O PROBLEMA DO ISOMORFISMO
PARA ÁLGEBRAS DE GRUPOS
Luiz Gonzaga Xavier de Barros

Tese apresentada ao
Instituto de Matemática e Estatística
da

Universidade de São Paulo
para obtenção do grau de
Mestre em Matemática

Orientador: Prof. Dr. Alfredo Rosálio Jones Rodriguez

Durante a elaboração deste trabalho o autor recebeu apoio financeiro do BNDE, contratos FUNTEC nº 154 e FINEP convênio 184/C.T.

Dezembro de 1974

São Paulo

À memória do Prof.

Dr. Carlos Benjamin de Lyra

A G R A D E C I M E N T O S

Agradeço:

ã Profa. Ofélia Teresa Alas Rossi por ter me iniciado na pós-graduação;

ao colega César Polcino Milies por ter me incentivado no estudo da Álgebra;

ao Prof. Alfredo R. Jones pela paciente e constante orientação na elaboração deste trabalho;

aos colegas e funcionários do IME-USP, que de um modo geral me ajudaram no preparo desta dissertação.

L.G.X.E.

I N T R O D U Ç Ã O

A álgebra de grupo RG do grupo finito G em relação ao anel comutativo com unidade R é o R -módulo das combinações lineares formais (com coeficientes em R) dos elementos de G .

$$RG = \left\{ \sum_{g \in G} a_g \cdot g \mid a_g \in R \right\}$$

cuja estrutura de álgebra é dada por

$$\left(\sum_{g \in G} a_g \cdot g \right) \left(\sum_{h \in G} b_h \cdot h \right) = \sum_{g, h \in G} (a_g b_h) (g h)$$

Claramente RG é uma álgebra com elemento unidade. A aplicação $G \longrightarrow RG : g \longmapsto 1 \cdot g$ é um monomorfismo que leva G sobre uma R -base de RG , o que permite considerar G como uma R -base de RG .

O problema do isomorfismo de álgebras de grupos admite diferentes versões. Em 1947, na conferência de Álgebra de Michigan, R.M. Thrall colocou o seguinte problema: "dados o grupo G e o corpo F , determinar todos os grupos H tais que $FG \cong FH$ ". Em 1950, S. Perlis e G.L. Walker [22] recolocaram o problema do isomorfismo de álgebras de grupo da seguinte maneira: "se G e H são grupos de ordem finita n , encontrar os corpos F tais que $FG \cong FH$ ".

Se G e H são grupos isomorfos e R é um anel comutativo com elemento unidade, então RG e RH são álgebras isomorfas.

Mas grupos não isomorfos podem ter álgebras de grupo / isomorfas. Por exemplo, se G e H são grupos abelianos finitos de mesma ordem então $\mathbb{C}G \cong \mathbb{C}H$, conforme se vê do teorema 1.1.2 (Wedderburn).

Neste trabalho, estaremos então estudando a seguinte / versão do problema do isomorfismo: "se G e H são grupos finitos de mesma ordem encontrar corpos F tais que $FG \cong FH$ implica $G \cong H$ ". Se F é um corpo que obedece essa condição diremos que o teorema / do isomorfismo vale para F .

É conhecido que se G e H são grupos abelianos finitos tais que $\mathbb{Z}G \cong \mathbb{Z}H$ então $G \cong H$ (conforme G. Higman [13], C.W. / Curtis e I. Reiner [9]). O problema do isomorfismo das $\mathbb{Z}$ - álgebras de grupo está em aberto para os grupos finitos não-abelianos. J.A. Cohn e D. Livingstone [6] (1963) provaram que as $\mathbb{Z}$ - álgebras dos dois grupos não abelianos de ordem p^3 , p primo $\neq 2$, não são iso - morfas. Outros resultados concernentes às álgebras de grupo em relação a $\mathbb{Z}$, ou, mais geral, aos anéis de inteiros algébricos de um corpo de números algébricos podem ser encontrados na bibliogra - fia de C.W. Curtis e I. Reiner [9] e nos artigos de D.B. Coleman [8] (1962), J.A. Cohn e D. Livingstone [7] (1965), D.S. Passman [20] e T. Obayashi [19] (1966).

Aqui trataremos apenas das álgebras de grupo em rela - ção a um corpo.

S. Perlis e G.L. Walker [22] (1950) estudaram o proble

ma do isomorfismo de álgebras de grupo quando G e H são grupos abelianos finitos e F é um corpo cuja característica não divide a ordem de G . Eles demonstraram que se G e H são grupos abelianos finitos, então $\mathbb{Q}G \cong \mathbb{Q}H \implies G \cong H$.

No capítulo II, demonstraremos que se G e H são grupos abelianos de ordem divisor de n e o polinômio ciclotômico de ordem n , $\phi_n(X)$, é irredutível no corpo F , então $FG \cong FH \implies G \cong H$.

Como caso particular tiraremos o resultado de S. Perlis e G.L. Walker. Esse teorema é devido a S.K. Sehgal [26] (1970), mas nós procuramos uma demonstração diferente daquela do seu artigo, usando um teorema de redução (teorema 2.2.4) devido a D.E. Cohen [5].

O resultado de S. Perlis e G.L. Walker não é válido no caso de grupos finitos não abelianos. Com efeito, S.D. Berman [2] (1955) provou que as $\mathbb{Q}$ -álgebras dos dois grupos não abelianos de ordem p^3 , com p primo $\neq 2$, são isomorfas. (É interessante comparar com o resultado de J.A. Cohn e D. Livingstone [6] (1963), já citado, referente ao problema das $\mathbb{Z}$ -álgebras desses mesmos grupos). Nesse artigo S.D. Berman provou também que se G e H são grupos hamiltonianos então $\mathbb{Q}G \cong \mathbb{Q}H \implies G \cong H$. Muito depois, D.S. Passman [20] (1965) obteve o seguinte resultado: se a característica do corpo F não é o número primo p , então existem pelo menos $p^2(n^3 - 17n^2)/27$ grupos não isomorfos de ordem p^n tendo as F -álgebras isomorfas. Nesse mesmo trabalho demonstrou que se $\mathbb{Q}G$ é isomorfo a $\mathbb{Q}H$; então para todo corpo F cuja característica não di-

vide a ordem de G , as álgebras FG e FH são isomorfas. Estes resultados de D.S.Passman serão demonstrados no capítulo III.

Quando a característica do corpo F divide a ordem do grupo G , o procedimento é completamente distinto, pois a álgebra FG não será semisimples. W.E.Deskins [10] (1956) provou que as álgebras FP e FP' dos p -grupos abelianos finitos P e P' em relação ao corpo F de característica p são isomorfas se e somente se P e P' são grupos isomorfos. O problema ficou em aberto para p -grupos não abelianos. O teorema de Deskins foi generalizado para: se G e H são p -grupos finitos e F é um corpo de característica p tais que $FG \cong FH$, então:

i) o centro de G é isomorfo ao centro de H (H.N.Ward [27] (1961), D.S. Passman [21] (1965), S.K.Sehgal [25] (1967))

ii) $G/G' \cong H/H'$ (H.N.Ward [27], D.S.Passman [21]).

No capítulo IV estudaremos alguns casos específicos, onde a característica do corpo divide a ordem do grupo não abeliano. São resultados que aparecem em R. Holvoet [15] (1968). De uma forma mais geral, D.S.Passman [21] mostrou que o teorema do isomorfismo vale para F_p com G um p -grupo tal que $|G| \leq p^4$.

São Paulo, dezembro de 1974

Luiz Gonzaga Xavier de Barros

Í N D I C E

Capítulo I - Preliminares

- 1.1. Dois teoremas básicos pag. 1
- 1.2. Corpos de decomposição pag. 2
- 1.3. Um resultado sobre grupos abelianos pag.13

Capítulo II - O problema do isomorfismo para álgebras de grupos abelianos

- 2.1. Estrutura das álgebras semisimples comutativas pag.14
- 2.2. Um teorema de redução pag.20
- 2.3. Uma classe de corpos para os quais vale o teorema do isomorfismo pag.29

Capítulo III - O problema do isomorfismo para álgebras de grupos quaisquer

- 3.1. Alguns resultados pag.36
- 3.2. Contra-exemplos com p-grupos pag.40

Capítulo IV - Álgebras de grupo sobre corpos cuja característica divide a ordem do grupo

- 4.1. As álgebras dos grupos diedrais e dos grupos quaterniônicos pag.55
- 4.2. As $\mathbb{Z}_2$ - álgebras dos grupos não abelianos de ordem 8 pag.58
- 4.3. As álgebras dos grupos não abelianos de ordem 12 relativamente a $\mathbb{Z}_2$ e $\mathbb{Z}_3$ pag.60
- 4.4. As $\mathbb{Z}_2$ - álgebras dos grupos não abelianos de ordem 16 pag.63

CAPÍTULO I - PRELIMINARES

1.1. DOIS TEOREMAS BÁSICOS.

Sabemos que a álgebra KG está relacionada com as representações de G sobre K . Todas essas relações e propriedades podem ser encontradas em C.W. Curtis e I.Reiner [9] e C. Polcino Milies [23], capítulos I e II, mas queremos realçar aqui dois teoremas básicos:

Teorema 1.1.1 - (Maschke): Seja K um corpo e G um grupo finito. Então KG é semisimples se e somente se $\text{car } K \nmid |G|$.

Teorema 1.1.2 - (Wedderburn): Se A é uma álgebra semisimples artimária sobre um corpo K então:

i) A tem um número finito de componentes simples $B_1, \dots, B_s$; cada ideal bilateral de A é da forma $B_{i_1} \oplus \dots \oplus B_{i_t}$ com $1 \leq i_1 < \dots < i_t \leq s$ e, em particular, $A = B_1 \oplus \dots \oplus B_s$.

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

iii) Cada componente simples B_i é isomorfa a uma álgebra de matrizes $M_{n_i}(D_i)$, onde D_i é um anel com divisão, que estende K e n_i é o número de ideais à esquerda minimais que aparecem na decomposição de B_i .

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

no isomorfismo $A \cong M_{n_1}(D_1) \oplus \dots \oplus M_{n_s}(D_s)$, o elemento α corresponde a um elemento $(p_1, \dots, p_s)$. Define-se então $\alpha \cdot (d_1, \dots, d_{n_i})$

como sendo o produto de matrizes $P_i \cdot \begin{bmatrix} d_1 \\ \vdots \\ d_{n_i} \end{bmatrix}$.

Além disso, $M_1 \oplus \dots \oplus M_s$ é um A -módulo completamente redutível fiel e reciprocamente, toda álgebra A de dimensão finita sobre K que tem um módulo completamente redutível fiel é semisimples.

1.2. CORPOS DE DECOMPOSIÇÃO.

Seja A uma álgebra sobre um corpo K , e seja E um corpo, extensão de K . Se T é uma representação de A sobre K , obviamente T é também uma representação de A sobre E . Na verdade, podemos introduzir a álgebra $A^E = A \otimes_K E$, que é uma álgebra sobre E , iden-

tificamos A como uma subálgebra de A^E através do monomorfismo $a \longmapsto a \otimes 1$, $a \in A$. Então A^E consiste nas combinações E -lineares $\sum e_i a_i$ dos elementos de A , e podemos estender T a uma representação T^E de A^E sobre E , pondo $T^E(\sum e_i a_i) = \sum e_i T(a_i)$, $e_i \in E$.

Notamos que se M é um KG -módulo associado à representação T então $M^E = M \otimes_K E$ é um EG -módulo associado à representação T^E .

Uma questão surge naturalmente: se T é irredutível (sobre K) será T^E irredutível (sobre E)? Tentaremos alguma resposta.

Definição 1.2.1 - Seja A uma K -álgebra. Um A -módulo irredutível M diz-se absolutamente irredutível se M^E é um A^E -módulo irredutível para toda extensão E de K .

Definição 1.2.2 - Um corpo E , extensão de K , diz-se um corpo de decomposição para a K -álgebra A se todo A^E -módulo irredutível é absolutamente irredutível.

Sabemos que nem todo módulo irredutível é absolutamente irredutível. Assim a resposta à pergunta é não.

Definição 1.2.3. - Seja G um grupo finito. Um corpo K diz-se um corpo de decomposição de G se é um corpo de decomposição para a álgebra KG .

Teorema 1.2.4. - Seja G um grupo finito e K um corpo perfeito. Então existe um corpo de decomposição $E \supset K$ de G tal que $\dim_K E$ é finita.

Teorema 1.2.5. - Seja n o expoente de G . Então $K(\sqrt[n]{1})$ é um corpo de decomposição de G .

Teorema 1.2.6. - Seja n o expoente de G . Seja K o corpo primo de p elementos, p primo. Então $K(\sqrt[n]{1})$ é um corpo de decomposição / de G .

Demonstrações dos teoremas 1.2.4, 1.2.5 e 1.2.6. podem ser encontradas em [9], páginas 462, 292 e 475 respectivamente.

Qualquer extensão de um corpo de decomposição é um corpo de decomposição. Mais precisamente, se K é um corpo de decomposição de G e E é um corpo, extensão de K , então E é um corpo de decomposição de G (1.2.7).

Seja K um corpo perfeito, por exemplo, um corpo de característica zero ou um corpo finito. Seja G um grupo finito e / consideremos uma representação T de G sobre K , isto é, $T: G \rightarrow GL(M)$ onde M é um espaço vetorial sobre K . Usaremos a notação $\text{env}(T)$ para denotar a menor subálgebra de $\text{Hom}_K(M, M)$, que contém as transformações lineares $\{T(g) / g \in G\}$, quer dizer

$$\text{env}(T) = \left\{ \sum_g \alpha_g T(g) / \alpha_g \in K \right\}.$$

Se T é uma representação matricial, definimos $\text{env}(T)$ de modo análogo.

A álgebra $\text{env}(T)$ também pode ser estudada em termos de KG - módulos. Seja M um KG - módulo e, para cada $a \in KG$, denotemos a_L a transformação linear $a_L : M \longrightarrow M$

$$m \longmapsto a.m$$

Então $A = (KG)_L = \{a_L / a \in KG\}$ é uma álgebra sobre K tal que M é um A -módulo fiel. Se T é uma representação associada a M , então $\text{env}(T) = (KG)_L$. Os KG -submódulos de M são idênticos aos $(KG)_L$ - submódulos de M . Em particular, se M é um KG - módulo completamente redutível, então, M é um $(KG)_L$ - módulo completamente redutível fiel, logo $(KG)_L$ é uma álgebra semisimples.

Agora seja E uma extensão de K . Notamos que $M^E = M \otimes_K E$ é um EG -módulo e é fácil provar que $(EG)_L \cong A^E = (KG)_L^E$. Por causa disso costumamos identificar $(EG)_L$ com $(KG)_L^E$ e olhar $(KG)_L$ como uma K -subálgebra de $(EG)_L$.

Teorema 1.2.8. - Se E é uma extensão separável de K então $A^E = (EG)_L$ é uma subálgebra semisimples de $\text{Hom}_E(M^E, M^E)$ e M^E é um EG - módulo completamente redutível (conforme [9] pg.462).

Voltemos à nossa questão original. Suponhamos que T é uma representação irredutível de G sobre K . Se E é um corpo de decomposição de G , queremos saber como a representação T^E de G sobre E se decompõe em componentes absolutamente irredutíveis. Vamos, /

então dar algumas definições e demonstrar alguns lemas visando o teorema 1.2.14 que nos dará a resposta a essa questão.

Começamos notando que pelos teoremas 1.2.4, 1.2.5 e 1.2.6 podemos achar uma extensão algébrica finita E de K , que é corpo de decomposição de G . Pela observação (1.2.7) podemos assumir que E é uma extensão normal separável de K .

Agora seja $\{U_1, \dots, U_r\}$ um conjunto completo de representações irredutíveis não equivalentes de G sobre E . Notamos que as representações U_i são absolutamente irredutíveis.

Os automorfismos $\sigma \in \text{Gal}(E, K)$ permutam as U_i do seguinte modo: para cada $g \in G$, seja $U_i^\sigma(g)$ a matriz obtida fazendo σ agir em todos os coeficientes de $U_i(g)$. Então é claro que U_i^σ é uma representação matricial absolutamente irredutível, e portanto, equivalente a uma das representações U_j , $1 \leq j \leq r$.

Definição 1.2.9. - A representação U_i^σ , com $\sigma \in \text{Gal}(E, K)$, diz-se uma representação conjugada de U_i .

Seja M um KG -módulo irredutível associado à representação T de G sobre K , e seja $A = (KG)_L$. Então A é uma subálgebra semisimples de $\text{Hom}_K(M^E, M^E)$ e M^E é um EA -módulo completamente redutível.

Sejam $\{\epsilon_1, \dots, \epsilon_t\}$ os idempotentes centrais primitivos em A^E .

