UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

EMANOEL FERREIRA DE SOUZA

CÓDIGOS DE GRUPO SOBRE GRUPOS NÃO ABELIANOS

FORTALEZA
2018

EMANOEL FERREIRA DE SOUZA

CÓGIGOS DE GRUPO SOBRE GRUPOS NÃO ABELIANOS

Dissertação apresentada ao Programa de Pós-graduação em Matemática do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Álgebra.

Orientador: Prof. Dr. Rodrigo Lucas Rodrigues
Coorientadora: Profa. Dra. Consuelo Martínez López

FORTALEZA
2018

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S237c Souza, Emanoel Ferreira de.
Códigos de grupo sobre grupos não abelianos / Emanoel Ferreira de Souza. – 2018.
61 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Matemática, Fortaleza, 2018.
Orientação: Prof. Dr. Rodrigo Lucas Rodrigues.
Coorientação: Profa. Dra. Consuelo Martínez López.

1. Decomposição abeliana. 2. Códigos de grupo abelianos. 3. Corpo base. I. Título.

CDD 510

EMANOEL FERREIRA DE SOUZA

CÓDIGOS DE GRUPO SOBRE GRUPOS NÃO ABELIANOS

Dissertação apresentada ao Programa de Pós-graduação em Matemática do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Álgebra.

Aprovado em: 19/02/2018.

BANCA EXAMINADORA

Prof. Dr. Rodrigo Lucas Rodrigues (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Francisco César Polcino Milies
Universidade de São Paulo (IME-USP)

Prof. Dr. Francisco Luís Rocha Pimentel
Universidade Federal do Ceará (UFC)

Prof. Dr. José Alberto Duarte Maia
Universidade Federal do Ceará (UFC)

Dedico este trabalho ao grande Matemático e Professor Elon Lages Lima(*in Memoriam*), que participou ativamente em minha formação através de sua obra.

AGRADECIMENTOS

À minha família em geral, em especial minha mãe Francisca (Leninha), meu pai Francisco (Chico Relojoeiro do Codiá), meus irmãos Francisca, Ivan e Renato, pelo apoio dado no decorrer desta etapa;

À minha noiva Jemima que sempre esteve comigo e foi meu ponto de apoio para superar muitas das adversidades que enfrentei ao longo desta trajetória;

Ao meu orientador Rodrigo Rodrigues pela paciência ao me passar diversos ensinamentos, que foram essenciais para que eu concluísse todas as etapas deste trabalho e tivesse um bom desempenho no curso de forma geral;

Aos membros da banca, Prof. C. Polcino Milies, Prof. Francisco Pimentel e Prof. Alberto Maia, pela disponibilidade.

A todos os professores do departamento de Matemática da UFC, em especial Edson Sampaio, Francisco Pimentel, Alberto Maia, Lev Birbrair e Fernanda Camargo; e todos os professores da FECLESC, em especial Antônio Grangeiro (que gentilmente me acolheu em sua casa e me possibilitou participar do verão que preparava para o ingresso no mestrado), Ulisses Parente (que me ajudou a me instalar em Fortaleza), Pereira, Jobson e Luzeilton (meu orientador na graduação).

Aos amigos Bira (que me ajudou bastante assim que cheguei a Fortaleza), Jordânia, Petrus, Davi, Valdir, Edvalter, Wendel, Firmino, Valéria, Tony, Patrícia, Liduíno (Lidú), Wilton e Heldemir pelos inúmeros momentos compartilhados;

A todos os meus colegas de curso, em especial Diego, André Costa, André Gadelha, Hamilton, Felipe, Rosa, Gauss, Sílvio, Pedro, Thiago, Thiago Gadelha e Danielson pelos vários momentos que compartilhamos.

A CAPES pelo apoio financeiro.

“Nada como se sentir vivo, mesmo que portador da morte...”
(EMANOEL FERREIRA)

RESUMO

Sejam G um grupo finito e F um corpo. Mostramos que todos os G-códigos sobre F são abelianos se a ordem de G é menor que 24, mas para $F = \mathbb{Z}_5$ e $G = S_4$ existe um G-código não abeliano sobre F, respondendo uma questão em aberto proposta por BERNAL, DEL RÍO, and SIMÓN (2009). Este problema está relacionado à existência de decomposição de um grupo como o produto de dois subgrupos abelianos. Consideramos este problema no caso de p-grupos, encontrando uma ordem minimal para a qual todos os p-grupos de tal ordem admitem a decomposição mencionada. Finalmente, estudamos quais imposições devem ser feitas a um corpo finito F e uma extensão finita E deste, para que todos os G-códigos abelianos sobre F sejam ainda códigos abelianos sobre E ou os G-códigos abelianos sobre E sejam códigos abelianos sobre F.

