AUTOMORFISMOS DE GRUPOS FINITOS

por

MARIA CECÍLIA BUENO FISCHER

ESTA DISSERTAÇÃO FOI JULGADA ADEQUADA PARA A OBTENÇÃO DO TÍTULO DE

"MESTRE EM CIÊNCIAS"

ESPECIALIDADE EM MATEMÁTICA, E APROVADA EM SUA FORMA FINAL PELO CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA DA UNIVERSIDADE FEDERAL DE SANTA CATARINA.

Prof. William Glenn Whitley, Ph.D
Coordenador

BANCA EXAMINADORA:

Prof. Andrzej Solecki, Ph.D
Orientador

Prof. Nelo da Silva Allan, Ph.D

Prof. William Glenn Whitley, Ph.D

UNIVERSIDADE FEDERAL DE SANTA CATARINA

AUTOMORFISMOS DE GRUPOS FINITOS

Maria Cecilia Bueno Fischer

Orientador: Andrzej Solecki

Março/1985

Agradeço a todos que, de alguma forma, contribuíram para a realização deste trabalho, em especial ao Andrzej, orientador de dissertação, ao Milton, orientador de curso, à Cleide, à Albertina, ao Flávio, ao Dani e a meu pai.

RESUMO

O objetivo deste trabalho é de obter uma descrição de Aut(G), o grupo de automorfismos de um grupo finito G, tendo como informação inicial apenas o conhecimento da rede de subgrupos de G.

A técnica básica usada aqui é de produto-grinalda. Os resultados obtidos são de dois tipos:

a) uma confirmação de resultados clássicos obtidos por meios diferentes;

b) uma caracterização original de automorfismos de uma classe de grupos que generaliza os grupos diedrais.

Este último resultado constitui o conteúdo do Capítulo VI do trabalho.

ABSTRACT

The objective of this Master's thesis is to obtain a description of Aut(G), the group of automorphisms of a finite group G, when one has only a description of its lattice of subgroups.

The basic technique used here is the wreath-product. The results obtained are of two tipes:

a) a confirmation of classic results obtained by other methods;

b) a original caracterization of automorphisms of a class of groups which generalizes the dihedral groups.

Chapter VI consists of a demonstration of this last result.

CONTEÚDO

INTRODUÇÃO

Neste trabalho, pretendemos estudar automorfismos de um grupo finito G, tendo como informação inicial apenas o conhecimento da rede de subgrupos de G.

Os subgrupos próprios de G têm, como regra, uma estrutura mais simples do que G. Por esta razão, é natural perguntar-se se, conhecendo o grupo de automorfismos Aut(H) para certos subgrupos próprios $H<G$ (onde $<$ denota a relação de inclusão entre os subgrupos), poderíamos obter algumas informações sobre Aut(G). Então, partindo da rede de subgrupos do grupo G e usando o "produto-grinalda" (wreath product) como a ferramenta principal, tentaremos caracterizar o grupo Aut(G).

Antes de iniciarmos este trabalho, fizemos uma consulta a "Reviews on Finite Groups" (veja [5], cap.XVIII - Automorphisms of Groups), que se refere às publicações sobre grupos finitos, do período 1940/1970, e também a "Mathematical Reviews", nas subdivisões referentes à teoria de grupos, nos volumes correspondentes ao período 1971/1983. Nessa consulta, não encontramos nada sobre automorfismos de grupos finitos com o enfoque pretendido neste trabalho.

CAPÍTULO I - NOÇÕES E NOTAÇÕES

Grafo e seus automorfismos:

Um grafo Γ é um par (V,E), onde V é um conjunto finito, não vazio, cujos membros são chamados vértices, e E é um subconjunto do conjunto $V \times V$, de pares de vértices. Os membros de E são chamados arestas (veja [1]).

Definimos um automorfismo de um grafo Γ, $Aut(\Gamma)$, como sendo uma permutação α de V tal que, se $(v, w) \in E$, então $(\alpha v, \alpha w) \in E$, para todos $v, w \in V$.

No nosso estudo, arestas serão formadas por pares de subgrupos, um deles incluído no outro, isto é, pares ordenados. Esta razão nos leva à seguinte definição:

Um grafo é orientado (que indicaremos por Γ_o) quando atribuímos uma ordem a cada um dos pares que constituem as arestas. Geometricamente, as arestas têm um sentido.

Um automorfismo α de um grafo orientado é um automorfismo de grafo que preserva a orientação das arestas; isto é, se (v, w) é uma aresta orientada do grafo, então $(\alpha v, \alpha w)$ é também uma aresta orientada deste grafo.

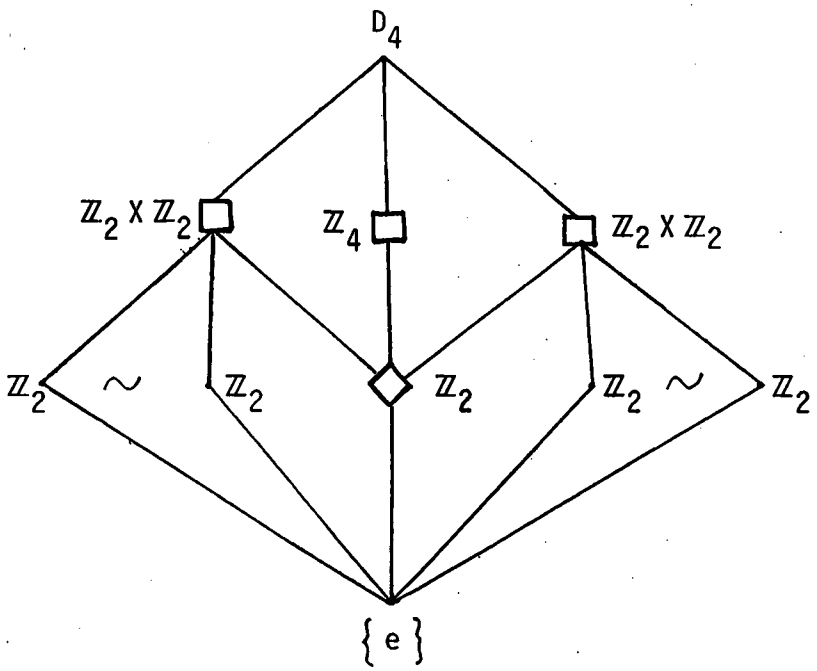
Rede de subgrupos:

A rede de subgrupos de um grupo finito G é um grafo orientado ($\Gamma_o(G)$), cujos vértices correspondem aos subgrupos de G e arestas orientadas (H_1, H_2) correspondem aos pares tais que $H_1 < H_2$.

Podemos visualizar a rede de subgrupos de um grupo num

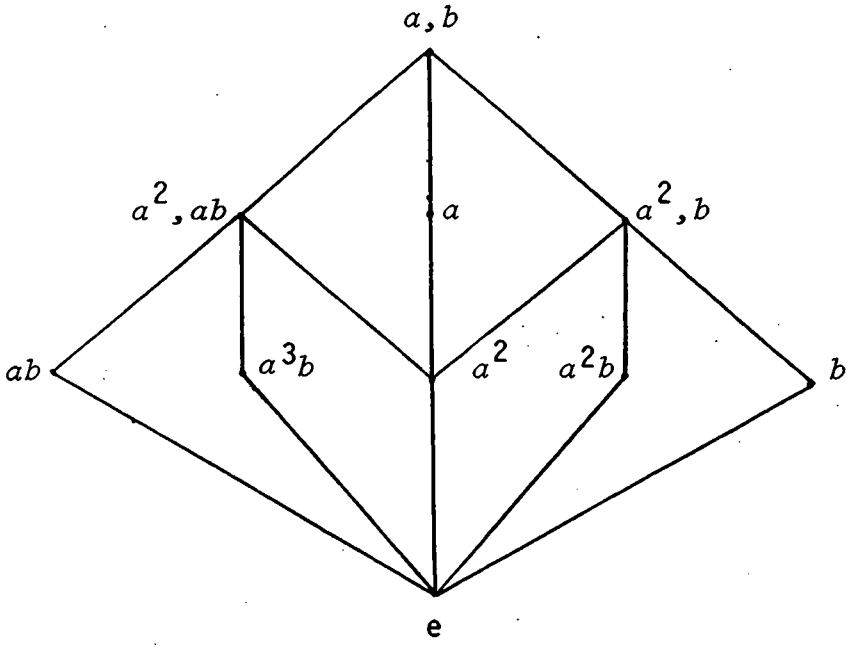
diagrama (isto é, o diagrama é uma interpretação geométrica do grafo). No diagrama, a linha que une dois subgrupos indica a relação de inclusão, onde aquele que está contido fica abaixo daquele que o contêm e, para tornar o diagrama mais transparente, evitam-se as linhas que resultariam, de modo óbvio, pela lei da transitividade.

Por exemplo, representemos a rede de subgrupos para o grupo diedral D_4 que aproveitaremos no Cap.II. (Lembre que grupo diedral D_n é definido por $D_n = (a^n = b^2 = e;\ bab^{-1} = a^{-1})$).



No diagrama, o símbolo $\sim$ entre dois subgrupos indica que os mesmos são conjugados; a moldura $\square$ informa que o subgrupo é normal e $\diamond$ indica o centro do grupo (veja na definição de centralizador, a seguir).

Num grafo, os subgrupos podem ser descritos por seus geradores, como vemos a seguir.



Em certas ocasioẽs, vai nos interessar a rede de subgrupos com certa propriedade, por exemplo, subgrupos normais.

Normalizador:

Seja G um grupo e H um subgrupo de G. O normalizador de H em G, denotado por $N_G(H)$, é o conjunto

$$N_G(H) = \{ g \in G \mid gHg^{-1} = H \}.$$

Note que $N_G(H)$ é subgrupo de G e o subgrupo H é normal em $N_G(H)$. (Notação: $H \lhd N_G(H)$).

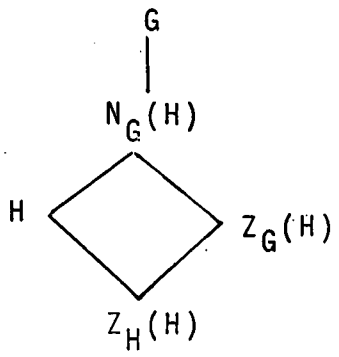
Centralizador:

Seja G um grupo e H um subgrupo de G. O centralizador de H em G, denotado por $Z_G(H)$, é o conjunto

$$Z_G(H) = \{ g \in G \mid ghg^{-1} = h, \quad \forall h \in H \}.$$

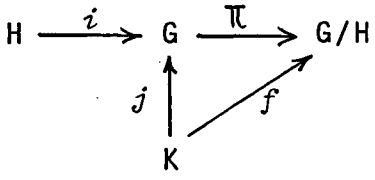
Obviamente, $Z_G(H)$ é subgrupo de G. Além disso, $Z_G(H)$ é também subgrupo de $N_G(H)$.

Note que $H \cap Z_G(H) = Z_H(H) = Z(H)$, o centralizador de H em H, isto é, o centro de H. Isto pode ser visualizado no diagrama



Produto cindido (normal product, splitting extension, semi-direct product):

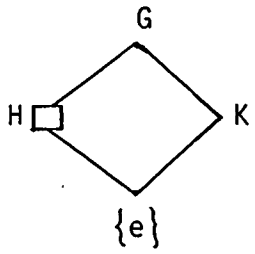
Seja G um grupo finito e H um subgrupo normal de G ($H \lhd G$). Se existe $K < G$, $K \cap H = \{e\}$, tal que $K \cong G/H$, ou seja, se existe isomorfismo $f: K \to G/H$, dizemos que G é produto cindido de H por K. Desta forma, o diagrama abaixo é comutativo



No diagrama, i e j são inclusões de H e K em G, respectivamente, e π é projeção de G em G/H.

Por definição, o subgrupo K atua em H por conjugação de seus elementos, isto é, $khk^{-1} \in H$, para $k \in K$ e $h \in H$.

O produto cindido G pode ser visualizado no seguinte diagrama



(1)

A definição dada explica como um grupo G pode "cindir" em seus dois subgrupos H e K. É óbvio que existe uma correspondência biunívoca entre os elementos de G e pares (h,k) do produto H x K (veja diagrama), com a lei de composição $(h,k).(h',k') = (h.\alpha_k(h'), kk')$, onde $\alpha_k(x) = kxk^{-1}$.