Então $A^E = \varepsilon_1 A^E \oplus \dots \oplus \varepsilon_t A^E$, onde cada $\varepsilon_i A^E$ é uma componente simples de A^E . Correspondendo a essa decomposição de A^E , temos:

$$M^E = \varepsilon_1 M^E \oplus \dots \oplus \varepsilon_t M^E.$$

Cada submódulo $\varepsilon_i M^E$ é um $\varepsilon_i A^E$ -módulo, onde $\varepsilon_i A^E$ é simples. Como todo módulo sobre um anel simples é irredutível ou soma direta de módulos irredutíveis isomorfos, tem-se que:

$$\varepsilon_i M^E = M_{i1} \oplus \dots \oplus M_{id_i}, \quad i \leq d_i, \text{ onde os } M_{ij}$$

$j = 1, \dots, d_i$ são EG-módulos absolutamente irredutíveis isomorfos. Podemos assumir que as representações U_i estão ordenadas de tal modo que U_i é a representação de G associada a algum módulo $M_{ij} \subset \varepsilon_i M^E$, $1 \leq j \leq d_i$.

Sendo T a representação associada a M , temos

$$T^E \sim d_1 U_1 \oplus \dots \oplus d_t U_t \quad (1.2.10)$$

Seja $\sigma \in \text{Gal}(K, E)$. Definimos as seguintes aplicações:

$$S_\sigma: M^E \longrightarrow M^E$$

$$\sum e_j \otimes m_j \longmapsto \sum e_j^\sigma \otimes m_j, \quad e_j \in E, m_j \in M.$$

$$e \sigma^*: A^E \longrightarrow A^E$$

$$\sum e_j \otimes a_j \longmapsto \sum e_j^\sigma \otimes a_j, \quad e_j \in E, a_j \in A.$$

A aplicação S_σ é um KG-automorfismo do módulo M^E , pois:

$$\begin{aligned} \text{i)} \quad S_{\sigma}(x+y) &= S_{\sigma}\left(\sum e_j \otimes m_j + \sum e_i^{\sigma} \otimes m_i^{\sigma}\right) = \sum e_j^{\sigma} \otimes m_j + \\ &+ \sum e_i^{\sigma} \otimes m_i^{\sigma} = S_{\sigma}(x) + S_{\sigma}(y) \quad ; \quad \forall x, y \in M^E. \end{aligned}$$

$$\begin{aligned} \text{ii)} \quad S_{\sigma}(k.x) &= S_{\sigma}\left(\sum k e_j \otimes m_j\right) = \sum (k e_j)^{\sigma} \otimes m_j = \sum k^{\sigma} \cdot e_j^{\sigma} \otimes m_j = \\ &= \sum k \cdot e_j^{\sigma} \otimes m_j = k \cdot \sum e_j^{\sigma} \otimes m_j = k S_{\sigma}(x) ; \quad \forall k \in K, x \in M^E. \end{aligned}$$

$$\begin{aligned} \text{iii)} \quad S_{\sigma}(g.x) &= S_{\sigma}\left(g \cdot \sum e_j \otimes m_j\right) = S_{\sigma}\left(\sum e_j \otimes g.m_j\right) = \\ &= \sum e_j^{\sigma} \otimes g.m_j = g \cdot \left(\sum e_j^{\sigma} \otimes m_j\right) = g \cdot S_{\sigma}(x) ; \quad \forall g \in G, x \in M^E \end{aligned}$$

$$\text{iv)} \quad \text{A aplicação } S_{\sigma^{-1}} : M^E \longrightarrow M^E$$

$$\sum e_j \otimes m_j \longmapsto \sum e_j^{\sigma^{-1}} \otimes m_j \text{ é a inversa}$$

de S_{σ} .

A aplicação σ^* é um K -automorfismo da álgebra A^E , pois

$$\text{i)} \quad \sigma^*(x+y) = \sigma^*(x) + \sigma^*(y) ; \quad \forall x, y \in A^E$$

$$\text{ii)} \quad \sigma^*(k.x) = k \cdot \sigma^*(x) ; \quad \forall k \in K, x \in A^E$$

$$\begin{aligned} \text{iii)} \quad \sigma^*(x.y) &= \sigma^*\left(\left(\sum_j e_j \otimes a_j\right) \cdot \left(\sum_i e_i^{\sigma} \otimes a_i^{\sigma}\right)\right) = \sigma^*\left(\sum_{i,j} e_j e_i^{\sigma} \otimes a_j a_i^{\sigma}\right) = \\ &= \sum_{i,j} (e_j e_i^{\sigma})^{\sigma} \otimes a_j a_i^{\sigma} = \sum_{i,j} e_j^{\sigma} e_i^{\sigma\sigma} \otimes a_j a_i^{\sigma} = \\ &= \left(\sum e_j^{\sigma} \otimes a_j\right) \left(\sum e_i^{\sigma\sigma} \otimes a_i^{\sigma}\right) = \sigma^*(x) \cdot \sigma^*(y) ; \quad \forall x, y \in A^E. \end{aligned}$$

$$\text{iv)} \quad \text{A aplicação } (\sigma^{-1})^* : A^E \longrightarrow A^E$$

$$\sum e_j \otimes a_j \longmapsto \sum e_j^{\sigma^{-1}} \otimes a_j \text{ é a inversa}$$

de σ^* .

Lema 1.2.11. - Sejam $\sigma \in \text{Gal}(E, K)$, $u \in A^E$, $x \in M^E$.

$$\text{Então } \sigma^*(u) \cdot S_\sigma(x) = S_\sigma(u \cdot x)$$

Demonstração - :

$$\begin{aligned} \sigma^*(u) \cdot S_\sigma(x) &= \sigma^*\left(\sum_j e_j \otimes a_j\right) \cdot S_\sigma\left(\sum_i e_i' \otimes m_i\right) = \\ &= \left(\sum_j e_j^\sigma \otimes a_j\right) \cdot \left(\sum_i e_i'^\sigma \otimes m_i\right) = \sum_{i,j} e_j^\sigma e_i'^\sigma \otimes a_j m_i = \\ &= \sum_{i,j} (e_j e_i')^\sigma \otimes a_j m_i = S_\sigma\left(\sum_{i,j} e_j e_i' \otimes a_j m_i\right) = S_\sigma(u \cdot x). \end{aligned}$$

Lema 1.2.12. Seja $u \in A^E$. Se $\sigma^*(u) = u$, $\forall \sigma \in \text{Gal}(E, K)$, então $u \in A$, isto é, $u \in K \otimes A \equiv A$.

Demonstração - Sejam $\{a_j\}$ uma base de A sobre K e $\{e_i\}$ uma base de E sobre K . Então $\{e_i \otimes a_j\}$ é uma base de $E \otimes A = A^E$ sobre K .

$$\text{Temos } u = \sum_j e_j' \otimes a_j. \text{ Por hipótese, } \sigma^*(u) = u,$$

$$\forall \sigma \in \text{Gal}(E, K), \text{ isto é, } \sum_j e_j'^\sigma \otimes a_j = \sum_j e_j' \otimes a_j, \forall \sigma \in \text{Gal}(E, K).$$

Logo $\sum_j (e_j'^\sigma - e_j') \otimes a_j = 0$, e escrevendo

$$e_i'^\sigma - e_j' = \sum_i \beta_{ij} e_i, \text{ com } \beta_{ij} \in K \text{ vem que } \sum_{i,j} \beta_{ij} e_i \otimes a_j = 0. \text{ Como}$$

$\{e_i \otimes a_j\}$ é base de A^E sobre K , segue que $\beta_{ij} = 0 \quad \forall i, j$

Portanto $e_j^\sigma - e_j = 0 \quad , \quad \forall \sigma \in \text{Gal}(E, K)$, o que implica $e_j \in K$.

Assim $u \in K \otimes A \equiv A$.

K

Lema 1.2.13 - Seja $\sigma \in \text{Gal}(E, K)$. Se V é um EG-submódulo de M^E / associado à representação U_i , então $S_\sigma(V)$ é o EG-submódulo de M^E / associado à representação U_i^σ , conjugada de U_i .

Demonstração : Quando dizemos que V é um EG-módulo associado à representação U_i , queremos dizer que se $U_i(g) = (\alpha_{ij}) \in M_n(E)$, / existe uma base $\{v_j\}$ de V sobre E tal que

$$g \cdot v_j = U_i(g) \cdot (v_j) = \sum_k \alpha_{jk} v_k, \quad \text{com } \alpha_{jk} \in E.$$

Por outro lado, a representação conjugada U_i^σ está definida por $U_i^\sigma(g) = (\alpha_{ij}^\sigma)$. Temos também que $\{S_\sigma(U_j)\}$ é uma base / de $S_\sigma(V)$ sobre E , pois, obviamente gera $S_\sigma(V)$, e é livre sobre E , já que

$$0 = \sum_j e_j S_\sigma(v_j) = \sum_j e_j^\sigma S_\sigma(v_j) = \sum_j S_\sigma(e_j^\sigma v_j) =$$

$$= S_\sigma\left(\sum_j e_j^\sigma v_j\right), \text{ o que implica } \sum_j e_j^\sigma v_j = 0, \text{ pois } S_\sigma \text{ é automorfismo.}$$

Como $\{v_j\}$ é base de V sobre E , segue que $e_j^\sigma = 0 \quad \forall j$ e portanto

$$e_j = e_j^\sigma = 0 \quad \forall j.$$

Então $g \cdot S_{\sigma}(v_j) = S_{\sigma}(g \cdot v_j) = S_{\sigma} \left(\sum_k \alpha_{jk} v_k \right) = \sum_k S_{\sigma}(\alpha_{jk} v_k) =$
 $= \sum_k \alpha_{jk}^{\sigma} \cdot S_{\sigma}(v_k) = U_1^{\sigma}(g) \cdot (S_{\sigma}(u_j))$, e isso é dizer que o EG-sub-
 módulo $S_{\sigma}(V)$ está associado à representação U_1^{σ} .

Teorema 1.2.14 - Sejam T uma representação irredutível de G sobre K , e E uma extensão normal finita de K , que é corpo de decomposição de G . Então as componentes $\{U_i\}$ de T^E (ver 1.2.10) são / conjugadas entre si.

Demonstração : sejam $\epsilon_1, \dots, \epsilon_t$ os idempotentes centrais primitivos de A^E . Se $\sigma \in \text{Gal}(E, K)$ então $\sigma^*(\epsilon_1)$ é também um idempotente / central primitivo, pois

$$i) \sigma^*(\epsilon_1) \cdot \sigma^*(\epsilon_1) = \sigma^*(\epsilon_1^2) = \sigma^*(\epsilon_1)$$

$$ii) \sigma^*(\epsilon_1) \cdot a = \sigma^*(\epsilon_1) \cdot \sigma^*(a') = \sigma^*(\epsilon_1 \cdot a') = \sigma^*(a' \epsilon_1) =$$

$$= \sigma^*(a') \cdot \sigma^*(\epsilon_1) = a \cdot \sigma^*(\epsilon_1) \quad , \quad \forall a \in A^E$$

$$iii) \text{ se } \sigma^*(\epsilon_1) = \epsilon' + \epsilon'' \text{ então } \epsilon_1 = (\sigma^{-1})^* (\sigma^*(\epsilon_1)) =$$

$$= (\sigma^{-1})^* (\epsilon') + (\sigma^{-1})^* (\epsilon'') \text{, contra a hipótese de } \epsilon_1 \text{ ser primitivo. Logo } \sigma^*(\epsilon_1) \text{ é primitivo.}$$

$$\text{Assim } \sigma^*(\epsilon_1) = \epsilon_j \text{ para algum } j, \quad i \leq j \leq t.$$

Sejam $\epsilon_1, \epsilon_2, \dots, \epsilon_s$ os diferentes conjugados $\sigma^*(\epsilon_1)$ de ϵ_1 . Vamos mostrar que $s = t$.

Se $\text{Gal}(E, K) = \{\sigma_1, \dots, \sigma_m\}$ com $\sigma_1 = 1_E$, então os conjugados de ε_1 são $\sigma_1^*(\varepsilon_1) = \varepsilon_1, \sigma_2^*(\varepsilon_1), \dots, \sigma_m^*(\varepsilon_1)$. Vamos supor que os distintos conjugados de ε_1 sejam $\varepsilon_1, \sigma_2^*(\varepsilon_1) = \varepsilon_2, \dots, \sigma_s^*(\varepsilon_1) = \varepsilon_s$.

Seja $f = \varepsilon_1 + \dots + \varepsilon_s$. Então $\sigma^*(f) = \sigma^*(\varepsilon_1) + \dots + \sigma^*(\varepsilon_s)$.

Como $\sigma^*(\varepsilon_i) \neq \sigma^*(\varepsilon_j)$, $i \neq j$, e como $\sigma^*(\varepsilon_i) = \sigma^*(\sigma_i^*(\varepsilon_1)) = (\sigma^*\sigma_i^*)(\varepsilon_1)$ é conjugado de ε_1 , segue que $\{\sigma^*(\varepsilon_1), \dots, \sigma^*(\varepsilon_s)\} = \{\varepsilon_1, \dots, \varepsilon_s\}$. Logo $\sigma^*(f) = f$, $\forall \sigma \in \text{Gal}(E, K)$. Pelo lema 1.2.12, $f \in A$. Além disso, f é um idempotente central, e como A é simples, tem-se $f = 1$. Logo $\{\varepsilon_1, \dots, \varepsilon_s\}$ são todos os idempotentes centrais primitivos de A^E e $s = t$.

Portanto, todos os idempotentes centrais primitivos são conjugados de ε_1 , e assim todos conjugados entre si.

Como já notamos T^E é completamente redutível, logo o EG-módulo M^E associado a T^E se decompõe

$M^E \cong M_{11} \oplus \dots \oplus M_{1d_1} \oplus \dots \oplus M_{t1} \oplus \dots \oplus M_{td_t}$, onde os M_{ij} são EG-submódulos irreduzíveis, e $M_{i1} \oplus \dots \oplus M_{id_i} = \varepsilon_i M^E$.

Se U_i é a representação absolutamente irreduzível associada a M_{i1} , pelo lema 1.2.13. segue que $S_\sigma(M_{i1})$ está associado à representação U_i^σ .

Mas pelo lema 1.2.11.,

$S_{\sigma}(M_{i1}) = S_{\sigma}(\epsilon_i M_{i1}) = \sigma^*(\epsilon_i) S_{\sigma}(M_{i1}) \subset \sigma^*(\epsilon_i) M^E$; e, se $\sigma^*(\epsilon_i) = \epsilon_j$, $S_{\sigma}(M_{i1})$ é o EG-módulo associado a U_j . Assim mostramos que se U_j é a representação de G associada com $\sigma^*(\epsilon_i) = \epsilon_j$ então U_i^{σ} é equivalente a U_j . Como todos os $\{\epsilon_i\}$ são conjugados entre si, tôdas as representações absolutamente irredutíveis $\{U_i\}$ que aparecem em (1.2.10) são representações conjugadas.

1.3. UM RESULTADO SOBRE GRUPOS ABELIANOS.

Teorema 1.3.1. Sejam G e H grupos abelianos da mesma ordem n . Se para cada divisor d de n , G e H tem o mesmo número n_d de elementos de ordem d , então $G \cong H$.

Demonstração: O número n_d de elementos de ordem d em G é dado por $n_d = N_d(G) \cdot \phi(d)$, onde ϕ denota a função de Euler e $N_d(G)$ é o número de subgrupos cíclicos de ordem d em G . Os números $N_d(G)$ são determinados por fórmulas (G.A. Miller | 18 |), que mostram que os invariantes do grupo G ficam determinados quando os $N_d(G)$ são conhecidos. Dois grupos abelianos com os mesmos invariantes são isomorfos.

CAPÍTULO II - O PROBLEMA DO ISOMORFISMO PARA ÁLGEBRAS DE GRUPOS ABELIANOS.

2.1. ESTRUTURA DAS ÁLGEBRAS SEMISIMPLES COMUTATIVAS.

Sejam G um grupo abeliano de ordem n e F um corpo, cuja característica não divide n . Nós sabemos do teorema de Maschke que neste caso a álgebra FG é semisimples. Podemos então aplicar o teorema de Wedderburn e temos

$$FG \cong M_{n_1}(D_1) \oplus \dots \oplus M_{n_t}(D_t) ,$$
 para convenientes inteiros positivos n_i , e anéis com divisão D_i , únicos, que são extensões de F .

Como o grupo G é abeliano, a álgebra FG é comutativa, e assim $n_i = 1$, $i = 1 , \dots , t$ e os anéis com divisão D_i são na verdade corpos F_i .

Reescrevemos então

$$FG \cong F_1 \oplus \dots \oplus F_t \quad (2.1.1.)$$

Pretendemos dar uma interpretação dessa decomposição em termos das representações do grupo G sobre F . Essa interpretação é devida a S. Perlis e G.L. Walker [22] .

Sabemos ainda do teorema de Wedderburn que cada componente simples F_i da formula (2.1.1.) determina uma única classe de representações irredutíveis de G sobre F .

Chamando ϕ o isomorfismo em (2.1.1), π_i a projeção canônica de $F_1 \oplus \dots \oplus F_t$ sobre F_i e M um ideal minimal da componente simples F_i , uma representação irredutível S_i de G sobre F , representante da classe determinada por F_i , é

$$\begin{aligned} S_i : G &\longrightarrow \text{Hom}_F(M, M) \\ g &\longmapsto S_i(g) : M \longrightarrow M \\ &\quad x \longmapsto (\pi_i \phi(g)) \cdot x. \end{aligned}$$

Temos assim $S_i(g) = (\pi_i \phi(g))_L$. Como F_i é um corpo, temos $M = F_i$. É trivial que $F_i \cong F_{iL} = \{x_L : F_i \rightarrow F_i / x \in F_i\}$, onde o isomorfismo é dado por $x \in F_i \longmapsto x_L \in F_{iL}$.