Palavras-chave: Decomposição abeliana. Códigos de grupo abelianos. Corpo base.

ABSTRACT

Let G be a finite group and F a field. We show that all G-codes over F are abelian if the order of G is less than 24, but for $F = \mathbb{Z}_5$ and $G = S_4$ there exist non-abelian G-codes over F, answering to an open problem posed in BERNAL, DEL RÍO, and SIMÓN (2009). This problem is related to the decomposability of a group as the product of two abelian subgroups. We consider this problem in the case of p-groups, finding the minimal order for which all p-groups of such order are decomposable. Finally, we study if the fact that all G-codes are abelian remains true when the base field is changed.

Keywords: Abelian decomposition. Abelian group codes. Base field.

SUMÁRIO

1 INTRODUÇÃO

Em 1948, o artigo "A Mathematical Theory of Communication" de Claude Shannon deu origem às disciplinas de *teoria da informação* e de *teoria de códigos*. Ambas visam melhorar a comunicação resguardando a conveniência, confidenciabilidade e eficiência. Ou seja, a transferência de informação deve ser tão rápida quanto possível, considerando a quantidade de dados, e tão confiável quanto necessário. Como estes dois objetivos têm conflitado-se, nosso intuito é encontrar um equilíbrio satisfatório.

A teoria de códigos é uma tentativa de resolver esta questão usando ferramentas algébricas. Em outras palavras, há dois aspectos essenciais nesta teoria, nomeadamente, compressão de dados e correção de erros. Na teoria de códigos existem duas seções trabalhando nesta problemática. A primeira é em *códigos lineares* e a segunda em *códigos convolucionais*. Ambas analisam propriedades essenciais dos códigos chamadas *parâmetros*, que são: o comprimento das palavras, a quantidade de palavras válidas no código e a distância mínima entre duas palavras válidas do código. Aqui, focaremos nos códigos lineares.

Os códigos algébricos são um bom exemplo para mostrar que quanto mais estrutura algébrica se adiciona a um sistema, mais capacitado se está para descrever o sistema. Por exemplo, indo de códigos para códigos lineares, obtém-se a facilidade em calcular a distância mínima, calculando o peso mínimo do código. Assim, usando *códigos cíclicos* em vez de códigos lineares, ganha-se uma descrição ainda mais frutífera.

Com o artigo "Error detecting and error correcting code" de R. W. Hamming, em 1950, os códigos lineares receberam cada vez mais atenção. Um código linear é um subespaço de um espaço vetorial sobre um corpo finito. O estudo em seu estágio inicial era focado em códigos binários, mas atualmente existe um interesse teórico em códigos sobre corpos finitos com características ímpares, devido as suas boas propriedades para correção de erros.

Os códigos lineares mais importantes são os códigos cíclicos, pois assim como mencionado antes, estes têm uma estrutura mais rica e consequentemente melhores propriedades para correção de erros. Estes e mais alguns fatos sobre tais códigos serão discorridos adiante.

Nas preliminares apresentamos os principais resultados sobre Anéis de Grupos que utilizaremos ao longo do texto, além das definições e resultados básicos necessários sobre códigos, para assim podermos definir código de grupo, que será o principal objeto de estudo desta dissertação e relaciona códigos lineares cíclicos à estrutura de álgebra de grupo. Mais especificamente, mostraremos que sendo $G = \{g_0 = e, g_1, \ldots, g_{n-1}\}$ um grupo finito e F um corpo finito, qualquer ideal (à esquerda) L do anel de grupo FG

define um código de grupo (à esquerda) $K(L)$ de comprimento n sobre F pela regra

$$(a_0, a_1, \ldots, a_{n-1}) \Leftrightarrow a_0g_0 + a_1g_1 + \cdots + a_{n-1}g_{n-1} \in L.$$

Qualquer código que seja equivalente por permutação a $K(L)$ para algum ideal (à esquerda) L do anel FG é chamado um G-código.