É natural perguntar-se como reverter essa construção ; isto é, dados dois grupos abstratos H e K, como construir um grupo G tal que G cinda, tendo $H' \cong H$ como seu subgrupo normal e tendo $K' \cong K$ isomorfo a sua imagem homomorfa G/H'.

Notamos que, para dar uma definição, é necessário saber como K atua em H, isto é, precisamos de um homomorfismo $\varphi : K \to Aut(H)$.

Definição: A extensão semi-direta de H por K, com dada ação φ , é o grupo de pares $(h,k) \in H \times K$, com a lei de composição: $(h,k).(h',k') = (h.\varphi_k(h'), kk')$ e será denotado por $G = H \rtimes_\varphi K$. Se não houver risco de ambigüidade quanto à ação de φ, escrevemos simplesmente $G = H \rtimes K$.

Verificamos facilmente que, de fato, G é um grupo e que G cinde, com componentes $H' = \{ (h,e) : h \in H \}$ e $K' = \{ (e,k) : k \in K \}$.

Então as duas noções, a do produto cindido e a da extensão semi-direta, estão relacionadas entre si do mesmo modo como as noções de soma direta e de produto cartesiano: a primeira é uma descrição interna, e a segunda, externa.

Produto-grinalda (wreath product):

Seja A um grupo finito e S_n o grupo de todas as permutações de um conjunto de n símbolos. Formemos a extensão semi-direta G, de H por K, onde $H = \underbrace{A \times \ldots \times A}_{n}$ é normal em G, $K \subset S_n$ e as permutações de K atuam em H, permutando somente os índices dos elementos $(a_1, \ldots, a_n) \in H$, isto é, para $\sigma \in K$, $(a_1, \ldots, a_n) \in H$, a ação φ de σ é dada por $\varphi(\sigma)(a_1, \ldots, a_n) = (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$.

Para simplificar a notação, os elementos de G serão indicados através de sequências $(a_1, \ldots, a_n; \sigma)$, onde $a_i \in A$, para $i = 1, 2, \ldots, n$ e $\sigma \in K$, em vez da notação mais correta, mas desnecessariamente formal, $((a_1, \ldots, a_n), \sigma)$.

Então, a lei de composição entre os elementos de G é dada por

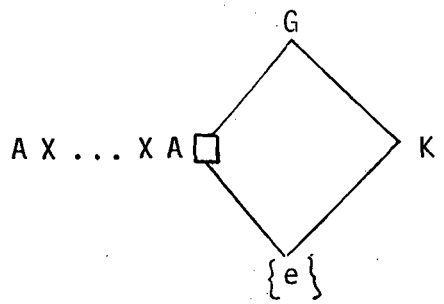
$$(a_1, \ldots, a_n; \sigma)(b_1, \ldots, b_n; \tau) = (a_1 b_{\sigma(1)}, \ldots, a_n b_{\sigma(n)}; \sigma\tau).$$

O grupo G, assim formado, é chamado produto-grinalda de A e $K \subset S_n$ e denotado por $A \wr K$.

Em geral, sabendo que G cinde em H e K, não podemos ainda determinar a classe de isomorfismo de G. Mas, no caso de produto-grinalda, a ação de K em H (determinada por φ), é dada explicitamente, e, por isso, pode-se falar sobre o produto-grinalda (já que é um grupo determinado univocamente).

Naturalmente, a ordem deste grupo é $o(H).o(K) = (o(A))^n.o(K)$. (A notação o(G) indica a ordem do grupo G.).

O diagrama correspondente ao grupo $A \wr K$ é



Um exemplo simples é o produto-grinalda $\mathbb{Z}_2 \wr S_n$. Este grupo é isomorfo ao grupo $G_n = GL(n, \mathbb{Z}) \cap \Phi(n, \mathbb{R})$, o grupo das matrizes monomiais com elementos 0, 1, -1. De fato, se identificarmos $\mathbb{Z}_2$ com o grupo multiplicativo $\{-1, 1\}$, os elementos de $\mathbb{Z}_2 \wr S_n$ da forma $(e_1, \ldots, e_n; \sigma)$ podem ser representados por:

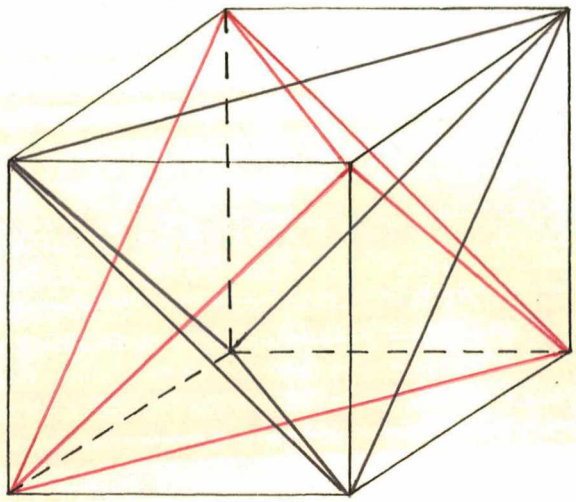
$$\begin{pmatrix} e_1 & & & \\ & e_2 & & \\ & & \ddots & \\ & & & e_n \end{pmatrix} \left(M_\sigma\right) = A$$

Aqui, M_σ é a matriz de permutação $\sigma: v_i \to v_{\sigma(i)}$, onde $\{v_i\}$ é uma base do espaço $\mathbb{R}^n$. Note que a matriz A permuta sequências (vetores no $\mathbb{R}^n$) da forma $\begin{pmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_n \end{pmatrix}$,

$\varepsilon_i = \pm 1$, $i = 1, 2, \ldots, n$.

Geometricamente, estas sequências representam vértices do cubo C^n. Então $\mathbb{Z}_2 \wr S_n$, isomorfo a G_n, é isomorfo ao grupo de simetrias do cubo C^n.

Por outro lado, o grupo de simetrias do cubo $C = C^3$ tem a estrutura do grupo $\mathbb{Z}_2 \times S_4$. Geometricamente, podemos interpretar este grupo da seguinte forma. Inscrevemos dois tetraedros regulares em um cubo, conforme vemos na figura abaixo



Qualquer simetria do cubo resulta em simetrias dos dois tetraedros, permutando os vértices de cada figura em si mesma ou um tetraedro em outro. O grupo S_4 é interpretado geometricamente como o grupo das simetrias do tetraedro regular, por possuir 4 vértices. A inversão central $-I_3$ é uma simetria do cubo, tem ordem 2, comuta com as demais simetrias e intertroca os dois tetraedros. Sendo assim, gera um fator direto do grupo de simetrias, isomorfo a $\mathbb{Z}_2$. Desta forma, vemos que $\mathbb{Z}_2 \times S_4$ corresponde ao grupo de simetrias do cubo.

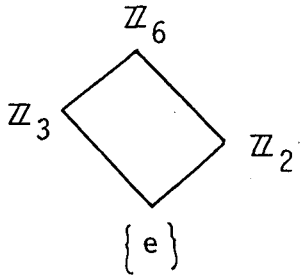
CAPÍTULO II - RELAÇÕES ENTRE Aut(G) e Aut(Γ(G))

Cada automorfismo do grupo G induz uma permutação de seus subgrupos. Então, temos um homomorfismo h de Aut(G) em Aut(Γ(G)).

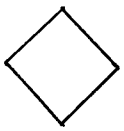
Muitos automorfismos do grafo Γ(G) não correspondem a automorfismos do grupo G. Então, vamos analisar a imagem h(Aut(G)) em Aut(Γ(G)). Mesmo assim, esse caminho não é muito promissor, como veremos analisando alguns grupos finitos, onde o grupo de automorfismos já é conhecido.

Consideremos o grupo $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Temos $Aut(\mathbb{Z}_p \times \mathbb{Z}_q) \cong Aut(\mathbb{Z}_p) \times Aut(\mathbb{Z}_q)$ se $(p,q) = 1$. Então, $Aut(\mathbb{Z}_6) \cong Aut(\mathbb{Z}_2) \times Aut(\mathbb{Z}_3) \cong \{e\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2$. (É mais fácil obter este resultado, notando que automorfismos de grupo levam geradores em geradores, então, para $\mathbb{Z}_n$, os automorfismos são da forma $\alpha_i : a \to a^i$, onde $\langle\langle a \rangle\rangle = \mathbb{Z}_n$ (a notação $\langle\langle a \rangle\rangle$ indica o grupo gerado pelo elemento a) e $(i,n) = 1$. Mas queremos, aqui, destacar o fato que o único automorfismo não trivial de $\mathbb{Z}_6$ atua dentro do subgrupo isomorfo a $\mathbb{Z}_3$).

A rede de subgrupos de $\mathbb{Z}_6$ é dada pelo diagrama



Vamos analisar os automorfismos do grafo $\Gamma(\mathbb{Z}_6)$.

Este grafo,  , possui 4 vértices e 4 arestas que formam um circuito fechado. Assim, identificando-o com um quadrado, vemos que possui 8 automorfismos e temos $Aut(\Gamma(\mathbb{Z}_6)) \cong D_4$. Mas $Aut(\mathbb{Z}_6) \cong \mathbb{Z}_2$ e, em $h: Aut(\mathbb{Z}_6) \longrightarrow Aut(\Gamma(\mathbb{Z}_6))$, a imagem $h(\mathbb{Z}_2)$ em D_4 é trivial.

Automorfismos de um grupo preservam a relação de inclusão entre seus subgrupos. Por essa razão, vamos considerar, agora, o grafo orientado $\Gamma_o(\mathbb{Z}_6)$.

O único automorfismo não-trivial em $Aut(\Gamma_o(\mathbb{Z}_6))$ é aquele que permuta os vértices correspondentes aos subgrupos $\mathbb{Z}_2$ e $\mathbb{Z}_3$. Em outras palavras, permuta dois subgrupos de níveis diferentes (nível, no grafo, corresponde à ordem dos subgrupos). E automorfismos de grupo permutam subgrupos dentro de um mesmo nível.

Temos $Aut(\Gamma_o(\mathbb{Z}_6)) \cong \mathbb{Z}_2$, mas, mesmo assim, $h(\mathbb{Z}_2)$ em $\mathbb{Z}_2$ é trivial.

Estas considerações já sugerem quais automorfismos de $\Gamma(G)$, ou de $\Gamma_o(G)$, não correspondem, com certeza, a automorfismos do grupo G. Por isso, seguiremos com a análise de diferentes níveis do grafo, separadamente.

Vamos analisar um segundo exemplo: o grupo diedral D_4. O conhecimento de todos os seus subgrupos próprios (veja diagrama no Cap.II) vem facilmente da sua interpretação geométrica como o grupo de simetrias do quadrado.

As possíveis imagens dos geradores a e b de D_4, onde $a^4 = b^2 = e$, sob um automorfismo α são

$$\alpha(a) = a^i \quad , \; i = 1, 3$$

$$\alpha(b) = a^j b \quad , \; j = 0, 1, 2, 3.$$

Daqui, temos que $o(Aut(D_4)) \leq 2.4 = 8$.

Por outro lado, note que, para os automorfismos α, β de D_4, dados por

$$\alpha : \begin{matrix} a \to a \\ b \to ab \end{matrix} \qquad \text{e} \qquad \beta : \begin{matrix} a \to a^3 \\ b \to b \end{matrix} \quad ,$$

temos $\alpha^4 = \beta^2 = e$ e $\beta\alpha\beta^{-1} = \alpha^3$.

Então $Aut(D_4) \cong D_4$.

Vamos procurar a imagem $h(Aut(D_4))$ em $Aut(\Gamma_o(D_4))$.

Observemos o nível 4. Temos aqui 3 subgrupos, mas os automorfismos de D_4 permutam apenas os subgrupos isomorfos entre si $(\mathbb{Z}_2 \times \mathbb{Z}_2)$, deixando $\mathbb{Z}_4 = \langle\langle a \rangle\rangle$ invariante. Isto significa que, entre os automorfismos do grafo orientado, devemos considerar aqueles que, dentro de cada nível, preservam a relação de isomorfismo entre os subgrupos.

Passemos ao nível 2. Aqui, temos 5 subgrupos isomorfos a $\mathbb{Z}_2$, mas um deles, $\langle\langle a^2 \rangle\rangle$, é o centro de D_4. E o centro é um subgrupo característico (um subgrupo é característico, quando permanece invariante sob a ação de qualquer automorfismo do grupo). Isso mostra que os subgrupos isomorfos, que são permutados, devem desempenhar o mesmo papel no grupo.