Logo $S_i(G) = \{(\pi_i \phi(g))_L \in \text{Hom}_F(F_i, F_i) / g \in G\} \subset F_{iL} \cong F_i$, e podemos identificar $S_i(g)$ com um elemento do corpo F_i .

A representação S_i de G sobre F origina uma representação de FG , definindo $S_i(\sum_{g \in G} \alpha_g \cdot g) = \sum_{g \in G} \alpha_g \cdot S_i(g)$, com $\alpha_g \in F$. É claro que $S_i(FG) = F(S_i(G)) \subset F_i$. Por outro lado, dado $x \in F_i$, então $x = \pi_i(y)$, onde $y = (0, \dots, 0, x, 0, \dots, 0) \in F_1 \oplus \dots \oplus F_t \stackrel{\phi}{=} FG$. Logo, $x = \pi_i(\phi(a)) = S_i(a)$ para alguma $a \in FG$ e $F_i \subset S_i(FG)$. Assim $S_i(FG) = F_i$.

Agora, como S_i é representação de G , segue que

$(S_i(g))^n = S_i(g^n) = S_i(1) = 1_L \equiv 1 \in F_i$. Quer dizer, $S_i(g)$ é identificado com uma raiz n -ésima da unidade em F_i . Logo $S_i(G)$ é um

subgrupo das raízes da unidade em F_i , isto é, $S_i(G)$ é um grupo cíclico de ordem d , para algum d dividindo n .

Seja θ_d uma raiz d -ésima primitiva da unidade sobre F . Então $F(\theta_d) \subset F_i$. Por outro lado, fazendo as identificações, $S_i(FG) \subset F(\theta_d)$, pois todo elemento de $S_i(FG)$ é da forma $\sum_{g \in G} \alpha_g S_i(g)$, com $\alpha_g \in F$, e cada $S_i(g)$, $g \in G$, pertence a $F(\theta_d)$. Como $S_i(FG) = F_i$, tem-se $F_i \subset F(\theta_d)$, e $F_i = F(\theta_d)$.

Daqui concluímos que a fórmula (2.1.1.) pode ser reescrita para

$$FG \cong \bigoplus_{d|n} a_d F(\theta_d) \quad (2.1.2.), \text{ onde } a_d \text{ é o número de represen-}$$

tações irredutíveis não equivalentes de G sobre F , que levam o grupo G num grupo cíclico de ordem d , e $a_d F(\theta_d)$ significa a soma direta de a_d cópias de $F(\theta_d)$.

Nosso próximo passo é mostrar que os coeficientes a_d em (2.1.2.) estão relacionados com o grupo abeliano G . É nossa intenção provar que $a_d \cdot |F(\theta_d):F|$ é o número de elementos de ordem d em G . Dessa forma teremos uma boa ferramenta para decidirmos isomorfismos de grupos, já que dois grupos abelianos, que tenham o mesmo número de elementos de ordem d , para todo d , pelo Teorema 1.3.1., são isomorfos.

Sendo assim consideremos o polinômio $X^n - 1$ e seu corpo de raízes K sobre F . K é então um corpo de decomposição de G . A fórmula correspondente de (2.1.2.) para K será $KG \cong \bigoplus_{d|n} n_d K(\theta_d)$,

onde n_d tem o significado análogo ao de a_d em (2.1.2.). Como

$\theta_d \in K$, podemos escrever $KG \cong \bigoplus_{d|n} n_d K$, com $\sum n_d = n$.

Lema 2.1.3. Existe uma correspondência bijetora entre as representações irredutíveis não equivalentes de G sobre K e os elementos do grupo G , tal que $g \longleftrightarrow T_g$ então $\phi(g) = |T_g(G)|$.

Demonstração: Como G é abeliano, podemos escrevê-lo como produto de grupos cíclicos $G = \langle a_1 \rangle \times \dots \times \langle a_t \rangle$, com $\phi(a_i) = q_i$, $i = 1, \dots, t$. Definimos então representações

$$T_i : G \longrightarrow \text{Hom}_K(K, K) \cong K$$

$$a_i \longmapsto \theta_{q_i}$$

$$a_j \longmapsto 1 \text{ se } j \neq i, \text{ onde } \theta_{q_i} \text{ é uma raiz } q_i\text{-ésima}$$

primitiva da unidade. Para um elemento genérico $g = a_1^{h_1} \dots a_t^{h_t} \in G$,

definimos $T_g = T_1^{h_1} \dots T_t^{h_t}$, com $T_g(x) = T_1^{h_1}(x) \dots T_t^{h_t}(x)$, $\forall x \in G$;

e $T_i^{h_i}(x) = (T_i(x))^{h_i}$, $i = 1, \dots, t$. Toda T_g é de grau 1 e portan

to irredutível. Além disso, se $g \neq g'$ então $T_g \neq T_{g'}$. Como $\#$

$\{T_g/g \in G\} = |G| = \# \{T/T \text{ é representação irredutível de } G \text{ sobre } K\}$,

as representações $\{T_g\}$ são todas as representações irredutíveis de G sobre K . Fica estabelecida uma relação bijetora

$g \longleftrightarrow T_g$ entre os elementos g do grupo G e as representações irredutíveis T_g de G sobre K . Vamos mostrar que essa relação tem a propriedade enunciada.

Primeiro vejamos que a imagem de G pela representação T_g é da forma $T_g(G) = \langle T_1^{h_1}(a_1) \times \dots \times T_t^{h_t}(a_t) \rangle$. Se $y \in T_g(G)$ então $y = T_g(x)$ para algum $x = a_1^{\ell_1} \dots a_t^{\ell_t} \in G$. Assim $y = T_g(x) = T_1^{h_1}(x) \dots T_t^{h_t}(x) = T_1^{h_1}(a_1^{\ell_1}) \dots T_t^{h_t}(a_t^{\ell_t}) = (T_1^{h_1}(a_1))^{\ell_1} \dots (T_t^{h_t}(a_t))^{\ell_t} \in \langle T_1^{h_1}(a_1) \times \dots \times T_t^{h_t}(a_t) \rangle$.

A inclusão contrária é também trivial.

Dessa forma $|T_g(G)| = \text{mmc}[o(T_1^{h_1}(a_1)), \dots, o(T_t^{h_t}(a_t))]$.

Como $T_i^{h_i}(a_i) = \theta_{q_i}^{h_i}$ e $o(\theta_{q_i}^{h_i}) = \frac{q_i}{(q_i, h_i)}$, temos

$$|T_g(G)| = \text{mmc}\left[\frac{q_1}{(q_1, h_1)}, \dots, \frac{q_t}{(q_t, h_t)}\right] = d.$$

Por outro lado, como $g = a_1^{h_1} \dots a_t^{h_t}$, temos

$$o(g) = \text{mmc}[o(a_1^{h_1}), \dots, o(a_t^{h_t})] = \text{mmc}\left[\frac{q_1}{(q_1, h_1)}, \dots, \frac{q_t}{(q_t, h_t)}\right] = d.$$

Assim o elemento g tem ordem d se e somente T_g leva G num grupo cíclico de ordem d .

Podemos reinterpretar o lema 2.1.3. do seguinte modo:

Teorema 2.1.4. O número n_d de representações de G sobre K , que levam G num grupo cíclico de ordem d , é igual ao número de elementos de ordem d em G .

Se S é uma representação de G sobre F , e K é uma extensão de F , no capítulo I definimos uma representação S^K de G sobre K .

Sejam S uma representação irredutível de G sobre F , e K o corpo de raízes do polinômio $X^n - 1$, sobre F , onde $n = |G|$. Estamos nas condições do teorema 1.2.14. e, por causa disso, podemos afirmar que S^K é completamente redutível e $S^K \sim d_1 T_1 \oplus \dots \oplus d_t T_t$ onde as $\{T_i\}$ são representações irredutíveis de G sobre K , todas conjugadas entre si. A representação S leva G num grupo cíclico de ordem d , logo S é determinada por uma das componentes $F(\theta_d)$ da decomposição de $FG(\text{ver}(2.1.2))$.

Por outro lado sabemos que $KG \cong K \oplus \dots \oplus K$, $|G|$ vezes.

$$\text{Por outro, } KG \cong K \otimes_F FG = K \otimes_F \left(\bigoplus_{d|n} a_d F(\theta_d) \right) =$$

$$= \bigoplus a_d F(\theta_d)^K. \text{ Como } \dim_K F(\theta_d)^K = \dim_F F(\theta_d) \text{ tem-se}$$

$F(\theta_d)^K = K \oplus \dots \oplus K$, $[F(\theta_d) : F]$ vezes. Além disso, como S^K está associada a $F(\theta_d)^K$, segue que S^K se parte em $[F(\theta_d) : F]$ representações irredutíveis de G sobre k .

Pelas mesmas considerações do início do capítulo podemos identificar $S^K(g)$, $T_1(g)$, ..., $T_t(g)$ com elementos de K . Como as representações $\{T_i\}$ são todas conjugadas entre si e

$$S^K \sim d_1 T_1 \oplus \dots \oplus d_t T_t,$$

tem-se que $S^K(g)$ tem ordem d se e somente se cada $T_i(g)$ tem ordem d . Portanto, S^K leva G num grupo cíclico de ordem d e se parte em $[F(\theta_d) : F]$ representações (absolutamente) irredutíveis /

que levam G num grupo cíclico de ordem d também. Existem a_d representações irreduzíveis de G sobre F , levando G num grupo cíclico de ordem d , logo existirão $a_d \cdot [F(\theta_d) : F]$ representações (absolutamente) irreduzíveis de G sobre K , com a propriedade de levar G num grupo cíclico de ordem d , logo

$$n_d = a_d \cdot [F(\theta_d) : F]$$

Uma reinterpretação da fórmula (2.1.2) nos dá o

Teorema 2.1.5. Sejam G um grupo abeliano de ordem n , F um corpo cuja característica não divide n , θ_d uma raiz d -ésima primitiva da unidade e n_d o número de elementos de ordem d em G . Então:

$$F[G] \cong \bigoplus_{d|n} \frac{n_d}{[F(\theta_d) : F]} F(\theta_d)$$

2.2 UM TEOREMA DE REDUÇÃO

Nesta seção necessitaremos de alguns fatos sobre extensões e produto tensorial de corpos.

Proposição 2.2.1. Se E e K são extensões finitas do corpo F , $E|F$ é separável e $E \supseteq K$ então $E \otimes_F K$ é soma direta (como corpos) de $[K : F]$ cópias de E .

Demonstração : Como $E|F$ é separável então $K|F$ é separável.

$$\begin{array}{c} E \\ | \\ K \\ | \\ F \end{array}$$

Logo $K = F(\alpha)$. Se $g = \text{Irr}(\alpha, F)$ então $K \cong \frac{F[X]}{(g)}$

$$\text{Portanto } E \otimes_F K \cong E \otimes_F \frac{F[X]}{(g)} \cong \frac{E[X]}{(g)}$$

Em $E[X]$, g se decompõe em fatores lineares $g = g_1 \dots g_t$,
 $t = [K:F] = \text{grau } g$.

$$\text{Assim } E \otimes_F K \cong \frac{E[X]}{(g)} \cong \bigoplus_{i=1}^t \frac{E[X]}{(g_i)} \cong E \oplus \dots \oplus E \text{ (t vezes)}$$

Proposição 2.2.2. Seja θ_p , p primo, uma raiz p -ésima primitiva da unidade. Se $\theta_p \in F$ então $[F(\theta_p) : F]$ é potência de p .

Demonstração : Consideremos $F(\theta_p^2)$ e seja $g = \text{Irr}(\theta_p^2, F)$. O polinômio $f = x^p - \theta_p \in F[X]$ tem θ_p^2 como raiz, logo grau $g \leq p$.

Se $a^p - \theta_p \neq 0$, $\forall a \in F$, então f é irredutível em $F[X]$ (conforme A. Albert [1], teorema 21, pg.188). Logo:

$$[F(\theta_p^2) : F] = p.$$

Se existe $a \in F$ tal que $a^p - \theta_p = 0$, então $a^p = \theta_p$, o que implica $a^{p^2} = \theta_p^p = 1$. Assim F contém uma raiz p^2 -ésima da unidade e $F = F(\theta_p^2)$. Logo $[F(\theta_p^2) : F] = 1$.

Repetindo sucessivamente esse argumento, temos a tese.

No caso em que $[F(\theta_p^j) : F] = p^i$ denotaremos $F(\theta_p^j) = F_i$.

Do mesmo modo K_i e E_i terão o mesmo significado quando o corpo / base for K ou E .

Proposição 2.2.3. Se $\theta_p \in F$ e $E = F(\theta_r)$ com $(p, \phi(r)) = 1$, onde ϕ é a função de Euler, então $E \otimes_F F_i = E_i$

Demonstração

Como $E|F$ é galoisiana, tem-se conforme Bourbaki [4], teorema 10.4.1, pg 149, que E e $F(\theta_{p^j})$ são linearmente disjuntos sobre $E \cap F(\theta_{p^j})$. Assim $m = n$.

Ainda conforme Bourbaki [4], porposição 11.2.2 pg.166, tem-se que $q|\phi(r)$. Logo $s|\phi(r)$ e $s|p^i$, o que implica $s = 1$. Assim $E \cap F(\theta_{p^j}) = F$ e $m = p^i$.

Então $n = m = p^i$, o que implica $[E(\theta_{p^j}) : E] = p^i$ e $E(\theta_{p^j}) = E_i$.

Seja $f = \text{Irr}(\theta_{p^j}, F)$, onde grau $f = p^i$.

Como $E(F_i) = E(\theta_{p^j})$ e $[E(\theta_{p^j}) : E] = p^i$ segue que f é irredutível em $E[X]$.

$$\text{Logo } F_i \otimes_F E \cong \frac{F[X]}{(f)} \otimes_F E \cong \frac{E[X]}{(f)} \cong E(\theta_p^j) = E_i.$$

Se G e H são grupos abelianos de mesma ordem n , a decomposição de n num produto de fatores primos distintos p_i , $n = p_1^{e_1} \dots p_t^{e_t}$, implica na decomposição de G e H como produto direto de suas componentes p_i -primárias G_{p_i} e H_{p_i} , respectivamente. Assim:

$$G = G_{p_1} \times \dots \times G_{p_t} \text{ e } H = H_{p_1} \times \dots \times H_{p_t} \text{ com } |G_{p_i}| = |H_{p_i}| = p_i^{e_i},$$

$$i = 1, \dots, t.$$

O teorema, que enunciaremos a seguir, é muito útil no sentido de permitir que trabalhem apenas com as componentes p -primárias. Ele é devido a D.E. Cohen [5].

Teorema 2.2.4. Sejam G e H grupos abelianos de ordem n , G_p e H_p suas respectivas componentes p -primárias e F um corpo, cuja característica não divide n . Então $FG \cong FH$ se e somente se $FG_p \cong FH_p$, para todo p .

Demonstração : As condições do teorema são suficientes, pois se $G = G_{p_1} \times \dots \times G_{p_t}$ então $FG \cong FG_{p_1} \otimes_F \dots \otimes_F FG_{p_t}$. Vamos mostrar que são necessárias.

Pela fórmula (2.1.2) e pelo teorema 2.1.5. sabemos que

$$FG \cong \bigoplus_{d|n} a_d F(\theta_d) \cong \bigoplus_{d|n} \frac{n_d}{[F(\theta_d) : F]} F(\theta_d), \text{ onde } \theta_d \text{ é uma raiz}$$

primitiva de ordem d da unidade e n_d é o número de elementos de ordem d em G . Valem também as seguintes igualdades :

$$F G_p \cong \bigoplus_{j \geq 0} a_{pj} F(\theta_{pj}) \quad (2.2.5)$$

e

$$F H_p \cong \bigoplus_{j \geq 0} b_{pj} F(\theta_{pj}).$$

Vamos demonstrar que FG determina $F G_p$, isto é, $F G$ determina de modo único os inteiros a_{pj} da decomposição de $F G_p$. Desse modo, o fato de $FG \cong FH$ implicará que $a_{pj} = b_{pj}$, $\forall j$, e assim $F G_p \cong F H_p$.

Primeiro vamos demonstrar que FG determina $F G_p$ quando p é o maior primo que divide n . Teremos então condições de provar o teorema por indução, pois assumindo que FG determina FG_q , para todo primo q , dividindo n , maior que p , poderemos mostrar que FG determina FG_p .

1ª. Parte: p é o maior primo dividindo n .

Escrevendo $G = G_0 \times G_p$, onde G_0 é o produto das componentes q -primárias com $q < p$, temos $FG \cong FG_0 \otimes_F FG_p$.

Denotemos $K = F(\theta_p)$.

Passo 1. $K G_p$ determina $F G_p$.

Se $\theta_p \in F$ então KG_p determina trivialmente $F G_p$.