Em seguida passamos a tratar dos resultados presentes no artigo base, a saber "*Group codes over non abelian groups*"(2013) dos autores C. G. Pillado, S. Gonzalez e C. Martinez, incluindo também resultados cruciais, como por exemplo alguns resultados encontrados em "*An intrinsical description of group codes*"(2009) dos autores J.J Bernal, Á. del Río e J. J. Simón. Um código de grupo é dito *abeliano*, se for um A-código para algum grupo abeliano A. Em BERNAL, DEL RÍO, and SIMÓN (2009) foi provado que existe um código de grupo à esquerda não abeliano mas nenhum código de grupo à esquerda não abeliano era conhecido. Neste trabalho descrevemos algumas classes de grupos e corpos para os quais todos os códigos de grupo são abelianos, assim como fornecemos um exemplo de um código de grupo não abeliano. Também notamos aqui que alguns exemplos de códigos de grupo à esquerda também foram dados em COUSELO *et al.* (2004)(onde foram chamados de códigos de grupo). Por exemplo, existem [8,3,5]-códigos de grupo à esquerda em $\mathbb{F}_4Q_8$, mas não existem códigos com os mesmos parâmetros em qualquer anel $\mathbb{F}_4A$, onde A é um grupo abeliano de ordem oito.

Mostramos que todo grupo G de ordem menor que 24, assim como todo grupo de ordem p^kq^l, p, q primos e $k, l \leq 2$, admite decomposição abeliana. Também mostramos que para qualquer primo $p > 2$ existe um grupo de ordem p^5 que não admite decomposição abeliana, mas todos os grupos de ordem $2^5 = 32$ possuem uma decomposição abeliana. Também fornecemos um exemplo de um grupo de ordem $2^6 = 64$ que não admite decomposição abeliana. O último exemplo fornece uma resposta negativa para o questionamento natural se todo grupo de comprimento nilpotente dois possui uma decomposição abeliana. Finalmente, mostramos que existem S_4-códigos sobre $\mathbb{Z}_5$ que são códigos não abelianos. O último aparece enunciado, sem prova, em PILLADO *et al.* (2011). Por último, analisaremos sob quais condições, dados corpos finitos F e E com $F \subset E$ e um grupo finito G vale que se todos os G-códigos sobre E são abelianos então todos os G-códigos sobre F são abelianos. Reciprocamente, se todos os G-códigos sobre F são abelianos então todos os G-códigos sobre E são abelianos.

2 PRELIMINARES

Ao longo de todo este trabalho, salvo menção do contrário, denotaremos por e ou 1 o elemento identidade de um grupo G, $Z(G)$ o centro do grupo G e $[x, y] = x^{-1}y^{-1}xy$ o comutador dos elementos $x, y \in G$. O subgrupo gerado por um subconjunto S de um grupo G será denotado por $\langle S \rangle$, ou simplesmente por $\langle a_1, \ldots, a_n \rangle$ caso $S = \{a_1, \ldots, a_n\}$.

2.1 Resultados clássicos

Os resultados apresentados a seguir são usados no decorrer do trabalho e podem ser encontrados, por exemplo, em MILIES and SEHGAL (2002). A menos de menção explícita do contrário, p denotará um número primo.

Proposição 2.1. *Seja G um grupo de ordem p. Então G é cíclico.*

Proposição 2.2. *Seja G um grupo de ordem p^2. Então G é abeliano.*

Proposição 2.3. *Se $G/Z(G)$ é um grupo cíclico, então G é abeliano.*

Teorema 2.4. *Seja G um grupo abeliano de ordem $p_1^{n_1} \cdots p_k^{n_k}$, onde p_i é um número primo. Então*

$$G \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}.$$

Definição 2.5. *Um grupo abeliano elementar (ou um p-grupo abeliano elementar) é um grupo abeliano que se escreve como produto direto de grupos de ordem p.*

Definição 2.6. *Sejam G um grupo e M um conjunto. Dizemos que G age em M via ϕ se existe um homomorfismo $\phi\colon G \to S_M$, onde S_M denota o grupo de simetria de M, ou seja, o grupo das bijeções deste conjunto com a operação de composição usual de funções.*

Definição 2.7. *Seja G um grupo de ordem $p^n m$ onde $p \nmid m$. Um subgrupo de G de ordem p^i, $0 \leq i < n$ é chamado de um p-subgrupo de G. Se $i = n$ tal subgrupo é chamado de p-subgrupo de Sylow de G.*

Teorema 2.8. ***(Sylow)*** *Seja G um grupo de ordem $p^n m$, onde $p \nmid m$. Então:*