Assim, temos 4 subgrupos que são permutados entre si,

no nível 2. Então, é como se tivéssemos o produto $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, com permutação de "eixos" dele, e, por isso, podemos formar o produto-grinalda $\mathrm{Aut}(\mathbb{Z}_2) \wr S_4 \cong \{e\} \wr S_4 \cong S_4$.

Neste momento, vamos procurar a imagem $h(\mathrm{Aut}(D_4))$ em $\mathrm{Aut}(\mathbb{Z}_2) \wr S_4$, pois já não interessam todas as permutações de $\mathrm{Aut}(\Gamma_0(D_4))$ mas, sim, aquelas dentro do nível que estamos considerando.

O homomorfismo $h:\mathrm{Aut}(D_4) \to \mathrm{Aut}(\mathbb{Z}_2) \wr S_4$, ou seja, $h:D_4 \to S_4$, é injetivo, pois qualquer automorfismo não-trivial de D_4 induz uma permutação não-trivial dos 4 subgrupos isomorfos a $\mathbb{Z}_2$. Basta tomar dois subgrupos isomorfos a $\mathbb{Z}_2$ que geram D_4 e observar que, se eles ficassem invariantes sob um automorfismo α de D_4, todo o grupo D_4 permaneceria invariante, isto é, teríamos $\alpha = e$; então, para $\alpha \neq e$, temos $h(\alpha) \neq e$.

Voltando ao nível 4, e já que estamos considerando classes de isomorfismo, podemos considerar o produto $(\mathbb{Z}_2 \times \mathbb{Z}_2)^2$ e formar o produto-grinalda $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \wr S_2 \cong S_3 \wr S_2$.

Aqui, também, o homomorfismo $h:D_4 \to S_3 \wr S_2$ é injetivo, pois, caso tivéssemos $h(\alpha) = e$ para $\alpha \neq e$, significaria que, sob o automorfismo $\alpha \in D_4$, os dois subgrupos isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$ não permutariam entre si (o que pode ocorrer) e permaneceriam invariantes, o que implicaria em não haver permutação entre os subgrupos isomorfos a $\mathbb{Z}_2$, que é uma

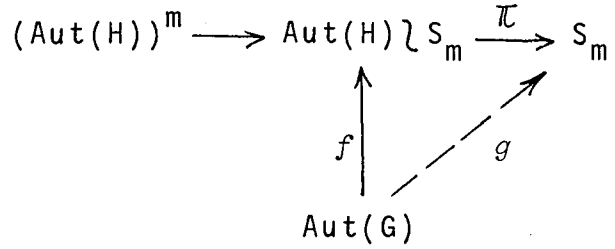
contradição, pela argumentação anterior.

Com a análise que fizemos, relacionando $Aut(D_4)$ com diferentes produtos-grinalda (que formamos a partir da verificação do grafo por níveis), conseguimos imergir o grupo $Aut(D_4) \cong D_4$ em dois grupos: S_4 e $S_3 \wr S_2$.

Observando a rede de subgrupos de D_4, inicialmente nos dá a impressão de que o nível 4 pode ser mais simples para buscarmos informações sobre $Aut(D_4)$, já que tem apenas 2 subgrupos isomorfos, do que o nível 2, que tem 5 subgrupos isomorfos, mas um deles característico. Mas observemos que $o(Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \wr S_2) = o(S_3 \wr S_2) = 72$ e $o(Aut(\mathbb{Z}_2) \wr S_4) = o(S_4) = 24$. A comparação das ordens sugere que a imagem de $Aut(D_4)$ em S_4 presta-se melhor à análise do que a de $Aut(D_4)$ em $S_3 \wr S_2$.

As considerações feitas neste capítulo mostram de que maneira vamos procurar informações sobre Aut(G) no grupo de automorfismos de seus subgrupos próprios, o que faremos nos próximos capítulos. Analisaremos os subgrupos separando-os por níveis e, em cada nível (talvez não seja necessário analisar todos), tomaremos subgrupos isomorfos, que desempenhem o mesmo papel no grupo. Analisando a ação de um automorfismo α de G restrita a este conjunto, procuraremos saber como α permuta os elementos dentro de cada subgrupo e como mistura os subgrupos entre si, isto é, procuraremos descrever α na forma $(\alpha|_{H_1}, \ldots, \alpha|_{H_m}; \tau)$, onde $\alpha|_{H_i}$ é a restrição de α ao i-ésimo subgrupo e $\tau \in S_m$ descreve a permutação de $H_1, \ldots, H_m$ induzida por α.

Então, na análise de exemplos que faremos nos capítulos seguintes, usaremos o seguinte diagrama



onde: π é projeção canônica de $Aut(H)\wr S_m$ em S_m;

f é homomorfismo de $Aut(G)$ em $Aut(H)\wr S_m$, dado pela ação de $Aut(G)$ nos m subgrupos isomorfos a H de G (ação dentro deles e por permutação deles);

g é homomorfismo de $Aut(G)$ em S_m, resultante da composição dos homomorfismos f e π ($g = \pi \circ f$), que reflete a ação de elementos de $Aut(G)$, permutando m cópias do subgrupo H.

Pela escolha dos subgrupos por níveis, para a formação de produtos-grinalda, pode ocorrer que a imagem do homomorfismo $f: Aut(G) \rightarrow Aut(H)\wr S_m$, para algum $H<G$, forneça informações suficientes sobre $Aut(G)$.

Se isto não ocorrer, há uma possibilidade de obtermos dados novos sobre $Aut(G)$ pela análise de $Ker(f)$, o núcleo de f, que, em geral, não é trivial.

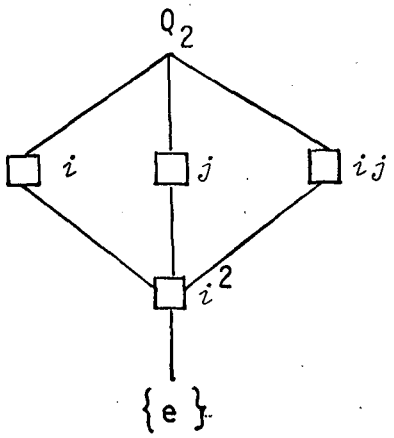
É claro que, se a escolha para certo $H<G$ não for suficiente, o mesmo procedimento será feito com uma nova escolha de H. Deste modo, obteremos um conjunto de subgrupos normais $Ker(f)$, de diversos homomorfismos f, que, em certo grau, caracterizam $Aut(G)$.

CAPÍTULO III - ANÁLISE DO GRUPO $Aut(Q_2)$

O grupo Q_2, dos quatérnios, é definido por:

$Q_2 = (i, j: i^2 = j^2 = (ij)^2)$.

Sua rede de subgrupos é visualizda no diagrama:



Observamos na rede que os três subgrupos isomorfos a $\mathbb{Z}_4$ são todos normais em Q_2, todos não característicos.

O interesse neste grupo foi provocado justamente por este fato: temos alguns subgrupos isomorfos entre si e todos com a mesma situação dentro da rede. Assim, como $Aut(\mathbb{Z}_4) \cong \mathbb{Z}_2$, formamos o produto-grinalda $\mathbb{Z}_2 \wr S_3$ e, a seguir, mostramos como podemos relacionar o grupo $Aut(Q_2)$ com o produto $\mathbb{Z}_2 \wr S_3$.

Em Q_2, temos 6 elementos de ordem 4. Assim, por um automorfismo α, enquanto o gerador i é levado em um dos 6 elementos, sobram 4 possibilidades para $\alpha(j)$ (6 menos 2 elementos do subgrupo gerado por $\alpha(i)$).

Desta forma, $o(Aut(Q_2)) \leq 24$.

As funções α e β, tais que

$$\alpha(i) = i \qquad \text{e} \qquad \beta(i) = j$$

$$\alpha(j) = (ij)^3 \qquad\qquad \beta(j) = i \quad ,$$

podem ser estendidas a todos os elementos de Q_2, assim que as extensões (denotadas pelas mesmas letras α e β) sejam automorfismos de Q_2.

Mostramos, agora, que α e β geram um grupo de 24 elementos: α tem ordem 4 e β, ordem 2. Verifica-se, facilmente, que $\alpha^2 \neq \beta$; portanto, $o(\ll \alpha, \beta \gg) \geqslant 8$. O automorfismo $\beta\alpha$, tal que $\begin{cases} i \to j \\ j \to ij \end{cases}$, tem ordem 3. Logo, $o(\ll \alpha, \beta, \beta\alpha \gg) \geqslant 8.3 = 24$. Como $\alpha, \beta \in \mathrm{Aut}(Q_2)$ e $o(\mathrm{Aut}(Q_2)) \leqslant 24$, afirmamos que $o(\ll \alpha, \beta, \beta\alpha \gg) = 24$.

Assim, $o(\mathrm{Aut}(Q_2)) = 24$.

O uso da notação $\begin{pmatrix} i \\ j \\ k \end{pmatrix}$ (como se tivéssemos um elemento do módulo $(\mathbb{Z}_4)^3$) permite-nos empregar a notação matricial para descrevermos a ação de automorfismos no conjunto de geradores $\{ i, j, k \}$ (onde $k = ij$ e $i^2 = j^2 = k^2 = -1$, como é convencionalmente usado para o grupo Q_2).

Escrevemos

$$\alpha \begin{pmatrix} i \\ j \\ k \end{pmatrix} = \begin{pmatrix} i \\ k^3 \\ j \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} i \\ j \\ k \end{pmatrix}$$

$$\beta\begin{pmatrix} i \\ j \\ k \end{pmatrix} = \begin{pmatrix} j \\ i \\ k^3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} i \\ j \\ k \end{pmatrix}$$

Assim, temos

$$\alpha \rightarrow A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\beta \rightarrow B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Desta forma, obtemos uma correspondência entre $\alpha, \beta \in \mathrm{Aut}(Q_2)$ e $A, B \in GL(3,\mathbb{Z}_3) \cap \Phi(3, \mathbb{R})$, que se estende a um homomorfismo $f: \mathrm{Aut}(Q_2) \rightarrow \mathbb{Z}_2 \wr S_3$. Ao indicarmos $f(\alpha) = \overline{\alpha}$, temos $\overline{\alpha} = (1, -1, 1; (23))$ e $\overline{\beta} = (1, 1, -1; (12))$.

Ao escrevermos um automorfismo $\gamma \in \mathrm{Aut}(Q_2)$ na forma $(e_1, e_2, e_3; \sigma) \in \mathbb{Z}_2 \wr S_3$, o fato que $\overline{\gamma} = (1, 1, 1; e)$ significa que $\gamma = id_{\mathrm{Aut}(Q_2)}$, pois interpretamos o elemento $(1, 1, 1; e)$ da seguinte maneira:

(i) permutação e : Não há intertroca entre os 3 subgrupos isomorfos a $\mathbb{Z}_4$;

(ii) $(1, 1, 1)$: a imagem de cada um dos 3 geradores é também um deles.

Então, o homomorfismo f é injetivo.

Verificamos, assim, que existe $H < \mathbb{Z}_2 \wr S_3$, onde H corresponde à $f(\mathrm{Aut}(Q_2))$, que é isomorfo a $\mathrm{Aut}(Q_2)$.

Temos que $o(\mathbb{Z}_2 \wr S_3) = 48$ e $o(H) = 24$.

Já verificamos que $\mathrm{Aut}(Q_2) \cong H$ e que $\mathbb{Z}_2 \wr S_3 \cong \mathbb{Z}_2 \times S_4$.

Como o grupo $\mathbb{Z}_2 \times S_4$, das simetrias do cubo, é bem conhecido por suas aplicações em cristalografia, é desnecessário provar que seus únicos subgrupos de ordem 24 são isomorfos a $\mathbb{Z}_2 \times A_4$ ou a S_4 (veja tab.2, p.135, em [3]). Uma das diferenças entre estes dois subgrupos é que só um deles possui elementos de ordem 4. O automorfismo α, exibido anteriormente, tem ordem 4, portanto, $\alpha \notin \mathbb{Z}_2 \times A_4$. Logo , $\mathrm{Aut}(Q_2) \cong S_4$.

Com o resultado da análise feita até aqui, temos caracterizado completamente o grupo $\mathrm{Aut}(Q_2)$.