Suponhamos que $\theta_p \notin F$. Então (2.2.5) com a proposição

2.2.2. aplicada a K , nos dá

$$F G_p \cong F \oplus a'_0 K \oplus \left(\bigoplus_{i \geq 1} a'_i K_i \right), \text{ onde}$$

$$a'_0 = a_p \text{ e } a'_i = a_{pj} \text{ para } j \text{ tal que } [K(\theta_{pj}) : K] =$$

$$= [F(\theta_{pj}) : F(\theta_p)] = p^i.$$

$$\text{Logo } K G_p = K \otimes_F F G_p \cong K \otimes_F F \oplus a'_0 K \otimes_F K \oplus \left(\bigoplus_{i \geq 1} a'_i K \otimes_F K_i \right)$$

Pela proposição 2.2.1. temos

$$K G_p \cong K \oplus a'_0 [K : F] K \oplus \left(\bigoplus_{i \geq 1} a'_i [K : F] K_i \right), \text{ que reescreveremos}$$

$$\text{para } K G_p \cong \alpha_i K_i, \text{ onde } \alpha_0 = 1 + a'_0 [K : F]$$

$$\alpha_i = a'_i [K : F], i \geq 1$$

Daqui concluímos que os coeficientes α_i determinam os /
coeficientes a'_i , e estes determinam os a_{pj} . Isto é, KG_p determi-
na $F G_p$.

Seja $|G_0| = r$ e denotemos $E = K(\theta_r)$. Pela escolha de G_0
temos $(\phi(r), p) = 1$, pois p é o maior primo dividindo n .

Passo 2. EG determina KG_p .

$$\text{Temos } EG_p \cong E \otimes_K KG_p \cong E \otimes_K \left(\bigoplus_{i \geq 0} \alpha_i K_i \right) \cong \bigoplus_{i \geq 0} \alpha_i E \otimes_K K_i$$

que em consequencia da proposição 2.2.3. pode ser reescrito

$$EG_p \cong \bigoplus_{i \geq 0} \alpha_i E_i.$$

Como $\theta_r \in E$, tem-se que $E(\theta_d) = E$ para todo $d|r$. Logo

E é um corpo de decomposição de G_0 e assim $EG_0 \cong r.E$.

Reunindo, vem que

$$EG \cong EG_0 \otimes_E EG_p = rE \otimes_E \left(\bigoplus_{i \geq 0} \alpha_i E_i \right) \cong \bigoplus_{i \geq 0} r \alpha_i E_i.$$

Se β_i é o número de somandos diretos de EG isomorfos a E_i então $\beta_i = r \cdot \alpha_i$, e portanto os inteiros β_i determinam os inteiros α_i , isto é, EG determina KG_p .

Passo 3. FG determina EG.

$$\text{Trivial, já que } EG \cong E \otimes_F FG$$

2ª. Parte : **Assumimos** que FG determina FG_q para todo primo q dividindo n , $q > p$, e vamos mostrar que FG determina FG_p .

Escrevendo $G = G_0 \times G_p \times G_1$, onde G_0 é o produto das componentes q -primárias de G com $q < p$, e G_1 é o produto das com

ponentes q -primárias de G com $q < p$, e G_1 é o produto das componentes q -primárias com $q > p$, temos:

$$FG \cong FG_0 \otimes_F FG_p \otimes_F FG_1,$$

onde supomos que FG_1 é conhecido por hipótese de indução.

$$\text{Denotemos } K = F(\theta_p).$$

Passo 1. KG_p determina FG_p .

Idêntico ao passo 1 da parte anterior.

$$FG_p \cong F \oplus a'_0 K \oplus \left(\bigoplus_{i \geq 1} a'_i K_i \right)$$

$$KG_p \cong \bigoplus_{i \geq 0} \alpha_i K_i \quad \text{onde } \alpha_0 = 1 + a'_0 [K : F]$$

$$\alpha_1 = a'_1 [K : F], \quad i \geq 1$$

os α_i determinam os a'_i .

Seja $|G_0| = r$ e denotemos $E = K(\theta_r)$. Do mesmo modo, /

$$(\phi(r), p) = 1, \quad EG_p \cong \bigoplus_{i \geq 0} \alpha_i E_i \quad \text{e} \quad EG_0 \cong r.E.$$

Passo 2. EG determina KG_p .

Como FG_1 está determinada, EG_1 também está, pois /

$$EG_1 \cong E \otimes_F FG_1.$$

Portanto:

$$EG \cong E G_0 \otimes_E E G_p \otimes_E E G_1 \cong r E \otimes_E \left(\bigoplus_{i \geq 0} \alpha_i E_i \right) \otimes_E E G_1.$$

Suponhamos que $E_j \otimes_E E G_1$ contenha s_{ji} somando isomorfos a E_i . Vemos que $s_{ji} = 0$ para $j > i$, pois pela proposição /

2.2.1., tem-se

$$E_j \otimes_E E_k = \begin{cases} E_j \oplus \dots \oplus E_j \quad ([E_k : E] \text{ vezes}) \text{ se } E_k \subset E_j \\ \text{ou} \\ E_k \oplus \dots \oplus E_k \quad ([E_j : E] \text{ vezes}) \text{ se } E_j \subset E_k. \end{cases}$$

e em ambos os casos $E_j \otimes_E E_k$ não contém nenhum somando isomorfo a E_i .

Além disso, $s_{ii} \geq 1$, pois $E G_1$ tem no mínimo um somando E , e $E_i \otimes_E E G_1$ terá no mínimo um somando E_i .

Se β_i é o número de somandos de EG isomorfos a E_i , então $\beta_i = r.(\alpha_i s_{ii} + \sum_{j < i} \alpha_j s_{ji})$. Dessa forma os inteiros α_j ficam

determinados indutivamente pelos inteiros β_i , isto é, EG determina $K G_p$.

Passo 3. $F G$ determina $E G$.

Trivial.

Logo, por indução, FG determina $F G_p$ para todo p . Assim se $FG \cong FH$ então $F G_p \cong F H_p$ para todo p .

2.3. UMA CLASSE DE CORPOS PARA OS QUAIS VALE O TEOREMA DO ISOMORFISMO.

Nesta seção pretendemos exibir uma classe razoavelmente grande de corpos F com a seguinte propriedade:

"Se G e H são dois grupos abelianos de ordem n e $FG \cong FH$ então $G \cong H$ ". A condição suficiente dada pelo Teorema 2.3.3 é devida a S.K.Sehgal [26].

Lema 2.3.1. Se o polinômio ciclotômico de ordem n , $\phi_n(x)$, é irreduzível num corpo F , então para todo divisor m de n , tem-se $[F(\theta_m) : F] = \phi(m)$, onde θ_m é uma raiz m -ésima primitiva da unidade e ϕ é a função de Euler.

Demonstração . Suponhamos $n = m \cdot s$.

Se $(m, s) = d$, escrevendo $m = dd'$, t com $(dd', t) = 1$, teremos $n = s dd' t$ com $(sdd', t) = 1$. Então $\theta_m = \theta_{dd' t} = \theta_{dd'} \theta_t$ e $F(\theta_m) = F(\theta_t) (\theta_{dd'})$.

Também $F(\theta_n) = F(\theta_t) (\theta_{sdd'})$ e afirmamos que

$F(\theta_n) = F(\theta_t) (\theta_{sdd'}) (\theta_{dd'})$, pois $\theta_{dd'}$ sendo raiz sdd' -ésima da unidade, pertence a $F(\theta_t) (\theta_{sdd'}) = F(\theta_n)$. Logo:

$$F(\theta_n) = F(\theta_t)(\theta_{sdd'})(\theta_{dd'}) = F(\theta_t)(\theta_{dd'}) (\theta_{sdd'})$$

Como o polinômio $X^s - (\theta_{sdd'})^s \in F(\theta_t)(\theta_{dd'})[X]$ temos
que $[F(\theta_n) : F(\theta_m)] = [F(\theta_t)(\theta_{dd'}) (\theta_{sdd'}) : F(\theta_t)(\theta_{dd'})] \leq s$ e

$$[F(\theta_m) : F] \geq \frac{\phi(n)}{s} = \frac{\phi(sdd') \cdot \phi(t)}{s}.$$

Escrevendo $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $\alpha_i > 0$ $i = 1, \dots, r$, como
 $(sdd', t) = 1$, temos $sdd' = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $k \leq r$. Como também
 $(s, t) = 1$, caso contrário $t \mid sdd'$, temos:

$$s = p_1^{\beta_1} \dots p_k^{\beta_k}, \quad 0 \leq \beta_i \leq \alpha_i,$$

o que implica $dd' = p_1^{\alpha_1 - \beta_1} \dots p_k^{\alpha_k - \beta_k}$. Naturalmente $\alpha_i - \beta_i > 0$,
pois se $\alpha_i - \beta_i = 0$, teríamos $p_i \nmid dd'$. Mas $p_i \beta_i \mid s$, o que implica
 $p_i \beta_i \mid d$ e $p_i^{\beta_i} \mid dd'$. Logo teríamos $\beta_i = 0$ e consequentemente
 $\alpha_i = 0$ (contra hipótese).

Assim

$$\frac{\phi(n)}{s} = \frac{\phi(sdd') \cdot \phi(t)}{s} = \frac{p_1^{\alpha_1-1}(p_1-1) \dots p_k^{\alpha_k-1}(p_k-1) \cdot \phi(t)}{p_1^{\beta_1} \dots p_k^{\beta_k}}$$

$$= p_1^{\alpha_1-\beta_1-1}(p_1-1) \dots p_k^{\alpha_k-\beta_k-1}(p_k-1) \cdot \phi(t)$$

$$= \phi(dd') \cdot \phi(t) = \phi(m)$$

Portanto $[F(\theta_m) : F] \geq \phi(m)$, o que nos dá ;

$$[F(\theta_m) : F] = \phi(m).$$

Lema 2.3.2. Seja F um corpo tal que $\phi_n(X)$ é irreduzível em F . Então para todo primo p e para todos α e β maiores ou iguais a 1 tais que $p^\alpha | n$ e $p^\beta | n$, $F(\theta_p^\alpha) = F(\theta_p^\beta)$ se e somente se $\alpha = \beta$.

Demonstração Se $F(\theta_p^\alpha) = F(\theta_p^\beta)$ então pelo lema anterior:

$$[F(\theta_p^\alpha) : F] = [F(\theta_p^\beta) : F], \text{ isto é, } \phi(p^\alpha) = \phi(p^\beta).$$

Assim $p^{\alpha-1}(p-1) = p^{\beta-1}(p-1)$, o que implica $\alpha = \beta$

A recíproca é trivial.

Daremos agora uma condição suficiente para caracterizar corpos para os quais vale o teorema do isomorfismo para álgebras de grupos comutativas.

Teorema 2.3.3. Seja F um corpo tal que o polinômio ciclotômico $\phi_n(X)$ é irreduzível sobre F . Então para todo grupo abeliano de ordem divisor de n , $FG \cong FH$ implica $G \cong H$.

Demonstração : Mostraremos que sem perda de generalidade podemos supor que $\text{car } F \nmid n$. Caso contrário, se $\text{car } F = p | n$ e se θ_n é uma raiz primitiva de ordem n da unidade, escrevendo $n = p^t \cdot q$, com $p \nmid q$, teremos para $\alpha = \theta_{\frac{n}{p^t}}$, $\alpha^{p^t} = 1$, o que implicará /

$\alpha^{p^t} - 1 = (\alpha - 1)^{p^t} = 0$. Isto é, $\alpha = \theta_n^{\frac{n}{p^t}}$. Logo

$$\phi(n) = [F(\theta_n) : F] \leq \phi\left(\frac{n}{p^t}\right) = \phi(q), \text{ isto é,}$$

$\phi(p^t \cdot q) = \phi(q)$. Assim $\phi(p^t) \cdot \phi(q) = \phi(q)$ e $p^{t-1}(p-1) = 1$, o que nos dará $p = 2$ e $t = 1$. Portanto, $\text{car } F = 2$ e $n = 2 \cdot q$ com q ímpar. Além disso, como $|G| \mid n$ teremos: ou $|G|$ é ímpar e $\text{car } F \nmid |G|$ ou $|G| = 2m$ com m ímpar. Neste caso, $G = G_0 \times G_1$ e $H = H_0 \times H_1$ onde $G_0 = \langle g \rangle$ com $g^2 = 1$, $H_0 = \langle h \rangle$ com $h^2 = 1$ e $|G_1| = |H_1| = m$, m ímpar.

$$\text{Ainda, } F G_0 \cong \frac{F[X]}{(X^2-1)} \cong \frac{F[X]}{(X+1)} \oplus \frac{F[X]}{(X-1)} \cong F \oplus F \text{ e}$$

analogamente $F H_0 \cong F \oplus F$. Finalmente $FG \cong FH$ implicará

$$(F \oplus F) \otimes_F F G_1 \cong (F \oplus F) \otimes_F F H_1, \text{ isto é, } F G_1 \oplus F G_1 \cong F H_1 \oplus F H_1$$

Logo $F G_1 \cong F H_1$ e $\text{car } F \nmid |G_1| = |H_1|$.

Se $|G| = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, $\alpha_i \geq 1$ escrevamos $G = G_1 \times \dots \times G_t$ e $H = H_1 \times \dots \times H_t$, onde G_i e H_i são as respectivas componentes p_i -primárias de G e H . Estamos nas condições do Teorema 2.2.5 e portanto sabemos que $FG \cong FH$ se e somente se $FG_i \cong FH_i$, $i=1, \dots, t$. Aplicando a fórmula (2.1.2) a FG_i e FH_i temos:

$$FG_i \cong F \oplus a_{p_i} F(\theta_{p_i}) \oplus a_{p_i}^2 F(\theta_{p_i}^2) \oplus \dots \oplus a_{p_i}^{\alpha_i} F(\theta_{p_i}^{\alpha_i})$$

$$FH_i \cong F \oplus b_{p_i} F(\theta_{p_i}) \oplus b_{p_i}^2 F(\theta_{p_i}^2) \oplus \dots \oplus b_{p_i}^{\alpha_i} F(\theta_{p_i}^{\alpha_i})$$

Pelos lemas 2.3.1 e 2.3.2., $F(\theta_{p_i}^j) = F(\theta_{p_i}^k)$ se e somente se $j = k$. Portanto dos isomorfismos $FG_i \cong FH_i$, $i = 1, \dots, t$, concluímos que $a_{p_i}^j = b_{p_i}^j$ para $j = 1, \dots, \alpha_i$ e $i = 1, \dots, t$.

Logo

$$\frac{n_{p_i}^j}{\phi(p_i^j)} = \frac{m_{p_i}^j}{\phi(p_i^j)}, \text{ onde pelo Teorema 2.1.5}$$

$n_{p_i}^j$ e $m_{p_i}^j$ são os números de elementos de ordem p_i^j respectivamente em G e H .

$$\text{Então } n_{p_i}^j = m_{p_i}^j \quad j = 1, \dots, \alpha_i \text{ e } i = 1, \dots, t;$$

e pelo teorema 1.3.1, $G_i \cong H_i$, o que implica

$$G = G_1 \times \dots \times G_t \cong H_1 \times \dots \times H_t = H.$$

Sabemos que para todo n , $\phi_n(X)$ é irreduzível sobre $\mathbb{Q}$.

Cabe então o seguinte:

Corolário 2.3.4. - Se G e H são grupos abelianos finitos, então $\mathbb{Q}G \cong \mathbb{Q}H$ implica $G \cong H$.

Conforme E.Weiss [28], teorema 7.4.2., pg.262, o polinômio ciclotômico $\Phi_p \alpha [X]$ é irredutível sobre $\mathbb{Q}_p$, o completamento p-ádico dos racionais.

Corolário 2.3.5. Se G e H são p-grupos abelianos então $\mathbb{Q}_p G \cong \mathbb{Q}_p H$ implica $G \cong H$.

Infelizmente a condição do Teorema 2.3.3. não é necessária para caracterizar os corpos F tais que $FG \cong FH$ implica $G \cong H$, com $|G| = |H| = n$ e G e H abelianos. Vamos dar um contra-exemplo.

Fixemos $n = 8$. Então $\Phi_8(X) = X^4 + 1 = (X^2 + \sqrt{2} X + 1)(X^2 - \sqrt{2} X + 1)$, e $[\mathbb{Q}(\sqrt{2})(\theta_8) : \mathbb{Q}(\sqrt{2})] < 4 = \phi(8)$. Tomemos os três grupos abelianos não isomorfos de ordem 8:

$$G_1 = \mathbb{Z}_8 \quad ; \quad G_2 = \mathbb{Z}_2 \times \mathbb{Z}_4 \quad ; \quad G_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Pelo teorema 2.1.5.

$$\mathbb{Q}(\sqrt{2}) G_1 \cong \mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{2}) \oplus \frac{2}{2} \mathbb{Q}(\sqrt{2})(i) \oplus$$

$$\frac{4}{2} \mathbb{Q}(\sqrt{2}) \left(\frac{\sqrt{2} + i\sqrt{2}}{2} \right) \cong 2 \mathbb{Q}(\sqrt{2}) \oplus 3 \mathbb{Q}(\sqrt{2}, i)$$

$$\mathbb{Q}(\sqrt{2}) G_2 \cong \mathbb{Q}(\sqrt{2}) \oplus 3 \mathbb{Q}(\sqrt{2}) \oplus \frac{4}{2} \mathbb{Q}(\sqrt{2})(i)$$

$$\cong 4 \mathbb{Q}(\sqrt{2}) \oplus 2 \mathbb{Q}(\sqrt{2}, i)$$

$$\mathbb{Q}(\sqrt{2}) G_3 \cong \mathbb{Q}(\sqrt{2}) \oplus 7 \mathbb{Q}(\sqrt{2}) = 8 \mathbb{Q}(\sqrt{2})$$

Quer dizer, $G_i \not\cong G_j$ implica $\mathbb{Q}(\sqrt{2}) G_i \not\cong \mathbb{Q}(\sqrt{2}) G_j$, ou
equivalentemente, $\mathbb{Q}(\sqrt{2}) G_i \cong \mathbb{Q}(\sqrt{2}) G_j$ implica $G_i \cong G_j$.

