. Então :

$$\alpha = k_i g_i + \sum_{j\neq i} k_j g_j$$

$$\alpha = h\,\alpha h^{-1} = k_i \bar{g}_i + \sum_{j\neq i} k_j (h g_j h^{-1})$$

Da unicidade de expressão de α vem que os coeficientes de g_i e $\bar{g}_i$ são iguais . □

Proposição I.2.1.- Seja K um corpo algebricamente fechado e G um grupo finito tal que $\mathrm{car}K \nmid |G|$. Então, o número de componentes simples de KG é igual ao número de classes conjugadas de G.

Demonstração . - Em presença do lema, provaremos que o número de componentes simples de KG é igual à dimensão de C(KG) sobre K.

Seja então, conforme aos teoremas I.2.1 e I.2.2.

$$KG \cong M_{n_1}(K) \oplus \ldots \oplus M_{n_t}(K)$$

Então : $C(KG) \cong C(M_{n_1}(K)) \oplus \ldots \oplus C(M_{n_t}(K))$.

Mostraremos que, se I_{n_i} indica a matriz identidade de $M_{n_i}(K)$ então $C(M_{n_i}(K)) = \{k\, I_{n_i} \mid k \in K\}$.

Seja $A = (a_{ij}) \in C(M_{n_i}(K))$ e consideremos as matrizes $I_{hk} = (e_{ij})$ tais que $e_{ij} = 0$ se $i \neq h$ ou $j \neq k$ e $e_{hk} = 1$.

Notando $A.I_{hk} = (c_{ij})$ e $I_{hk}.A = (c'_{ij})$ tem-se que:

$c_{ij} = 0$ se $j \neq k$ e $c_{ik} = a_{ih}$; $c'_{ij} = 0$ se $i \neq h$, $c_{hj} = a_{jk}$

como deve ser $AI_{hk} = I_{hk}A$ também resulta $a_{ih} = 0$ se $i \neq h$, - $a_{jk} = 0$ se $j \neq k$ e $a_{hh} = a_{kk}$, e $A \in \{ kI_{n_i} \mid k \in K\}$

A inclusão de sentido contrário resulta trivialmente

Agora

$$C(KG) \cong K \oplus \ldots \oplus K \qquad (t \text{ vezes})$$

logo a dimensão de C(KG) sobre K é precisamente t, o número de componentes simples de KG □

No caso em que KG é semisimples temos ainda bastante - informação sobre os KG-módulos .

Inicialmente, observamos que se M é um KG-módulo, M - admite uma estrutura natural de espaço vetorial sobre K definindo o produto por escalares de K por:

$$(k,m) \rightarrow (k.1_G) \cdot m$$

Dos resultados enunciados no capítulo 0 vem:

Proposição I.2.2.- i) KG é semisimples artiniano, se e somente se, todo KG - módulo é completamente redutível .

ii) Se KG é semisimples artiniano, todo KG-módulo simples é isomorfo a um ideal à esquerda minimal de KG .

Finalmente mostraremos que, no caso semisimples, a estrutura de álgebras de grupos abelianos sobre corpos algebricamente fechados é bem determinada.

Proposição I.2.3. - Seja G um grupo abeliano de ordem n e K um corpo algebricamente fechado tal que car K $\nmid$ |G| . Então KG é isomorfo a uma soma direta de n cópias de K .

Demonstração . - Como car K $\nmid$ |G|, KG se decompõe numa soma direta de álgebras simples $KG \cong I_1 \oplus \ldots \oplus I_t$

e $n = \dim_K KG = \sum_{i=1}^{t} \dim_K I_t$

Mas, da proposição I.2.1, t = n, logo $\dim_K I_t = 1$ para $1<i<t$;

$I_i \cong K$ e $KG \cong K \oplus \ldots \oplus K$ (|G| vezes) . □

Corolário.- Sejam G, H grupos abelianos de ordem n e K um corpo algebricamente fechado tal que car K $\nmid$ n .

Então $KG \cong KH$. A demonstração segue trivialmente da proposição anterior .

O corolário acima mostra que dados dois grupos G e H e um corpo K, pode acontecer que $KG \cong KH$ embora G e H não sejam isomorfos. Exemplos deste tipo motivaram o seguinte problema, proposto por R.M. Thrall na conferencia de Álgebra de Michigan de 1947 e que tem dado origem a muitos trabalhos de pesquisa (por exemplo Perlis-Walker |26|, Deskins |19|, Coleman |14|, Raggi Cardenas |29| , Gulliksen-Viswanathan-Ribemboim |20|, etc.)

"Dado um grupo G e um corpo K, determinar todos os grupos H tais que $KG \cong KH$ "

Do corolário acima segue que, se K é algebricamente fechado e G é abeliano, todo outro grupo abeliano da mesma ordem é uma solução do problema de Thrall .

Estudaremos em continuação a possibilidade de decompor KG em somas diretas quando K é um corpo de característica prima

p que divide a ordem de G. Para isso, começaremos obtendo informações no caso em que G é precisamente um p grupo. Neste caso - KG diz-se um anel de grupo modular .

O seguinte resultado clássico, devido a Wedderburn será de utilidade .

Teorema I.2.3.- Seja A uma álgebra de dimensão finita sobre - um corpo K. Se existe uma base de A sobre K - formada por elementos nilpotentes, então a própria A é uma álgebra nilpotente.

Pode-se ver uma demonstração deste teorema em Herstein |3| teorema 2.3.1 .

Teorema I.2.4.- Seja K um corpo de característica p e G um grupo de ordem p^m . Então o radical de KG é o conjunto :

$$J(KG) = \{x \in KG \mid \varepsilon(x) = 0\}$$

Ainda mais, o conjunto $\{g-1 \mid g \in G, g \neq 1\}$ é uma base de J(KG) sobre K e o radical tem, portanto, dimensão p^m-1 sobre K .

Demonstração .-

Seja $U = \{x \in KG \mid \varepsilon(x) = 0\} = \ker(\varepsilon)$.

Claramente U é um ideal bilateral de KG (já que $\varepsilon: KG \to K$ é um homorfismo de anéis)

Por outro lado, o conjunto $\{g_i-1\}_{2 \leq i \leq p^m}$ U é linearmente independente e dado $x = \sum_i k_i g_i \in U$, como $\varepsilon(x) = \sum_i k_i = 0$, podemos escrever :

$$x = \sum_i k_i g_i - \sum_i k_i . 1_G = \sum_i k_i (g_i - 1)$$

e o conjunto também é gerador.

Agora $(g_i-1)^{p^m} = g_i^{p^m} - 1 = 0$ logo U é nilpotente, do teorema - anterior, e $U \subset J(KG)$.

Como a dimensão de U e $p^m - 1$ e a dimensão de KG é p^m , U é um ideal maximal e U = J(KG) □

Para determinar se o anel de grupo é ou não decomponível em soma direta de dois ideais à esquerda, deveremos estudar a existência de elementos idempotentes no anel de grupo. O resultado que damos em continuação, devido a D.B. Coleman |16| dá uma resposta adequada .

Teorema I.2.5.- Seja R um domínio de integridade e G um grupo finito de ordem n. RG contém um idempotente não trivial (i.é., diferente de 0,1), se e somente se, algum divisor primo de n é inversível em R .

Demonstração-

Seja p um divisor primo de n inversível em R.

G contém algum subgrupo de ordem p, que notaremos por P .
Indicaremos por p^{-1} o inverso de p em R e mostraremos que

$$e = p^{-1} \cdot \sum_{g_i \in P} g_i$$

é um idempotente não trivial de RG .

De fato, claramente $e \neq 0,1$ e :

$$e^2 = (p^{-1})^2 \sum_{g_i \in P} \sum_{g_j \in P} g_i g_j$$

Mas $\sum_{g_j \in P} g_i g_j = \sum_{g_j \in P} g_j = p.e$ e temos :

$$e^2 = (p^{-1}) \cdot \sum_{g_i \in P} e = (p^{-1}) .p.e = e$$

Para provar o recíproco estudaremos separadamente dois casos:

1º CASO - Car R = 0 .

Tal como já fizemos, indicamos por T_α: RG → RG a função linear definida por $T_\alpha(x) = \alpha.x$, $x \in RG$

Seja então $e = \sum_i \alpha_i g_i$ um idempotente não trivial. Calculando - como no teorema I.2.1 temos que : $tr(T_e) = n.\alpha_1$

logo T_e é uma função linear idempotente e os seus únicos valores próprios são 0 e 1 (já que o seu polinômio minimal é X^2-X) . Agora, $tr(T_e) = n\alpha_1$ é a soma dos valores próprios; portanto, um inteiro q tal que $1 \leq q \leq n-1$.

Calculando $d = mdc(n,q)$ e escrevendo $n_1 = n/d$, $q_1 = q/d = \alpha_1 n_1$ existem $a, b \in \mathbb{Z}$ tais que $an_1+b\,q_1 = 1$.

Logo, em R podemos escrever $n_1(a+b\alpha_1) = 1$ e n_1 é inversível em R. Como $q<n$ deve ser $d \neq n$ e, consequentemente, $n_1 \neq 1$. Todo divisor primo de n_1 será um divisor primo de $n = |G|$, inversível em R .

2º CASO car $k = p \neq 0$

Seja K o corpo de quocientes de R, então $RG \subset KG$.

Escrevendo $n = p^r.t$ com $mdc(p, t) = 1$ vem que deve ser $t \neq 1$. De fato, se G for um p-grupo provaremos independentemente no - próximo capítulo (teorema II.1.2.), que todo elemento de KG que não pertence ao radical é inversível . Portanto, todo divisor - de zero pertence ao radical e é nilpotente. KG não poderia conter elementos idempotentes não triviais.

Provaremos então que t é inversível em R. Como mdc $(p,t) = 1$ existem $a, b \in \mathbb{Z}$ tais que $ap + bt = 1$ e em R, temos $b.t = 1$. □

Corolário . - Seja K um corpo de característica p e G um grupo de ordem $|G| = p^m.t$ com $mdc(p,t) = 1$

Então KG é decomponível em soma direta, se e somente se, $t \neq 1$

I.3. RELAÇÕES ENTRE O ANEL DE GRUPO KG E AS REPRESENTAÇÕES LINEARES DE G SOBRE K

A importância da teoria das representações lineares para o estudo dos grupos é bem conhecida. Nesta seção mostraremos que muitos dos resultados importantes da teoria podem ser obtidos a partir de informações sobre a álgebra KG. Nosso objetivo é, não só dar uma ideia da importância da teoria dos anéis de grupos, mas obter também novos exemplos concreto de anéis de grupos cuja estrutura é conhecida, a partir de informação sobre representações do grupo considerado .

Começaremos por expor brevemente algumas noções e resultados básicos da teoria de representações .

Se K é um corpo e V um espaço vetorial sobre K que, no que segue, será sempre de dimensão finita n; indicaremos por $\mathrm{Hom}_K(V, V)$ o conjunto das funções K-lineares de V em V. $M_n(K)$ indicará o conjunto das matrizes de nxn elementos com coeficientes em K e GL(n,K) o conjunto das matrizes inversíveis de $M_n(K)$.

Definição I.3.1.- Seja G um grupo e K um corpo. Uma <u>representação de G sobre K</u> é um homomorfismo $T:G\to GL(V)$, onde V é um espaço vetorial de dimensão finita sobre K .

A dimensão de V diz-se o <u>grau da representação</u> . Notaremos por $T_g: V \to V$ a função linear correspondente ao elemento $g\in G$ pela representação T .

Se $T:G \to GL(V)$ é uma representação de G sobre K de grau n, fixando uma base B de V e compondo com o isomorfismo $f_B: GL(V) \to GL(n,K)$ que a cada função linear associa a sua matriz na base B, obtém-se um homomorfismo $\overline{T} = f_B \circ T:G\to GL(n,K)$. Um tal homomorfismo diz-se uma <u>representação matricial</u> de G de grau n sobre K .

Obviamente, a cada representação de G sobre K pode-se associar mais de uma representação matricial, dependendo da esco

lha de uma base em V.

A uma dada representação $\overline{T}:G \to GL(n,K)$ pode-se associar, da forma óbvia, uma representação de G sobre K, $T:G \to GL(K^n)$ usando a base canônica de K^n.

Definição I.3.2.- Duas representações de um grupo G sobre um mesmo corpo K, $T:G \to GL(V)$, $T':G \to GL(V')$ dizem-se equivalentes se existe um isomorfismo $f : V \to V'$ tal que $T'_g = f \circ T_g \circ f^{-1}$, para todo $g \in G$.

Definição I.3.3.- Seja $T:G \to GL(V)$ uma representação de G sobre K. Um subespaço S de V diz-se G-invariante sob T se $T_g(S) \subset S$, para todo $g \in G$.

Uma representação $T:G \to GL(V)$ diz-se irredutível se os únicos subespaços de V, G-invariantes sob T, são (0) e V. Em caso contrário, a representação diz-se redutível.

Definição I.3.4.- Uma representação $T:G \to GL(V)$ diz-se redutível se existem subespaços não nulos S_1, S_2 G-invariantes sob T, tais que $V = S_1 \oplus S_2$.

Se S_1, S_2 são subespaços G-invariantes sob T de dimensões n_1, n_2 respectivamente, podemos definir representações $T^i: G \to GL(S_i)$ por $T^i_g = T_g|_{S_i}$, $i = 1, 2$. Neste caso diz-se que T é soma direta das representações T^1, T^2 e se escreve $T = T^1 \oplus T^2$.

Definição I.3.5.- Uma representação $T:G \to GL(V)$ diz-se completamente redutível se para todo subespaço S e V G-invariante sob T existe um subespaço S' G-invariante sob T tal que $V = S \oplus S'$.