No diagrama

$$\begin{array}{ccccc} \mathbb{Z}_2^3 & \longrightarrow & \mathbb{Z}_2 \wr S_3 & \longrightarrow & S_3 \\ & & \uparrow f & \nearrow g & \\ & & \mathrm{Aut}(Q_2) & & \end{array} \quad ,$$

podemos observar que g é um homomorfismo sobrejetivo, não injetivo, dado por

$$g : \mathrm{Aut}(Q_2) \longrightarrow S_3$$

$$\alpha \longrightarrow (23)$$

$$\beta \longrightarrow (12) \quad .$$

Assim, por $\mathrm{Ker}(g)$, confirmamos facilmente o fato que $\mathbb{Z}_2 \times \mathbb{Z}_2 \lhd S_4$, onde $\mathrm{Ker}(g) \cong \langle\!\langle \alpha^2, (\alpha^2\beta)^2 \rangle\!\rangle$.

CAPÍTULO IV - SUBGRUPOS DE SYLOW DE S_n

Neste capítulo, utilizaremos a mesma técnica do capítulo anterior, mas em situação reversa. Lá, conhecíamos o grupo de automorfismos de $H<G$ e obtivemos informações sobre $Aut(G)$. Aqui, conhecemos o grupo $Aut(G)$ e buscaremos informações sobre o nº de subgrupos de uma classe de subgrupos isomorfos de G, como mostramos no teorema a seguir.

Teorema: Tome p primo, $p \leq n$. Seja H um Sylow p-subgrupo de S_n e seja k o número de subgrupos de S_n, isomorfos a H. Então, para $n>4$, tem-se $k \geq n$.

Demonstração: Para $n>4$, $n \neq 6$, $Aut(S_n) \cong S_n$. Para $n = 6$, $o(Aut(S_n)) = 2.n!$ (veja [2]). Neste caso, $Inn(S_6) \cong S_6$. Assim, o argumento que usaremos a seguir para S_n refere-se, no caso de $n = 6$, ao subgrupo $Inn(S_6)$, dos automorfismos internos de S_6.

Formemos o produto-grinalda $Aut(H) \wr S_k$ e o diagrama

$$\begin{array}{ccccc} (Aut(H))^k & \longrightarrow & Aut(H)\wr S_k & \xrightarrow{\pi} & S_k \\ & & \uparrow f & \nearrow g & \\ & & Aut(S_n) \cong S_n & & \end{array}$$

Já que $g: S_n \to S_k$ é homomorfismo (note que $g = \pi \circ f$), é suficiente mostrar que g é injetivo e o teorema estará demonstrado.

A imagem de g em S_k é um subgrupo do grupo de permutações de k símbolos. Este subgrupo corresponde às permutações dos k subgrupos H_i de S_n, induzidas pelos automorfismos de S_n.

Os possíveis núcleos para g são $\{e\}$, A_n e S_n, já que são os únicos subgrupos normais em S_n $(n>4)$. (A_n, como é usado normalmente, indica o subgrupo de S_n das permutações pares).

Vamos supor $Ker(g) = A_n$. Neste caso, para todo $\propto \in A_n$ $(A_n < Aut(S_n))$ e para todo $i = 1, 2, \ldots, k$, $\propto(H_i) = \tilde{\propto} H_i \tilde{\propto}^{-1} \in H_i$, onde $\tilde{\propto} \in A_n$ é o elemento que, sob o automorfismo $\propto$, conjuga H_i. Assim, para qualquer i fixo, $A_n < N_{S_n}(H_i)$. Este fato implica em $N_{S_n}(H_i) = S_n$ ou A_n, já que o normalizador contém A_n como subgrupo. E, assim, $A_n \triangleleft N_{S_n}(H_i)$.

A intersecção de dois subgrupos normais em G é também normal em G. Assim, como $A_n \triangleleft N_{S_n}(H_i)$ e como temos sempre $H_i \triangleleft N_{S_n}(H_i)$, segue que $H_i \cap A_n \triangleleft A_n$, o que implica em $H_i \cap A_n = A_n$ ou $H_i \cap A_n = \{e\}$.

Em $H_i \cap A_n = A_n$, temos uma contradição, já que A_n não é p-subgrupo de Sylow.

Se $H_i \cap A_n = \{e\}$, então $H_i \cong \mathbb{Z}_2$ ou $H_i = \{e\}$, que também é uma contradição, já que nem $\mathbb{Z}_2$ nem $\{e\}$ são p-subgrupos de Sylow de S_n $(n>3)$.

Vamos supor, agora, $Ker(g) = S_n$. Neste caso, para todo $\alpha \in S_n \cong Aut(S_n)$ e para todo $i = 1, 2, \ldots, k$, temos $\alpha(H_i) = \tilde{\alpha} H_i \tilde{\alpha}^{-1} = H_i$, onde $\tilde{\alpha} \in S_n$ é o elemento que, sob o automorfismo α, conjuga H_i. Assim, $H_i \triangleleft S_n$, o que também é uma contradição, já que $H_i \neq A_n$.

Então, $Ker(g) = \{ e \}$ e temos g injetivo. Logo, $k \geqslant n$.

CAPÍTULO V - AUTOMORFISMOS DE CERTO PRODUTO CINDIDO

Consideremos o grupo G:

$G = (a, b, c;\ a^3 = b^3 = c^4 = e,\ ba = ab,\ cac^{-1} = b,\ cbc^{-1} = a^2)$.

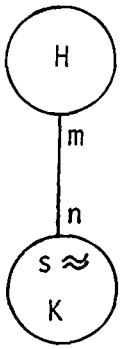
Podemos definí-lo, também, em termos de dois geradores, a e c, já que b fica determinado por esses dois elementos. Escrevemos, então:

$G = (a, c;\ a^3 = c^4 = e,\ c^2ac^{-2} = a^2,\ [cac^{-1}, a] = e)$.

Aqui, $[x, y] = xyx^{-1}y^{-1}$ indica o comutador de elementos x, y.

O uso desta segunda definição nos facilitará ao escrevermos automorfismos de G.

Mostramos, a seguir, o diagrama correspondente à rede de subgrupos de G, onde usamos a seguinte convenção:



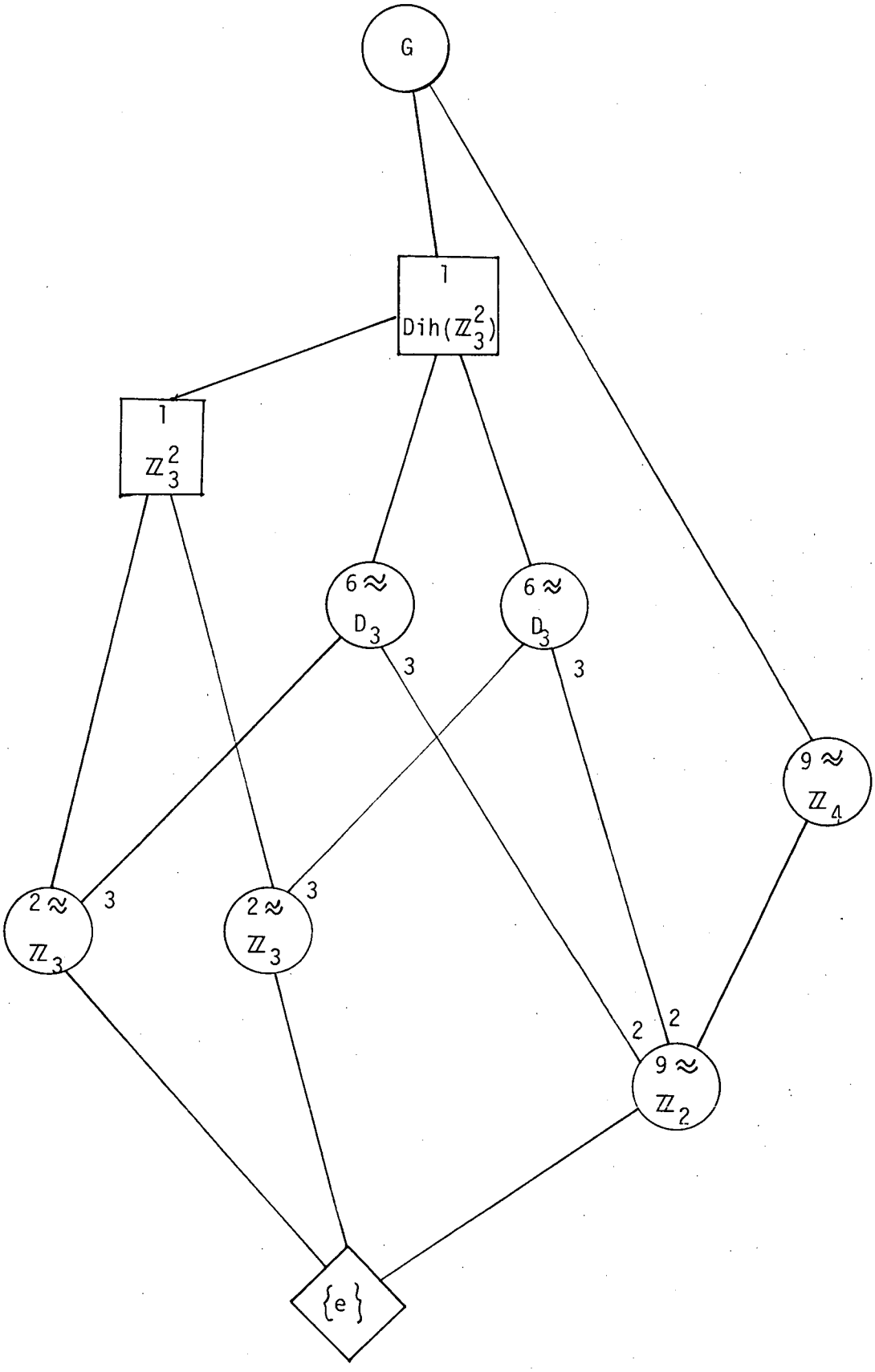
H, K: subgrupos de G

s: nº de subgrupos conjugados a K

n: nº de cópias de H nas quais uma fixa cópia de K aparece

m: nº de cópias de K contidas em cada cópia de H

O símbolo Dih indica um grupo diedral generalizado, em que temos: $Dih(A) = \ll A, c \gg$, onde $A \tilde{=} \mathbb{Z}_m^n$, $m > 2$, $c^2 = e$ e $\underset{a \in A}{\forall} cac^{-1} = a^{-1}$.


G
1
Dih($\mathbb{Z}_3^2$)
1
$\mathbb{Z}_3^2$
6 ≈
D_3
6 ≈
D_3
3
3
9 ≈
$\mathbb{Z}_4$
2 ≈
$\mathbb{Z}_3$
3
2 ≈
$\mathbb{Z}_3$
3
2
2
9 ≈
$\mathbb{Z}_2$
{e}

Uma análise visual do diagrama de subgrupos de G explica as razões que nos levaram a analisar justamente este grupo:

- é um grupo de ordem relativamente pequena (o(G) = 36);
- não é abeliano nem um outro grupo que tenha a estrutura de Aut(G) bem conhecida;
- tem vários níveis (os níveis 2, 3, 4 e 6) com abundância de subgrupos que desempenham o mesmo papel em G.

Vamos caracterizar completamente o grupo Aut(G). Dividiremos essa caracterização nas etapas:

1. Ordem do grupo Aut(G) ;
2. Geradores ;
3. Condições de comutação de β_{ij} com γ_{uv} ;
4. Homomorfismo de Aut(G) em $Aut(\mathbb{Z}_4) \wr S_9$ e
5. Homomorfismo de Aut(G) em $Aut(\mathbb{Z}_3 \times \mathbb{Z}_3) \wr S_1$.

1. Ordem de Aut(G)

Qualquer automorfismo de G fica determinado por sua ação em a e c, se utilizarmos a segunda definição de G. Neste grupo, temos 8 elementos de ordem 3 e 18 elementos de ordem 4 que poderiam ser, respectivamente, as imagens de a e c sob um automorfismo. Assim, $o(Aut(G)) \leq 8.18 = 144$. Como o centro de G é o subgrupo trivial, isto é, $Z(G) = \{e\}$, e sabemos que $Inn(G) \cong G/Z(G)$, temos $Inn(G) \cong G$. O subgrupo Inn(G), dos automorfismos internos, é gerado por γ_a e γ_c , que representam conjugação por a e por c , respectivamente. Escrevemos, então: $Inn(G) = \langle\langle \gamma_a , \gamma_c \rangle\rangle$.