CAPÍTULO III - O PROBLEMA DO ISOMORFISMO PARA ÁLGEBRAS DE GRUPOS
QUAISQUER.

3.1. ALGUNS RESULTADOS.

Seja G um grupo de ordem n e seja F um corpo de característica zero ou um primo não dividindo n .

Lema 3.1.1. Se N é um subgrupo normal de G e $L(N)$ é o ideal de FG gerado pelo conjunto $\{x - 1 / x \in N\}$, então $FG \cong F(G/N) \oplus L(N)$.

Demonstração : Seja q a ordem de N . Definimos $e = \frac{1}{q} \sum_{x \in N} x$. Se

$\{1 = y_1, y_2, \dots, y_k\}$ é um conjunto completo de representantes de G módulo N então $G = N \cup y_2 N \cup \dots \cup y_k N$. O ideal (e) gerado por e em FG é um F -subespaço vetorial de FG . Afirmamos que o conjunto $E = \{e, ey_2, \dots, ey_k\}$ é uma base de (e) sobre F ,

i) é linearmente independente sobre F .

$$\sum_{i=1}^k \alpha_i (ey_i) = 0, \alpha_i \in F \implies e \cdot \left(\sum_{i=1}^k \alpha_i y_i \right) = 0 \implies$$

$$\sum_{i=1}^k \alpha_i y_i = 0 \implies \alpha_i = 0 \quad i = 1, \dots, k \quad \text{pois } \{1, y_2, \dots, y_k\} \text{ faz}$$

parte de uma base de FG sobre F .

ii) gera (e)

$a \in (e) \Rightarrow a = e \cdot \left(\sum_{i=1}^n \alpha_i g_i \right) = \sum_{i=1}^n \alpha_i e g_i$. Mas se g_i e g_k per-

tencem a mesma classe lateral, isto é, $g_i = n \cdot g_h$ para algum /

$n \in N$, então $e g_i = e n \cdot g_h = \left(\frac{1}{q} \sum_{x \in N} x \right) n \cdot g_h =$

$$= \left(\frac{1}{q} \sum_{x \in N} (xn) \right) g_h = \left(\frac{1}{q} \sum_{y \in N} y \right) g_h = e \cdot g_h$$

$$\Rightarrow a = \sum_j \left(\sum_{g_i \in N_{y_j}} \alpha_i \right) e_{y_j}.$$

O conjunto E é também um grupo multiplicativo já que

$$i) e \cdot (e y_i) = e^2 y_i = e y_i \quad ; \quad (e y_i) e = e (y_i e) = e (e y_i) = e y_i$$

$$ii) (e y_i) (e y_j) = e e y_i y_j = e^2 y_l = e y_l$$

$$iii) (e y_i)^{-1} = y_i^{-1} e = e y_i^{-1}$$

A aplicação $\phi : E \longrightarrow G/N$ é um isomorfismo de grupos.

$$e y_i \longmapsto \bar{y}_i$$

Logo $F(E) \cong F(G/N)$, isto é, $(e) \cong F(G/N)$

Como $e^2 = e$, temos $(1-e)^2 = 1-e$; $e(1-e) = 0$ e /

$1 = e + (1-e)$, o que implica $FG = (e) \oplus (1-e)$.

O ideal $A = (1-e)$ pode ser caracterizado como
 $\{x \in FG / x.e=0\}$, pois se $x \in A$ então $x = \alpha.(1-e)$, $\alpha \in FG$ e

$$x . e = \alpha(1-e).e = \alpha(e - e^2) = \alpha . 0 = 0,$$

e se x é tal que $x . e = 0$ então $x = x - xe = x(1 - e) \in A$.

Claramente $L(N) \subset A$, pois $L(N) = (x - 1 / x \in N)$ e

$(x - 1) . e = xe - e$. Como $x \in N$ temos $x . e = e$, o que implica
 $(x - 1) . e = e - e = 0$.

Agora, $\dim_F A = \dim_F FG - \dim_F (e) = n - k = qk - k =$
 $= (q - 1) k$.

O subconjunto $\{(x-1)y_i / x \in N, x \neq 1, i = 1, \dots, k\}$

de $L(N)$ é linearmente independente, pois

$$\sum_{j=2}^q \sum_{i=1}^k \alpha_{ij} (x_j - 1) y_i = \sum_{j=2}^q \sum_{i=1}^k \alpha_{ij} x_j y_i - \sum_{j=2}^q \sum_{i=1}^k \alpha_{ij} y_i ;$$

sendo $x_j y_i \neq y_\ell$ $\ell = 1, \dots, n$ (senão y_i e y_ℓ estariam na mesma
 classe lateral) tem-se que $\{x_j y_i\} \cup \{y_i\}$ $\begin{matrix} i=1, \dots, k \\ j=2, \dots, q \end{matrix}$

Como $\# \{(x-1)y_i / x \in N, x \neq 1, i = 1, \dots, k\} = (q-1)k$

tem-se $A = L(N)$. Portanto $FG \cong F(G/G') \oplus L(N)$.

Lema 3.1.2. Seja I um ideal de FG . Então a álgebra $\frac{FG}{I}$ é co

mutativa se e só se $I \supset L(G')$, onde G' é o comutador de G .

Demonstração Notemos primeiro que se S é um sistema de geradores de um subgrupo N então $L(N) = (x - 1 / x \in S)$, pois se $y \in N$, /
 $y = x_1 \dots x_s$ com $x_i \in S$ e

$$y - 1 = x_1 \dots x_s - 1 = x_1(x_2 \dots x_s - 1) + (x_1 - 1) = \\ = x_1(x_2(x_3(\dots(x_{s-1}(x_s - 1)))) + (x_{s-1} - 1) + \dots + (x_2 - 1)(x_1 - 1)$$

$\in (x - 1 / x \in S)$. Logo $L(N) \subset (x - 1 / x \in S) \subset (x - 1 / x \in N) =$

$L(N)$, isto é, $L(N) = (x - 1 / x \in S)$.

Suponhamos que $L(G') \subset I$. Então $g h g^{-1} h^{-1} - 1 \in I$

$\forall g, h \in G$. Logo $(g h g^{-1} h^{-1} - 1) h g = g h - h g \in I$, o que implica $g h = h g \pmod{I}$.

Agora suponhamos que $\frac{F G}{I}$ é comutativa.

Tomemos $x \in L(G')$. Pelas observações feitas no início da demonstração podemos tomar $x = g h g^{-1} h^{-1} - 1$.

$$\begin{aligned} \text{Então } x \pmod{I} &= g h \pmod{I} g^{-1} h^{-1} \pmod{I} - 1 \pmod{I} \\ &= h g \pmod{I} g^{-1} h^{-1} \pmod{I} - 1 \pmod{I} \\ &= 1 \pmod{I} - 1 \pmod{I} = 0 \pmod{I}, \text{ o que} \end{aligned}$$

implica $x \in I$.

Teorema 3.1.3. Seja F um corpo cuja característica não divide $|G|$.

Então $FG \cong FH$ se e somente se $F(\frac{G}{G'}) \cong F(\frac{H}{H'})$ e $L(G') \cong L(H')$.

Demonstração

Se $F(G/G') \cong F(H/H')$ e $L(G') \cong L(H')$ então pelo lema 3.1.1.

tem-se $FG \cong FH$. Recíprocamente seja $\phi: FG \longrightarrow FH$ um isomorfismo.

Pelo lema 3.1.1 $FG \cong F(G/G') \oplus L(G')$.

Então $FH = \phi(F(G/G')) \oplus \phi(L(G'))$, donde

$\frac{F \quad H}{\phi(L(G'))} \cong \phi(F(G/G'))$ que é comutativa. Pelo lema 3.1.2. tem-se

$L(H') \subset \phi(L(G'))$. De forma análoga se demonstra que

$L(G') \subset \phi^{-1}(L(H'))$, o que implica $\phi(L(G')) \subset L(H')$.

Logo $\phi|_{L(G')} : L(G') \longrightarrow L(H')$ é isomorfismo

$$e \quad F(G/G') \cong \frac{F \quad G}{L(G')} \cong \frac{F \quad H}{L(H')} \cong F(H/H')$$

Corolário 3.1.4 $\mathbb{Q}G \cong \mathbb{Q}H$ se e somente se $L(G') \cong L(H')$ e

$$G/G' \cong H/H'.$$

3.2. CONTRA-EXEMPLOS COM P-GRUPOS

Agora pretendemos mostrar que o estudo das álgebras FG com $\text{car } \neq |G|$ e G um grupo finito qualquer. Não vai conduzir a novos resultados no que se refere à nossa versão do problema do isomorfismo: "determinar corpos F tais que $FG \cong FH$ implica $G \cong H$ ". Assim culminaremos esta seção com um teorema que mostra que existe uma classe de p -grupos não isomorfos, cujas álgebras de grupos

sobre qualquer corpo de característica diferente de p são isomorfas. Este resultado é de D.S. Passman [15].

Seja χ o carater de uma representação absolutamente irredutível da álgebra KG em alguma extensão de K . Denotamos $K(\chi)$ o corpo obtido juntando-se a K todos os $\chi(g)$, $g \in G$.

Se ϵ é uma raiz $|G|$ -ésima primitiva da unidade então $K(\chi) \subset K(\epsilon)$, pois cada $\chi(g)$ é soma de raízes $|G|$ -ésimas da unidade.

Se $K = \mathbb{Q}$, o corpo dos números racionais, denotamos $\mathbb{Z}[\chi]$ o anel extensão de $\mathbb{Z}$, que se obtém juntando-se a $\mathbb{Z}$ todos os $\chi(g)$, $g \in G$.

Denotando $\text{int } \mathbb{Q}(\chi)$ os inteiros algébricos de $\mathbb{Q}(\chi)$, claramente $\mathbb{Z}[\chi] \subset \text{int } \mathbb{Q}(\chi)$, pois cada $\chi(g)$, sendo soma de raízes $|G|$ -ésimas da unidade, é soma de inteiros algébricos e portanto inteiro algébrico, e todo elemento de $\mathbb{Z}$ é trivialmente inteiro algébrico.

Pretendemos mostrar que vale uma espécie de recíproca.

Lema 3.2.1. Se χ é o carater de uma representação absolutamente irredutível da álgebra $\mathbb{Q}G$ em alguma extensão de $\mathbb{Q}$, então $\mathbb{Z}[\chi] \supset |G|^r \text{int } \mathbb{Q}(\chi)$ para um r suficientemente grande.

Demonstração. Temos que $\mathbb{Q}(\chi) \subset \mathbb{Q}(\epsilon)$ e, sendo $\mathbb{Q}'(\epsilon)$ uma extensão normal abeliana de $\mathbb{Q}$, $\mathbb{Q}(\chi)$ também é uma extensão normal de $\mathbb{Q}$.

Seja $H = \text{Gal } (\mathbb{Q}(\chi), \mathbb{Q})$ cuja ordem é $h = \dim_{\mathbb{Q}} \mathbb{Q}(\chi)$. Escrevendo $H = \{\sigma_1, \dots, \sigma_n\}$ com $\sigma_1 = 1_{\mathbb{Q}(\chi)}$, os caracteres conjugados de χ , $\chi^{\sigma_i} = \chi_i, i = 1, \dots, h$, são todos distintos. Vamos assumir que os caracteres irreduzíveis de G estão enumerados de tal forma que os h primeiros sejam os $\chi^{\sigma_i}, \sigma_i \in H$.

Seja $g_i \in G$ um representante da i -ésima classe de G e seja $n_i = |G : C(g_i)|$ o número de conjugados de g_i . Suponhamos / que G tenha k classes conjugadas. Construimos as seguintes matrizes

$$X = \begin{bmatrix} \chi_1(g_1) & \chi_1(g_2) & \dots & \chi_1(g_k) \\ \chi_2(g_1) & \chi_2(g_2) & \dots & \chi_2(g_k) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_k(g_1) & & \dots & \chi_k(g_k) \end{bmatrix} \quad \text{onde } \chi_i = \chi^{\sigma_i}, i=1, \dots, h$$

$$e \quad N = \begin{bmatrix} n_1 & & & 0 \\ & n_2 & & \\ & & \ddots & \\ 0 & & & n_k \end{bmatrix}$$

Se X^* denota a matriz conjugada transposta de X temos

$$X N X^* = [\chi_i(g_j)] \cdot [n_i \delta_{ij}] \cdot [\overline{\chi_j(g_i)}] = [\gamma_{il}] \quad , \quad \text{onde}$$

$$\gamma_{il} = \sum_{j=1}^k n_j \chi_i(g_j) \overline{\chi_l(g_j)}$$

Como $\mathbb{Q}(\epsilon)$ é corpo de decomposição de G , pelas relações de ortogonalidade para caracteres irredutíveis em um corpo de decomposição de característica 0 temos:

$$\gamma_{il} = |G| \cdot \delta_{il}, \text{ donde}$$

$$X N X^* = |G| \cdot I_k.$$

Seja p primo, $p \nmid |G|$ e denotemos $(p) = p \cdot \mathbb{Z}[\epsilon]$. Da igualdade matricial acima vem que $\det(X N X^*) = |G|^k \not\equiv 0 \pmod{p}$, o que implica $\det X \not\equiv 0 \pmod{p}$.

Desenvolvendo $\det X$ pela expansão de Laplace em relação às h primeiras linhas de X , temos

$$\det X = \sum_{\lambda} \pm \det M_{\lambda} \cdot \det N_{\lambda} \not\equiv 0 \pmod{p}, \text{ onde } M_{\lambda} \text{ é matriz}$$

$h \times h$ nas primeiras h linhas e N_{λ} é a sua complementar. Portanto $\det M_{\lambda} \not\equiv 0 \pmod{p}$ para algum λ . Podemos assumir que é o principal, isto é, $M_{\lambda} = (\chi_i(g_j))_{i,j=1,\dots,h}$, pois caso contrário reordenamos as linhas de X para que isso aconteça-

Seja $m_p = \det[\chi_i(g_j)]^2_{i,j=1,\dots,h}$. Então m_p é um inteiro algébrico e como

$$\sigma(m_p) = \sigma(\det[\chi_i(g_j)]^2) = (\sigma \det[\chi_i(g_j)])^2 =$$

$$= (\det[\sigma(\chi_i(g_j))])^2 = (\det[\chi_i^\sigma(g_j)])^2 = \det[\chi_i^\sigma(g_j)]^2 = m_p,$$

$\forall \sigma \in H$, temos que $m_p \in \mathbb{Q}$. Portanto, $m_p \in \text{int } \mathbb{Q}(\varepsilon) \cap \mathbb{Q} = \mathbb{Z}$.

$$\text{Em particular, } m_p = (\det M_\lambda)^2 \not\equiv 0 \pmod{p}$$

Os $\chi(g_1), \dots, \chi(g_h)$ são linearmente independentes sobre $\mathbb{Q}$, pois se fossem linearmente dependentes existiriam racionais $q_1, \dots, q_h$ não todos nulos tais que

$$q_1 \chi(g_1) + \dots + q_h \chi(g_h) = 0, \text{ o que implicaria,}$$

$$\sigma_i(q_1 \chi(g_1) + \dots + q_h \chi(g_h)) = q_1 \chi^{\sigma_i}(g_1) + \dots + q_h \chi^{\sigma_i}(g_h) = 0$$

$i = 1, 2, \dots, h$, e teríamos $m_p \equiv 0 \pmod{p}$.

Logo $\chi(g_1), \dots, \chi(g_h)$ formam uma base de $\mathbb{Q}(\chi)$ sobre $\mathbb{Q}$.

Seja $\alpha \in \text{int } \mathbb{Q}(\chi)$. Então $\alpha = \sum_{j=1}^h q_j \chi(g_j)$, $q_j \in \mathbb{Q}$.