A importância destes conceitos será mais facilmente visualizada procurando a sua interpretação matricial. Tal interpretação, assim como diversos exemplos, pode-se ver em Curtis - Reiner |2| , Jones |7| ou em nossas notas |9| .

Definição I.3.6. - Seja A uma álgebra de dimensão finita sôbre um corpo K. Uma representação de A sobre K é um homomorfismo de álgebras $T:A \to Hom_K(V, V)$ tal que $T_e = I$, a função identidade de V, onde e indica a unidade de A.

Mais uma vez, a dimensão de V diz-se o grau da representação . De forma análoga define-se representação matricial de A sobre K.

É interessante notar que a condição $T_e = I$ não é supérflua. De fato, seja $T:A \to M_n(K)$ uma representação matricial de A, nas condições acima e indiquemos $T_a = (a_{ij})$. $a \in A$. A função $f:A \to M_{n+1}(K)$ definida por $f_a = (a'_{ij})$ onde $a'_{ij} = a_{ij}$ se $i,j \neq n+1$ e $a'_{n+1,j} = a'_{i,n+1} = 0$, $i,j = 1,\ldots,n$, é um homomorfismo de álgebras que não satisfaz a condição $T_e = I$.

As proposições seguintes dão relações entre as representações de G sobre K e as da álgebra KG. Mais adiante mostraremos como, das informações sobre a estrutura de KG, podem-se obter resultado relativos as representações de G sobre K .

Proposição I.3.1.- Dado um grupo G e um corpo K, existe uma correspondência bijetora entre as representações da álgebra KG e as representações de G sobre K

Demonstração.- A cada representação $T:G \to GL(V)$ pode-se associar a função $\overline{T}:KG \to Hom_K(V,V)$ definida por:

$$T\left(\sum_i k_i g_i\right) = \sum_i k_i T_{g_i} \quad , \quad \forall \sum_i k_i g_i \in KG \ .$$

É imediato verificar que $\overline{T}$ é uma representação de KG no sentido da definição I.3.6.

Reciprocamente, se $\overline{T}:KG \to Hom_K(V, V)$ é uma representação de KG, por restrição se obtém uma representação : $T = \overline{T}_G : G \to GL(V)$.

Como as correspondências acima são inversas uma da outra resulta imediatamente a tese □

Proposição I.3.2.- Existe uma correspondência bijetora entre as representações de G sobre K e os KG-módulos de dimensão finita sobre K .

Demonstração.- A cada representação $T:G \to GL(V)$ de G sobre K pode-se associar o KG-módulo de dimensão finita V, onde a estrutura de KG-módulo é dada por :

$$\left(\sum_i k_i g_i, x\right) \longmapsto \sum_i k_i T_{g_i}(x) \quad ,$$

Reciprocamente, se M é um KG-módulo de dimensão finita sobre K definimos $T:G \to GL(M)$ associando a cada elemento $g \in G$ a função linear $T_g:M \to M$ definida por

$$T_g(x) = g.x \quad , \forall\ x \in M$$

Novamente, é fácil verificar que as correspondências acima são inversas uma da outra □

A seguinte proposição, de demonstração simples, estabelece relações entre certas propriedades de KG-módulos e propriedades das representações correspondentes.

Proposição I.3.3.- i) Duas representações T, T' de G sobre K são equivalentes se e somente se os KG-módulos correspondentes são isomorfos

ii) Uma representação T de G sobre K é irredutível, decomponível ou completamente redutível se e somente se o KG-módulo associado é simples, decomponível em soma direta ou semisimples, respectivamente.

Proposição I.3.4.- Sejam : G um grupo, K um corpo, $T:G \to GL(V)$ uma representação de G sobre K e M o KG-módulo associado a T. Se M admite uma decomposição em soma direta $M = \bigoplus_{i=1}^{t} M_i$ e indicamos por T^i a representação correspondente ao módulo M^i, $1 \leq i \leq t$, tem-se que $T = \bigoplus_{i=1}^{t} T^i$

Agora, usando as proposições I.3.3, I.2.2 e o teorema de Maschke obtemos :

Proposição I.3.5.- Todas as representações de um grupo G sobre um corpo K são completamente redutíveis se e somente se KG é semisimples i.e. se e só se car $K \nmid |G|$

Neste caso, da proposição I.3.4 e o teorema 0.1.1. temos :

Proposição I.3.6.- Se car $K \nmid |G|$ toda representação de G sobre K é soma direta de representações irredutíveis.-

Da proposição anterior resulta que para conhecer todas as representações de G sobre K - no caso em que car $K \nmid |G|$ - é suficiente conhecer todas as representações irredutíveis de G sobre K . De acordo com a proposição I.3.3 estas estarão em correspondência bijetora com os KG-módulos simples de dimensão finita sobre K e estes, pela sua vez, com os ideais à esquerda minimais de KG, como se segue do corolário da proposição I.2.2.

Finalmente, do teorema de Wedderburn e, particularmente de sua aplicação a KG (ver teorema I.2.2. parte ii)) resulta - que o número de representações irredutíveis, não equivalentes, de G sobre K é igual ao número de componentes simples de KG. Cada representação irredutível T_i correspondente a um somando direto da forma $M_{n_i}(D_i)$; do teorema I.2.2. parte iv) segue que - grau $(T_i) = n_i \dim_K D_i$.

Em presença da proposição I.2.1. podemos enunciar ainda:

Proposição I.3.7.- O número de representações irredutíveis, - não equivalentes, de um grupo G sobre um - corpo K algebricamente fechado e tal que car $K \nmid |G|$ é igual ao número de classes conjugadas de G.

Para finalizar esta seção daremos alguns exemplos mostrando como, do conhecimento da estrutura de KG, podem-se obter as representações de G sobre K e, reciprocamente, como o conhecimento das representações de G sobre K ajuda a determinar a estrutura de KG (sempre no caso semisimples) .

Exemplo I.3.1.- Seja G o grupo cíclico de ordem 7 . Queremos determinar todas as representações irredutíveis de G sobre o corpo $\mathbb{Q}$ dos números racionais .

No exemplo I.13 temos mostrado que $\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q}(\xi)$ onde ξ é uma raíz do polinômio $X^6+X^5+X^4+X^3+X^2+X+1$.

Correspondentemente, existirão duas representações irredutíveis de G sobre $\mathbb{Q}$, uma de ordem 1 e outra de ordem 6 - (já que $\dim_{\mathbb{Q}} \mathbb{Q}(\xi) = 6$) .

Como todo grupo admite a representação trivial $T: G \to GL(1, K)$ que a cada $g \in G$ associa a matriz 1, essa é a representação irredutível de ordem 1 .

Para dar uma representação T de um grupo cíclico, basta obviamente dar a imagem do gerador do grupo, a . Lembramos ainda que, se M é o módulo associado a T, temos que $T_a: M \to M$ é a - função K-linear definida por $T_a(x) = ax, \forall\ x \in M$.

Do teorema I.2.2. parte iv) podemos tomar $M \cong \mathbb{Q}(\xi)$ e, do exemplo I.1.3, multiplicação por a corresponde a multiplicação por ξ . Agora, uma base de $\mathbb{Q}(\xi)$ sobre $\mathbb{Q}$ é $\{ 1, \xi, \xi^2, \xi^3, \xi^4, \xi^5 \}$ e a matriz associada a T_a nessa base é:

$$\overline{T}_a = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

Exemplo I.3.2.- Determinaremos agora todas as representações irredutíveis, não equivalentes, do grupo cíclico de ordem 7 sobre o corpo $\mathbb{C}$ dos números complexos .

Conforme a proposição I.2.3 temos que :

$$\mathbb{C}G \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$$

Existem então sete representações irredutíveis, não - equivalentes, de G sobre $\mathbb{C}$. Estas representações podem-se obter associando a um gerador a de G cada uma das matrizes 1x1, ξ_i, $1 \leq i \leq 7$, onde cada ξ_i é uma das raízes 7-ésimas da unidade

Exemplo I.3.3.- Indicaremos por Q_2 o grupo dos quatérnios de ordem 2 i.e. o grupo gerado por dois elementos a, b verificando as relações $a^2 = b^2$, $a^4 = 1$, $bab^{-1} = a^{-1}$.

Explicitamente, pode-se escrever :

$$Q_2 = \{e, a, a^2 = b^2, a^3 = b^2a, b, ab=ba^3, a^2b=b^3, a^3b=ba\}$$

Pode-se ver que $N = \{e, a, a^2\}$ é um subgrupo normal de Q_2 e Q_2/N, sendo de ordem 4, é comutativo.

Para dar representações de Q_2 bastará dar as imagens - dos geradores de modo tal que verifiquem as relações dadas.

Vamos determinar a estrutura de $\mathbb{Q}\, Q_2$

Definido $\overline{\omega} : \mathbb{Q}\, Q_2 \to \mathbb{Q}\, Q_2/N$ como extensão da projeção canônica $\omega : Q_2/N$ temos, da proposição I.1.3, que :

$$\mathbb{Q}\, Q_2 \cong \mathrm{Ker}(\overline{\omega}) \oplus \mathbb{Q}(Q_2/N)$$

Agora $Q_2/N \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ admite quatro representações irredutíveis não equivalentes de ordem 1 sobre $\mathbb{Q}$. De fato, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ pode-se definir também como o grupo gerado por dois elementos a, b que verificam as relações $a^2 = b^2 = 1$, $ab = ba$. e é fácil ver que as seguintes, são representações:

$T_a = 1$	$T'_a = 1$	$T''_a = -1$	$T'''_a = -1$
$T_b = 1$	$T'_b = -1$	$T''_b = 1$	$T'''_b = -1$

Logo $\mathbb{Q}\, .\, Q_2/_N \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$.

Finalmente, pode-se demonstrar, calculando, que $\mathrm{Ker}(\overline{\omega})$ é isomorfo ao anel com divisão D dos quatérnios racionais, de dimensão 4 sobre $\mathbb{Q}$ (ver Jones |7|) . Temos então:

$$\mathbb{Q}\, Q_2 \cong D \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} .$$

Ainda, se queremos determinar a estrutura de $\mathbb{C}Q_2$ como as quatro representações acima podem interpretar-se também como representações complexas podemos escrever :

$$\mathbb{C}Q_2 \cong \mathrm{Ker}\ (\overline{\omega}) \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$$

de onde $\dim_{\mathbb{C}} \mathrm{Ker}\ (\overline{\omega}) = 4$.

Do teorema I.2.2 parte iii) $\mathrm{Ker}(\overline{\omega})$ só pode ser soma direta de álgebras de matrizes com coeficientes em $\mathbb{C}$ e levando em consideração as respectivas dimensões, só existem duas possibilidades : $\mathrm{Ker}\ (\overline{\omega}) \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$ ou $\mathrm{Ker}(\overline{\omega}) = M_2(\mathbb{C})$

No primeiro caso, $\mathbb{C}Q_2$ resultará comutativa, o que não pode acontecer pois $Q_2 \subset \mathbb{C}Q_2$ não é abeliano, logo :

$$\mathbb{C}Q_2 \cong M_2(\mathbb{C}) \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$$

Exemplo I.3.4.- Indicaremos por D_4 o grupo dihedro de ordem 2, i.é. o grupo gerado por dois elementos a, b satisfazendo as relações $a^4 = b^2 = 1$ e $baba = 1$, que explicitamente pode-se escrever na forma :

$$D_4 = \{e, a, a^2, a^3, b, ab = ba^3, a^2b = ba^2, a^3b = ba\}$$

É fácil achar quatro representações não equivalentes de grau 1 sobre $\mathbb{Q}$:

$$T_a = 1 \qquad T'_a = 1 \qquad T''_a = -1 \qquad T'''_a = -1$$

$$T_b = 1 \qquad T'_b = -1 \qquad T''_b = 1 \qquad T'''_b = -1$$

Ainda, uma representação irredutível de grau 2 sobre $\mathbb{Q}$ e dada por :

$$T_a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad T_b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

A representação T corresponde a um somando direto da forma $M_n(D)$ e grau $T = n.\dim_{\mathbb{Q}} D$ logo $D = \mathbb{Q}$ e $n = 2$ ou $\dim_{\mathbb{Q}} D = 2$ e $n = 1$

Como $\dim_{\mathbb{Q}} \mathbb{Q}D_4 = |D_4| = 8$, no segundo caso ter-se-ía:

$$\mathbb{Q}D_4 \cong D \oplus D' \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$$

onde D e D' são de dimensão 2 sobre $\mathbb{Q}$. Mas toda extensão de grau 2 é comutativa e $\mathbb{Q}D_4$ seria comutativa .

Logo, T corresponde a um somando da forma $M_2(\mathbb{Q})$ e temos:

$$\mathbb{Q}D_4 \cong M_2(\mathbb{Q}) \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$$

Como as representações acima também são irredutíveis sobre $\mathbb{C}$ (Jones |7|) temos ainda:

$$\mathbb{C}D_4 \cong M_2(\mathbb{C}) \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$$

Comparando com o exemplo anterior resulta $\mathbb{Q}Q_2 \not\cong \mathbb{Q}D_4$ mas $\mathbb{C}Q_2 \cong \mathbb{C}D_4$.

Estes exemplos ilustram mais uma vez o interêsse do problema de Thrall, agora no caso não comutativo.

I.4 SUBGRUPOS DE G E IDEAIS DE KG

Nesta seção estudaremos uma certa correspondência entre subgrupos de G e ideais de KG introduzida por W.E. Deskins|19| para estender os primeiros resultados obtidos em relação ao problema de Thrall por S. Perlis e G.L. Walker |26|

Os resultados que damos em continuação provém do trabalho de Deskins e dos artigos de I.G. Connell |18| e D.B. Coleman |14| .