γ_c é descrito pelas órbitas de sua ação: (a, b, a^2, b^2) e (c), a órbita trivial, enquanto que γ_a é descrito pelas ór-

bitas (a) e $(c,\ ab^2c,\ a^2bc)$.

Sabemos que $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$. Então $[\mathrm{Aut}(G) : \mathrm{Inn}(G)] =$ $= 1, 2,$ ou 4, já que $o(\mathrm{Inn}(G)) = 36$ e $o(\mathrm{Aut}(G)) \leq 144$.

Precisamos verificar a existência ou não de automorfismos externos.

Seja α uma função definida para $\{a, c\}$ em G tal que $\begin{cases} \alpha(a) = ab^2 \\ \alpha(c) = c \end{cases}$. Podemos estender α a um automorfismo de G (que denotaremos pela mesma letra α). O automorfismo α não é interno, pois não existe $x \in G$ tal que x conjugue a com $\alpha(a)$.

Seja, agora, β uma função de $\{a, c\}$ em G tal que $\begin{cases} \beta(a) = a \\ \beta(c) = c^3 \end{cases}$. Também podemos estender β a um automorfismo de G (que também será denotado por β). O automorfismo β também não é interno, já que não existe $x \in G$ que conjugue c com $\beta(c)$ e, obviamente, β não pertence ao subgrupo gerado por Inn(G) e α.

Verificamos, assim, que existem pelo menos 3 classes de automorfismos externos (módulo Inn(G)): $\{[e], [\alpha], [\beta]\}$.

O automorfismo $\alpha\beta$ não é interno, pois temos $\begin{cases} \alpha\beta(a) = ab^2 \\ \alpha\beta(c) = c^3 \end{cases}$. Então $[\alpha\beta] \neq [e]$.

Temos, também, $\alpha\beta \notin [\alpha]$, pois se $\alpha\beta = \alpha.k$, $k \in \mathrm{Inn}(G)$, teríamos $\beta \in \mathrm{Inn}(G)$.

Analogamente, descartamos $\alpha\beta \in [\beta]$, já que isto implicaria em $\beta^{-1}\alpha\beta \in \mathrm{Inn}(G)$, mas Inn(G), sendo normal em Aut(G), nos levaria à conclusão que $\alpha \in \mathrm{Inn}(G)$.

Temos, então, pelo menos 4 classes de automorfismos exter-

nos, dadas por: $\{[e], [\alpha], [\beta], [\alpha\beta]\}$, mas não podemos ter mais do que 144/36, então temos $o(Aut(G)) = 36.4 = 144$.

2. Geradores

Já conhecemos $Inn(G) = \ll \gamma_a, \gamma_c \gg$. Conhecemos, também, α e β, automorfismos externos.

O automorfismo α é descrito pelas órbitas de sua ação $(a, ab^2, b, ab, a^2, a^2b, b^2, a^2b^2)$ e (c), a órbita trivial. (As demais órbitas formam-se de maneira óbvia). Note que α^2 coincide com γ_c.

O automorfismo β tem ordem 2. Obviamente não conseguiremos m tal que $\beta^m = \gamma_a$, já que $\gamma_a^3 = e$.

Como γ_a e $\alpha^2 = \gamma_c$ geram $Inn(G)$ e como α e β geram todos os automorfismos externos, temos $Aut(G) = \ll \alpha, \beta, \gamma_a \gg$.

Em seguida, vamos gerar $Aut(G)$ com apenas 2 automorfismos.

Seja β_{ij} uma função de $\{a, b, c\}$ em G tal que

$$\begin{cases} \beta_{ij}(a) = a^i b^j \\ \beta_{ij}(b) = a^j b^{2i} \\ \beta_{ij}(c) = c^3 \end{cases}.$$

As órbitas começam assim: $a \to a^i b^j \to a^{i^2 + j^2} \to \ldots$

$$b \to a^j b^{2i} \to b^{i^2 + j^2} \to \ldots$$

$$c \to c^3 \to c$$

Se $i = 0$ ou $j = 0$, temos $i^2 + j^2 \equiv 1 \pmod 3$ e, consequentemente, $\beta_{ij}^2 = e$.

Se $i \neq 0$ e $j \neq 0$, temos $i^2 + j^2 \equiv 2 \pmod 3$ e, então, $\beta_{ij}^4 = e$.

Denotemos por γ_{uv} o automorfismo de conjugação por $a^u b^v$. Obviamente $\gamma_{uv}^3 = e$.

Para uma escolha conveniente de geradores, precisamos conhecer as condições em que os automorfismos β_{ij} e γ_{uv} comutem.

3. Condições para que $\beta_{ij}\gamma_{uv} = \gamma_{uv}\beta_{ij}$

Para o gerador a, temos $\begin{cases} \beta_{ij}\gamma_{uv}(a) = \beta_{ij}(a) \\ \gamma_{uv}\beta_{ij}(a) = \beta_{ij}(a) \end{cases}$, o

que implica em $\beta_{ij}\gamma_{uv} = \gamma_{uv}\beta_{ij}$, para quaisquer u e v, i e j.

Para o gerador c, temos

$$\beta_{ij}\gamma_{uv}(c) = \beta_{ij}(a^u b^v c a^{2u} b^{2v}) = \beta_{ij}(a^u b^v b^{2u} a^v c) =$$

$$= \beta_{ij}(a^{u+v} b^{2u+v} c) = (a^i b^j)^{u+v}(a^j b^{2i})^{2u+v} c^3 =$$

$$= a^{u(i+2j)+v(i+j)} b^{u(i+j)+v(2i+j)} c^3 \qquad \text{e}$$

$$\gamma_{uv}\beta_{ij}(c) = \gamma_{uv}(c^3) = a^u b^v c^3 a^{2u} b^{2v} = a^u b^v b^u a^{2v} c^3 =$$

$$= a^{u+2v} b^{u+v} c^3 .$$

Já que temos a unicidade de notação de elementos de G na forma $a^m b^n c^p$, a igualdade existe se, e somente se, todas as potências são iguais. Assim, $\beta_{ij}\gamma_{uv} = \gamma_{uv}\beta_{ij}$

quando $\begin{cases} u(i+2j) + v(i+j) = u + 2v \\ u(i+j) + v(2i+j) = u + v \end{cases}$.

O sistema é equivalente a $\begin{cases} 2u = u(2i) + v(2j) \\ v = u(j) + v(2i) \end{cases}$.

Ou ainda $\begin{cases} (2i+1)u + 2jv = 0 \\ ju + (2i+2)v = 0 \end{cases}$, que equivale a

$$\begin{pmatrix} 2i+1 & j \\ j & i+1 \end{pmatrix}\begin{pmatrix} u \\ 2v \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} .$$

Para que o sistema tenha solução, temos que ter $\det A = 0$, onde $A = \begin{pmatrix} 2i+1 & j \\ j & i+1 \end{pmatrix}$, $A \in M(2, \mathbb{Z}_3)$, o anel das matrizes do espaço 2-dimensional, sobre o corpo $\mathbb{Z}_3$. Então

$$\det A = (2i+1)(i+1) + 2j^2 = 2i^2 + 3i + 1 + 2j^2 =$$

$$= 2i^2 + 2j^2 + 1 = 2(i^2 + j^2) + 1 .$$

$$\det A = 0 \Rightarrow 2(i^2 + j^2) + 1 = 0$$

$$2(i^2 + j^2) = 2$$

$$i^2 + j^2 = 1 \Rightarrow i = 0 \text{ ou } j = 0.$$

Se $i = 0$ (e $j = 1,2$):

$$\begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}\begin{pmatrix} u \\ 2v \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow \begin{cases} u + 2jv = 0 \Rightarrow u = jv \\ ju + 2v = 0 \end{cases}$$

$(j^2 + 2)v = 0 \Rightarrow v = 0$ ou $j^2 + 2 = 0$.

Se $v = 0 \Rightarrow u = 0$.

Se $j^2 + 2 = 0 \Rightarrow j = 1,2$. Então: $v = 0, 1, 2$.

Quando $\begin{cases} v = 1 \Rightarrow u = 1,2 \\ v = 2 \Rightarrow u = 1,2 \end{cases}$. Então, se $v = 1,2 \Rightarrow u = 1,2$.

Se $j = 0$ (e $i = 1,2$):

$$\begin{pmatrix} 2i+1 & 0 \\ 0 & i+1 \end{pmatrix}\begin{pmatrix} u \\ 2v \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow \begin{cases} (2i+1)u = 0 \\ (i+1)2v = 0 \end{cases}$$

$(2i+1)u = 0 \Rightarrow u = 0$ ou $i = 1$.

Se $u = 0$, $\begin{cases} i = 1 \Rightarrow v = 0 \\ i = 2 \Rightarrow v = 0, 1, 2 . \end{cases}$

Se $i = 1$, $u = 0, 1, 2 \Rightarrow v = 0$.

O automorfismo β, descrito anteriormente, satisfaz a condição: $j = 0$ e $i = 1$. O automorfismo que comuta com β é γ_{uv}, $u = 0, 1, 2$ e $v = 0$. Vamos tomar $u = 2$. Assim, o produto $\beta\gamma_2$ tem ordem 6, $(\beta\gamma_2)^3 = \beta$ e $(\beta\gamma_2)^2 = \gamma_a$.

Encontramos, assim, um novo sistema de geradores : $Aut(G) = \langle\langle \alpha, \beta\gamma_2 \rangle\rangle$.

4. Homomorfismo de Aut(G) em $Aut(\mathbb{Z}_4) \wr S_9$

Como podemos escolher, para nosso objetivo, subgrupos em diversos níveis, uma escolha natural é iniciarmos por Sylow-subgrupos de G. Temos apenas 1 Sylow 3-subgrupo , $\mathbb{Z}_3 \times \mathbb{Z}_3$, e 9 Sylow 2-subgrupos, isomorfos a $\mathbb{Z}_4$. Então, começaremos a análise no nível 4.

Para encontarmos um homomorfismo de Aut(G) em $Aut(\mathbb{Z}_4) \wr S_9 \cong \mathbb{Z}_2 \wr S_9$, vamos verificar a ação dos geradores de Aut(G) nos 9 subgrupos $\mathbb{Z}_4$.

Veremos que o grupo Aut(G) é um produto cindido de translações em $\mathbb{Z}_3^2$ por transformações lineares do espaço 2-dimensional sobre $\mathbb{Z}_3$. Por este motivo, é mais conveniente utilizarmos, nesta fase dos nossos cálculos, os geradores γ_a, γ_b, α e β do que α e $\beta\gamma_2$, apesar desta última escolha apresentar-se em forma mais compacta.

Os 9 subgrupos $\mathbb{Z}_4$ são gerados por $x_{ij} = a^i b^j c$, $i,j = 0, 1, 2$. Assim, podemos indicá-los por meio de vetores $\begin{pmatrix} i \\ j \end{pmatrix} \in \mathbb{Z}_3^2$.

Lembrando que $\alpha : a \to ab^2$

$b \to ab$

$c \to c$,

segue que $\alpha(a^i b^j c) = a^{i+j} b^{2i+j} c$.

A notação $\begin{pmatrix} i \\ j \end{pmatrix}$ nos permite associar ao automorfismo α uma matriz A, $A \in GL(2, \mathbb{Z}_3)$, o grupo das matrizes inversíveis, do espaço 2-dimensional, sobre o corpo $\mathbb{Z}_3$.

$$\alpha\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} i + j \\ 2i + j \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} i \\ j \end{pmatrix} \longrightarrow A = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} .$$

Agora, verifiquemos a ação de β sobre os 9 subgrupos. Temos que $\beta : a \to a$

$b \to b^2$

$c \to c^3$.

Então $\beta(a^i b^j c) = a^i b^{2j} c^3$.

Queremos escrever a imagem de β em termos do gerador x_{ij}. Então $a^i b^{2j} c^3 = x_{ij}^3 = (a^l b^m c)^3$.

Seja $y = a^l b^m$. Então $(yc)^3 = (yc)^{-1} = c^{-1} y^{-1} = c^3 y^2$. Temos $a^i b^{2j} c^3 = c^3 y^2 \Rightarrow c a^i b^{2j} c^3 = y^2 \Rightarrow a^j b^i = y^2 \Rightarrow$ $y = a^{2j} b^{2i}$. Assim, $\beta(a^i b^j c) = a^i b^{2j} c^3 = (a^{2j} b^{2i} c)^3$.