1. *G contém p-subgrupos de Sylow e, além disso, todo p-subgrupo de G está contido em um p-subgrupo de Sylow de G.*
2. *Todos os p-subgrupos de Sylow de G são conjugados em G.*
3. *Se n_p denota o número de p-subgrupos de Sylow de G, então*

$$n_p \equiv 1 (\mathrm{mod}\, p).$$

2.2 Anéis de grupo

Sejam R um anel comutativo, associativo com identidade e G um grupo multiplicativo arbitrário. O *anel de grupo RG* é uma R-álgebra na qual os elementos de G formam uma base e o produto se define de forma distributiva utilizando o produto do

grupo G. De forma mais precisa, os elementos de RG são da forma

$$a = \sum_{g \in G} a_g \cdot g,$$

onde os coeficientes a_g são elementos do anel R não nulos apenas para um número finito de elementos de G. Se

$$b = \sum_{g \in G} b_g \cdot g$$

é outro elemento de RG, então a adição e a multiplicação se definem como segue:

$$a + b = \sum_{g \in G} a_g \cdot g + \sum_{g \in G} b_g \cdot g = \sum_{g \in G} (a_g + b_g) \cdot g$$

e

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

sendo

$$c_z = \sum_{gh=z} a_g b_h = \sum_{g} a_g b_{g^{-1}z} = \sum_{h} a_{zh^{-1}} b_h.$$

Com estas operações RG é um anel e é, além disso, uma R-álgebra associativa na qual a multiplicação por escalar é dada por

$$\alpha a = \alpha \left(\sum_{x \in G} a_x \cdot x \right) = \sum_{x \in G} (\alpha a_x) \cdot x.$$

Observemos que se identificarmos $g \in G$ com $1 \cdot g \in RG$, então tem-se que $G \subseteq RG$ e, portanto, os elementos de G formam uma R-base. Esta identificação converte as somas e produtos formais em somas e produtos ordinários, pois podemos escrever $a_g g$ em vez de $a_g \cdot g$. Além do mais, o elemento $e \in G$ é o elemento identidade de RG.

Exemplo 2.9. *Quando $G = \langle x \rangle$ é finito, temos que $e, x, x^2, \ldots, x^{n-1}$ formam uma base de RG e cada elemento de RG se escreve de forma única como*

$$a = \sum_{i=0}^{n-1} a_i x^i.$$

Uma propriedade básica dos anéis de grupo é sua simetria. Seja $*\colon RG \to RG$ uma aplicação dada por

$$* \left(\sum a_x x \right) = \left(\sum a_x x \right)^* = \sum a_x x^{-1}.$$

Como para $x, y \in G$ tem-se $(xy)^{-1} = y^{-1}x^{-1}$, vê-se sem muito esforço que para $a, b \in RG$,

valem:

$$\begin{aligned}(a+b)^* &= a^* + b^* \\ (ab)^* &= b^*a^* \\ (a^*)^* &= a^{**} = a.\end{aligned}$$

Portanto, $*$ é um antiautomorfismo de ordem 2, o que nos leva ao fato de RG possuir propriedades similares à esquerda e à direita.

Definição 2.10. *Seja $a = \sum a_x x \in RG$. Define-se o suporte de a, denotado por* $\mathrm{Supp}(a)$*, como o conjunto dos elementos do grupo cujos coeficientes na representação de a são não nulos,*

$$\mathrm{Supp}(a) = \{x \in G \mid a_x \neq 0\}.$$

Definimos também o subgrupo suporte de a como sendo $\langle \mathrm{Supp}(a) \rangle$.

Portanto, $\mathrm{Supp}(a)$ é um subconjunto finito de G que é vazio se, e somente se, $a = 0$. Note que assim, $\langle \mathrm{Supp}(a) \rangle$ é o subgrupo de G finitamente gerado pelos elementos de $\mathrm{Supp}(a)$.

Se $H \leq G$ então $H \subseteq G \subseteq RG$ e a expansão R-linear de H em RG é RH. Deste modo, RH está contido de forma natural em RG. De fato,

$$RH = \{a \in RG \mid \mathrm{Supp}(a) \subseteq H\}.$$

É claro que, para $a \in RG$, $\langle \mathrm{Supp}(a) \rangle$ é o menor subgrupo H de G tal que $a \in RH$.

Proposição 2.11. *Se $a \in RG$, $a \neq 0$ e $g \in G$, então* $\mathrm{Supp}(ga) = g(\mathrm{Supp}(a))$ *e* $\mathrm{Supp}(ag) = (\mathrm{Supp}(a))g$. *Em particular, se $x \in \mathrm{Supp}(a)$, então $e \in \mathrm{Supp}(x^{-1}a) \cap \mathrm{Supp}(ax^{-1})$.*

Demonstração. Seja $a = \sum_{h \in G} a_h h$. Segue que $ga = \sum_{h \in G} a_h gh$, de onde $\mathrm{Supp}(ga) = \{gh \in G \mid a_h \neq 0\} = g\{h \in G \mid a_h \neq 0\} = g(\mathrm{Supp}(a))$. Analogamente vê-se que $\mathrm{Supp}(ag) = (\mathrm{Supp}(a))g$. Além disso, se $x \in \mathrm{Supp}(a)$, do que provamos acima, $\mathrm{Supp}(x^{-1}a) = x^{-1}(\mathrm{Supp}(a))$ e $\mathrm{Supp}(ax^{-1}) = (\mathrm{Supp}(a))x^{-1}$. Por isso, $e = x^{-1}x = xx^{-1} \in \mathrm{Supp}(x^{-1}a) \cap \mathrm{Supp}(ax^{-1})$. □

Um caso particularmente interessante de anel de grupo é obtido quando $R = F$ é um corpo.