Seja G um grupo finito de ordem n, K um corpo, S(G) o conjunto dos subgrupos de G e I (KG) o conjunto dos ideais de KG .

Definiremos uma função L: S(G) $\to$I(KG) da seguinte forma: a cada subgrupo $H = \{h_1, \ldots, h_m\}$ de G associamos o ideal L(H) de KG gerado pelo conjunto $\{h_i - 1 \mid 2 \leq i \leq m\}$

Dado um subgrupo H notaremos por $Q_H = \{q_1 = 1, \ldots, q_t\}$ um conjunto completo de representantes de classes lateriais, módulo H. Temos assim

$$G = q_1 H \cup \ldots \cup q_t H$$

Proposição I.4.1.- O conjunto $B_H = \{q_i(h_j - 1) \mid 1 \leq i \leq t,\ 2 \leq j \leq m\}$ é uma base de L(H) como espaço vetorial sobre K .

Demonstração.- O fato de que B_H é linearmente independente sobre K resulta imediatamente .

Para provar que também é gerador basta mostrar - que todo elemento da forma $kg(h_j - 1)$ com $k \in K$, $g \in G$ pode-se escrever como uma combinação linear de elementos de B_H com coeficientes em K .

Mas g pode-se escrever na forma $g = q_s h_r$ logo:

$$kg(h_j-1) = k\, q_s h_r\, (h_j-1)$$

Chamando $h_r h_j = h_p$ temos,

$$kg(h_j-1) = kq_s(h_p-h_r) = kq_s(h_m-1) + kg_s(h_r-1) \quad \square$$

Proposição I.4.2.- Se S é um conjunto de geradores do subgrupo H, então $\{s-1 \mid s \in S\}$ é um conjunto de geradores de L(H).

Demonstração.- De fato, $h \in H$ pode-se escrever na forma $h = s_1 . s_2 \ldots s_r$ com $s_i \in S$

Como $s_1 . s_2 \ldots, s_r - 1 = s_1(s_2 \ldots s_r - 1) + s_1 - 1$ um argumento de indução prova que h-1 pertence ao ideal gerado por $s-1$ $s \in S$ para todo $h \in H$, de onde resulta a tese $\square$

Nossa intenção agora é definir uma função "em sentido contrário" $H: (KG) \to S(G)$. Para isso observaremos que, se $J \in I(KG)$ o conjunto $H_j = \{g \in G \; g-1 \in J\}$ é um subgrupo de G .

De fato:

i) $0 \in J$ implica que $1 \in H_j$

ii) Se $g, g'g \in H_j$ temos $gg'-1 = g(g'-1) + g-1 \in J$ e $gg' \in H_j$

iii) Se $g \in H_j$ temos que $g-1 \in J$, logo : $-g^{-1}(g-1) \in J$ e $g^{-1}-1 \in J$ donde, também $g^{-1} \in H_j$

Podemos definir então H por $H(J) = H_j$, $J \in I(KG)$

Lema.- Seja $q \in Q_H$, $q \neq 1$. Então $q-1 \notin L(H)$

Demonstração.- De fato, se $q-1 \in L(H)$ ter-se-ia :

$$q-1 = \sum_{ij} k_{ij}\, q_i (h_j - 1) = \sum_{ij} k_{ij}\, q_i h_j - \sum_i \Big(\sum_{j \neq 1} k_{ij} \Big) q_i$$

Como os elementos de G são linearmente independentes sobre K tem-se que :

$$\sum_{ij} k_{ij}\, q_i\, h_j = 0 \qquad e \qquad \sum_i \Big(\sum_{j \neq 1} k_{ij} \Big) q_i = q-1$$

Como a primeira igualdade implica $k_{ij} = 0$, para todo par ij, na segunda resultaria $q = 1$

Proposição I.4.3.- A composta $H_o L$ é a identidade em $S(G)$

Demonstração.-

Dado $H \in S(G)$ mostraremos que $H_o L(H) = H$

Da definição de H, se $g \in H(L(H))$ temos que $g-1 \in L(H)$

Se $g \in H$, pode-se escrever na forma $g = qh$ com $1 \neq q \in Q_H$, $h \in H$

logo $g-1 = q(h-1) + (q-1)$ e $q-1 \in L(H)$ o que contraría o lema acima .

Temos provado então que $H \circ L(H) \subset H$. A inclusão simétrica é imediata □

Corolário.- A função $L: S(G) \to I(KG)$ é injetora e $H: I(KG) \to S(G)$ sobrejetora .

Desafortunadamente as funções L e H não são inversas uma da outra .

De fato, basta considerar o próprio KG e calcular $L_o H(KG)$

$$H(KG) = \{g \in G \mid g-1 \in KG\} = G$$

$L \circ H(KG) = L(G)$ é, então, o ideal de KG gerado por elemento da forma g-1. É fácil ver que, se $\alpha \in L(G)$ então $\varepsilon(\alpha) = 0$ e $L(G) \neq KG$.

Porém, a seguinte proposição dá alguma informação sobre esta composição.

Proposição I.4.4.- Para todo $J \in I(KG)$ tem-se que $L_o H(J) \subset J$.

Demonstração.- Como $h \in H(J)$ se e somente se $h-1 \in J$ é imediato que $L \circ H(J)$ que é o ideal gerado por $\{h-1 \mid h \in H(J)\}$ é contido em J □

Seja agora H um subgrupo de G e $H_1 = H, H_2, \ldots, H_t$ todos os subgrupos de G que são conjugados de H. Sejam $L_i = L(H_i)$, $1 \leq i \leq t$, os ideais associados a estes subgrupos.

Cada automorfismo interior de G induz um automorfismo de KG (ver proposição I.1.1) e resulta imediatamente que se H_i, H_j são subgrupos correspondentes em um dado automorfismo interior, os ideais L_i, L_j se correspondem no automorfismo induzido.

Proposição I.4.5.- Os ideais $S(H) = L + \ldots + L_t$ e $T(H) = L_i \cap \ldots \cap L_t$ são ideais bilaterais de KG .

Demonstração.- Precisamos unicamente que são também ideais à direita.

Temos que $g^{-1} S(H) g = \sum_{i=1}^{t} g^{-1} L_i g = \sum_{i=1}^{t} L_i = S(H)$. Logo:

$S(H).g = g.S(H) \subset S(H)$ e S(H) é ideal à direita .

Um argumento similar prova que T(H) é bilateral □

Corolário.- Se H é um subgrupo normal de G, L(H) é um ideal bilateral de KG .

Demonstração.- Basta observar que, neste caso $L(H) = S(H) = T(H)$ □

Proposição I.4.6.- Seja J um ideal bilateral de KG e H'=H(J).

Então:

i) $H' \lhd G$

ii) Se J = S(H) para algum subgrupo H de G, então H' é o menor subgrupo normal de G que contém H

iii) Se J = T(H) para algum subgrupo H de G, então H' é a intersecção de todos os conjugados de H.

Demonstração.-

i) $H' = \{h \in G \mid h-1 \in J\}$ Dados $g \in G$, $h \in H'$ temos:

$g^{-1}hg-1 = g^{-1}(h-1)\, g \in J$; logo, $g^{-1}hg \in H'$

ii) Se $J = S(H)$ é claro que $H_i = H(J) = H'$ para cada i .

Ainda, seja $N \lhd G$ tal que $H_i \subset N$ para todo i. Então

$L(N) \supset L(H_i)$ e $L(N) \supset J$

Então $N = H \circ L(N) \supset H(J) = H'$

iii) Agora $h \in H'$ se e somente se $h-1 \in T$ i.é. $h-1 \in L(H_i)$ para cada $i = 1,\ldots, t$ ou, equivalentemente, $h \in H_i$ para $i=1,..,t$ de onde resulta a tese □

Proposição I.4.7.- Se H é um subgrupo normal de G tem-se que:

$$KG/_{L(H)} \cong K(G/H)$$

Demonstração.- Seja $\overline{f} : KG \to K(G/H)$ o homomorfismo induzido pela aplicação canônica $f : G \to G/H$. Claramente $\overline{f}$ é epimorfismo; portanto, será suficiente mostrar que $Ker(\overline{f}) = L(H)$.

Como $\overline{f}$ é homomorfismo de anéis, para provar que $L(H) \subset Ker(\overline{f})$, basta mostrar que $\forall\, g \in G, \forall\, h \in H$, $\overline{f}(g(h-1)) = 0$

Mas: $\overline{f}(g(h-1)) = \overline{gh} - \overline{g} = 0$

Para a inclusão contrária, seja $\alpha \in KG$ tal que $\overline{f}(\alpha)=0$ Tomando $H = \{h_1,\ldots, h_m\}$, $Q_H = \{q_1,\ldots, q_t\}$ como no início desta seção podemos escrever $\alpha = \sum_{ij} k_{ij} q_i h_j$.

$\overline{f}(\alpha) = 0$ implica $\sum_i (\sum_j k_{ij})\, \overline{q}_i = 0$ i.e. $\sum_j k_{ij} = 0$ para $1 \leq i \leq t$

Logo $\alpha = \sum_{ij} k_{ij}\, q_i(h_j-1) \in (H)$ □

Uma adaptação da proposição I.1.3 dá agora a seguinte:

Proposição I.4.8.- Se H é um subgrupo normal de G, e K um corpo tal que carK $\nmid$ |H| então $KG \cong K(G/H) \oplus (H)$

Finalmente, daremos algumas soluções parciais do problema de Thrall que resultam quase imediatamente das considerações desta seção .

Proposição I.4.9.- Seja I um ideal bilateral de KG. A álgebra quociente KG/I é comutativa se e somente se $I \supset L(G')$, onde G' indica o subgrupo comutador de KG .

Demonstração.- Da proposição I.4.2, $L(G') \subset I$ se e somente se $g^{-1}h^{-1}gh-1 \in I$ para todos $g,h \in G$.

Logo, $L(G') \subset I$ se e só se $hg(g^{-1}h^{-1}gh-1) = gh-hg \in I \ \forall g,h \in G$ i.e. $L(G') \subset I$ se e só se $gh = hg \pmod I$ □

Corolário 1- Sejam G, H grupos finitos da mesma ordem e K um corpo tal que car K $\nmid$ |G| então $KG \cong KH$ se e somente se $K(G/G') \cong K(H/H')$ e $L(G') \cong L(H')$

Demonstração.- Da proposição I.4.8 temos $KG \cong K(G/G') \oplus L(G')$ e $KH \cong K(H/H') \oplus L(H')$; portanto, a suficiência é imediata.

Seja $f: KG \to KH$ a função que realiza o isomorfismo e $I = f(L(G'))$ então: $KG/_{L(G')} \cong KH/_{I}$ e como $KG/_{L(G')}$ é comutativo, $I \supset L(H')$.

De forma análoga se $J = f^{-1}(L(H'))$ vem que $J \supset L(G')$ de onde $I = L(H')$, $J = L(G')$ e $f|_{L(G')} : L(G') \to L(H')$ é um isomorfismo .

Uma passagem ao quociente prova que $K(G/_{G'}) \cong K(H/H')$ □

Perlis e Walker |26| provaram que se $\mathbb{Q}$ é o corpo dos números racionais e G, H são grupos abelianos então $\mathbb{Q}G \cong \mathbb{Q}H$ implica $G \cong H$. Usaremos este resultado para obter:

Corolário 2.- Sejam G, H grupos finitos. Então $\mathbb{Q}G \cong \mathbb{Q}H$, se e somente se, $L(G') \cong L(H')$ e $G_{/G'} \cong H/H'$.

Demonstração. -

Como $\mathbb{Q}$ é de característica 0 podemos usar o resultado anterior para obter que $\mathbb{Q}G \cong QH$ se e somente se $\mathbb{Q}(G_{/G'}) \cong \mathbb{Q}(H/H')$ e $L(G') \cong L(H')$. Como os quocientes G/G', H/H' são grupos abelianos, o resultado de Perlis e Walker implica imediatamente a tese □

- // -

CAPÍTULO II

UNIDADES EM ANÉIS DE GRUPOS

II - 1 DEFINIÇÃO E PRIMEIROS RESULTADOS

Definição II:1.1.- Seja A um anel com unidade. Um elemento $a \in A$ diz-se inversível ou uma unidade de A se existe outro elemento, que notaremos a^{-1}, em A tal que $a.a^{-1} = a^{-1}.a = 1$.

É fácil verificar que o conjunto de todas as unidades de A, que indicaremos por U(A), é um grupo em relação à multiplicação induzida pelo anel .

Nosso objetivo neste capítulo é estudar as unidades de anel de grupo KG, onde K é um corpo e G indicará sempre um grupo finito.

Em vários dos resultados, KG está escrito como soma direta de álgebras e ao considerar os grupos de unidades, temos conservado o símbolo $\oplus$. Usaremos então este símbolo, sempre que queiramos escrever um produto direto de grupos, embora utilizemos para estes a notação multiplicativa.

Lema II.1.1.- Se $A = A_1 \oplus A_2$ então $U(A) = U(A_1) \oplus U(A_2)$

Demonstração .-

Seja $\alpha = (\alpha_1, \alpha_2) \in A$ com $\alpha_i \in A_i$, i=1,2 um elemento inversível e $\alpha^{-1} = (\overline{\alpha}_1, \overline{\alpha}_2)$ o seu inverso. Então $\alpha\alpha^{-1} = (\alpha_1\overline{\alpha}_1 \ \alpha_2\overline{\alpha}_2) = (1,1)$ e $\alpha_i \in U(A_i)$, i = 1,2 .