Usando a notação de vetores $\begin{pmatrix} i \\ j \end{pmatrix}$, escrevemos

$$\beta\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} 2j \\ 2i \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} i \\ j \end{pmatrix} \quad .$$

Associamos, então, ao automorfismo β, a matriz

$$B = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \quad B \in GL(2,\mathbb{Z}_3) .$$

Introduzindo esta notação, aproveitamos do homomorfismo $h: \langle\langle \alpha, \beta \rangle\rangle \to GL(2,\mathbb{Z}_3)$, dado por: $\begin{cases} h(\alpha) = A \\ h(\beta) = B \end{cases}$, já que composição de automorfismos corresponde à multiplicação de matrizes. Este homomorfismo é injetivo, pois seu núcleo é o automorfismo trivial.

Operando com as matrizes A e B, verificamos a relação $BAB^{-1} = A^3$. Como temos o homomorfismo h injetivo, essa relação se preserva para α e β. Temos, então, $\beta\alpha\beta^{-1} = \alpha^3$ e, como $\alpha^8 = \beta^2 = e$, temos a descrição da classe de isomorfismo $\langle\langle \alpha, \beta \rangle\rangle \cong 16\Gamma_3 a_2$ (veja [7]).

Salientamos, aqui, que este grupo, $16\Gamma_3 a_2$, de 16 elementos, é Sylow 2-subgrupo de grupos $Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$, para p primo e $p \equiv 3 \pmod 8$.

A ação de γ_a e γ_b nos subgrupos isomorfos a $\mathbb{Z}_4$ em G é dada por $\gamma_a(a^i b^j c) = a(a^i b^j c)a^{-1} = a^{i+1} b^{j+2} c$.

Então $$\gamma_a \begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} i+1 \\ j+2 \end{pmatrix} = \begin{pmatrix} i \\ j \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} .$$

E $\gamma_b(a^i b^j c) = b(a^i b^j c)b^{-1} = a^{i+1} b^{j+1} c$.

Ou seja $$\gamma_b \begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} i+1 \\ j+1 \end{pmatrix} = \begin{pmatrix} i \\ j \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} .$$

A ação de γ_a sobre o vetor $\begin{pmatrix} i \\ j \end{pmatrix}$ é de uma translação. O mesmo acontece com γ_b. Como estamos trabalhando no corpo $\mathbb{Z}_3$, podemos colocar $\langle\langle \gamma_a, \gamma_b \rangle\rangle = \mathbb{Z}_3^2$, associando $a \to \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ e $b \to \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, que são vetores linearmente independentes.

Os automorfismos α e β geram um grupo de 16 elementos, que é um subgrupo de $GL(2,\mathbb{Z}_3)$, e os automorfismos γ_a e γ_b geram um grupo de 9 elementos, de translações. Assim, temos $o(\langle\langle \alpha, \beta, \gamma_a, \gamma_b \rangle\rangle) = 16.9 = 144$.

Este grupo é um produto normal de translações em $\mathbb{Z}_3^2$ por transformações lineares de $GL(2,\mathbb{Z}_3)$. Anotemos $\langle\langle \gamma_a, \gamma_b, \alpha, \beta \rangle\rangle = \mathbb{Z}_3^2 \rtimes 16\Gamma_3 a_2$.

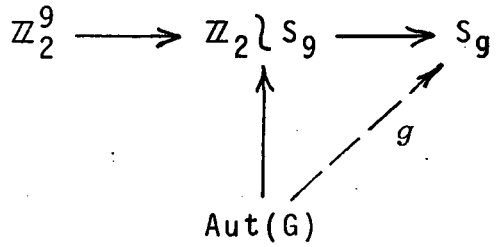
Os elementos deste grupo podem ser escritos como pares (t,l), onde t é translação em $\mathbb{Z}_3^2$ e $l \in 16\Gamma_3 a_2$, com a lei de composição $(t,l)(t',l') = (t + lt', ll')$.

Assim, Aut(G) é isomorfo a um subgrupo do grupo afim $A(2,\mathbb{Z}_3)$, do espaço de dimensão 2, sobre o corpo $\mathbb{Z}_3$.

Pelos cálculos que fizemos, os automorfismos α, β, γ_a e γ_b podem ser escritos como elementos de $\mathbb{Z}_2 \wr S_g$, da forma $(e_1, \ldots, e_g; \sigma)$, onde α, γ_a e γ_b correspondem a elementos em que $e_1 = e_2 = \ldots = e_g = 1$. Ao automorfismo β corresponde um elemento onde $e_1 = e_2 = \ldots = e_g = -1$. Quanto à permutação σ, podemos determiná-la facilmente para α, β,

γ_a e γ_b, com o uso da notação $\binom{i}{j}$ para cada gerador $a^i b^j c$ dos 9 subgrupos.

Com relação às permutações σ, destacamos o fato que o homomorfismo g que aparece no diagrama



é injetivo.

5. Homomorfismo de $Aut(G)$ em $Aut(\mathbb{Z}_3 \times \mathbb{Z}_3) \wr S_1$

Em G, temos um Sylow 3-subgrupo, isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_3$. Este subgrupo pode ser interpretado como espaço vetorial sobre $\mathbb{Z}_3$.

Qualquer automorfismo do espaço linear $\mathbb{Z}_p^n$ é automorfismo do grupo $\underbrace{\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{n} = \mathbb{Z}_p^n$.

Assim, temos $GL(n,\mathbb{Z}_p) \hookrightarrow Aut(\mathbb{Z}_p^n)$ (onde $\hookrightarrow$ indica um homomorfismo injetivo).

Para que a outra inclusão seja verdadeira, é preciso verificar que $\forall_{k,g \in \mathbb{Z}_p} \alpha(kg) = k\alpha(g)$, onde $\alpha \in Aut(\mathbb{Z}_p^n)$.

Esta verificação é imediata por indução sobre k, apesar de só precisarmos usá-la para um número finito de valores de k.

Desta forma, $Aut(\mathbb{Z}_p^n) \hookrightarrow GL(n,\mathbb{Z}_p)$. Temos, então,

$\mathrm{Aut}(\mathbb{Z}_p^n) \cong \mathrm{GL}(n,\mathbb{Z}_p)$.

Por isto, escrevemos $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3) \cong \mathrm{GL}(2,\mathbb{Z}_3)$.

Uma análise da relação entre $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3) \wr S_1 \cong \mathrm{Aut}(\mathbb{Z}_3^2)$ e Aut(G) torna-se desnecessária neste momento, em função dos resultados obtidos com a análise anterior, pois, lá, caracterizamos completamente o grupo Aut(G).

Mas, se tivéssemos iniciado o estudo deste grupo pela análise do homomorfismo $f:\mathrm{Aut}(G) \to \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3) \wr S_1$, obteríamos o resultado que descrevemos a seguir.

Sabemos que $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3) \wr S_1 \cong \mathrm{GL}(2,\mathbb{Z}_3)$. Então, o diagrama

$$\begin{array}{ccccc} \mathrm{Aut}(\mathbb{Z}_3^2) & \longrightarrow & \mathrm{Aut}(\mathbb{Z}_3^2) \wr S_1 & \longrightarrow & S_1 \\ & & \uparrow f & & \\ & & \mathrm{Aut}(G) & & \end{array}$$

pode ser reescrito como

$$\begin{array}{ccccc} \mathrm{GL}(2,\mathbb{Z}_3) & \longrightarrow & \mathrm{GL}(2,\mathbb{Z}_3) & \longrightarrow & \{e\} \\ & & \uparrow f & & \\ & & \mathrm{Aut}(G) & & \end{array}$$

.

Seja, então, o homomorfismo $f:\mathrm{Aut}(G) \to \mathrm{GL}(2,\mathbb{Z}_3)$ e considere $\alpha \in \mathrm{Ker}(f)$. Isto é, $f(\alpha)$ é um automorfismo trivial de $\mathbb{Z}_3^2$. Portanto, $\alpha(a) = a$ e $\alpha(b) = b$. As possíveis imagens para c, sob α, são: $\alpha(c) = a^i b^j c^k$, $i,j = 0, 1, 2$ e $k = 1, 3$.

É fácil verificar que $k = 3$ não define um automorfismo de G e, como todas as escolhas para i e j são possíveis, temos $\mathrm{Ker}(f) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Podemos observar que, assim, recebemos apenas uma das informações obtidas pela análise do caso em que a escolha foi $H \cong \mathbb{Z}_4$.

Para destacarmos o resultado obtido pela análise deste grupo, reescrevemos este resultado em forma de teorema.

Teorema: Seja o produto semi-direto $G = \mathbb{Z}_3^2 \rtimes \mathbb{Z}_4$, isomorfo a um subgrupo do grupo $A(2,\mathbb{Z}_3)$, onde elementos de $\mathbb{Z}_4$ atuam por conjugação em $\mathbb{Z}_3^2$, com a ação dada pela matriz $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$.

Nestas condições, o grupo $Aut(G)$ pode também ser injetado em $A(2,\mathbb{Z}_3)$ e herda a estrutura de produto cindido de $A(2,\mathbb{Z}_3)$, cindindo da forma $\mathbb{Z}_3^2 \rtimes 16\,\Gamma_3 a_2$.

No capítulo seguinte, demonstramos um teorema para uma classe de grupos que abrange G, recebendo uma generalização do resultado acima.

CAPÍTULO VI - GENERALIZAÇÃO: $Aut(G) < A(n,\mathbb{Z}_p)$

No capítulo anterior, estudamos o produto semi-direto $G = \mathbb{Z}_3^2 \rtimes \mathbb{Z}_4$, considerado como subgrupo do grupo afim $A(2,\mathbb{Z}_3)$. Verificamos que o grupo $Aut(G)$ também cinde e é isomorfo a um subgrupo do grupo $A(2,\mathbb{Z}_3)$.

Este resultado nos motivou a buscarmos uma generalização deste grupo G. Gostaríamos de encontrar um grupo que seja um produto cindido, que possa ser injetado no grupo afim, cujo grupo de automorfismos também cinda e seja isomorfo a um subgrupo do grupo afim.

Com esta finalidade, no lugar de $\mathbb{Z}_3^2$ tomamos o grupo abeliano elementar $\mathbb{Z}_p^n$, p primo, e formamos uma extensão semi-direta deste grupo por um grupo cíclico $\mathbb{Z}_q$. A ação de conjugação de elementos de $\mathbb{Z}_q$ em $\mathbb{Z}_p^n$ é dada por: $\gamma_c(a) = cac^{-1}$, onde $\gamma: \mathbb{Z}_q \to Aut(\mathbb{Z}_p^n) : c \to \gamma_c$, e é suficiente definí-la para n geradores a_j de $\mathbb{Z}_p^n$, obtendo expressões da forma $ca_jc^{-1} = a_1^{m_{1j}} a_2^{m_{2j}} \ldots a_n^{m_{nj}}$. Como $\mathbb{Z}_p^n$ pode ser tratado como espaço vetorial n-dimensional, vamos considerar seqüência $(m_{1j}, \ldots, m_{nj})$ como vetor em $\mathbb{Z}_p^n$ (a imagem do j-ésimo vetor básico) e a ação γ_c em $a_j \in \mathbb{Z}_p^n$ será descrita, então, por uma matriz $M = (m_{ij})$ de $GL(n,\mathbb{Z}_p)$, com

a convenção comum de apresentar vetores-imagens como colunas.

Além disso, encontraremos a situação do subgrupo H de algum grupo G tal que todos os seus automorfismos possam ser realizados por conjugação em G. Então, considere o homomorfismo $\gamma: N_G(H) \to Aut(H) : u \to \gamma_u$, onde γ_u atua por conjugação em elementos de H: $\gamma_u = uhu^{-1}$, $u \in N_G(H)$, $h \in H$.

Naturalmente $\ker(\gamma) = Z_G(H)$. Temos $Im(\gamma) = {}^{N_G(H)}/_{Z_G(H)}$.

No caso de G finito, para que $Im(\gamma) \cong Aut(H)$ é necessário e suficiente que $\left[N_G(H) : Z_G(H)\right] = o(Aut(H))$. Por isso , introduzimos a noção que segue.

Definição: Dizemos que um subgrupo H de um grupo finito G é versátil quando há a igualdade $\left[N_G(H) : Z_G(H)\right] = o(Aut(H))$.

A generalização que buscamos será descrita no teorema a seguir, onde precisaremos das seguintes definições:

Definição: Seja G grupo finito e M espaço vetorial sobre o corpo K. Uma representação T é um homomorfismo $T: g \to T(g)$ de G em GL(M).