Aplicando os automorfismos σ_i de H a essa igualdade temos:

$$\alpha_i = \sigma_i(\alpha) = \sum_{j=1}^h q_j \chi^{\sigma_i}(g_j), \quad i = 1, \dots, h, \quad \text{que nos}$$

dá a seguinte igualdade matricial

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_h \end{bmatrix} = [\chi_i(g_j)] \begin{bmatrix} q_1 \\ \vdots \\ q_h \end{bmatrix}$$

Multiplicando ambos os membros por $[\chi_i(g_j)]$ temos

$$[\chi_i(g_j)] \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_h \end{bmatrix} = [\chi_i(g_j)]^2 \begin{bmatrix} q_1 \\ \vdots \\ q_h \end{bmatrix}$$

e multiplicando agora ambos os membros pela matriz adjunta clássica de $[\chi_i(g_j)]^2$ temos

$$\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_h \end{bmatrix} = \text{adj}[\chi_i(g_j)]^2 \cdot [\chi_i(g_j)] \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_h \end{bmatrix} = \det[\chi_i(g_j)]^2 \begin{bmatrix} q_1 \\ \vdots \\ q_h \end{bmatrix} = m_p \begin{bmatrix} q_1 \\ \vdots \\ q_h \end{bmatrix}$$

Portanto $m_p \cdot q_j = \beta_j$, $j = 1, \dots, h$ onde $\beta_j \in \mathbb{Z}$. Podemos reescrever $\alpha = \sum_{j=1}^h \frac{\beta_j}{m_p} \chi(g_j) = \frac{1}{m_p} \sum_{j=1}^h \beta_j \chi(g_j)$ o que implica $m_p \cdot \alpha = \sum_{j=1}^h \beta_j \chi(g_j) \in \mathbb{Z}[\chi]$.

Assim $m_p \cdot \text{int } \mathbb{Q}(\chi) \subset \mathbb{Z}[\chi]$

Seja J o ideal de $\mathbb{Z}$ gerado pelos m_p para todos os primos p tais que $(p, |G|) = 1$. Notemos que se $m \in J$ então

$m \cdot \text{int } \mathbb{Q}(\chi) \subset \mathbb{Z}[\chi]$, pois $m = \sum_p a_p m_p$, $a_p \in \mathbb{Z}$ e para cada $(p, |G|) = 1$

$m_p \cdot \text{int } \mathbb{Q}(\chi) \subset \mathbb{Z}[\chi]$.

Agora J sendo ideal de $\mathbb{Z}$ é da forma $J = a \cdot \mathbb{Z}$. Se p é um primo dividindo a , então $p \mid |G|$, pois $p \nmid |G|$ implica $p \nmid m_p = n \cdot a$ e assim $p \nmid a$.

Se $a = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ então $|G| = p_1^{\beta_1} \dots p_t^{\beta_t} \cdot q$ com

$(q, p_i) = 1, i = 1, \dots, t$. Seja r o menor inteiro tal que $r \cdot \beta_i \geq \alpha_i, i = 1, \dots, t$. Tem-se $|G|^r = a \cdot q'$ e $|G|^r \in J$. Assim $|G|^r \in \text{int } \mathbb{Q}(\chi) \subset \mathbb{Z}[\chi]$

Teorema 3.2.2. Suponhamos que $\mathbb{Q}G \cong \mathbb{Q}H$, onde $\mathbb{Q}$ é o corpo dos números racionais. Então para todos os corpos K , cuja característica não divide $|G| = |H| = n$ temos $KG \cong KH$.

Demonstração - É suficiente assumir que K é um corpo primo, pois se P é o corpo primo de K temos $KG \cong K \otimes_P PG$. Como o caso em que $K = \mathbb{Q}$ é dado precisamos apenas provar o teorema para $K = \mathbb{Z}_p$, o corpo dos inteiros módulo p , com p primo não dividindo $|G|$.

Sabemos do teorema 1.2.2. (Wedderburn) que:

$KG \cong \bigoplus a_i M_{r_i}(D_i)$, onde D_i é um anel com divisão que contém K e $a_i M_{r_i}(D_i)$ significa a soma direta de a_i cópias de $M_{r_i}(D_i)$.

Sejam $\bar{\epsilon}$ uma raiz n -ésima primitiva da unidade sobre K e $\bar{\chi}_i$ um caráter absolutamente irredutível de G sobre $K(\bar{\epsilon})$ associado a uma componente simples $M_{r_i}(D_i)$. Temos que $K(\bar{\chi}_i) = \text{centro } D_i$ (con-

finito, isto é, D_i é um corpo. Logo centro $D_i = D_i$ e $K(\bar{\chi}_i) = D_i$.

Portanto $KG \cong \bigoplus a_i M_{r_i}(K(\bar{\chi}_i))$.

Sabemos também que $\mathbb{Q}G \cong \bigoplus \alpha_i M_{n_i}(D_i)$. Vamos mostrar

que $\mathbb{Q}G$ determina KG , isto é, $\mathbb{Q}G$ determina de modo único os coeficientes a_i , os inteiros r_i e os corpos $K(\bar{\chi}_i)$ da decomposição de KG . Dessa forma $\mathbb{Q}G \cong \mathbb{Q}H$ implicará $KG \cong KH$.

Passo 1. $\mathbb{Q}G$ determina r_i

i) grau $\bar{\chi}_i = r_i$

se W é um KG -módulo irredutível associado à componentes simples M_{r_i} então por L. Dornhoff [22], teorema 24.14, o $K(\bar{\chi}_i)G$ -módulo $W^{K(\bar{\chi}_i)}$ se decompõe do seguinte modo:

$$W^{K(\bar{\chi}_i)} \cong s(V \oplus V^{\alpha_2} \oplus \dots \oplus V^{\alpha_t}), \quad (3.2.3.), \text{ onde } s \text{ é}$$

o índice de Schur $s_K(\bar{\chi}_i)$, V é um $K(\bar{\chi}_i)G$ -módulo absolutamente irredutível associado a $\bar{\chi}_i$, $\{\alpha_1, \alpha_2, \dots, \alpha_t\} = \text{Gal}(K(\bar{\chi}_i), K)$ e V^{α_j} é um $K(\bar{\chi}_i)G$ -módulo absolutamente irredutível associado ao caráter conjugado $\bar{\chi}_i^{\alpha_j}$ de $\bar{\chi}_i$.

Como $K(\bar{\chi}_i) = D_i$, $s_K(\bar{\chi}_i) = \sqrt{\dim_{K(\bar{\chi}_i)} D_i} = 1$, e tomando

dimensões sobre K em ambos os membros da igualdade (3.2.3) temos

$$r_i \dim_K K(\bar{\chi}_i) = 1 \cdot \text{grau } \bar{\chi}_i \cdot \dim_K K(\bar{\chi}_i)$$

$$\text{Donde grau } \bar{\chi}_i = r_i.$$

Se χ é um carater de G sobre $\mathbb{Q}(\epsilon)$, onde ϵ é uma raiz n -ésima primitiva da unidade sobre $\mathbb{Q}$, podemos vê-lo como um carater sobre $\mathbb{Z}[\epsilon]$, pois $\mathbb{Z}[\chi] \subset \mathbb{Z}[\epsilon] = \text{int } \mathbb{Q}(\epsilon)$. Seja P um divisor de p em $\mathbb{Z}[\epsilon]$. Temos:

$$\frac{\mathbb{Z}[\epsilon]}{P} = K(\bar{\epsilon}). \text{ Se } \pi \text{ denota a projeção canônica}$$

$$\mathbb{Z}[\epsilon] \longrightarrow \frac{\mathbb{Z}[\epsilon]}{P}, \text{ a todo carater } \chi \text{ de } G \text{ sobre } \mathbb{Z}[\epsilon] \text{ fica asso-}$$

ciado um carater $\bar{\chi}$ de G sobre $K(\bar{\epsilon})$, definindo $\bar{\chi} = \pi \circ \chi$.

$$G \longrightarrow \mathbb{Z}[\epsilon] \xrightarrow{\pi} \frac{\mathbb{Z}[\epsilon]}{P} = K(\bar{\epsilon})$$

ii) Todo carater absolutamente irreduzível $\bar{\chi}_i$ de G sobre $K(\bar{\epsilon})$ é da forma $\bar{\chi}_i = \pi \circ \chi_i$ e $\text{grau } \chi_i = \text{grau } \bar{\chi}_i$.

Conforme C.W. Curtis e I. Reiner [7], teorema 86.3., sabemos que se χ é irreduzível então $\bar{\chi}$ também é irreduzível. Ainda por [7], teorema 76.17, temos que $\chi \sim \theta$ se e somente se $\bar{\chi} \sim \bar{\theta}$.

Além disso, conforme [7], teorema 83.5 (Brauer), podemos afirmar que o número $\bar{\lambda}$ de caracteres absolutamente irreduzíveis não equivalentes de G sobre $K(\bar{\epsilon})$ é igual ao número de classes conjugadas p -regulares, isto é, classes onde todo elemento tem ordem não divisível por p . Como $p \nmid |G|$, toda classe conjugada

da é p -regular. Agora o número λ de caracteres absolutamente irreduzíveis não equivalentes de G sobre $\mathbb{Q}(\epsilon)$ é igual ao número de classes conjugadas de G . Logo $\bar{\lambda} = \lambda$.

Podemos concluir pelo exposto acima que todo caráter absolutamente irreduzível $\bar{\chi}_i$ de G sobre $K(\epsilon)$ é da forma $\bar{\chi}_i = \pi \circ \chi_i$,

onde χ_i é um caráter absolutamente irreduzível de G sobre $\mathbb{Q}(\epsilon)$

(ou $\mathbb{Z}[\epsilon]$) e π é a projeção canônica $\mathbb{Z}[\epsilon] \xrightarrow{\pi} \frac{\mathbb{Z}[\epsilon]}{P}$

Se T_i é a matriz da representação de caráter χ_i , então $\bar{T}_i$, a matriz da representação de caráter $\bar{\chi}_i$, é obtida de T_i tomando-se os coeficientes em $\frac{\mathbb{Z}[\epsilon]}{P}$.

Portanto $\text{grau } \chi_i = \text{grau } \bar{\chi}_i$

iii) $\mathbb{Q}G$ determina grau χ_i .

Temos que $\mathbb{Q}G \cong \bigoplus \alpha_i M_{n_i}(D_i')$. Se W é um $\mathbb{Q}G$ -módulo irreduzível associado à componente $M_{n_i}(D_i')$ e χ_i é um caráter absolutamente irreduzível de G sobre $\mathbb{Q}(\epsilon)$ associado à mesma componente temos que $\text{centro } D_i' = \mathbb{Q}(\chi_i)$.

Conforme L. Dornhoff [22], teorema 24.14, o $\mathbb{Q}(\chi_i)G$ -módulo $W^{\mathbb{Q}(\chi_i)}$ se decompõe do seguinte modo:

$$W^{\mathbb{Q}(\chi_i)} = s \cdot (V \oplus V^{\sigma_2} \oplus \dots \oplus V^{\sigma_k}), \quad (3.2.4.),$$

onde agora $s = s_{\mathbb{Q}}(\chi_i) = \sqrt{\dim_{\mathbb{Q}(\chi_i)} D_i^r}$, V é um $\mathbb{Q}(\chi_i)$ - G -módulo /
absolutamente irredutível associado a χ_i , $\{\sigma_1, \sigma_2, \dots, \sigma_k\} =$ /
 $= \text{Gal}(\mathbb{Q}(\chi_i), \mathbb{Q})$ e V^{σ_j} é um $\mathbb{Q}(\chi_i)$ G -módulo absolutamente irre-
dutível associado ao carater conjugado $\chi_i^{\sigma_j}$ de χ_i .

Tomando dimensão sobre $\mathbb{Q}$ em (3.2.4), vem $n_i \cdot \dim_{\mathbb{Q}} D_i =$
 $s \cdot \dim_{\mathbb{Q}} \mathbb{Q}(\chi_i) \cdot \text{grau } \chi_i = s \cdot k \cdot \text{grau } \chi_i$, donde $\text{grau } \chi_i = \frac{n_i \dim_{\mathbb{Q}} D_i}{s \cdot k}$

Por i), ii) e iii) concluimos que $\mathbb{Q}G$ determina os in-
teiros r_i .

Passo 2.. $\mathbb{Q}G$ determina $K(\bar{\chi}_i)$.

Pelo lema 3.2.1, $\text{int } \mathbb{Q}(\chi_i) \supset \mathbb{Z}[\chi_i] \supset |G|^r \text{ int } \mathbb{Q}(\chi_i)$

Como $(p, |G|^r) = 1$, existem inteiros a e b tais que

$$a \cdot |G|^r + bp = 1, \text{ e } \text{int } \mathbb{Q}(\chi_i) = a|G|^r \text{ int } \mathbb{Q}(\chi_i) + bp.$$

$$\text{int } \mathbb{Q}(\chi_i) \subset \mathbb{Z}[\chi_i] + P.$$

Assim

$$\frac{\text{int } \mathbb{Q}(\chi_i) + P}{P} = \frac{\mathbb{Z}[\chi_i] + P}{P} \cong \frac{\mathbb{Z}[\chi_i]}{\mathbb{Z}[\chi_i] \cap P} = K(\bar{\chi}_i)$$

Temos que $\mathbb{Q}G$ determina $\mathbb{Q}(\chi_i)$. Este determina /

$$\text{int } \mathbb{Q}(\chi_i) \text{ e } K(\bar{\chi}_i) = \frac{\text{int } \mathbb{Q}(\chi_i) + P}{P}. \text{ Logo } \mathbb{Q}G \text{ determina } K(\bar{\chi}_i).$$

Passo 3. $\mathbb{Q}G$ determina os coeficientes a_i da decomposição de KG .

$\mathbb{Q}G$ possui α_i somandos isomorfos a $M_{n_i}(D_i)$. Cada somando $M_{n_i}(D_i)$ está associado a um caráter irreduzível de G sobre $\mathbb{Q}$ que se parte por (3.2.4.) em $s_{\mathbb{Q}}(\chi_i) \cdot \dim_{\mathbb{Q}} \mathbb{Q}(\chi_i)$ caracteres absolutamente irreduzíveis não equivalentes de G sobre $\mathbb{Q}(\epsilon)$. Logo existem $n_i = \alpha_i \cdot s_{\mathbb{Q}}(\chi_i) \cdot \dim_{\mathbb{Q}} \mathbb{Q}(\chi_i)$ caracteres absolutamente irreduzíveis não equivalentes de G sobre $\mathbb{Q}(\epsilon)$ que dão origem a n_i caracteres absolutamente irreduzíveis não equivalentes de G sobre $K(\bar{\epsilon})$, e esses são todos os de grau r_i .

KG possui a_i somandos isomorfos a $M_{r_i}(K(\bar{\chi}_i))$. Cada somando $M_{r_i}(K(\bar{\chi}_i))$ está associado a um caráter irreduzível de G sobre K que se parte por (3.2.3.) em $t = \dim_K K(\bar{\chi}_i)$ caracteres absolutamente irreduzíveis não equivalentes de G sobre $K(\bar{\epsilon})$. Logo existem $a_i \cdot t$ caracteres absolutamente irreduzíveis não equivalentes de G sobre $K(\bar{\epsilon})$ de grau r_i e esses são todos. Logo

$n_i = a_i \cdot t$. Onde

$$a_i = \frac{n_i}{t} = \frac{\alpha_i \cdot s_{\mathbb{Q}}(\chi_i) \cdot \dim_{\mathbb{Q}} \mathbb{Q}(\chi_i)}{\dim_K K(\bar{\chi}_i)}$$

Portanto $\mathbb{Q}G$ determina os coeficientes a_i .

Teorema 3.2.5. Existem pelo menos $p^{B(n)}$ grupos não isomorfos de ordem p^n , onde $B(n) = \frac{2(n^3 - 17n^2)}{27}$, cujas álgebras de grupo, sobre todos os corpos de característica diferente de p , são isomorfas.

Demonstração - Em virtude do teorema 3.2.2. é suficiente provar que existem pelo menos $p^{B(n)}$ grupos de ordem p^n não isomorfos, com álgebras de grupo sobre $\mathbb{Q}$ isomorfas.

Seja então G um p -grupo. Sabemos que $\mathbb{Q}G \cong \bigoplus M_{n_i}(D_i)$.

Seja T uma representação absolutamente irredutível / associada a $M_n(D)$ de grau r , cujo carater é χ . Conforme P. Roquette [23] (satz 1 e pg. 249), se $p > 2$ então $D = \mathbb{Q}(\chi)$ e $r = n$; se $p = 2$ então $D = \mathbb{Q}(\chi)$ e $r = n$ ou $\mathbb{Q}(\chi)$ é um corpo real, D é o / anel com divisão dos quatêrnios racionais e $r = 2n$.

Vamos supor que G tem período p^2 . Sejam θ_p^i $i = 1, 2$, raízes primitivas da unidade de ordem p^i sobre $\mathbb{Q}$. Então / $\mathbb{Q}(\theta_p) \subseteq \mathbb{Q}(\chi) \subseteq \mathbb{Q}(\theta_{p^2})$.

A segunda inclusão é clara, pois todo $\chi(g)$ é soma de raízes p^2 -ésimas da unidade. Para a primeira inclusão basta notar que considerando g um elemento de ordem p no centro de G então $T(g)$ é uma matriz que comuta com todas as outras, logo escalar. Além disso $(T(g))^p = I_r$, o que implica $T(g) = \theta_p \cdot I_r$. Portanto $\chi(g) = r \cdot \theta_p$, isto é, $\theta_p = \frac{\chi(g)}{r} \in \mathbb{Q}(\chi)$. Assim $\mathbb{Q}(\theta_p) \subseteq \mathbb{Q}(\chi)$.