Reciprocamente, dados $\alpha_i \in U(A_i)$, i=1,2 e $\alpha = (\alpha_1, \alpha_2)$ o elemento $\overline{\alpha} = (\alpha_1^{-1}, \alpha_2^{-1})$ é o inverso de α e $\alpha \in U(A)$ □

O resultado se estende facilmente, por indução, a um número finito de somandos .

Teorema II.1.1.- Seja G um grupo finito e K um corpo tal que - car K $\nmid$ |G|. Escrevendo $KG \cong M_{n_1}(D_1) \oplus \ldots \oplus M_{n_t}(D_t)$, como no teorema I.2.2. então

$$U(KG) \cong GL(n_1, D_1) \oplus \ldots \oplus GL(n_t, D_t)$$ onde $GL(n_i, D_i)$ indica o grupo das matrizes inversíveis de $M_{n_i}(D_i)$.

Demonstração.-

Basta observar que um elemento $\alpha \in KG$ é uma unidade, se e somente se, o seu correspondente no isomorfismo o é, e aplicar o lema acima

Exemplo II.1.1.- Vimos no exemplo I.1.4 que, se G é um grupo cíclico de ordem 7, tem-se que:

$$\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q}(\xi)$$

onde ξ é uma raíz primitiva 7-ésima de 1. Logo:

$$U(\mathbb{Q}G) \cong \mathbb{Q}^* \oplus \mathbb{Q}(\xi)^*$$

onde $\mathbb{Q}^*$, $\mathbb{Q}(\xi)^*$ indicam respectivos conjuntos, sem o elemento 0.

Exemplo II.1.2.- No exemplo I.3.4. calculamos:

$$\mathbb{Q}D_4 \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q})$$

onde D_4 indica o grupo dihedro de ordem 2 . Logo:

$$U(\mathbb{Q}D_4) \cong \mathbb{Q}^* \oplus \mathbb{Q}^* \oplus \mathbb{Q}^* \oplus \mathbb{Q}^* \oplus GL(2, \mathbb{Q}) .$$

Lema II.1.2.- Seja N um nilideal de um anel com unidade A. Então, o conjunto 1+N é um subgrupo do grupo das unidades U(A) .

Demonstração.- Provaremos inicialmente que, se $x \in N$ então $1+x$ é inversível. De fato, chamando $\alpha = 1 - x + x^2 - \ldots + (-1)^{n(x)-1} . x^{n(x)-1}$ vem, computando, que $x.\alpha = \alpha .x = 1$; logo, $\alpha = x^{-1}$. Claramente $\alpha \in 1+N$

Só falta provar que, dados $x_1, x_2 \in N$, $(1+x_1)(1+x_2) \in N$, o que é imediato □

Teorema II.1.2.- Seja K um corpo de característica prima p e G um p-grupo. Então:

$$U(KG) = \{x \in KG \mid \varepsilon(x) \neq 0\}$$

Demonstração.-

Seja $x \in U(KG)$. Então existe $x^{-1} \in U(KG)$ tal que $x.x^{-1} = 1$ e $\varepsilon(x) . \varepsilon(x^{-1}) = 1$. Necessariamente, $\varepsilon(x) \neq 0$.

Reciprocamente, se $x = \sum_i k_i g_i$ é tal que $\varepsilon(x)=k \neq 0$ temos que $k^{-1}x = \sum_i (k^{-1}k_i)g_i$ é tal que $\varepsilon(k^{-1}x) = 1$.

Então $k^{-1} = 1 + (\sum_i (k^{-1}.k_i)\, g_i - 1) \in 1 + J(KG)$ pois

$\varepsilon (\sum_i (k^{-1}.k_i)\, g_i - 1) = 0$.

Agora, J(KG) é um ideal nilpotente e, do lema anterior, vem que $k^{-1}. x \in U(KG)$. Finalmente, se y é o inverso de $k^{-1}x$, então $k^{-1}y$ é o inverso de x e $x \in U(KG)$ □

Corolário.- KG contém um único ideal maximal, que é precisamente J(KG), o seu radical de Jacobson .

Demonstração.- Basta observar que, do teorema I.2.4 e do teorema acima vem que $KG = U(KG) \cup J(KG)$.

Se I é um ideal próprio de KG, deve ser $I \cap U(KG) = \emptyset$; logo $I \subset J(KG)$ e este é o único ideal maximal □

O teorema anterior dá um critério muito cômodo para determinar unidades num anel de grupo. Infelizmente a caracteriza

ção acima só é válida no caso modular, como mostra o seguinte - teorema recíproco :

Teorema II.1.3.- Seja K um corpo e G um grupo finito. Se $U(KG) = \{x \in KG \mid \varepsilon(x) \neq 0\}$ então K é de característica prima p e G é um p-grupo .

Demonstração.-

Suponhamos que exista algum primo $q \neq$ car K que divide a ordem de G .

Como q é inversível em K, do teorema I.2.5, KG contém algum - elemento idempotente e .

Agora $e^2 = e$ implica $e(1-e) = 0$ e, sendo divisores de zero, - certamente, e,(1-e) não pertencem a U(KG). Mas, na equação acima obtemos $\varepsilon(e) \cdot \varepsilon(1-e) = 0$ de onde vem que a função índice, calculada num elemento idempotente, só pode assumir os valores 0 e 1 .

Se $\varepsilon(e) = 1$, temos que $\varepsilon(e) \neq 0$ e $e \notin U(KG)$. Se $\varepsilon(e) = 0$ então $\varepsilon(1-e) = 1$ e $1-e \in U(KG)$. Em ambos os casos obtém-se uma contradição □

Exemplo II.1.3.- Se $K = \{0,1\}$ é o corpo com dois elementos e $G = \{e, g, g^2, g^3\}$ é o grupo cíclico de ordem 4, usando o teorema II.1.2. pode-se computar diretamente:

$$U(KG) = \{e,g,g^2,g^3, e+g+g^2, e+g+g^3, e+g^2+g^3, g+g^2+g^3\}$$

Exemplo II.1.4.- Se $K = \{0,1,2\}$ é o corpo com três elementos e $G = \{e,g,g^2\}$ o grupo cíclico de ordem 3 um cálculo direto mostra que:

$$U(KG) = \{e,g,g^2, 2e,2g,2g^2, e+g, e+g^2, g+g^2, 2e+2g,2e+2g^2,$$
$$2g+2g^2, e+g+2g^2,e+2g+g^2,2e+g+g^2, 2e+2g+g^2, 2e+g+2g^2, e+2g+2g^2\}$$

Para o caso em que car K $\mid$ |G| não se tem resultados gerais. Porém, pode-se ter alguma informação no caso em que -

car K = p e G é um produto direto G = P ⊕ N onde p ∤ |N| e P é um p-grupo. Para isso provaremos o seguinte resultado .

Proposição II.1.1.- Seja G um grupo finito que é produto direto de dois subgrupos H e N, e K um corpo. Então

$$KG \cong KH \underset{K}{\otimes} KN .$$

Demonstração.-

Seja $f: KH \times KN \to K(H \otimes N)$ a função definida por :

$$\left(\sum_i k_i h_i, \sum_j k'_j n_j \right) \xrightarrow{f} \sum_{ij} k_i k'_j (h_i, n_j)$$

É fácil ver que f verifica :

i) $f(\alpha_1 + \alpha_2, \beta) = f(\alpha_1, \beta) + f(\alpha_2, \beta)$ $\alpha_1, \alpha_2 \in KH$, $\beta \in KN$

ii) $f(\alpha, \beta_1 + \beta_2) = f(\alpha, \beta_1) + f(\alpha, \beta_2)$ $\alpha \in KH$, $\beta_1, \beta_2 \in KN$

iii) $f(k\alpha, \beta) = f(\alpha, k\beta)$ $\alpha \in KH$, $\beta \in KH$, $k \in K$

Logo, usando um resultado bem conhecido sobre produtos tensoriais (ver por exemplo Curtis-Reiner |2|) existe

$\overline{f}: KH \otimes KN \to K(H \otimes KN \to K(H \oplus N)$ linear, tal que se

$w: KH \times KN \to KH \underset{K}{\otimes} KN$ indica a aplicação canônica, então

$\overline{f} \circ w = f$.

Em elementos da forma $h \otimes n \in KH \underset{K}{\otimes} KN$ deve valer então: $\overline{f}(h \otimes n) = (h, n)$ e $\overline{f}$ leva assim uma base de $KH \underset{K}{\otimes} KN$ em uma base de $K(H \oplus N)$ e é, portanto, um isomorfismo. □

O resultado acima pode ser usado para calcular o grupo de unidades de um anel de grupo em certos casos particulares. Em continuação damos um exemplo nesse sentido.

Exemplo II.1.5.- Seja T_3 o grupo cíclico de ordem 3 e D_4 o grupo dihedro de ordem 2, como foi definido no exemplo I.3.4. Consideramos então $G = T_3 \oplus D_4$ e $\mathbb{C}$ o corpo dos números complexos . Determinaremos a estrutura de $U(\mathbb{C}G)$.

Da proposição acima : $\mathbb{C}G \cong \mathbb{C}T_3 \underset{\mathbb{C}}{\otimes} \mathbb{C}D_4$

Do exemplo I.1.4 $\mathbb{C}T_3$ é isomorfo a uma soma direta de cópias de $\mathbb{C}$ e, como $\dim_{\mathbb{C}} \mathbb{C}T_3 = 3$ temos que $\mathbb{C}T_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$.

Logo: $\mathbb{C}G \cong (\mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}) \underset{\mathbb{C}}{\otimes} (\mathbb{C}D_4) \cong (\mathbb{C} \underset{\mathbb{C}}{\otimes} \mathbb{C}D_4) \oplus (\mathbb{C} \underset{\mathbb{C}}{\otimes} \mathbb{C}D_4) \oplus (\mathbb{C} \underset{\mathbb{C}}{\otimes} \mathbb{C}D_4) \cong$

$\cong \mathbb{C}D_4 \oplus \mathbb{C}D_4 \oplus \mathbb{C}D_4$

Usando a estrutura de $\mathbb{C}D_4$ calculada no exemplo I.3.4. e o teorema II.1. obtemos :

$U(\mathbb{C}D_4) \cong GL(2, \mathbb{C}) \oplus \mathbb{C}^* \oplus \mathbb{C}^* \oplus \mathbb{C}^* \oplus \mathbb{C}^*$ logo :

$U(\mathbb{C}G) \cong 12.\ \mathbb{C}^* \oplus 3.GL(2,\mathbb{C})$

onde 12 $\mathbb{C}^*$ indica uma soma de 12 cópias de $\mathbb{C}^*$ e $3.GL(2,\mathbb{C})$ uma soma de 3 cópias de $GL(2,\mathbb{C})$.

Voltaremos a usar a proposição II.1.1, como técnica auxiliar, na próxima seção e no capítulo III .

Definição II.1.3.- Seja K um corpo e G um grupo finito. Chamaremos subgrupo das unidades normalizadas ao subgrupo de U(KG) :

$$U_1(KG) = \{x \in U(KG) \mid \varepsilon(x) = 1\}$$

Proposição II.1.2.- Nas condições da definição acima, vale:

$$U(KG) = K^* \oplus U_1(KG)$$

Demonstração.-

É fácil ver que K^* e $U_1(KG)$ são subgrupos normais de U(KG), tais que $K^* \cap U_1(KG) = \{1\}$. Ainda, dado $x \in U(KG)$ sempre podemos escrever $x = \varepsilon(x) \cdot \frac{x}{\varepsilon(x)}$ onde $\varepsilon(x) \in K^*$ e $\frac{x}{\varepsilon(x)} \in U_1(KG)$ □

II. 2 UM EXEMPLO .

Em geral se tem poucas informações sobre a estrutura do grupo das unidades de um anel de grupo. F.F. Raggi Cárdenas estudou em |27|, |28| e |29| a estrutura do grupo das unidades no caso em que G é um grupo abeliano finito e os coeficientes se tomam num corpo finito, no anel dos inteiros módulo p^n ou nos inteiros p-ádicos .

Nesta seção estudaremos a estrutura de U(KG) quando G é abeliano finito e K um corpo finito de característica p, seguindo |29| .

Lema II. 2.1.- Seja A um anel com unidade, G um grupo abeliano e $G = \bigoplus_{i\in I} G_i$ uma decomposição de G em soma direta.

Indicaremos por $\alpha_i : G_i \to G$ e $\beta_i : G \to G_i$ a inclusão canônica e a projeção no i-ésimo somando, respectivamente. Então α_i, β_i induzem homomorfismos $\overline{\alpha}_i : U(AG_i) \to U(AG)$ e $\overline{\beta}_i : U(AG) \to U(AG_i)$, $i\in I$, tais que $\overline{\beta}_i \circ \overline{\alpha}_i = 1_{U(AG_i)}$ e $\overline{\beta}_i \circ \overline{\alpha}_j = 0$ se $i \neq j$.

Demonstração.- Basta definir $\overline{\alpha}_i$, $\overline{\beta}_i$, $i\in I$, como na proposição I.1.1. e restringí-los a $U(AG_i)$, U(AG) respectivamente; notando que imagem de uma unidade é uma unidade. O resto é de verificação trivial □

Lema II.2.2.- Seja $p \in \mathbb{N}$ um número primo, G um p-grupo, $f: G \to G$ o automorfismo definido por $f(x) = x^p$, $x\in g$, e $G' = Im(f)$. Então $G' \cong \bigoplus_{i=1}^{n} r_i\, T_{p^i}$, se e somente se, $G \cong \bigoplus_{i=1}^{n+1} r_{i-1}$ onde T_{p^i} indica o grupo cíclico de ordem p^i e r_i o número de vêzes que o somando T_{p^i} comparece na decomposição de G .