Definição: Uma representação T é fiel se T é injetivo.

Definição: Seja T uma representação de G em GL(M) e seja N um subespaço de M. N é subespaço invariante de T(G) se $T(N) \subset N$.

Definição: Uma representação $T: G \to GL(M)$ é irredutível se os únicos subespaços invariantes de T(G) são os triviais.

Teorema: Seja $G = \mathbb{Z}_p^n \rtimes \mathbb{Z}_q$, p primo, e seja $\zeta: \mathbb{Z}_q \to GL(n, \mathbb{Z}_p)$: $c \to M$ uma representação fiel de $\mathbb{Z}_q$, onde $\zeta(\mathbb{Z}_q)$ é versátil e M não tem valor próprio 1.

Nestas condições, o grupo Aut(G) tem uma injeção natural no grupo afim $A(n,\mathbb{Z}_p)$ e possui a estrutura de produto cindido $\mathbb{Z}_p^n \rtimes K$, onde

$$K \cong N_{GL(n,\mathbb{Z}_p)}(\zeta(\mathbb{Z}_q)) .$$

Se ζ é irredutível, a ordem de Aut(G) é $p^n.(p^n - 1).\varphi(q)$.

Demonstração: A demonstração do teorema será dividida nos seguintes pontos:

1. Aplicação injetiva $G \hookrightarrow A(n,\mathbb{Z}_p)$;
2. Número de cópias de $\mathbb{Z}_q$ em G ;
3. As p^n cópias de $\mathbb{Z}_q$ são conjugadas ;
4. Homomorfismo $Aut(G) \to S_k$, $k = p^n$;
5. Conjugações por $b \in \mathbb{Z}_p^n$ atuam como translações ;
6. Existe uma única cópia de $\mathbb{Z}_p^n$ em G ;
7. Automorfismos de G levantam-se para $A(n,\mathbb{Z}_p)$;
8. A unicidade do levantamento e
9. Ordem de Aut(G) para ζ irredutível

1. Aplicação injetiva $G \hookrightarrow A(n,\mathbb{Z}_p)$

Seja $ac^i \in G$. Como a pertence a um subgrupo $\mathbb{Z}_p^n$, que corresponde ao espaço vetorial $\mathbb{Z}_p^n$ sobre $\mathbb{Z}_p$, e a ação γ_c, de conjugação por c no grupo $\mathbb{Z}_p^n$, corresponde à ação da matriz $M \in GL(n,\mathbb{Z}_p)$, é natural anotar o elemento ac^i em forma de um par (a, M^i) (entendendo que a é um vetor), isto é, defi-

nir um monomorfismo $\Phi: G \to A(n, \mathbb{Z}_p) : ac^i \to (a, M^i)$.

Verificamos que Φ é homomorfismo:

$$(ac^i)(bc^j) = ac^i bc^j = ac^i bc^{-i} c^i c^j = a\gamma_{c^i}(b)c^i c^j =$$

$$= (a + M^i(b), M^{i+j}) = (a, M^i)(b, M^j).$$

Obviamente Φ é injetivo, pois temos unicidade de notação para elementos de G, na forma ac^i.

Graças à injeção de G em $A(n, \mathbb{Z}_p)$, podemos fazer cálculos em G tratando seus elementos como pares $(a, M^i) \in A(n, \mathbb{Z}_p)$.

2. Número de cópias de $\mathbb{Z}_q$ em G

Vamos verificar que cada elemento da forma ac gera uma cópia de $\mathbb{Z}_q$. Para obtermos isso, verificaremos que a ordem desse elemento é q.

Temos que $(ac)^i = (\sum_{k=0}^{i-1} M^k(a)).c^i$, o que provamos a seguir por indução:

Primeiro passo indutivo:

Para $i = 1 \Rightarrow (ac)^1 = (\sum_{k=0}^{0} M^k(a)).c^1 = I(a)c = ac.$

Em seguida, vamos supor que a igualdade vale para arbitrário, mas fixo, $i = j - 1$:

$$(ac)^{j-1} = (\sum_{k=0}^{j-2} M^k(a)).c^{j-1}$$

e verificamos a validade da fórmula para $i = j$:

$$(ac)^j = (ac)^{j-1}.(ac)^1 = (\sum_{k=0}^{j-2} M^k(a)).c^{j-1}).(ac) =$$

$$= \left(\sum_{k=0}^{j-2} M^k(a)\right).c^{j-1}ac = \left(\sum_{k=0}^{j-2} M^k(a)\right).c^{j-1}ac^{-(j-1)}c^{j-1}c =$$

$$= \left(\sum_{k=0}^{j-2} M^k(a)\right).(M^{j-1}(a)).c^j = \left(\sum_{k=0}^{j-1} M^k(a)\right).c^j \quad .$$

Assim, temos $(ac)^i = bc^i$, $b \in \mathbb{Z}_p^n$.

Em seguida, vamos calcular a ordem de ac.

Como temos unicidade de notação para elementos de G na forma bc^i, o fato que $bc^i = e$ implica em $b = e$ e $c^i = e$. Esta última igualdade implica em $q \mid i$, já que $o(c) = q$.

Então, o menor candidato para a ordem de ac é o número q. Calculamos a parte translacional de $(ac)^q$, que é igual a $\left(\sum_{k=0}^{q-1} M^k(a)\right)$.

Notamos que $\left(\sum_{k=0}^{q-1} M^k\right)(M - I) = M^q - I$ e, em seguida, que $M^q - I$ é a matriz 0 (lembre que $\mathbb{Z}_q \to GL(n,\mathbb{Z}_p): c \to M$ é representação fiel), assim como $(M - I)$ é inversível, já que M não tem valor próprio 1. Em conseqüência , $\sum_{k=0}^{q-1} M^k = 0$ e $\left(\sum_{k=0}^{q-1} M^k\right)(a) = 0(a) = o$.

Então, cada elemento da forma ac gera uma cópia de $\mathbb{Z}_q$. Diferentes $a, b \in \mathbb{Z}_p^n$ geram cópias diversas de $\mathbb{Z}_q$, pois $bc \in \langle\langle ac \rangle\rangle$ implica em $\exists_i\ bc = (ac)^i$, o que implica em $i = 1$ e $a = b$. Como $a \in \mathbb{Z}_p^n$, temos tantas cópias de $\mathbb{Z}_q$ quantos $a \in \mathbb{Z}_p^n$, isto é, p^n.

3. As p^n cópias de $\mathbb{Z}_q$ são conjugadas

Vamos verificar se duas cópias de $\mathbb{Z}_q$ são conjugadas.

Dados dois geradores de $\mathbb{Z}_q$, ac e $a'c$, vamos verificar se existe $b \in \mathbb{Z}_p^n$ que os conjugue. Para isso, é necessário que $(b, I)(a, M)(b, I)^{-1} = (a', M)$,
o que é equivalente a

$$(b, I)(a, M) = (a', M)(b, I) .$$

Então

$$(b + I(a), IM) = (a' + M(b), MI),$$

que implica em

$$\begin{cases} b + a = a' + M(b) & (1) \\ IM = MI & (2) \end{cases} .$$

A igualdade da equação (2) é óbvia.

Da equação (1), temos

$$b - M(b) = a' - a \implies (I - M)(b) = a' - a.$$

Em virtude da existência de $(I - M)^{-1}$ (como notamos no ponto 2), temos

$$b = (I - M)^{-1}(a' - a).$$

Assim, para duas cópias quaisquer de $\mathbb{Z}_q$, encontramos $b \in \mathbb{Z}_p^n$ que as conjugue. Logo, temos que as p^n cópias de $\mathbb{Z}_q$ são conjugadas.

4. Homomorfismo $Aut(G) \to S_k$, $k = p^n$

Como temos $k = p^n$ cópias conjugadas de $\mathbb{Z}_q$, obviamente automorfismos de G vão permutar essas k cópias. Assim,

temos homomorfismo g: $\mathrm{Aut}(G) \to S_k$, que age permutando os k subgrupos $\mathbb{Z}_q$. Mas, em vez de considerarmos um índice k como elemento do conjunto $\{1, 2, \ldots, p^n\}$, vamos pensar em k como vetor de $\mathbb{Z}_p^n$. Veremos que, desta forma, estas permutações correspondem a translações em $\mathbb{Z}_p^n$.

5. Conjugações por $b \in \mathbb{Z}_p^n$ atuam como translações

Indicaremos as p^n cópias de $\mathbb{Z}_q$ por meio de vetores

$$\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \in \mathbb{Z}_p^n \ .$$

Os automorfismos de conjugação por elemento $b \in \mathbb{Z}_p^n$ em $ac \in \mathbb{Z}_q$ ($\gamma_b(ac)$) resultam em translações em $\mathbb{Z}_p^n$:

$$\gamma_b(ac) = b(ac)b^{-1} = bacb^{-1} = bacb^{-1}c^{-1}c =$$

$$= ab\gamma_c(b^{-1})c = ab(\gamma_c(b))^{-1}c \ .$$

Associamos $\gamma_b(ac) \longrightarrow (a + b - M(b), M)$, ou melhor,

γ_b: $(a, M) \longrightarrow (a + b - M(b), M) = ((I - M)(b), I) + (a, M)$.

Desta última expressão, temos que $(I - M)(b) = d$.

Como já sabemos que $(I - M)^{-1}$ existe, para cada $b \in \mathbb{Z}_p^n$ temos um elemento $d \in \mathbb{Z}_p^n$, pois se b percorre $\mathbb{Z}_p^n$, então d também o fará.

Então, temos $\begin{cases} \gamma_b((a, M)) = (d, I) + (a, M) \ , \\ \qquad \text{com} \quad b = (I - M)^{-1}(d). \end{cases}$

6. Existe uma única cópia de $\mathbb{Z}_p^n$ em G

Vamos supor que c^i é de ordem p. Mas c^i não comuta com n - 1 vetores linearmente independentes (LI) de $\mathbb{Z}_p^n$ pois, se comutasse, $M^i(a) = c^i a c^{-i}$ teria n - 1 valores próprios 1.

O polinômio minimal de M^i, neste caso $(\lambda - 1)^{n-1}$, divide o polinômio característico $\chi_{M^i}(\lambda)$ e o quociente $(\lambda - 1)^{n-1} \mid \chi_{M^i}(\lambda)$ tem grau 1. Assim, M^i teria n-ésimo valor próprio z:

$$M^i \sim \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & z \end{pmatrix}.$$

Como supomos $(c^i)^p = e$, temos

$$I = (M^i)^p \sim \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & z \end{pmatrix}^p = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & z^p \end{pmatrix}.$$

Mas $z^p \equiv z \pmod p$. Então $z = 1$ e

$$M^i \sim \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \Rightarrow M^i \sim I_n \Rightarrow M^i = I_n .$$

Daqui, teríamos $q \mid i$ e M^i, contrário à hipótese, teria ordem $1 \neq p$.

Assim, verificamos que não há outro elemento em G, de ordem p, que, junto com n - 1 elementos LI de $\mathbb{Z}_p^n$, possa gerar uma outra cópia de $\mathbb{Z}_p^n$.

7. Automorfismos de G levantam-se para $A(n,\mathbb{Z}_p)$

Seja $\alpha \in Aut(G)$. Vamos considerar que α atua na cópia de G em $A(n,\mathbb{Z}_p)$. Neste caso, α é definido em $\{e_1,\ldots,e_n, M\}$, onde $[e_i]$ é base para $\mathbb{Z}_p^n$ e $M \in GL(n,\mathbb{Z}_p)$ tal que $M^q = I$.

Qualquer automorfismo α leva $\mathbb{Z}_p^n$ em $\mathbb{Z}_p^n$ ($\mathbb{Z}_p^n$ é característico, já que não tem outra cópia de $\mathbb{Z}_p^n$ em G, veja ponto 6).

No Capítulo 5, ponto 5, mostramos que $Aut(\mathbb{Z}_p^n) \cong GL(n,\mathbb{Z}_p)$. Então α, restrito a $\mathbb{Z}_p^n$, será dado por uma matriz, que chamaremos A_α, $A_\alpha \in GL(n,\mathbb{Z}_p)$.

Suponha inicialmente que $\alpha(M) = M$. Neste caso, temos $\alpha: \{e_1, \ldots, e_n, M\} \to \{A_\alpha(e_1), \ldots, A_\alpha(e_n), M\}$.