Como não existe corpo intermediário entre $\mathbb{Q}(\theta_p)$ e $\mathbb{Q}(\theta_{p^2})$ tem-se que

$$\mathbb{Q}(\chi) = \mathbb{Q}(\theta_p) \quad \text{e} \quad \dim_{\mathbb{Q}} \mathbb{Q}(\theta) = p-1$$

ou $\mathbb{Q}(\chi) = \mathbb{Q}(\theta_{p^2}) \quad \text{e} \quad \dim_{\mathbb{Q}} \mathbb{Q}(\chi) = p \cdot (p-1)$

Como grau $T = r$ divide $|G|$, tem-se $r = p^i$.

Suponhamos $p > 2$. Como

$$\mathbb{Q}G \cong \mathbb{Q} \oplus \bigoplus_i a_i M_{p^i}(\mathbb{Q}(\theta_p)) \oplus \bigoplus_j b_j M_{p^j}(\mathbb{Q}(\theta_{p^2})), \quad \text{tomando dimen}$$

sões sobre $\mathbb{Q}$, supondo $|G| = p^n$, temos

$$p^n = 1 + \sum_i a_i p^{2i} (p-1) + \sum_j b_j p^{2j} \cdot p \cdot (p-1).$$

o que implica

$$0 \leq a_i \leq \frac{p^n - 1}{(p-1)p^{2i}} \leq p^{n-2i-1}$$

$$0 \leq b_j \leq \frac{p^{n-1}}{(p-1)p^{2j+1}} \leq p^{n-2j-1-1}$$

Assim o número de possíveis álgebras de grupo é menor ou igual a

$$\prod_{i,j} p^{n-2i} p^{n-2j-1} = \prod_{k=0}^n p^k = p^{\frac{n(n+1)}{2}}$$

Agora suponhamos $p = 2$. Então

$$\mathbb{Q}G \cong \bigoplus_i a_i M_{2^i}(\mathbb{Q}) \oplus \bigoplus_j b_j M_{2^j}(\mathbb{Q}(\sqrt{-1})) \oplus \bigoplus_k c_k M_{2^k}(D),$$

onde D é o anel dos quaternions racionais. Tomando dimensões sobre $\mathbb{Q}$ temos

$$2^n = \sum_i a_i 2^{2i} + \sum_j b_j 2^{2j+1} + \sum_k c_k 2^{2k+2}$$

Daqui tiramos:

$$1 \leq a_0 \leq 2^n \quad 0 \leq a_i \leq 2^{n-2i} - 1, \quad i > 0$$

$$0 \leq b_j \leq 2^{n-2j-1} - 1$$

$$0 \leq c_k \leq 2^{n-2k-2} - 1$$

Portanto existem no máximo

$$\left\{ \prod_i 2^{n-2i} \right\} \left\{ \prod_j 2^{n-2j-1} \right\} \left\{ \prod_k 2^{n-2k-2} \right\} \leq 2^{\frac{3n^2}{4}} \quad \text{possíveis algebras.}$$

Como $\frac{3n^2}{4} \geq \frac{n(n+1)}{2}$ vemos que para todo primo p existem no máximo $p^{e(n)}$ algebras de grupo sobre $\mathbb{Q}$ para grupos de ordem p^n e período p^2 , onde $e(n) = \frac{3n^2}{4}$.

Conforme G. Higman [24], teorema 2.3., existem no máximo $p^{f(n)}$ grupos de ordem p^n e período p^2 , onde $f(n) = \frac{2(n^3 - 6n^2)}{27}$.

Portanto existe um conjunto com pelo menos $p^{f(n) - e(n)} \geq \frac{1}{27} p^{\frac{2(n^3 - 17n^2)}{27}}$ grupos de ordem p^n não isomorfos com álgebras de grupo sobre $\mathbb{Q}$ (e portanto sobre todos os corpos de característica diferente de p) isomorfas.

CAPÍTULO IV - ÁLGEBRAS DE GRUPOS SOBRE CORPOS CUJA CARACTERÍSTICA
DIVIDE A ORDEM DO GRUPO.

4.1. AS ÁLGEBRAS DOS GRUPOS DIEDRAIS E DOS GRUPOS QUATERNIÔNICOS.

Designaremos por D_{2n} o grupo diedral de ordem $2n$.

$$D_{2n} = \{1, a, a^2, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b\} \text{ com } a^n = b^2 = (ab)^2 = 1.$$

Designaremos por Δ_{4m} o grupo quaterniônico de ordem $4m$.

$$\Delta_{4m} = \{1, c, c^2, \dots, c^{2m-1}, d, cd, \dots, c^{2m-1}d\}$$

$$\text{com } c^m = d^2 = (cd)^2 \text{ e } c^{2m} = 1.$$

O resultado seguinte é conhecido:

Proposição 4.1.1. Sejam R um anel comutativo com elemento unidade;

G um grupo finito; $C_1, C_2, \dots, C_s$ as classes conjugadas de G e

$$\gamma_i = \sum_{x \in C_i} x \text{ a soma dos elementos da classe } C_i. \text{ Então o centro de } RG$$

é a subálgebra de RG com base $\{\gamma_1, \gamma_2, \dots, \gamma_s\}$ sobre R .

Proposição 4.1.2. A dimensão do centro de RD_{2n} é $\frac{n+6}{2}$ se n é par,
ou $\frac{n+3}{2}$ se n é ímpar.

Demonstração: Em D_{2n} , para todos i, j temos

$$(a^j b) a^i (a^j b)^{-1} = a^j b a^i a^j b = a^{-i}$$

$$a^j a^i b a^{-j} = a^{i+2j} b$$

$$(a^j b) (a^i b) (a^j b)^{-1} = a^{-i+2j} b$$

Se n é par, escrevendo $n = 2m$, uma base do centro de RD_{2n} é

$$B = \{1, a+a^{2m-1}, a^2+a^{2m-2}, a^3+a^{2m-3}, \dots, a^{m-1}+a^{m+1}, a^m, \\ b+a^2b+a^4b+\dots+a^{2m-2}b, ab+a^3b+\dots+a^{2m-1}b\}.$$

$$\text{Logo dim centro } RD_{2n} = 1+m+2 = 3+\frac{n}{2} = \frac{n+6}{2}.$$

Se n é ímpar, escrevendo $n=2m+1$, uma base do centro de RD_{2n} é

$$B' = \{1, a+a^{2m}, a^2+a^{2m-1}, \dots, a^m+a^{m+1}, b+ab+a^2b+\dots+a^{2m}b\} \quad (II)$$

$$\text{Logo dim centro } RD_{2n} = 1+m+1 = 2+\frac{n-1}{2} = \frac{n+3}{2}.$$

Proposição 4.1.3. A dimensão do centro de $R\Delta_{4m}$ é $m+3$.

Demonstração: Em Δ_{4m} , para todos i, j , temos

$$(c^j d) c^i (c^j d)^{-1} = c^i$$

$$c^j (c^i d) c^{-j} = c^{i+2j} d$$

$$(c^j d) (c^i d) (c^j d)^{-1} = c^{-i+2j} d$$

Uma base para o centro de $R\Delta_{4m}$ é

$$C = \{1, c+c^{2m-1}, c^2+c^{2m-2}, c^3+c^{2m-3}, \dots, c^{m-1}+c^{m+1}, c^m, \\ d+c^2d+\dots+c^{2m-2}d, cd+c^3d+\dots+c^{2m-1}d\}$$

$$\text{Logo dim centro } R\Delta_{4m} = m+3.$$

Proposição 4.1.4. Para todo m par, o centro de RD_{4m} e o centro de $R\Delta_{4m}$ são álgebras isomorfas.

Demonstração: Como $\dim \text{centro } RD_{4m} = \dim \text{centro } R\Delta_{4m} = m+3$, segue que $\text{centro } RD_{4m} \cong \text{centro } R\Delta_{4m}$ como R -módulos. Comparando a tábua

de multiplicação da base B do centro de RD_{4m} com a tábua de multiplicação da base C do centro de RA_{4m} , vemos que o isomorfismo de R-módulos que a cada elemento $x_i \in B$ associa o elemento $y_i \in C$, é um isomorfismo de anéis.

Seja $\mathbb{Z}_2$ o corpo com dois elementos.

Proposição 4.1.5. Para todo m ímpar, $m \neq 1$, o centro de $\mathbb{Z}_2 D_{4m}$ e o centro de $\mathbb{Z}_2 \Delta_{4m}$ são álgebras não isomorfas.

Demonstração: Seja m um natural ímpar $\neq 1$. Seja $x \in \mathbb{Z}_2 D_{4m}$. Então

$$\begin{aligned} x = & x_1 + x_2(a + a^{2m-1}) + x_3(a^2 + a^{2m-2}) + x_4(a^3 + a^{2m-3}) + \dots + \\ & + x_m(a^{m-1} + a^{m+1}) + x_{m+1}a^m + \\ & + x_{m+2}(b + a^2b + a^4b + \dots + a^{2m-2}b) + \\ & + x_{m+3}(ab + a^3b + a^5b + \dots + a^{2m-1}b) \end{aligned}$$

$$\begin{aligned} e x^2 = & (x_1 + x_{m+1} + x_{m+2} + x_{m+3}) + (x_2 + x_m + x_{m+2} + x_{m+3})(a^2 + a^{2m-2}) + \\ & + (x_3 + x_{m-1} + x_{m+2} + x_{m+3})(a^4 + a^{2m-4}) + \\ & + (x_4 + x_{m-2} + x_{m+2} + x_{m+3})(a^6 + a^{2m-6}) + \\ & + \dots + \left(\frac{x_{m+1}}{2} + \frac{x_{m+3}}{2} + x_{m+2} + x_{m+3}\right)(a^{m-1} + a^{m+1}). \end{aligned}$$

Seja $s \neq 0$ tal que $m | 2^s - 1$, por exemplo $s = \phi(m)$, onde ϕ é a função de Euler.

Então $(a^2)^{2^s} = a^2$. Para todo $x \in$ centro $\mathbb{Z}_2 D_{4m}$ tem-se

$$(x^2)^{2^s} = x^2.$$

No centro de $\mathbb{Z}_2^{\Delta_{4m}}$, pelo contrário, tem-se

$$(d+c^2d+c^4d+\dots+c^{2m-2}d)^2 = c + c^3 + c^5 + \dots + c^{2m-1} \text{ e para todo } s \neq 0$$

$$((d+c^2d+c^4d+\dots+c^{2m-2}d)^2)^{2^s} = 1 + c^2 + c^4 + \dots + c^{2m-2}.$$

Logo, centro $\mathbb{Z}_2^{D_{4m}} \neq$ centro $\mathbb{Z}_2^{\Delta_{4m}}$ como álgebras.

Corolário 4.1.6. Para todo m ímpar $\neq 1$, as álgebras $\mathbb{Z}_2^{D_{4m}}$ e $\mathbb{Z}_2^{\Delta_{4m}}$ não são isomorfas.

4.2. AS $\mathbb{Z}_2$ -ÁLGEBRAS DOS GRUPOS NÃO ABELIANOS DE ORDEM 8.

Provaremos que as $\mathbb{Z}_2$ -álgebras dos dois grupos não abelianos de ordem 8 não são isomorfas. Esses dois grupos são:

$$D_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\} \text{ com } a^4 = b^2 = (ab)^2 = 1$$

$$\text{e } \Delta = \{1, \bar{1}, i, \bar{i}, j, \bar{j}, k, \bar{k}\} \text{ com } i\bar{i} = j\bar{j} = k\bar{k} = 1 \text{ e}$$

$$i^2 = j^2 = k^2 = ijk = \bar{1} \quad (\text{isomorfo a } \Delta_8)$$

Lema 4.2.1. Se $x = x_1 + \bar{x}_1\bar{1} + x_i i + \bar{x}_i\bar{i} + x_j j + \bar{x}_j\bar{j} + x_k k + \bar{x}_k\bar{k}$ e $\mathbb{Z}_2(\Delta)$ então

$$(a) \quad x^2 = (x_1 + \bar{x}_1) + (x_i + \bar{x}_i + x_j + \bar{x}_j + x_k + \bar{x}_k)\bar{1} + (x_j + \bar{x}_j)(x_k + \bar{x}_k)(i + \bar{i}) + (x_k + \bar{x}_k)(x_i + \bar{x}_i)(j + \bar{j}) + (x_i + \bar{x}_i)(x_j + \bar{x}_j)(k + \bar{k})$$

$$(b) \quad x^2 = 1 \iff \{x_1, \bar{x}_1\} = \{0, 1\}, \quad x_i = \bar{x}_i, \quad x_j = \bar{x}_j, \quad x_k = \bar{x}_k$$

$$(c) \quad x^4 = 1 \iff \{x_1 + \bar{x}_1, x_i + \bar{x}_i + x_j + \bar{x}_j + x_k + \bar{x}_k\} = \{0, 1\}$$

Demonstração: (a) é imediato. (c) resulta de (a) e (b). Vamos demonstrar (b). Ora, $x^2=1$ se e somente se $x_1 + \bar{x}_1 = 1$ e

$$x_i + \bar{x}_i + x_j + \bar{x}_j + x_k + \bar{x}_k = (x_j + \bar{x}_j)(x_k + \bar{x}_k) = (x_k + \bar{x}_k)(x_i + \bar{x}_i) = (x_i + \bar{x}_i)(x_j + \bar{x}_j) = 0.$$

Segue que se $x^2 = 1$ então $\{x_1, \bar{x}_1\} = \{0, 1\}$ e

$$\begin{aligned} 0 &= (x_j + \bar{x}_j)(x_k + \bar{x}_k) \\ &= (x_j + \bar{x}_j)((x_i + \bar{x}_i) + (x_j + \bar{x}_j)) \\ &= (x_j + \bar{x}_j)(x_i + \bar{x}_i) + (x_j + \bar{x}_j)^2 \end{aligned}$$

Como $(x_j + \bar{x}_j)(x_i + \bar{x}_i) = 0$ tem-se $(x_j + \bar{x}_j)^2 = 0$, ou, $x_j + \bar{x}_j = 0$.

Analogamente $x_i = \bar{x}_i$ e $x_k = \bar{x}_k$.

A recíproca é uma consequência imediata de (a).

Teorema 4.2.2. As álgebras $\mathbb{Z}_2 D_8$ e $\mathbb{Z}_2 \Delta$ não são isomorfas.

Demonstração: É suficiente mostrar que não existem $x, y \in \mathbb{Z}_2 \Delta$ tais que $x^4 = y^2 = (xy)^2 = 1$, $x^2 \neq 1$.

Sejam $x, y \in \mathbb{Z}_2(\Delta)$ tais que $x^4 = y^2 = 1$. Em virtude do lema 4.2.1., partes (b) e (c) esses elementos se escrevem

$$x = a_1 + \bar{a}_1 \bar{1} + a_i i + \bar{a}_i \bar{1} + a_j j + \bar{a}_j \bar{j} + a_k k + \bar{a}_k \bar{k}$$

$$y = b_1 + \bar{b}_1 \bar{1} + b_i (i + \bar{1}) + b_j (j + \bar{j}) + b_k (k + \bar{k}),$$

$$\text{com } \{a_1 + \bar{a}_1, a_i + \bar{a}_i + a_j + \bar{a}_j + a_k + \bar{a}_k\} = \{b_1, \bar{b}_1\} = \{0, 1\} \quad (I)$$

Se $(xy)^2 = 1$, então os coeficientes de i e $\bar{i}$ na expressão de xy são iguais, segundo o lema 4.2.1., donde

$$\begin{aligned} a_1 b_i + \bar{a}_1 b_i + a_i b_1 + \bar{a}_i \bar{b}_1 + a_j b_k + a_k b_j + \bar{a}_k b_j &= \\ = a_1 b_i + \bar{a}_1 b_i + a_i \bar{b}_1 + \bar{a}_i b_1 + a_j b_k + \bar{a}_j b_k + a_k b_j + \bar{a}_k b_j \end{aligned}$$

o que implica $a_i b_1 + \bar{a}_i \bar{b}_1 = a_i \bar{b}_1 + \bar{a}_i b_1$

donde, em virtude de (I): $a_i = \bar{a}_i$ (II).

Do mesmo modo se prova que $a_j = \bar{a}_j$ e $a_k = \bar{a}_k$ (III).

Segue $a_i + \bar{a}_i + a_j + \bar{a}_j + a_k + \bar{a}_k = 0$ e levando em conta (I), deduzimos que $a_1 + \bar{a}_1 = 1$ (IV).

De (I), (III) e (IV) tem-se pelo lema 4.2.1. que $x^2 = 1$ o que termina a demonstração.

Em [8], conforme citamos na introdução, W.E. Deskins demonstrou

Teorema 4.2.3. Se P e P' são p -grupos abelianos e F é um corpo de característica p , então $FP \cong FP'$ se e somente se $P \cong P'$.

Combinando este resultado com o teorema 4.2.2. temos

Teorema 4.2.4. Se G e H são grupos de ordem 8 então $\mathbb{Z}_2 G \cong \mathbb{Z}_2 H$ se e somente se $G \cong H$.