Demonstração.-

Seja $G \cong \bigoplus_{i=1}^{n+1} r_{i-1}\, T_{p^i}$, então $f(G) \cong f(\bigoplus_{i=1}^{n+1} r_{i-1}\, T_{p^i}) \cong \bigoplus_{i=1}^{n+1} r_{i-1} f(T_{p^i})$

Agora, é fácil ver que $f(T_{pi}) \cong T_{pi-1}$. De fato, se $a \in T_{pi}$ é um gerador, $f(a)=a^p$ é um gerador de $f(T_{pi})$ de ordem p^{i-1} .

Reenumerando, podemos escrever $G' = f(G) \cong \bigoplus_{i=1}^{n} r_i\, T_{pi}$.

Reciprocamente, seja $G' \cong \bigoplus_{i=1}^{n} r_i\, T_{pi}$ e suponhamos $G \cong \bigoplus_{i=1}^{m} k_i\, T_{pi}$. Da parte anterior, $G' \cong \bigoplus_{i=1}^{m-1} k_{i+1}\, T_{pi}$ e, da unicidade do teorema de estrutura para grupos abelianos finitos, temos :

$m-1 = n$ e $k_{i+1} = r_i$, $1 \leq i \leq n$. □

Teorema II.2.1.- Seja G um p-grupo abeliano e K um corpo finito de característica p. Então G é um somando direto de U(KG) .

Demonstração.-

Seja $G = \bigoplus_{i=1}^{n} G_i$, onde os G_i são grupos cíclicos . Mostraremos inicialmente que G_i é um somando direto de $U_1(KG_i)$, o subgrupo das unidades normalizadas de $U(KG_i)$.

De fato, se $x = k_j g_j \in U_1(KG_i)$ e G_i é de ordem p^i temos:

$$x^{p^i} = (\Sigma_j k_j g_j)^{p^i} = \Sigma_j k_j^{p^i}\, g_j^{p^i} = \Sigma_j k_j^{p^i} = (\Sigma_j k_j)^{p^i} = 1$$

Logo, G_i é um subgrupo cíclico de ordem máxima de $U_1(KG_i)$ e, portanto, um somando direto .

Ainda, da proposição II.1.2. $U(KG_i) = K^* \oplus U_1(KG_i)$;

logo, G_i é um somando direto de $U(KG_i)$.

Finalmente, mostraremos que $\bigoplus_{i=1}^{n} U(KG_i)$ é um somando direto de $U(KG)$. Consideramos para isso o epimorfismo $\Sigma_i \beta_i : U(KG) \to \bigoplus_{i=1}^{n} U(KG_i)$

e seja $W = \mathrm{Ker}\left(\sum_i \beta_i\right)$. Então, a sequência:

$$\{1\} \to W \to U(KG) \xrightarrow{\Sigma\beta_i} \bigoplus_{i=1}^{n} U(KG_i) \to \{1\}$$

onde i indica a inclusão, é exata e cinde já que, do lema II. 2.1, o homomorfismo $\Sigma\alpha_i : \bigoplus_{i=1}^{n} U(KG_i) \longrightarrow U(KG)$

é tal que $\Sigma\beta_i$ o $\Sigma\alpha_i$ é a função identidade de $\bigoplus_{i=1}^{n} U(KG_i)$.

A tese resulta agora imediatamente □

Lema II.2.3. - Seja G um p-grupo finito e K um corpo finito com p^n elementos. Então :

$$|U(KG)| = (p^n-1)\, p^{n(|G|-1)}$$

Demonstração.-

O número de elemntos de KG é o número de combinações lineares - do tipo $\sum_{i=1}^{|G|} k_i g_i$ com $k_i \in K$; portanto, igual ao número de - arranjos com repetição de p^n elementos tomando $|G|$ de cada vez; i.é, $p^{n|G|}$

Ainda, o número de elementos $x \in KG$ tais que $\varepsilon(x)$ assume um valor $k \in K$ fixo é $p^{n|G|} / p^n = p^{n(|G|-1)}$

Como $KG = J(KG) \cup U(KG)$ com $J(KG) \cap U(KG) = \emptyset$ resulta:

$$U(KG) = p^{n|G|} - p^{n(|G|-1)} = (p^n-1)\, p^{n(|G|-1)} \quad ||$$

Corolário.- $U_1(KG) = p^{n(|G|-1)}$

Teorema II.2.2.- Seja $G \cong \bigoplus_{i=1}^{m} r_i\, T_{pi}$ e K um corpo finito com p^n elementos . Então $U_1(KG) \cong \bigoplus_{i=1}^{m} s_k\, T_{pk}$ onde

$$s_k = n(p^{a_{k-1}} - 2p^{a_k} + p^{a_{k+1}}) \text{ com } a_k = \sum_{i=k}^{m} (i-k)\, r_i \text{ e } a_{m+1} = 0$$

Demonstração.- Um raciocínio análogo ao empregado na primeira parte da demonstração do teorema II.2.1. mostra que, para todo $x \in U_1(KG)$ tem-se que $x^{p^m} = 1$; portanto $U_1(KG)$ deve ser da forma :

$$U_1(KG) \cong \bigoplus_{k=1}^{m} s_k\, T_p{}^k$$

Faremos o cálculo dos coeficientes s_k por indução sobre a ordem de G .

Se $|G| = 1$ então $U_1(KG) = \{1\}$ e o resultado é trivial - mente válido .

Seja agora $|G|$ 1 e suponhamos o resultado válido para todo grupo de ordem menor .

Consideramos agora o subgrupo $G^p = \{g^p \mid g \in G\}$. Do lema II.2.2. temos que $G^p \cong \bigoplus_{i=1}^{m-1} r_{i+1}\, T_p{}^i$.

Seja então $f: U_1(KG) \to U_1(KG^p)$ o homomorfismo definido por:

$$x \in U_1(KG) \xmapsto{f} x^p$$

Provaremos que, efetivamente, $x^p \in U_1(KG^p)$. De fato, x^p é, claramente, uma unidade de KG^p e, se $x = \sum_i k_i g_i$ com $\sum_i k_i = 1$ temos que $x^p = \sum_i k_i^p . g_i^p$ e $\varepsilon(x^p) = \sum_i k_i{}^p = 1$

Para poder utilizar novamente o lema II.2.2. mostrare - mos que $U_1(KG^p) = Im(f)$

Dado $y = \sum_i k_i g_i{}^p \in U_1(KG)$, como K é um corpo perfeito, $K = K^p$

e a função $\psi: K \to K$ definida por $\psi(k) = k^p$, $k \in K$, é um automorfismo. (Ver, por exemplo, Jacy Monteiro |6|) .

Logo, existem elementos $\overline{k}_i \in K$ tais que $\overline{k}_i^{\,p} = k_i$ e podemos escrever :

$$y = \sum_i \overline{k}_i^{\,p}\, g_i^{\,p} = \left(\sum_i \overline{k}_i g_i\right)^p$$

Agora : $\left(\sum_i \overline{k}_i\right)^p = \sum_i k_i = 1$, logo $\sum_i \overline{k}_i = 1$ e

$x = \sum_i \overline{k}_i g_i \in U_1(KG)$ é tal que $f(x) = y$.

Usando então o lema II.2.2. vem que $U_1(KG^p)$ é da forma

$$U_1(KG^p) \cong \bigoplus_{k=1}^{m-1} s_{k+1}\ T_{p^k}$$

Usando a hipótese de indução obtemos :

$$s_{k+1} = n\,(\,p^{a'k} - 2p^{a'k+1} + p^{a'k+2})$$

onde $a'_{k+1} \sum_{i=k}^{m-1} (i-k)\, r_{i+1} = \sum_{i=k+1}^{m} (i-k)\, r_i = a_{k+1} \quad 1 \leq k \leq m-1$

Falta provar ainda que a fórmula é válida para s_1 .

Para isso calculamos:

$$|U_1(KG)| = \prod_{k=1}^{m} p^{k.s_k} = p^{n(|G|-1)} \quad \text{logo} \sum_{k=1}^{n} k s_k = n(|G| - 1)$$

com $|G| = p^{\sum_{i=1}^{m} i.r_i}$. Então :

$$s_1 = n.(p^{\sum_{i=1}^{m} i.r_i} - 1\,) - \sum_{k=2}^{m} k.\, s_k$$

Calculando três termos consecutivos da última soma temos :

$$(k-1)\, s_{k-1} = (k-1)\, n \left[p^{a_{k-2}} - 2p^{a_{k-1}} + p^{a_k} \right]$$

$$k\, s_k = k\, n \left[p^{a_{k-1}} - 2p^{a_k} + p^{a_{k+1}} \right]$$

$$(k+1)\, s_k = (k+1)\, n \left[p^{a_k} - 2p^{a_{k+1}} + p^{a_{k+2}} \right]$$

e os termos em p^{a_k} cancelam-se. É fácil ver então que

$$\sum_{k=2}^{m} k.s_k = n \left| 2p^{a_1} - p^{a_2} - (m+1)\, p^{a_m} + m\, p^{a_{m+1}} \right| =$$

$$= n \left[2p^{a_1} - p^{a_2} - 1 \right]$$

logo :

$$s_1 = n \left[p^{\sum_{i=1}^{m} i.r_i} - 1 - 2p^{a_1} + p^{a_2} + 1 \right] = n \left[p^{a_0} - 2p^{a_1} + p^{a_2} \right] \square$$

Exemplo II.2.5.- Se tomamos $K = \{0,1\}$, o corpo com dois elementos e $G = \{e, g, g^2, g^3\}$, o grupo cíclico de ordem 4, temos que $U(KG) = U_1(KG) = \{e, g, g^2, g^3, e+g+g^2, e+g+g^3, e+g^2+g^3, g+g^2+g^3\}$

Chamando $G' = \{e, g+ g^2+g^3\}$ vem que $U_1(KG) = G \oplus G'$

logo $U_1(KG) \tilde{=} T_2 \oplus T_2 2$

Usando o teorema acima poderíamos ter calculado :

$a_0 = 2$, $a_1 = 1$, $a_2 = 0$, $a_3 = 0$ e

$s_1 = 1(2^3 - 4 + 1) = 1$

$s_2 = 1(2^1 - 2+1) = 1$

Exemplo II.2.6.- Tomando $K = \{0, 1, 2\}$, o corpo com três elementos e $G = \{e, g, g^2\}$ o grupo cíclico de ordem 4, considerando em U(KG) calculado no exemplo II. 2.4 unica

mente as unidades de índice 1 vem :

$U_1(KG) = \{e, g, g^2, 2e+2g, 2e+2g^2, 2g+2g^2, e+g+2g^2, e+2g+g^2, 2e+g+g^2\}$

Chamando $G' = \{e,\ 2g+2g^2,\ 2e+g+g^2\}$ temos que :

$U_1(KG) = G \oplus G'$ logo $U_1(KG) \cong 2\ T_3$

Usando o teorema acima vem :

$$a_0 = 1,\quad a_1 = 0,\quad a_2 = 0$$

$$s_1 = 1(3^1 - 2 + 1) = 2\ .$$

Em continuação, vamos estudar a estrutura de $U_1(KG)$ quando K é um corpo com p^n elementos e G um grupo abeliano finito qualquer. Para isso, utizaremos o seguinte resultado, devido a Perlis e Walker |26| que enunciamos sem demonstração.

Teorema II.2.3.- Seja K um corpo e G um grupo abeliano finito tal que car $K \nmid |G|$, então:

$$KG \cong \bigoplus_d \frac{n_d}{v_d}\ K(\xi_d)$$

onde d percorre todos os divisores da ordem de G, ξ_d indica uma raíz primitiva d-ésima de 1, n_d indica o número de elementos de ordem d em G e v_d é a dimensão de $K(\xi_d)$ como espaço vetorial sobre K .

Corolário.- Nas condições do teorema acima, e com as mesmas notações, tem-se que: $U(KG) \cong \bigoplus_d \frac{n_d}{v_d}\ K(\xi_d)^*$

onde $K(\xi_d)^* = K(\xi_d) - \{0\}$.

A demonstração segue imediatamente do lema II.1.1.

Teorema II.2.4.- Seja K um corpo com p^n elementos e G um grupo abeliano finito. Escrevendo $G = G_s \oplus G_p$ onde

$p \nmid |G_s|$ e G_p é um p-grupo, então:

$$U(KG) \cong \bigoplus_d \frac{n_d}{v_d} U(K(\xi_d) \cdot G_p)$$

onde d percorre todos os divisores da ordem de G tais que $p \nmid d$ e n_d, v_d estão definidas como no teorema II.2.3 .

Demonstração.-

$$KG \cong (KG_s) \underset{K}{\otimes} (KG_p) \cong \left(\bigoplus_d \frac{n_d}{v_d} K(\xi_d) \right) \underset{K}{\otimes} (KG_p) \cong \bigoplus_d \frac{n_d}{v_d} (K(\xi_d).G_p)$$

Logo, como no teorema II.1.1. temos

$$U(KG) = \bigoplus_d \frac{n_d}{v_d} U(K(\xi_d) \cdot G_p) \qquad \square$$

II - 3 SUBGRUPOS DE G COMO SUBGRUPOS DE U(KG) .

Já observamos que G pode ser considerado como um sub - grupo de U(KG) . Desta forma, todo subgrupo de G é um subgrupo de U(KG) . Nesta seção estudaremos algumas propriedades dos - subgrupos normais de G como subgrupos de U(KG) .

Em primeiro lugar, mostraremos com exemplos que a normalidade de H em G não implica normalidade de H em U(KG) .

Exemplo II.3.1.- Seja D_4 o grupo dihedro de ordem 2, como foi definido no exemplo I.3.4. Então:

$$D_4 = \{e, a, a^2, a^3, b, ab = ba^3, a^2b = ba^2, a^3b = b\,a\}$$

e seja $R_4 = \{e, a, a^2, a^3\}$.