Como α é automorfismo, temos, para $a \in \mathbb{Z}_p^n$,

$$\alpha[(o, M).(a, I)] = \alpha(o, M).\alpha(a, I).$$

Do termo à esquerda da igualdade, temos

$$\alpha[(o, M).(a, I)] = \alpha(M(a), M) = (A_\alpha M(a), M).$$

Do termo à direita da igualdade, temos

$\alpha(o, M).\alpha(a, I) = (o, M).(\alpha(a), I) = (o, M).(A_\alpha(a), I) =$

$= (MA_\alpha(a), M).$

Então, $\forall_{a \in \mathbb{Z}_p^n}$ $A_\alpha M(a) = MA_\alpha(a)$, que implica em

$A_\alpha M = MA_\alpha$. Como A_α é inversível (pois $A_\alpha \in GL(n,\mathbb{Z}_p)$), segue α tem que ser tal que $A_\alpha MA_\alpha^{-1} = M$, ou seja, A_α deve pertencer ao centralizador de M em $GL(n,\mathbb{Z}_p)$.

Vamos verificar se é possível realizar α por meio de conjugação em $A(n,\mathbb{Z}_p)$, isto é, veremos se existe um par $(t,N) \in A(n,\mathbb{Z}_p)$ tal que

$$\begin{cases} (t,N)(o,M)(t,N)^{-1} = (o,M) & (1) \\ (t,N)(e_i,I)(t,N)^{-1} = (A_\alpha(e_i), I), \ i = 1,\ldots,n & (2) \end{cases} .$$

Da equação (1), temos: $(t, N)(o, M) = (o, M)(t, N)$, que equivale a $(t + N(o), NM) = (o + M(t), MN)$, que implica em

$$\begin{cases} t = M(t) & (3) \\ NM = MN & (4) \end{cases} .$$

Da equação (2), temos: $\forall_{1 \leq i \leq n}$ $(t, N)(e_i, I) = (A_\alpha(e_i), I)(t,N)$, que equivale a $(t + N(e_i), NI) = (A_\alpha(e_i) + I(t), IN)$, que implica em

$$\begin{cases} t + N(e_i) = A_\alpha(e_i) + t & (5) \\ NI = IN & \end{cases} .$$

Claramente, a última igualdade não impõe nenhuma restrição à matriz N.

Com as equações 3 - 5, formamos o sistema

$$\begin{cases} (I - M)(t) = o & (3') \\ NMN^{-1} = M & (4') \\ \forall\ N(e_i) = A_\alpha(e_i) & (5') \\ 1 \leq i \leq n \end{cases}$$

Da equação (3'), temos $t = o$, pois M não possui valor próprio 1. Da equação (5'), temos $N = A_\alpha$, que satisfaz também (4').

Assim, o automorfismo α é realizado por conjugação pelo elemento $(o, A_\alpha) \in A(n, \mathbb{Z}_p)$.

Em seguida, suponha que $\beta \in Aut(G)$ atue em M assim: $\beta(o, M) = (d, M^i)$.

Considere o automorfismo $\alpha_{d,i}$, induzido por conjugação em $A(n, \mathbb{Z}_p)$ pelo par $((I - M^i)^{-1}(d), N_i)$, onde $N_i \in GL(n, \mathbb{Z}_p)$ satisfaz a igualdade $N_i M N_i^{-1} = M^i$.

A existência de N_i está garantida, pois $\mathcal{C}(\mathbb{Z}_q)$ é versátil.

Defina $\alpha = \beta \circ \alpha_{d,i}^{-1}$. Note que $\alpha(o, M) = (o, M)$, então α é induzido (como a nossa análise anterior mostrou) por conjugação por um elemento do tipo (o, A_α), onde $A_\alpha \in Z_{A(n, \mathbb{Z}_p)}(\Phi(G))$. Então, $\beta = \alpha \circ \alpha_{d,i}$ é induzido por conjugação pelo produto $(o, A_\alpha)((I - M^i)^{-1}(d), N_i) =$

$= (A_\alpha(I - M^i)^{-1}(d), A_\alpha N_i)$.

8. A unicidade do levantamento

No ponto 7, provamos que $\phi(G)$ é versátil em $A(n, \mathbb{Z}_p)$. Agora, mostraremos que $Z_{A(n, \mathbb{Z}_p)}(\phi(G)) = \{ e \}$, o que equivale à constatação que $N_{A(n,\mathbb{Z}_p)}(\phi(G)) \to Aut(G)$ é uma bijeção.

Seja $(t, N) \in N_{A(n,\mathbb{Z}_p)}(\phi(G))$. Se (t, N) pertence ao centralizador, então atua trivialmente também em $\mathbb{Z}_p^n \in \phi(G)$. Mas $(t, N)(a, I)(t, N)^{-1} = (a, I)$ para todos $a \in \mathbb{Z}_p^n$, isto é,

$$\forall_{a \in \mathbb{Z}_p^n} \quad (t, N)(a, I) = (a, I)(t, N) \text{ , significa}$$

$$\forall_{a \in \mathbb{Z}_p^n} \begin{cases} t + N(a) = a + t \\ N = N \end{cases}$$

o que implica em $N = I$, então $(t, N) = (t, I)$.

Se $(t, I)(o, M)(t, I)^{-1} = (o, M)$, isto é, se $(t, I)(o, M) = (o, M)(t, I)$, temos $(t, M) = (M(t), M)$, de onde vem que $t = M(t)$, o que implica em $t = o$.

Daqui, temos $Z_{A(n,\mathbb{Z}_p)}(\phi(G)) = \{ (o, I) \} = \{ e \}$.

9. Ordem de Aut(G) para $\mathcal{L}$ irredutível

Vamos assumir, neste ponto, que M seja irredutível sobre $\mathbb{Z}_p$. Note que os vetores $e_1, M(e_1), \ldots, M^{n-1}(e_1)$ são linearmente independentes pois, se $M^k(e_1) \in U$, onde $U = \ll e_1, M(e_1), \ldots, M^{k-1}(e_1) \gg$ para algum $k < n - 1$, isto im-

plicaria que $M^{k+s}(e_1) \in U$ (o que se demonstra indutivamente) e este fato significaria que $\ll e_1, \ldots, M^{k-1}(e_1) \gg$ geraria um subespaço invariante não-trivial com relação à ação de M, contrário à hipótese de irredutibilidade.

Então $\underset{v \in \mathbb{Z}_p^n}{\forall} \quad \underset{u_1,\ldots,u_n \in \mathbb{Z}_p}{\exists} \quad v = \sum_{i=0}^{n-1} u_i M^i(e_1)$ (1).

Note que o conjunto

$$P = \left\{ A \in GL(n, \mathbb{Z}_p) \ : \ A = \sum_{i=0}^{q-1} u_i M^i \ : \ u_i \in \mathbb{Z}_p \right\} \qquad (2)$$

está contido no centralizador $H = Z_{GL(n,\mathbb{Z}_p)}(\prec(\mathbb{Z}_q))$.

Em vista de (1) e (2), no centralizador H temos matrizes com a primeira coluna pré-fixada:

$$\underset{v \neq o}{\forall} \quad \underset{A \in H}{\exists} \quad A(e_1) = v \ .$$

Então $o(H) \geqslant p^n - 1$. Para provar a desigualdade inversa, tomamos $A \in Z_{GL(n,\mathbb{Z}_p)}(M)$ e escolhemos a base de $\mathbb{Z}_p^n$ de vetores $e_i = M^{i-1}(e_1)$. Se conhecemos $A(e_1) = v$, temos $A(e_j) = AM^{j-1}(e_1) = M^{j-1}A(e_1) = M^{j-1}(v)$.

Então, o fato que A centraliza M, irredutível, e a primeira coluna de A determinam toda a matriz A.

Temos que $Aut(G) = \left\{ (t, N) \in N_{A(n,\mathbb{Z}_p)}(\Phi(G)) \right\}$.

A parte translacional de Aut(G) corresponde à ação de elementos (α, I) por conjugação em $A(n, \mathbb{Z}_p)$. Como obtemos todas as translações em $\mathbb{Z}_p^n$, temos

$o(Aut(G)) = p^n . o(N_{GL(n,\mathbb{Z}_p)}(\angle(\mathbb{Z}_q)))$.

Mas $\angle(\mathbb{Z}_q)$ é versátil, então:

$\text{Normalizador}/\text{Centralizador} \cong Aut(\mathbb{Z}_q)$.

Então, a ordem do normalizador é o produto das ordens do centralizador e de $Aut(\mathbb{Z}_q)$. Daí, temos que a ordem do normalizador é $(p^n - 1).\varphi(q)$ e, conseqüentemente,

$o(Aut(G)) = p^n.(p^n - 1).\varphi(q)$.

Está demonstrado o teorema.

Por último, mostramos que as hipóteses: a) $\angle$ é fiel e b) $\angle(\mathbb{Z}_q)$ é versátil são necessárias para a validade da nossa tese.

a) Vamos supor $\angle: \mathbb{Z}_q \to \mathbb{Z}_s \subset GL(n, \mathbb{Z}_p)$, onde $s = \frac{q}{r}$. Se $r \neq 1$, temos $c^s \to I$. No entanto, em $\mathbb{Z}_q$ temos o automorfismo $\alpha_{s+1} : c \to c^{s+1}$, mas $\phi: G \to A(n, \mathbb{Z}_p) : c \to (o, M)$ e $(\phi \circ \alpha_{s+1})(c) = \phi(c^{s+1}) = (o, M)$.

Então, $Ker(\angle)$ não seria trivial. Assim, não teríamos distinção, em matrizes, dos elementos c e c^{s+1}, então nenhum automorfismo de matrizes conseguiria distinguir dois diferentes elementos da imagem inversa $\phi^{-1}(M)$.

b) É claro que, em geral, nem todo subgrupo de G é versátil, por exemplo, subgrupos do grupo abeliano tem normalizadores triviais. No entanto, poder-se-ia suspeitar que os

subgrupos cíclicos dos grupos matriciais sobre um corpo finito gozassem desta propriedade. Para remover a suspeita da redundância da nossa hipótese, damos um contra-exemplo:

Sabemos que $o(Aut(\mathbb{Z}_q)) = \varphi(q)$.

Seja $r_p = o(GL(n,\mathbb{Z}_p)) = (p^n-1)(p^n - p) \ldots (p^n - p^{n-1})$.

Como a ordem de um subgrupo divide a ordem do grupo, temos $q \mid r_p$ e, como queremos ter $Aut(\mathbb{Z}_q)$ imagem homomorfa de um subgrupo de $GL(n, \mathbb{Z}_p)$, então queremos $\varphi(q) \mid r_p$.

Consideremos $n = 2$, $p = 23$ e $q = 11$.

Neste caso, $11 \mid r_{23} = 22^2.23.24$.

Como $q = 11$ é primo, pelo 1º Teorema de Sylow, existe cópia $\mathbb{Z}_{11}$ em $GL(2,\mathbb{Z}_{23})$. Por outro lado, $Aut(\mathbb{Z}_{11}) \cong \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$, e como $\mathbb{Z}_{10}$ é cíclico e $5 \mid 10$, $\mathbb{Z}_{10}$ possui subgrupo de ordem 5, que também seria subgrupo de $GL(2, \mathbb{Z}_{23})$. Mas $5 \nmid o(GL(2,\mathbb{Z}_{23}))$. Então, $\mathbb{Z}_{11}$ não é versátil em $GL(2, \mathbb{Z}_{23})$.

ÍNDICE DE NOÇÕES

INDICE DE SÍMBOLOS

REFERÊNCIAS

[1] N.L.Biggs and A.T.White - Permutations Groups and Combinatorial Estrutures - Cambridge University Press, 1979 (LMS, Lecture Note Series 33).

[2] W.Burnside - Theory os Groups of Finite Order - Dover Publications, Inc.- 2^{nd} ed., 1911.

[3] H.S.M.Coxeter and W.O.J.Moser - Generators and Relations for Discrete Groups - Springer-Verlag - 4^{th} ed.,1984.

[4] C.W.Curtis and I.Reiner - Representation Theory of Finite Groups and Associative Algebras - Interscience Publishers, 1962.

[5] D.Gorenstein (editor) - Reviews on Finite Groups - AMS, Providence, RI, 1974.

[6] M.Hall Jr - The Theory of Groups - The Macmillan Company, 1959.

[7] M.Hall Jr and J.K.Senior - The Groups of Order $2^n (n \leq 6)$ - The Macmillan Company, 1964.