4.3. AS ÁLGEBRAS DOS GRUPOS NÃO ABELIANOS DE ORDEM 12 RELATIVAMENTE A $\mathbb{Z}_2$ E $\mathbb{Z}_3$.

Provaremos que as $\mathbb{Z}_2$ -álgebras (respectivamente $\mathbb{Z}_3$ -álgebras) dos três grupos não abelianos de ordem 12 são duas a duas

não isomorfas.

Esses três grupos são

o grupo alternado de grau 4

$$A_4 = \{1, r, s, r^2, rs, sr, s^2, rs^2, r^2s, sr^2, s^2r, rs^2r\}$$

com $r^3 = s^3 = (sr)^2 = 1$;

o grupo diedral de ordem 12

$$D_{12} = \langle a, b \rangle \text{ com } a^6 = b^2 = (ab)^2 = 1 ;$$

e o grupo quaterniônico de ordem 12

$$\Delta_{12} = \langle c, d \rangle \text{ com } c^3 = d^2 = (cd)^2, c^6 = 1.$$

Uma base do centro de RA_4 é

$$\{1, r+s^2+r^2s+sr^2, s+r^2+s^2r+rs^2, rs+sr+rs^2r\}$$

donde $\dim \text{centro } RA_4 = 4$.

Sabemos pelas proposições 4.1.2. e 4.1.3. que

$$\dim \text{centro } RD_{12} = \dim \text{centro } R\Delta_{12} = 6, \text{ donde se deduz}$$

imediatamente

Proposição 4.3.1. Para todo anel comutativo R com elemento unida-
de tem $RA_4 \not\cong RD_{12}$ e $RA_4 \not\cong R\Delta_{12}$.

Proposição 4.3.2. As álgebras $\mathbb{Z}_2 D_{12}$ e $\mathbb{Z}_2 \Delta_{12}$ não são isomorfas.

Demonstração: Caso particular do corolário 4.1.6.

Em [8], W.E. Deskins demonstrou:

Proposição 4.3.3. Se H é um p -subgrupo de Sylow normal de G e F é
um corpo de característica p então $\text{rad } FG = L(H)$.

Proposição 4.3.4. As álgebras $\mathbb{Z}_3 D_{12}$ e $\mathbb{Z}_3 \Delta_{12}$ não são isomorfas.

Demonstração: Provaremos que o radical de $\mathbb{Z}_3 D_{12}$ não é isomorfo ao radical $\mathbb{Z}_3 \Delta_{12}$.

O subgrupo $H = \{1, a^2, a^4\}$ é o único 3-subgrupo de Sylow de D_{12} , donde $\dim \text{rad } \mathbb{Z}_3 D_{12} = 8$ e uma base do radical de $\mathbb{Z}_3 D_{12}$ é $\{a^2-1, a^4-1, a^3-a, a^5-a, a^4b-b, a^2b-b, a^5b-ab, a^3b-ab\}$.

Um cálculo direto mostra que um elemento $x = \alpha_1(a^2-1) + \alpha_2(a^4-1) + \alpha_3(a^3-a) + \alpha_4(a^5-a) + \alpha_5(a^4b-b) + \alpha_6(a^2b-b) + \alpha_7(a^5b-ab) + \alpha_8(a^3b-ab)$ do radical está no centro do radical de $\mathbb{Z}_3 D_{12}$ se e somente se $\alpha_1 = \alpha_2, \alpha_3 = \alpha_4, \alpha_5 = \alpha_6, \alpha_7 = \alpha_8$. Portanto uma base do centro do radical de $\mathbb{Z}_3 D_{12}$ é $\{1+a^2+a^4, a+a^3+a^5, b+a^2b+a^4b, ab+a^3b+a^5b\}$.

Prolongamos essa base à base $\{1+a^2+a^4, a+a^3+a^5, b+a^2b+a^4b, ab+a^3b+a^5b, 2+a^2+2b+a^2b, 2+a^2+ab+2a^3b, 1+2a^2+2b+a^2b, 2+a^3+2b+a^2b\}$ do radical de $\mathbb{Z}_3 D_{12}$. Todos os elementos dessa base são de quadrado nulo.

Se os radicais de $\mathbb{Z}_3 D_{12}$ e $\mathbb{Z}_3 \Delta_{12}$ fossem isomorfos, existiria uma base de $\mathbb{Z}_3 \Delta_{12}$ formada por elementos de quadrado nulo. Vamos mostrar que isso não é possível.

Como $\{1, c^2, c^4\}$ é o único 3-subgrupo de Sylow de Δ_{12} , o radical de $\mathbb{Z}_3 \Delta_{12}$ é de dimensão 8. Um cálculo direto mostra que $\{1+c^2+c^4, c+c^3+c^5, d+c^2d+c^4d, cd+c^3d+c^5d\}$ é uma base do centro do radical de $\mathbb{Z}_3 \Delta_{12}$. Prolonguemos essa base à base

$e = \{1+c^2+c^4, c+c^3+c^5, d+c^2d+c^4d, cd+c^3d+c^5d, 2+2c+c^2+c^3+d+cd+2c^2d+2c^3d, 1+c+2c^2+2c^3+d+cd+2c^2d+2c^3d, 2+c^2, 2d+c^2d\}$

do radical de $\mathbb{Z}_3\Delta_{12}$. Os seis primeiros elementos desta base são de quadrado nulo.

Se $x = \sum_{i=1}^8 x_i e_i$ é um elemento do radical de $\mathbb{Z}_3\Delta_{12}$, com

$\{e_1, e_2, \dots, e_8\} = e$, então

$$x^2 = (x_5x_6 + 2x_5x_7 + 2x_5x_8 + x_6x_7 + 2x_6x_8 + x_7^2)(1 + c^2 + c^4) + \\ + (x_5x_6 + 2x_5x_7 + 2x_5x_8 + x_6x_7 + 2x_6x_8 + 2x_8^2)(c + c^3 + c^5).$$

Assim $x^2 = 0$ se e somente se os dois coeficientes são zero.
$$\begin{cases} x_5x_6 + 2x_5x_7 + 2x_5x_8 + x_6x_7 + 2x_6x_8 + x_7^2 = 0 \\ x_5x_6 + 2x_5x_7 + 2x_5x_8 + x_6x_7 + 2x_6x_8 + 2x_8^2 = 0 \end{cases}$$

As únicas soluções desse sistema em $\mathbb{Z}_3$ são

$$(x_5, x_6, x_7, x_8) = (1, 0, 0, 0) ; (x_5, x_6, x_7, x_8) = (2, 0, 0, 0) ;$$

$$(x_5, x_6, x_7, x_8) = (0, 1, 0, 0) ; (x_5, x_6, x_7, x_8) = (0, 2, 0, 0) , \text{ de onde}$$

deduzimos que os elementos não centrais de quadrado nulo no radical de $\mathbb{Z}_2\Delta_{12}$ são os elementos de

$$\text{centro rad } \mathbb{Z}_3\Delta_{12} + \mathbb{Z}_3^* \cdot (2+2c+c^2+c^3) + \mathbb{Z}_3^* \cdot (d+cd+2c^2d+2c^3d).$$

Segue que no radical de $\mathbb{Z}_3\Delta_{12}$, toda família livre de vetores de quadrado nulo compreende no máximo 6 elementos, o que termina a demonstração.

4.4. AS $\mathbb{Z}_2$ -ÁLGEBRAS DOS GRUPOS NÃO ABELIANOS DE ORDEM 16.

Provaremos que as $\mathbb{Z}_2$ -álgebras dos 9 grupos não comutativos de ordem 16 são duas a duas não isomorfas.

Sabemos que o centro de um grupo não abeliano de ordem 16 tem ordem 2 ou 4.

Consideremos as $\mathbb{Z}_2$ -álgebras dos grupos de ordem 16 cujo centro é isomorfo a $\mathbb{Z}_2$. Os três grupos desse tipo são: D_{16} , Δ_{16} e $G = \{1, s, s^2, s^3, s^4, s^5, s^6, s^7, st, s^2t, s^3t, s^4t, s^5t, s^6t, s^7t\}$ com $s^8 = t^2 = 1$ e $ts = s^3t$.

Proposição 4.4.1. Os radicais de $\mathbb{Z}_2 D_{16}$, $\mathbb{Z}_2 \Delta_{16}$ e $\mathbb{Z}_2 G$ são dois a dois não isomorfos.

Demonstração: Com efeito

$e = \{1+a^4, 1+a^2+a^4+a^6, a+a^3+a^5+a^7, b+a^2b+a^4b+a^6b, ab+a^3b+a^5b+a^7b, a+a^7b+a^2b, b+1, ab+1, a^2b+1, a^3b+1, a^4b+1, a^5b+1, a+a^5, a^2+a^4, 1+a\}$ é uma base do radical de $\mathbb{Z}_2 D_{16}$.

Os 13 primeiros elementos da base são de quadrado nulo.

Por cálculo direto se demonstra então que toda família livre de vetores de quadrado nulo no radical de $\mathbb{Z}_2 D_{16}$ compreende no máximo 13 elementos.

De maneira análoga, se mostra que esse número é no máximo 10 no radical de $\mathbb{Z}_2 \Delta_{16}$ e no máximo 12 no radical de $\mathbb{Z}_2 G$.

Consideremos agora as $\mathbb{Z}_4$ -álgebras dos grupos de ordem 16 cujo centro é isomorfo a $\mathbb{Z}_4$. Os grupos desse tipo são:

$X = \{1, p, p^2, p^3, p^4, p^5, p^6, p^7, q, pq, p^2q, p^3q, p^4q, p^5q, p^6q, p^7q\}$ com $p^8 = q^2 = 1$, $qp = p^5q$.

$Y = \{1, r, s, t, rs, sr, rt, tr, st, ts, rst, tsr, rsr, srs, rtr, rsrs\}$ com $r^2 = s^2 = t^2 = 1$, $rst = str = trs$.

Proposição 4.4.2. $\text{rad } \mathbb{Z}_2 X \not\cong \text{rad } \mathbb{Z}_2 Y$

Demonstração: Para todo $x \in \text{rad } \mathbb{Z}_2 Y$ tem-se $x^4 = 0$.

No radical de $\mathbb{Z}_2 X$ tem-se

$$(p^3 q + 1)^4 = p^4 + 1 \neq 0.$$

Consideremos agora as $\mathbb{Z}_2$ -álgebras dos grupos de ordem 16 cujo centro é isomorfo ao grupo de Klein. Os quatro grupos desse tipo são:

$$A = \langle r, s, t \rangle \text{ com } r^2 = s^2 = t^2 = (tr)^2 = (rs)^2 = (st)^4 = 1 \\ (\cong \mathbb{Z}_2 \times D_8)$$

$$B = \langle r, s, t \rangle \text{ com } r^2 = s^2 = (rs)^2; t^2 = r^{-1}trt = s^{-1}tst = 1 \\ (\cong \mathbb{Z}_2 \times \Delta_8)$$

$$C = \langle s, t \rangle \text{ com } s^4 = t^4 = 1, t^{-1}st = s^{-1}$$

$$D = \langle r, s \rangle \text{ com } r^4 = s^4 = (rs)^2 = (r^{-1}s)^2 = 1$$

Proposição 4.4.3. Os radicais de $\mathbb{Z}_2 A$, $\mathbb{Z}_2 B$, $\mathbb{Z}_2 C$ e $\mathbb{Z}_2 D$ são dois a dois não isomorfos.

Demonstração: Por cálculo direto se mostra que o número máximo de vetores linearmente independentes de quadrado nulo é respectivamente

14 em $\text{rad } \mathbb{Z}_2 A$

12 em $\text{rad } \mathbb{Z}_2 B$

12 em $\text{rad } \mathbb{Z}_2 C$

13 em $\text{rad } \mathbb{Z}_2 D$

Vamos mostrar que $\text{rad } \mathbb{Z}_2 B \neq \text{rad } \mathbb{Z}_2 C$.

Em $\text{rad } \mathbb{Z}_2 B$, o subespaço vetorial gerado pelos quadrados admite como base $\{1+r^2, r+r^3, s+s^3, rs+sr, tr+tr^3, ts+ts^3, trs+tsr\}$ e é portanto de dimensão 7. Tal não acontece em $\text{rad } \mathbb{Z}_2 C$, pois o sub-espaço vetorial gerado pelos quadrados admite como base $\{1+t^2, 1+s^2, s+s^3, t^2+s^2+t+s^2t, t^2+s^2+st^3+s^3t^3, 1+t^2+s+s^3+st^2+s^3t^2, 1+s^2+st+s^3t+st^3+s^3t^3, 1+t^2+t+s^2t+t^3+s^2t^3\}$, e sua dimensão é 8.

Em [21], conforme citamos na introdução, H.N. Ward (ou em [16] D. Passman) demonstrou.

Teorema 4.4.4. Se G e H são p -grupos finitos e F é um corpo de característica p então $FG \cong FH$ implica $\text{centro } G \cong \text{centro } H$.

Em consequência das proposições 4.4.1., 4.4.2., 4.4.3., e do teorema 4.4.4., segue

Teorema 4.4.5. As $\mathbb{Z}_2$ -álgebras dos 9 grupos não comutativos de ordem 16 são duas a duas não isomorfas.

Combinando com o teorema 4.2.3. temos

Teorema 4.4.6. Se G e H são grupos de ordem 16 então $F_2 G \cong F_2 H$ se e somente se $G \cong H$.

B I B L I O G R A F I A

- |1| Albert, A. A.; Modern Higher Algebra, University of Chicago Press, Chicago (1944).
- |2| Berman, S. D.; Sur certaines propriétés d'anneaux de groupes sur le champ de nombres rationnels (Russe), Uzgorod. Gos. Univ. Nauch. Zap. Him. Fiz. Mat. 12 (1955), 88 - 110.
- |3| Bourbaki, N.; Algèbre, Chap. III, "Algèbre Multilinéaire", Herman, Paris (1958).
- |4| Bourbaki, N.; Algèbre, Chap. V, "Corps Commutatifs", Herman, Paris (1967)
- |5| Cohen, D. E.; On abelian group algebras, Math. Zeitschr. 105 (1968), 267 - 268.
- |6| Cohn J. A. and Livingstone D.; On groups of order p^3 , Canad. J. Math. 15 (1963), 622 - 624.
- |7| Cohn J. A. and Livingstone D.; Finite groups with isomorphic group algebras, I, Canad. J. Math. 17 (1965), 583 - 593.
- |8| Coleman D. B.; Finite groups with isomorphic group algebras, Trans. Amer. Math. Soc. 105 (1962), 1 - 8.

- |9| Curtis, C. W. and Reiner I.; Representation theory of finite groups and associative algebras, 2^a. ed., Interscience Publishers, N. York (1966).
- |10| Deskins W. E.; Finite abelian groups with isomorphic group algebras, Duke Math. J. 23 (1956), 35 - 40.
- |11| Dornhoff. L.; Group Representation Theory, Part A, Marcel Dekker, Inc., N. York, (1971).
- |12| Guliksen, T., Ribenboim P., Viswanathan T. M., On elementary note on group-rings, Journal für die reine und angewandte Mathematik, 242 (1970), 148 - 162.
- |13| Higman, G.; The units of group rings, Proc. London Math. Soc. 46 (1940), 231 - 248.
- |14| Higman, G.; Enumerating p-groups I: inequalities, Proc. London Math. Soc. (3) 37 (1960), 24 - 30.
- |15| Holvoet, R.; Sur l'isomorphie d'algèbres de groups, Bulletin de la Societé Mathématique de Belgique 20 (1968), 264 - 282.
- |16| Jacobson, N.; Lectures on Abstract Algebra, vol. 3, Princeton, N. J., Van Nostrand, (1964).
- |17| Jones, A.; Representações de álgebras, notas de aula (1973) IME - USP.

- |18| Miller, G. A.; Number of the subgroups of any abelian group, Proc. Nat. Acad. Sci. U.S.A., vol. 25, (1939), 256 - 262.
- |19| Obayashi T.; Solvable groups with isomorphic group algebras, J. Math. Soc. Japan 18 (1966), 394 - 397.
- |20| Passman D. S.; Isomorphic groups and group rings, Pacific J. Math. 15 (1965), 561 - 583.
- |21| Passman D. S.; The group algebras of groups of order p^4 over a modular field, Michigan Math. J. 12 (1965), 420 - 426.
- |22| Perlis, S. and Walker, G. L.; Abelian group algebras of finite order, Trans. Amer. Math. Soc. 68 (1950), 420 - 426.
- |23| Polcino Milies, C.; Sobre as unidades de anéis de grupo, Tese de Mestrado, (1972) , IME - USP.
- |24| Roquette, P.; Realisierung von Darstellungen endlicher nilpotenter Gruppen, Archiv. der Math. 9 (1958), 241 - 250.
- |25| Sehgal, S. K.; On the isomorphism of group algebras, Math. Z. 95 (1967), 71 - 75.
- |26| Sehgal, S. K.; Isomorphism of p-adic group rings, Journal of Number Theory, 2 (1970), 500 - 508.
- |27| Ward, H. N.; Some results on the group algebra of a group over a prime field, Seminar on Finite Groups and Related Topics at Harvard.

|28| Weiss, E., Algebraic Number Theory, Mc Graw - Hill (1963)
N. York.