R_4 é um subgrupo de índice 2 de D_4; portanto normal .

Agora, se K é um corpo de característica 2 temos que :

$$(1+a+b)^{-1} = a + a^2 + b + ab + a^3b \quad .$$

Agora :

$$(1+a+b) \,.a.\,(1+a+b)^{-1} = a^3 + b + ab + a^2b + a^3b \notin R_4$$

Exemplo II.3.2.- Sejam D_4 e R_4 como no exemplo anterior e $\mathbb{R}$ o corpo dos números reais .

Calculando diretamente, vem que:

$$(\sqrt{2} + b)(\sqrt{2} - b) = 1 \quad \text{logo}$$

$$\sqrt{2} + b \in U(\mathbb{R}.D_4) \quad \text{e} \quad (\sqrt{2} + b)^{-1} = \sqrt{2} - b \; .$$

Agora: $(\sqrt{2} + b)a(\sqrt{2}-b)^{-1} = 2a-\sqrt{2}\, ab + \sqrt{2}\, a^3b-a^3 \notin R_4$

Voltaremos a nos referir a estes exemplos adiante .

Em certas condições, é possível determinar o normalizante de H em U(KG) .

Teorema II.3.1.- Seja K um corpo de característica p, G um grupo finito e H um p-subgrupo normal de G. Se N(H, U) e C(H, U) indicam o normalizante e o centralizante de H em U(KG) respectivamente, então:

$$N(H,U) = G.\ C(H,\ U)$$

onde $G.C(H,U) = \{x.y \mid x \in G, \quad y \in C(H,U)\}$

Demonstração.-

Mostraremos primeiro que $G.\ C(H,U) \subset N(H,U)$. De fato, sejam

$g \in G$, $z \in C(H,U)$. Então :

$$(gz)\, H(gz)^{-1} = gzHz^{-1}\, g^{-1} = gHg^{-1} = H$$

logo $gz \in N(H,U)$.

Para provar a inclusão em sentido contrário, consideramos um - elemento qualquer $x = \sum_i k_i g_i \in N(H,U)$

Para cada $h_j \in H$ existe um único $h_K \in H$ tal que $xh_k = h_j\, x$ (*)

Sejam então α_j, β_j, γ_j as permutações de G definidas por:

$$\alpha_j(g) = h_j.g,\ \beta_j(g) = g.h_k^{-1}\ ,\ \gamma_j(g) = h_j.g.h_k^{-1}\ ,\ \forall\, g \in G$$

É claro que $\gamma_j = \alpha_j \circ \beta_j = \beta_j \circ \alpha_j$. Além disso, como $o(\alpha_j) = o(h_j)$, $o(\beta_j) = o(h_k)$ são potências de p, a ordem de γ_j é um potência de p .

Seja $S = \{\gamma_j \mid h_j \in H\}$

Mostraremos que S é um p-grupo de permutações de G. De fato, se h_i, h são tais que $xh = h_i\, x$ tem-se que :

$$\gamma_i \circ \gamma_j(g) = h_i h_j\, g\, h_k^{-1} h_m^{-1} = (h_i h_j)\, x (h_m h_k)^{-1}$$

Deveremos provar então que $(h_i h_j)\, x = x(h_m h_k)$. Mas :

$h_i h_j\, x = h_i x h_k = x\, h_m h_k$.

Ainda, é claro que $\gamma_j^{-1}(g) = h_j^{-1}\, g\, h_k \quad \forall g \in G$

De (*) podemos escrever $x = h_i.x\, h_k^{-1}$ e tomando $x = \sum_i k_i g_i$ tem - se $x = \sum_i k_i\, \gamma_j(g_i)$, $\forall\, h_j \in H$,

Se g_r, g_s pertencem a uma mesma órbita das determinadas - por S em G, deve ser $k_r = k_s$. Como S é um p-grupo, toda órbita é de ordem potência de p e, se toda órbita tivesse mais de um elemento, resultaria $\varepsilon(x) = 0$, o que é absurdo, pois $x \in U(KG)$.

Existe, então, algum elemento $g \in G$ tal que $g = h_j g h_k^{-1}$,

$\forall h_j \in H$, isto é : $g^{-1} h_j g = h_k = x^{-1} h_j x$ ou, equivalentemente, $(x g^{-1})h_j = h_j(x g^{-1})$, $\forall h_j \in H$ logo $xg^{-1} \in C(H.U)$

de onde se conclui, facilmente, a tese □

Corolário 1.- (Coleman) - Se G é um p-grupo, tem-se que $N(G,U) = G.Z$, onde Z indica o centro de U(KG)

Demonstração .- Basta observar que $C(G,U) = Z$ e usar o teorema anterior .

Coleman |15| demonstrou que, indicando por U', G' o grupo comutador de U(KG) e G respectivamente, vale $G' = G \cap U'$. Resulta então o seguinte :

Corolário 2 Se G é um p-grupo, H um subgrupo de G, e K um corpo de característica p, vale : $H \cap U' = H \cap G'$

Demonstração

$$H \cap G' = H \cap G \cap U' = H \cap U' \qquad \square$$

Nota.- É fácil ver que C(H,U) é uma subálgebra de KG . Pode-se exibir uma base de C(H,U) sobre K da seguinte forma:

Definimos em G uma relação de equivalência por :

$g_1 \tilde{} g_2$, se e só se, existe $h \in H$ tal que $h^{-1}.g_1.h = g_2$

Chamando $\{C_i\}_{1 \leq i \leq t}$ as classes determinadas por essa relação e $J_i = \sum_{x \in C_i} x$ é fácil ver que $\{J_i\}_{1 \leq i \leq t}$ é uma base de C(H,U) sobre K.

A demonstração é análoga à dada no lema I.2.1.

II - 4. OUTROS SUBGRUPOS DE U(KG)

Nesta seção estudaremos certos subgrupos de U(KG) que podem ser obtidos de forma natural a partir dos subgrupos de G.

Se H é um subgrupo de um grupo finito G e K é um corpo, o grupo U(KH) das unidades do anel do grupo KH pode ser identificado naturalmente a um subgrupo de U(KG) .

Proposição II.4.1.- Nas condições acima $U(KH) = U(KG) \cap KH$

Demonstração.-

É fácil ver que $U(KH) \subset U(KG) \cap KH$. Provaremos a inclusão de sentido contrário .

Seja $\alpha \in U(KG) \cap KH$. Sendo α uma unidade de U(KG) deve existir $\bar{\alpha} \in \bar{U}(KG)$ tal que $\alpha\bar{\alpha} = \bar{\alpha}\alpha = 1$. Sempre é possível escrever $\bar{\alpha}$ na forma $\bar{\alpha} = \alpha_1 + \alpha_2$, onde $\alpha_1 \in KH$ e α_2 é da forma $\alpha_2 = \sum_j k_j g_j$ onde os elementos g_j que comparecem na expressão de α_2 são elementos de G que não pertencem a H .

Agora: $\alpha\bar{\alpha} = \alpha(\alpha_1 + \alpha_2) = \alpha\alpha_1 + \alpha\alpha_2 = 1$

Mas $\alpha\alpha_2$ é da forma $\alpha\alpha_2 = \sum_{ij} k_{ij} h_i g_j$, onde $h_i g_j \notin H$;

logo $\alpha_2 = 0$ e $\alpha\alpha_1 = 1$

Da mesma forma vem que $\alpha_1\alpha = 1$ e α_1 é o inverso de α em U(KH) □

É fácil ver que, se U(KH) é um subgrupo normal de U(KG), então H deve ser um subgrupo normal de G . A recíproca não é, em geral, verdadeira . Ver os exemplos II.3.1. e II.3.2.

Notaremos agora $H = \{h_1, h_2, \ldots, h_m\}$ e seja $Q = \{q_1, q_2, \ldots, q_t\}$ um conjunto completo de representantes das classes laterais à esquerda de G módulo H . Todo elemento de KG pode então ser expresso

na forma $x = \sum_{ij} k_{ij}\, q_i\, h_j$, $k_{ij} \in K$, e definimos :

$$U^*(KH) = \{x \in KG \mid \sum_j k_{1j} \neq 0,\ \sum_j k_{ij} = 0,\ 2 \leq i \leq t\}$$

$$U_1^*(KH) = \{x \in U^*(KH) \mid \varepsilon(x) = 1\}$$

Proposição II.4.2.- Seja K um corpo de característica p, G um p-grupo e H um subgrupo normal de G. Então $U^*(KH)$ e $U_1^*(KH)$ são subgrupos normais de U(KG) e vale:

i) $\dfrac{U(KG)}{U_1^*(KH)} \cong U(KG/H)$.

ii) $\dfrac{U(KG)}{U^*(KH)} \cong U_1(KG/H)$

Demonstração.-

Consideremos a aplicação ϕ: U(KG) → U(KG/H) definida por:

$$\alpha = \sum_i \lambda_i g_i \in U(KG) \xrightarrow{\phi} \phi(\alpha) = \sum_i \lambda_i \bar{g}_i \in U(KG/H) \text{ onde } \bar{g}_i = g_i H$$

É fácil ver que ϕ é um epimorfismo e

$\alpha \in Ker(\phi)$, se e só se, $\phi(\alpha) = 1$, i.é., $\alpha \in U_1^*(KH)$

Logo $U_1^*(KH)$ é um subgrupo normal de U(KG) e vale i) .

Para obter ii) basta definir ψ :U(KG) → $U_1(KG/H)$ por:

$$\alpha = \sum_i \lambda_i g_i \in U(KG) \xrightarrow{\psi} \psi(\alpha) = \frac{\sum_i \lambda_i \bar{g}_i}{\sum_i \lambda_i} \in U(KG/H)$$

e concluir em forma análoga □

Observação.- No caso particular em que H = G, $U_1^*(KG) = U_1(KG)$ e, da proposição acima, vem que $\dfrac{U(KG)}{U_1(KG)} \cong K^*$, o

que é um resultado bem conhecido já que provamos na proposição II.1.2 que $U_*(KG) = U_1(KG) \oplus K^*$.

Corolário.- Nas condições da proposição acima, $U(KG)/U^*(KH)$ é comutativo, se e somente se, H contém o subgrupo comutador G' de G .

Demonstração.- $U(KG)/U^*(KH)$ será comutativo, se e somente se, $U(KG/H)$ o for .

Este grupo é comutativo, se e só se, G/H é abeliano, i. é., se e só se, H contém G' □

Indicando por L(H) o ideal à esquerda de KG associado a H como no início da seção I-4, e por E(H) o conjunto: $E(H) = \{x \in KH \mid \varepsilon(x) \neq 0\}$ podemos dar a seguinte caracterização de $U^*(KH)$ como subconjunto de KG .

Proposição II.4.3.- $U^*(KH) = (E(H) + L(H)) \cap U(KG)$, onde

$$E(H)+L(H) = \{x+y \mid x \in E(H),\ y \in L(H)\}$$

Demonstração.- Dado $\alpha = \sum_{ij} k_{ij} q_i h_j \in U^*(KH)$ podemos escrever:

$$\alpha = \sum_j k_{1j} h_j + \sum_{i=2}^{t} q_i \sum_j k_{ij} h_j = \sum_j k_{1j} h_j + \sum_{i=2}^{t} q_i \left(\sum_j k_{ij} h_j - \sum_j k_{ij}\right) =$$

$$= \sum_j k_{1j} h_j + \sum_{ij} k_{ij} q_i (h_j - 1)$$

onde $\sum_j k_{1j} h_j \in E(H)$ e $\sum_{ij} k_{ij} q_i (h_j - 1) \in (H)$

É fácil verificar, em forma análoga, que dados $x \in E(H)$, $y \in L(H)$ então $x + y \in U^*(KH)$ □

Corolário.- Seja K um corpo de características p e G um p-grupo .

Então:

$$U^*(KH) = U(KH) + \mathcal{L}(H)$$

Observação.- A decomposição de um elemento de $U^*(KH)$ como soma de um elemento de E(H) mais um de $\mathcal{L}(H)$ não é, em geral, única . Basta tomar, por exemplo, $h \in H$ diferente de h_1 e temos $1 = h - (h-1)$ com $h \in E(H)$, $(h-1) \in \mathcal{L}(H)$

Lembramos agora os seguintes fatos, da teoria dos grupos.

Definição II.4.1.- Um grupo G diz-se um produto semidireto de dois grupos H e N se H é normal em G e se verifica:

i) $H \cap N = \{1\}$

ii) $G = H.N$

Um subgrupo N de G diz-se um fator semidireto de G se existe um subgrupo H normal em G tal que G é o produto semidireto de H e N .

Definição II.4.2.- Um grupo G diz-se uma extensão de um grupo N por um grupo H se existe um epimorfismo de G sobre N cujo núcleo é, precisamente, H .

A extensão diz-se uma extensão que cinde se existe um homomorrismo g de N em G tal que fog é a função identidade de N.

Pode-se provar que G é uma extensão que cinde de um grupo N por um grupo H, se e somente se, G é produto semidireto de subgrupos H', N' isomorfos a H e N respectivamente (Ver, por exemplo, Curtis-Reiner |2|)

Teorema II.4.1.- Seja K um corpo de característica prima p e G um p-grupo finito, que é produto direto - de dois subgrupos H e N. Então U(KG) é uma extensão que cinde de U(KN) por $U_1^*(KH)$.