Proposição 2.12. *Sejam $H \leq G$ e $a \in FH$. Então a é invertível em FH se, e somente se, a é invertível em FG. Ademais, a é divisor de zero à esquerda (à direita) de FH se, e somente se, é um divisor de zero à esquerda (à direita) de FG.*

Demonstração. Consultar PASSMAN (2011), página 7, Lema 1.4. □

Um dos interesses em anéis de grupo é a relação entre os ideais do anel de grupo FG e os subgrupos normais de G. Notemos, inicialmente, que G age por conjugação sobre FG. Para cada $x \in G$, consideremos a aplicação $\alpha_x : FG \to FG$ definida por

$$\alpha_x(a) = a^x = x^{-1}ax.$$

Então, para

$$a = \sum_{g \in G} a_g g \text{ e } b = \sum_{h \in G} b_h h$$

temos

$$(a+b)^x = x^{-1}(a+b)x = \sum_{g \in G}(a_g + b_g)x^{-1}gx = \sum_{g \in G} a_g x^{-1}gx + \sum_{g \in G} b_g x^{-1}gx = a^x + b^x$$

e

$$(ab)^x = x^{-1}abx = \sum_{g,h \in G} a_g b_h x^{-1}gxx^{-1}hx = \left(\sum_{g \in G} a_g x^{-1}gx\right)\left(\sum_{h \in G} b_h x^{-1}hx\right) = a^x b^x.$$

Além disso,

$$(a^x)^y = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy) = a^{xy}.$$

Portanto, lembrando que S_{FG} denota o grupo das simetrias de FG, $\rho\colon G \to S_{FG}$ dada por $\rho(x) = \alpha^x$ (onde α^x é um automorfismo com inversa $\alpha^{x^{-1}} = xax^{-1}$) é um homomorfismo e, portanto, determina uma ação de grupos de G sobre FG.
Dado um subconjunto S de FG, dizemos que S é G-invariante se $\alpha^x(S) = S^x = S$ para qualquer $x \in G$. Em particular, temos que o seguinte resultado é válido.

Proposição 2.13. *Nas notações acima descritas, se H é um subgrupo normal de G, então FH é G-invariante, e, se I é um ideal de FG, então I é também G-invariante.*

Demonstração. Decorre diretamente das definição de α^x, para $x \in G$, da normalidade de H em G e do fato de I ser ideal de FG. □

Relembre que se FG é uma álgebra de grupo e L é um ideal de FG, denotamos por $L \cdot FG$ as somas finitas de produtos de elementos de L por elementos de FG.

Lema 2.14. *Seja $H \lhd G$. Então:*

(*i*) *Se L é um ideal G-invariante de FH, então $L \cdot FG = FG \cdot L$ é um ideal de FH.*

(*ii*) *Se I é um ideal de FG, então $(I \cap FH) \cdot FG \subseteq I$ e $I \cap FH$ é um ideal G-invariante de FH.*

Demonstração. Consultar PASSMAN (2011), página 8, Lema 1.5. □

Um dos resultados mais conhecidos em Teoria de Representações é o

Teorema 2.15. ***(Teorema de Maschke, 1898)*** *Sejam F um corpo e G um grupo finito. Então FG é completamente redutível se, e somente se,* $\mathrm{char}(F) \nmid |G|$.

Demonstração. Consultar MILIES and SEHGAL (2002), página 142. □

Uma versão mais geral deste resultado é o

Teorema 2.16. ***(Connell, 1963)*** *Sejam G um grupo qualquer e R um anel associativo com identidade. Então RG é completamente redutível se, e somente se, são satisfeitas:*

(i) *R é completamente redutível.*

(ii) *G é finito.*

(iii) *$|G|$ é invertível em R.*

Demonstração. Consultar MILIES and SEHGAL (2002),pagina 140. □

Uma tradução do Teorema de Wedderburn-Artin neste contexto nos dará muita informação sobre a estrutura da álgebra de grupo.