Demonstração.-

Podemos definir um epimorfismo f: U(KG) → U(KN) compondo o epimorfismo ϕ definido na demonstração da proposição II.4.2 com o isomorfismo natural ω: U(K G/H)→U(KN) . Assim

$$x = \sum_{ij} k_{ij}\, n_i h_j \xrightarrow{\ f\ } \sum_i \Big(\sum_j k_{ij}\Big)\, n_i$$

Claramente Ker(f) = $U_1^*(KH)$ e, se g: U(KN) → U(KG) indica a inclusão, é fácil ver que f o g é a função identidade de U(KN) □

Corolário 1.- U(KN) é um fator semidireto de U(KG)

Corolário 2.- Se U(KN) é um subgrupo normal de U(KG), tem-se que $U(KG) = U(KN) \oplus U_1^*(KH)$

Teorema II.4.2.- Seja K um corpo de característica prima p e G = H ⊕ N um p-grupo. Então $U_1(KH) \oplus U_1(KN)$ é uma extensão de $U_1(KG)$ por um certo subgrupo, que notaremos - $U_1(H, N)$.

Demonstração.-

Se β_1:G ⟶H, β_2 : G ⟶N indicam as projeções canônicas, basta - definir o epimorfismo $f = \beta_1 + \beta_2$: $U_1(KG) \to U_1(KH) \oplus U_1(KN)$ como demonstração do teorema II.2.1 e chamar $U_1(H, N) = Ker(f)$.

Notamos ainda que :

$$U_1(H,N) = \Big\{ \sum_{ij} k_{ij}\, n_i h_j \;\Big|\; \sum_j k_{1j} = \sum_i k_{i1} = 1,\ \sum_j k_{ij} = \sum_i k_{ij} = 0,$$

$$2 \leq i \leq |N|\ ,\ 2 \leq j \leq |H| \Big\}$$

Corolário 1.- Nas condições do teorema acima, se G é abeliano, vale:

$$U(KG) = K^* \oplus U_1(H,N) \oplus U_1(KH) \oplus U_1(KN)$$

Corolário 2.- Nas condições do teorema acima, $U_1^*(KH)$ é uma extensão de $U_1(KH)$ por $U_1(H, N)$

A demonstração é inteiramente análoga à do teorema II. 4.1.

Finalmente, daremos uma condição para que $U_1(KH)$ seja um subgrupo normal de $U(KG)$.

Teorema II.4.3.- Seja K um corpo de característica prima p e $G = H \oplus N$ um p-grupo, com H e N não triviais. Então $U_1(KH)$ é um subgrupo normal de U(KG), se e somente se, H é abeliano .

Demonstração.-

Se H é abeliano, está contido no centro de G; portanto, U(KG) está contido no centro de U(KG) e, consequentemente, é um subgrupo normal.

Suponhamos agora U(KH) normal em U(KG) . Então, U(KH) também é normal em $U_1^*(KH)$ e, do corolário 2 acima, temos que:

$$U_1^*(KH) = U_1(KH) \oplus U_1(H, N)$$

e todo elemento de $U_1(H, N)$ deve comutar com todo elemento de $U_1(KH)$. Mostraremos então que se H não é abeliano, tal coisa não é verdadeira .

Para isso estudaremos dois casos .

Se car $K \neq 2$, sejam $h, h' \in H$ tais que $h.h' \neq h'.h$ e $n \in N$, $n \neq 1$

Então $\alpha = 1/2 + 1/2\ h + 1/2n - 1/2\ nh$ pertence a $U(H, N)$ e

$$\alpha h' = 1/2\ h' + 1/2\ hh' + 1/2\ nh' - 1/2\ nhh'$$

$$h'\alpha = 1/2\ h' + 1/2\ h'h + 1/2\ nh' - 1/2\ nh'h$$

Logo $\alpha h' \neq h'\alpha$

Se car $K = 2$ tomamos h, h' e n como acima e $\alpha = h+n + nh$

Então $\alpha \in U(H,N)$ e

$$h'\alpha = h'h + nh' + nh'h$$

$$\alpha h' = hh' + nh' + nhh'$$

Logo : $\alpha h' \neq h'\alpha$ □

- // -

CAPÍTULO III

NILPOTÊNCIA

Em |13| J.M. Bateman e D.B. Coleman deram uma condição necessária e suficiente para que o grupo das unidades de um anel de grupo KG - onde K é um corpo e G um grupo finito - seja nilpotente .

A demonstração estava baseada no lema III.1.2. que damos neste capítulo, mas este continha um pequeno erro na sua formulação; que foi corrigido posteriormente pelo próprio Bateman em |12| .

Independentemente, K. Motose e H. Tominaga deram em |24| outra correção do lema - o lema III.1.3. nesta exposição que permitia extender os resultados a anéis de grupo SG, onde o anel de coeficiente é um anel semisimples artiniano.

Finalmente, usando o lema de Motose-Tominaga, e outros resultados, pudemos estender o teorema para aneis de grupo com coeficientes num anel de integridade qualquer.

Daremos aqui a demonstração original de Bateman-Coleman para anéis de grupo com coeficientes num corpo, e usaremos o nosso resultado para obter uma demonstração mais simples do teorema de Motose-Tominaga .

Neste capítulo usamos livremente vários resultados sobre grupos nilpotentes. Uma referência standard ao respeito é J.J. Rotman: The theory of groups: an introduction Allyn and Bacon, Boston, 1965 .

III.1 ALGUNS LEMAS

Nesta seção usaremos as seguintes notações. Se R é um anel, dados $x, y \in R$ notaremos $|x, y| = xy-yx$ e dados n ele -

mentos $x_1,\ldots, x_n \in R$ notaremos $|x_1,\ldots x_n| = ||x_1,\ldots, x_{n-1}|, x_n|$
Da mesma forma, dados $x, y \in U(R)$ notaremos $(x,y) = x^{-1}y^{-1}xy$ e dados $x_1,\ldots, x_n \in U(R)$ notaremos $(x_1,\ldots, x_n) = ((x_1,\ldots,x_{n-1}),x_n)$

Lema III.1.1.- Seja R um anel, $n>1$ um inteiro e $x_1,\ldots,x_n \in U(R)$
Então, vale a fórmula:

$$(x_1,\ldots,x_n) = 1 + (x_1,\ldots, x_{n-1})^{-1}.x_n^{-1}.|(x_1,\ldots,x_{n-1}), x_n|$$

Demonstração.-

$$(x_1,\ldots,x_{n-1})^{-1}.x_n^{-1}|(x_1,\ldots,x_{n-1}),x_n| =$$

$$(x_1,\ldots,x_{n-1})^{-1}.x_n^{-1}((x_1,\ldots,x_{n-1})x_n - x_n(x_1,\ldots,x_{n-1})) =$$

$$= (x_1,\ldots,x_{n-1})^{-1}.x_n^{-1}(x_1,\ldots, x_{n-1})x_n - 1 = (x_1,\ldots,x_n) - 1 \square$$

Lema III.1.2.-(Bateman-Coleman).- Seja N um ideal bilateral nilpotente de índice a, de um anel R . Então o conjunto 1+N é um subgrupo normal nilpotente de U(R) de classe $c \leq a$. Se R é uma álgebra sobre um corpo F de característica p, então 1+N é um p-grupo que admite um expoente(i.e., existe um inteiro $n \geq 1$ tal que, para todo $x \in 1+N$, $x^n = 1$)

Demonstração.-

Do lema II.1.2. vem que 1+N é um subgrupo de U(R) . Dados $n \in N$ e $x \in U(R)$ temos:
$x^{-1}(1+n)x = 1+x^{-1}.n.x \in 1+N$ logo, 1+N é normal em U(R) .

Para provar a nilpotência mostraremos previamente que dados $x_1,\ldots,x_k \in 1+N$ então $(x_1,\ldots,x_k)-1 \in N^{k-1}$. Para isso faremos indução em k .

Se x_1, $x_2 \in 1+N$ então $(x_1,x_2) \in 1+N$ e $(x_1,x_2) -1 \in N$

Agora, supondo que $(x_1,\ldots,x_{k-1}) -1 \in N^{k-2}$ e escrevendo x_k na forma $x_k = 1 + n$, com $n \in N$ temos :

$$|(x_1,\ldots, x_{k-1}), 1+n| = |(x_1,\ldots,x_{k-1}), n| =$$

$$|(x_1,\ldots,x_{k-1})-1,n| \in N^{k-1}$$

Como N^{k-1} é um ideal, usando o lema III.1.1. temos :

$$(x_1,\ldots,x_k)-1=(x_1,\ldots,x_{k-1})^{-1}.x_k^{-1}.|(x_1,\ldots,x_{k-1}),x_k| \in N^{k-1}$$

Agora, tomando k=a+1 temos que, para todos $x_1\ldots,x_k \in 1+N$ $(x_1,..,x_k)-1 \in N^a =(0)$, logo $1+N$ é nilpotente de classe $c \leq a$.

Suponhamos ainda R uma F-álgebra e seja $e=\min\{m \mid p^m \geq a\}$. Dado $n \in N$ temos que $(1+n)^{p^e} = 1+n^{p^e} = 1$. Logo, $1+N$ é um p-grupo, com expoente. □

Na publicação original |13| o lema enunciava que, sob as mesmas hipóteses, se ainda R/N é comutativo, então U(R) é um grupo nilpotente. Para mostrar que nessa generalidade o lema é falso, Motose-Tominaga deram o seguinte exemplo .

Exemplo III.1.1.- Seja $D=\mathbb{Q}+\mathbb{Q}i+\mathbb{Q}j+\mathbb{Q}k$ a álgebra dos quatérnios racionais, e

$$R = \left\{ \begin{bmatrix} a & o \\ d & a \end{bmatrix} \mid d \in D,\ a \in \mathbb{Q}+\mathbb{Q}i \right\}$$

$$N = \left\{ \begin{bmatrix} o & o \\ d & o \end{bmatrix} \mid d \in D \right\}$$

Então é fácil verificar que:

i) N é ideal bilateral de R

ii) $N^2=0$; logo, N é nilpotente .

iii) R/N é comutativo .

Ainda, se n é um inteiro positivo arbitrário, é fácil ver que:

$$\begin{bmatrix}1 & 0\\ n_j & 1\end{bmatrix}\begin{bmatrix}i & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}1 & 0\\ n_j & 1\end{bmatrix}^{-1}\begin{bmatrix}i & 0\\ 0 & i\end{bmatrix}^{-1} = \begin{bmatrix}1 & 0\\ 2nj & 1\end{bmatrix}$$

Portanto U(R) não pode ser um grupo nilpotente

Lema III.1.3.- (Motose - Tominaga) Seja N um ideal bilateral nilpotente de um anel com unidade R. Se R/N é comutativo e $|N,R| = \{xy-yx \mid x\in N,\ y\in R\}$ está contido em N^2, então U(R) é um grupo nilpotente.

Demonstração

Mostraremos inicialmente que $|N^k, R| \subset N^{k+1}$ por indução em k.
A proposição é verdadeira para k=1 por hipótese.
Sejam então $x_1,\ldots,x_k \in N$ e $s\in R$. Será suficiente provar que

$$|x_1\ldots,x_k,s| \quad N^{k+1}$$

Agora $|x_1\ldots x_k,s| = |x_1\ldots x_k|s-s|x_1\ldots,x_k| =$
$= x_1\ldots x_k.s-x_kx_1\ldots x_{k-1}.s-s.x_1\ldots x_k+s.x_kx_1\ldots x_{k-1}$
Como R/N é comutativo, existe $n\in N$ tal que $\begin{cases} sx_1 = x_1 s+n \\ sx_k = x_k s+n' \end{cases}$
Temos entao:

$$|n_1,\ldots, n_k,s| = x_1(x_2\ldots x_k s-sx_2\ldots x_k)+nx_2\ldots x_k - x_k(x_1\ldots x_{k-1}s-sx_1\ldots x_{k-1})+n'x_1\ldots x_{k-1}\in N^k$$

Usando a fórmula do lema III.1.1 vem agora que $(x_1,\ldots,x_k)$-$-1 \in N^{k-1}$ e podemos concluir a demonstração como no lema anterior □.

Motose e Tominaga também mostravam que o recíproco do lema III.1.3 é falso. Para isso, deram o seguinte exemplo.

Exemplo III.1.2.- Seja $K = \{0,1\}$, o corpo com 2 elementos, e

$$R=\left\{\begin{vmatrix} a & 0 \\ b & c \end{vmatrix} \;\middle|\; a,b,c \in K\right\}$$

Os ideais maximais de R são :

$$I_1=\left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \mid a,b \in K\right\}$$

$$I_2=\left\{\begin{bmatrix} 0 & 0 \\ b & c \end{bmatrix} \mid b,c,\in \right\}$$

Logo, o radical de Jacobson de R é:

$$J(R)= \left\{\begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix} \mid b\in K\right\}$$

Agora é fácil ver que $R/J(R) \cong K \oplus K$ logo comutativo e que $U(R) =\left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\right\}$ é comutativo, logo nilpotente. Mas:

$$|J(R), R| \neq 0 = N^2$$

II - 2 O TEOREMA DE BATEMAN - COLEMAN

Proposição III.2.1- Seja K um corpo de característica p e G um p-grupo. Então o grupo das unidades do anel - de grupo KG é nilpotente .

Demonstração.-

Seja K um corpo de característica prima p e G um p-grupo. Da - proposição II.1.2 temos que $U(KG) = K^* \oplus U_1(KG)$.

Ainda, da demonstração do teorema II.1.2. vem que

$$U_1(KG) = 1 + J(KG)$$

Agora, do lema III.1.2, $U_1(KG)$ é nilpotente e, portanto, U(KG) também o é □

Teorema III.2.1.- Seja K um corpo e G um grupo finito. Então - U(KG) é nilpotente, se e somente se, alguma das seguintes condições estiver verificada .

i) G é abeliano

ii) K é de característica prima p e G é um grupo nilpotente - tal que, para todo primo $q \neq p$ o q-subgrupo de Sylow de G é abeliano .