Teorema 2.17. *Seja G um grupo finito e F um corpo tal que* $\mathrm{char}(F) \nmid |G|$. *Então:*

(i) *FG é uma soma direta de um número finito de ideais (bilaterais) $\{B_i\}_{1\leq i\leq r}$, que são as componentes simples de FG. Cada B_i é um anel simples.*

(ii) *Qualquer ideal bilateral de FG é uma soma direta dos membros da família $\{B_i\}_{1\leq i\leq r}$.*

(iii) *Cada componente simples B_i é isomorfa a um anel de matrizes da forma $M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia isomorfa de F em seu centro, e o isomorfismo*

$$FG \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i)$$

é um isomorfismo de F-álgebras.

(iv) *Em cada anel de matriz $M_{n_i}(D_i)$, o conjunto*

$$I_i = \left\{ \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ & & \cdots & \\ x_{n_i} & 0 & \cdots & 0 \end{pmatrix} : x_1, x_2, \ldots, x_{n_i} \in D_i \right\} \cong D_i^{n_i}$$

é um ideal minimal à esquerda.

Demonstração. Consultar MILIES and SEHGAL (2002), página 142. □

A decomposição de RG como soma direta de componentes simples corresponde a um conjunto de elementos $\{e_1, \ldots, e_s\}$ tais que $A_i = RGe_i$ para $1 \leq i \leq s$ e

(i) $e_i \neq 0$ é um idempotente central, $1 \leq i \leq s$.

(ii) Se $i \neq j$ então $e_i e_j = 0$.

(iii) $1 = e_1 + \cdots + e_s$.

(*iv*) e_i não pode ser escrito como $e_i = e_i^{'} + e_i^{''}$, onde $e_i^{'}$, $e_i^{''}$ são idempotentes centrais tais que $e_i^{'}, e_i^{''} \neq 0$ e $e_i^{'}e_i^{''} = 0$, $1 \leq i \leq s$.

Os elementos $e_1, \ldots, e_s$ recebem o nome de *idempotentes centrais primitivos.*

Assim como pode ser visto em PASSMAN (2011), há uma forma natural de obter idempotentes centrais em uma álgebra de grupo FG.

Proposição 2.18. *Dados um corpo F e um subgrupo H de um grupo G tal que* $\mathrm{char}(F) \nmid |H|$. *Então o elemento*

$$\hat{h} = \frac{1}{|H|} \sum_{h \in H} h$$

é um idempotente em FG. Ademais, H é normal se, e somente se, $\hat{h}$ é central.

Demonstração. Note que $\hat{h}$ é idempotente, ou seja, denotando $\hat{H} = \sum_{h \in H} h$, temos

$$\hat{h}\hat{h} = \frac{1}{|H|^2} \left(\sum_{h \in H} h \right) \hat{H} = \frac{1}{|H|^2} \left(\sum_{h \in H} h\hat{H} \right) = \frac{1}{|H|^2} \left(\sum_{h \in H} \hat{H} \right) = \frac{1}{|H|^2} |H| \hat{H} = \hat{h}.$$

Para as implicações restantes, ver MILIES and SEHGAL (2002), página 139, Lema 3.4.3. □

2.3 Códigos

Nesta seção são definidas as noções básicas sobre códigos e recordaremos algumas de suas propriedades. Os resultados sobre códigos, códigos lineares e códigos cíclicos abaixo citados estão em HEFEZ and VILLELA (2008). Ao final da seção será então introduzida a noção de código de grupo.

Definição 2.19. *Seja A um conjunto finito, denominado alfabeto. Um código de comprimento n sobre A é um subconjunto do produto cartesiano A^n.*

Os elementos de A^n são chamados de *vetores*, e para um código dado C, chamamos de *palavras* os seus elementos. O número $k = \log_q m$, onde $q = |A|$ e $m = |C|$, é dito a *dimensão combinatória* de C. Nestas condições dizemos que C é um (n, m)-código, ou um (n, k)-código. Se $q = |A|$, um código sobre A se diz um código q-ário (se $q = 2, 3, 4$, binário, terciário e quaternário, respectivamente). Denotamos palavras de C por $a = (a_1, \ldots, a_n)$ e a_i, para $i = 1, \ldots, n$, recebe o nome de *entrada de a na i-ésima posição.*

Definição 2.20. *Dados dois elementos $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$ de A^n, a distância de Hamming entre a e b é definida como*

$$d(a, b) = |\{i \mid 1 \leq i \leq n,\ a_i \neq b_i\}|.$$

O valor

$$d = \min\{d(a,b) \mid a, b \in C, a \neq b\}$$

é dito a *distância mínima* de C. Se C é um (n,m)-código cuja distância mínima é d, denotamos C como sendo um (n,m,d)-código. Os números n, m (ou k) e d, que fazem referência ao comprimento do código, ao seu número de palavras (ou sua dimensão combinatória) e a sua distância mínima, respectivamente, se chamam *parâmetros fundamentais* do código C.

Definição 2.21. *Seja $A_q(n,d)$ o número máximo de palavras que um código de comprimento n e distância mínima d sobre um alfabeto de q elementos (é habitual omitir-se o subíndice e escrever apenas $A(n,d)$ quando $q = 2$). Um $(n, A_q(n,d), d)$-código se diz ótimo.*

Obtiveram-se diversas cotas superiores para o valor de $A_q(n,d)$: Hamming, Gilbert, Plotkin, Varshamov, entre outras. Vamos destacar a *Cota de Singleton*. Sejam n, q, d tais que $d \leq n$. Então

$$A_q(n,d) \leq q^{n-d+1}.$$

Definição 2.22. *Diz-se que um (n,m,d)-código sobre um alfabeto A de cardinal q é um MDS-código se $m = q^{n-d+1}$.*

Ou seja, o número de palavras de um código qualquer de comprimento n e distância mínima d sobre um alfabeto com q elementos é menor ou igual ao número de palavras de um código MDS com os mesmos parâmetros.

2.3.1 Códigos lineares

Atualmente os códigos mais utilizados são os códigos com uma estrutura algébrica de espaço vetorial: os chamados códigos lineares.
A partir de agora, salvo menção do contrário, denotaremos por F um corpo com q elementos, onde q é uma potência de um primo p.

Definição 2.23. *Um código linear de comprimento n sobre um corpo finito F é um subespaço vetorial de F^n.*

Todo código linear C é por definição um subespaço vetorial de dimensão finita. Seja k a dimensão do código C e seja $\{v_1, \ldots, v_k\}$ uma base de C, portanto, todo elemento de C se escreve de modo único na forma

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k,$$

onde os λ_i, $i = 1,...,k$, são elementos de F. Segue daí que

$$m = |C| = q^k,$$

e, consequentemente,

$$\dim_F C = k = \log_q q^k = \log_q m.$$

Assim, a dimensão de C como F-espaço vetorial coincide com a dimensão combinatória. Um código linear de comprimento n sobre um corpo finito F, com dimensão k e distância mínima d, se diz um $[n, k, d]$-código (linear).

Nos códigos lineares se pode caracterizar a distância mínima utilizando a noção de peso de Hamming (o que é bem mais vantajoso do ponto de vista computacional).

Definição 2.24. *Dado $a \in F^n$, define-se o peso de Hamming de a como sendo o inteiro*

$$\omega(a) = |\{1 \leq i \leq n \mid a_i \neq 0\}|.$$

Em outras palavras, temos que

$$\omega(a) = d(a, 0),$$

sendo $0 = (0, \ldots, 0)$. É fácil ver que ω assim definida é uma norma em F^n e que a distância de Hamming d é a distância associada a esta norma. De modo análogo à distância mínima de um código, podemos definir seu *peso mínimo* como

$$\omega(C) = \min\{\omega(c) \mid c \in C\}.$$

Proposição 2.25. *Seja $C \subset F^n$ um código linear com distância mínima d. Temos que*

1. *Para quaisquer $x, y \in F^n$, $d(x, y) = \omega(x - y)$.*
2. *$d = \omega(C)$.*

Demonstração. O item 1. é consequência direta das definições de distância e peso de Hamming. O item 2. decorre de que, para todo par de elementos x, y em C com $x \neq y$, tem-se $z = x - y \in C \setminus \{0\}$ e $d(x, y) = \omega(z)$.

□

Definição 2.26. *Sejam $C \subset F^n$ um código linear e $\beta = \{v_1, \ldots, v_k\}$ uma base ordenada de C. Considere a matriz G, cujas linhas são os vetores $v_i = (v_{i1}, \ldots, v_{in})$, $i = 1, \ldots, k$, isto é,*

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

A matriz G é chamada de matriz geradora de C associada à base β.

Sejam a, b vetores de F^n. Denotamos por $a \cdot b$ o produto interno usual, representado por

$$a \cdot b = \sum_{i=1}^{n} a_i b_i.$$

Dado um código linear $C \subset F^n$, define-se

$$C^{\perp} = \{v \in F^n \mid v \cdot u = 0, \ \forall \ u \in C\},$$

que é dito o *código dual* de C. Note que em particular, $C^{\perp}$ é um código linear. Seja H a matriz geradora de $C^{\perp}$. É imediato ver que H é a matriz definida a seguir.