Demonstração.-

Se a hipótese i) estiver verificada, U(KG) é abeliano; portanto, nilpotente.

Se a hipótese ii) estiver verificada, podemos escrever G na forma $G = P \oplus N$, onde P é um p-grupo e N é um subgrupo abeliano tal - que $p \nmid |N|$

Então:

$$KG \cong KP \underset{K}{\otimes} KN \cong KP \underset{K}{\otimes} (K_1 \oplus \ldots \oplus K_t)$$

onde $K_1, \ldots, K_t$ são extensões de K (conforme ao exemplo II.1.4)

Logo:

$$KG \cong (KP \underset{K}{\otimes} K_1) \oplus \ldots \oplus (KP \underset{K}{\otimes} K_t) \cong K_1P \oplus \ldots \oplus K_tP$$

Então:

$$U(KG) \cong U(K_1P) \oplus \ldots \oplus U(K_tP)$$

Como cada anel de grupo K_iP, $1 \leq i \leq t$, está nas condições da proposição anterior, U(KG) é soma direta de grupos nilpotentes; portanto, nilpotente.

Para provar o recíproco, suponhamos inicialmente que - $\text{car } K \nmid |G|$

Então, do teorema II.1.1 temos que U(KG) é da forma:

$$U(KG) \cong GL(n_1, D_1) \oplus \ldots \oplus GL(n_t, D_t)$$

onde os D_i são anéis com divisão, $1 \leq i \leq t$.

Se U(KG) é nilpotente, cada $GL(n_i, D_i)$ deve ser nilpotente. Agora, e sabido que, se $n>1$ e D é um anel com divisão, GL(n,D) não é nilpotente (ver porexemplo, Artin E, Geometric Algebra,Interscience, New York, 1966) .

Ainda, L.K. Hua provou em |23| que um anel com divisão D não é solúvel se D não é comutativo (pode-se ver também Scott |31|); logo, cada D_i é comutativo $1 \leq i \leq t$ e

$$G \subset KG \cong D_1 \oplus \ldots \oplus D_t \text{ é abeliano .}$$

Finalmente, suponhamos que car $K \nmid |G|$. Como G é um subgrupo de U(KG), deve ser nilpotente. Ainda, se H é um q-subgrupo de Sylow de G, $q \neq$ car K, U(KH) sendo um subgrupo de U(KG) também é nilpotente e, do caso anterior, H deve ser abeliano □

III - 3. ANÉIS DE GRUPO COM COEFICIENTES NUM DOMÍNIO DE INTEGRIDADE

Nesta seção vamos demonstrar que vale um resultado inteiramente análogo ao teorema de Bateman-Coleman, quando os coeficientes se tomam num domínio de integridade .

Proposição III.3.1.- Seja R um domínio de integridade e G um grupo finito, tal que car $R \nmid |G|$. Se o grupo de unidades U(RG) é nilpotente, então G é comutativo .

Demonstração.- Seja K o corpo de quocientes de R. Então temos:

$$RG \subset KG \cong M_{n_1}(D_1) \oplus \ldots \oplus M_{n_t}(D_t)$$

$$U(RG) \subset U(KG) \cong GL(n_1, D_1) \oplus \ldots \oplus GL(n_t, D_t)$$

Notaremos por $p_h : KG \to M_{n_h}(D_h)$ as compostas do isomorfismo acima com as projeções naturais.

Mostraremos, inicialmente, que dado $\alpha_h \in M_{n_h}(D_h)$ sempre existem $x \in U(RG)$ e algum $b \in R$ tais que $p_h(x) = b\alpha_h$.

De fato, sempre existe $y = \sum_{i=1}^{|G|} k_i g_i \in U(KG)$ tal que $p_h(y) = \alpha_h$

Escrevendo $k_i = a_i/b_i$ com $a_i b_i \in R$ $1 \leq i \leq |G|$ e $b = \prod_i b_i$ temos que $b \in R$ e $x = by \in RG$ é tal que $p_h(x) = b\alpha_h$.

Agora mostraremos que cada somando $GL(n_h, D_h)$ deve ser nilpotente.

De fato, como $U(RG)$ é nilpotente, existe um inteiro $n>1$ tal que, para todos $x_1, \ldots, x_n \in U(RG)$ vale $(x_1, \ldots x_n) = 1$.

Dados $\alpha_h^1, \ldots, \alpha_h^n \in GL(n_h, D_h)$, determinamos $x_1, \ldots x_n \in U(RG)$ e $b_1, \ldots, b_n \in R$ tais que $p_h(x_i) = k_i \alpha_h^i$, $1 \leq i \leq n$.

Então: $1 = p_h(x_1, \ldots, x_n) = (k_1 \alpha_h^1, \ldots, k_n \alpha_h^n) = (\alpha_h^1, \ldots, \alpha_h^n)$

Logo $GL(n_h, D_h)$ é nilpotente .

A demonstração se conclui agora como no teorema II.2.1 □

Para a nossa próxima proposição vamos precisar do resultado que enunciamos a seguir .

Lema III.3.1.- (I. Herstein, L. Small, |21|) . Seja A uma algebra sobre um anel R, que é finitamente gerado como R-módulo . Se A tem um conjunto de geradores, cada um dos quais é nilpotente, então A é nilpotente .

Proposição III.3.2.- Seja R um anel comutativo, de característica prima p e $G = P \oplus N$ um grupo finito tal que P é um p-grupo, $p \nmid |N|$ e N é abeliano. Então U(RG) é um grupo nilpotente.

Demonstração.-

O homomorfismo canônico $\omega: G \to N$ induz um epimorfismo $f: KG \to KN$.

Escrevendo $H = \{h_1, \ldots, h_r\}$ e $N = \{n_1, \ldots, n_s\}$ todo elemento de KG é da forma $x = \sum_{ij} k_{ij} n_i h_j$ e temos:

$$f(x) = \sum_{i=1}^{s} \left(\sum_{j=1}^{r} k_{ij} \right) n_i$$

Como $KG/Ker(f) \cong KN$ é abeliano, bastará provar que Ker(f) é nilpotente e $|Ker(f), KG| \subset Ker(f)^2$ para obter a tese, a partir do lema III.1.3.

Dado $x = \sum_{ij} k_{ij} n_i h_j \in Ker(f)$ temos :

$$x = \sum_{ij} k_{ij} n_i h_j - \sum_{i} \left(\sum_{j} k_{ij} \right) n_i = \sum_{ij} k_{ij} n_i (h_j - 1)$$

Logo o conjunto $n_i(h_j-1)$ $1 \leq i \leq s$, $2 \leq j \leq r$ é um conjunto de geradores de Ker(f) sobre K.

Ainda, se $p^e = r$ é a ordem de P: $(n_i(h_j-1))^{p^e} (h_j-1)^{p^e} =$

$$= n_i^{p^e} (h_j^{p^e} - 1) = 0$$

Do lema III.3.1, Ker(f) é nilpotente.

Finalmente, seja $x \in Ker(f)$ e $y = \sum_{ij} k_{ij} n_i h_j$ um elemento de KG . Chamando $\sum_{j} k_{ij} = \lambda_i$ $1 \leq i \leq s$ podemos escrever $y = u+v$, onde

$$u = \sum_{i=1}^{s} \lambda_i n_i \in Centro(KG) \text{ e } v = \sum_{ij} k_{ij} n_i h_j - \sum_{i} \lambda_i n_i \in Ker(f)$$

Agora: $|x, y| = |x, u+v| = xv - vx \in Ker(f)^2$ □

Estamos agora em condições de enunciar:

Teorema III.3.1.- Seja R um anel de integridade e G um grupo finito. Então U(RG) é nilpotente, se e somente se, alguma das seguintes condições estiver verificada .

i) G é abeliano

i) R é de característica prima p e G é um grupo nilpotente - tal que, para todo primo q ≠ p o q-subgrupo de Sylow de G é abeliano .

Demonstração

A hipótese i) novamente implica que U(KG) é abeliano; portanto nilpotente.

Se a hipótese ii) estiver verificada, U(KG) é nilpotente, a - partir da proposição anterior.

Para o recíproco basta usar a proposição III.3.1 no caso em que car R $\nmid$ |G| e um raciocínio análogo ao empregado no teorema III. 2.1, se car R | |G| □

Finalmente, usando nosso resultado daremos uma demons - tração de um dos resultados de Motose- Tominaga :

Teorema III.3.2.- Seja S um anel semisimples artiniano e G um grupo finito. Então U(SG) é nilpotente, se e somente se, S é comutativo e i) G é abeliano ou ii) S é de característica prima p e G é um grupo nilpotente tal que, para - todo primo q ≠ p o q-subgrupo de Sylow de G é abeliano.

Demonstração.-

Se S é comutativo e G verifica as condições i) ou ii) a demonstração se conduz como antes, usando a proposição III.3.2 .

Suponhamos agora S semisimples artiniano, tal que U(SG) é nilpotente.

I.G. Connell provou em |18| que se S é semisimples artiniano e G é finito, então SG é semisimples . Do teorema de Wedderburn:

$$SG \cong M_{n_1}(D_1) \oplus \ldots \oplus M_{n_t}(D_t)$$

com D_i anéis com divisão, $1 \leq i \leq t$.

Agora, o fato de U(SG) ser nilpotente permite concluir como no teorema II.2.1 que cada D_i é comutativo, $1 \leq i \leq t$, e

$$SG \cong D_1 \oplus \ldots \oplus D_t$$

Portanto S e G são comutativos □

- // - ⌟

BIBLIOGRAFIA

TEXTOS

|1| BOURBAKI, N. - Algèbre, Chap. VIII "Modules et anneaux semisimples" Hermann, Paris 1958

|2| CURTIS C., REINER I.- Representation theory of finite groups and associative algebras. Interscience, New - York, 1962

|3| HERSTEIN I. - Non Commutative Rings . John Wiley, New - York, 1968

|4| - _____ - Tópicos de Algebra . Editora da Universidade de São Paulo e Polígono, São Paulo, 1970

|5| JACY MONTEIRO, L.H. - Elementos de Álgebra . Ao Livro - Técnico e Editora da Universidade de São Paulo. São - Paulo, 1969

|6| _____. - Teoría de Galois - 7º Colóquio Brasileiro de Matemática, Poços de Caldas, 1969

|7| JONES, A. - Representações de Grupos Finitos - Notas de Aulas, Instituto de Matemática e Estatística da U:S.P. São Paulo, 1970

|8| - LAMBEK, J. - Lectures on Rings and Modules . Blaidell, Waltham 1968

|9| POLCINO, C. - Representações de Grupos Finitos . Notas de aula - I.M.E. São Paulo, 1972 .

|10| _____ - Anéis e Módulos . Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo . (No prelo)

|10| RIBEMBOIM, P. - Rings and Modules. Interscience, New -

ARTIGOS

|12| BATEMAN, J.M. - On the Solvability of the Unit Groups of Group Algebras. Trans. Amer. Math. Soc. 157 (1971)

|13| BATEMAN, J.M - COLEMAN, D.B. - Group algebras with nil-potent unit groups. Proc. Amer. Math. Soc. 19, 2 (1968) 448-449

|14| COLEMAN, D.B. - Finite groups with isomorfic group álge-bras . Trans. Amer. Math. Soc. 105, 1(1962) 1-8

|15| ———————— - On the modular group ring of a p-group. Proc. Amer. Math. Soc. 15,4 (1964) 511 - 514

|16| ———————— - Idempotents in group rings. Proc. Amer. Math. Soc. 17, 4 (1966) 962

|17| ———————— - On group rings . Can. J. Math, XXII, 2(1970) 249 - 254

|18| CONNELL, I. G. - On the group ring . Can. J. Math XV . (1963) 650 - 685 .

|19| DESKINS, W. E. - Finite abelian groups with isomorfic group álgebras . Duke Math. J. 23(1956) 35-40

|20| GULLIKSEN T., WISWANATHAN T.RIBEMBOIM, P. - An element-ary note on group rings, Jour. reine angew . Math.

|21| HERSTEIN, I., Small L. - Nil rings satisfying certain chain conditions: an addendum - Canad. J. Math 18 (1966) 300-302

|22| HIGMAN, G. - The units of group rings. Proc. Lon. Math. Soc. 2, 46(1940) 231-248

|23| HUA, L. K. - On the multiplicative groups of a field. Acad. Sin. Science Record 3(1950) 1-6

|24| MOTOSE, K - TOMINAGA M. - Group rings with nilpotent unit groups Math. J. Okayama Univ. 14(1969) 43-46

|25| ———————— - Group rings with solvable - unit groups.Math J. Okayama Univ. 15(1971) 37-41

|26| PERLIS, S. - WALKER, G.L. - Abelian group algebras of finite order.Trans. Amer. Math. Soc. 68(1950) 420-426

|27| RAGGI, Cardenas F. - Las unidades en anillos de grupos- I. Anal. Inst. Mat. Univ. Nac. Aut. Mex 7(1967) 27-34

|28| ———————— - Las unidades en anillos de grupos II Anal. Inst. Mat. Univ. Nac. Aut. Mex 8(1968) 91-103

|29| ———————— - Las unidades en anillos de grupos con coeficientes en $K_p n$, $\mathbb{Z}_p n$, $\hat{\mathbb{Z}}_p$. Anal. Inst. Mat. Univ. Nac. Aut. Mex. 10(1970) 29-65

|30| REINER,I. - A survey of integral representation theory. Bull. Amer. Math. Soc. 76(1970) 159-227

|31| SCOTT, W. R. - On the multiplicative group of a division ring. Proc. Amer. Math. Soc. 8(1957) 303-305

- o0o -