Definição 2.27. *Diremos que uma matriz H é uma matriz de controle do código C se, dado um vetor arbitrário $a \in F^n$ se verifica que $a \in C$ se, e somente se, $Ha^t = 0$, onde $0 = (0, \cdots, 0)$.*

A seguinte proposição pode ser provada de maneira direta a partir da definição e das propriedades fundamentais de códigos lineares.

Proposição 2.28. *A distância mínima d de um código linear C é igual ao número de colunas linearmente dependentes de sua matriz de controle H.*

2.3.2 Códigos cíclicos

Os códigos cíclicos são muito utilizados nas aplicações, por formarem uma classe de códigos lineares que possui bons algoritmos de codificação e de decodificação. No que se segue, representaremos as coordenadas de um vetor em F^n por $(x_0, \ldots, x_{n-1})$.

Definição 2.29. *Um código linear $C \subset F^n$ será chamado de código cíclico se, para todo $c = (c_0, \ldots, c_{n-1})$ pertencente a C, o vetor $(c_{n-1}, c_0, \ldots, c_{n-2})$ também pertence a C. Em palavras, um tal código linear é cíclico se dado um qualquer de seus elementos, todas as permutações cíclicas deste também estão no código.*

Consideremos o anel de polinômios $F[x]$ módulo $x^n - 1$, isto é,

$$R_n = F[x]/\langle x^n - 1 \rangle.$$

Sabe-se que R_n é um F-espaço vetorial e que seus elementos são classes de polinômios, as quais são representadas por polinômios de grau menor que n. Assim, a aplicação $\phi : F^n \to R_n$ dada por

$$\phi(c_0, \cdots, c_{n-1}) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

é um isomorfismo de F-espaços vetoriais.

Temos então que todo código linear $C \subset F^n$ pode ser levado para R_n mediante o isomorfismo ϕ. A vantagem de R_n é que este, além de ser um F-espaço vetorial, possui também uma estrutura de anel. Veremos nos resultados seguintes as vantagens de trabalharmos com a identificação $\phi(C)$.

Teorema 2.30. *O código $C \subset F^n$ é cíclico se, e somente se, $\phi(C) \subset R_n$ é um ideal.*

Demonstração. Assuma que C é um código cíclico. Como C é um subespaço vetorial, em particular $(C, +)$ é um grupo abeliano. O mesmo vale para $\phi(C)$, devido ao isomorfismo. Portanto, para mostrarmos que $\phi(C)$ é um ideal de R_n, basta mostrarmos que dado $a(x)$ em R_n, vale $a(x)\phi(C) \subset \phi(C)$. De fato, se $c(x) \in \phi(C)$ então $x^i c(x) \in \phi(C)$, para $i = 0, \ldots, n-1$, uma vez que C é cíclico. Deste modo, dado $a(x) = \sum_{i=0}^{n-1} \alpha_i x^i \in R_n$ e $c(x) \in \phi(C)$, temos

$$a(x)c(x) = \sum_{i=0}^{n-1} \alpha_i (x^i c(x)).$$

Assim, como $\phi(C)$ é fechado para a multiplicação por elementos de F e para a soma, segue que $a(x)c(x) \in \phi(C)$.

Reciprocamente, se $\phi(C)$ é um ideal, então C é um espaço vetorial (via o isomorfismo) e além disso, $x^i c(x) \in \phi(C)$, para qualquer $c(x) \in \phi(C)$, para $i = 0, \ldots, n-1$, de onde decorre que C é um código cíclico. □

Tendo em vista o isomorfismo explicitado anteriormente, no enunciado dos próximos resultados, trataremos C como $\phi(C)$ sempre que for conveniente.

Teorema 2.31. *Se C é um código cíclico e $g(x)$ é o polinômio mônico de menor grau em C, então $C = \langle g(x) \rangle$ e $g(x)$ é único.*

Demonstração. Seja $a(x) \in C$. Então, em $F[x]$, pelo Algoritmo da Divisão, temos $a(x) = b(x)g(x) + r(x)$, onde $r(x) = 0$ ou $\deg(r(x)) < \deg(g(x))$. Mas, $r(x) = a(x) - b(x)g(x) \in C$, já que C é ideal. Logo, pela minimalidade do grau de $g(x)$, segue que $r(x) = 0$ e $a(x) = b(x)g(x)$. Suponha que $g(x)$ e $h(x)$ são polinômios mônicos de mesmo grau minimal em C. Então, $g(x) - h(x) \in C$ e tem grau menor que o grau de $g(x)$, de onde $g(x) = h(x)$. □

O polinômio $g(x)$ descrito no teorema acima é chamado de *polinômio gerador* de C. Se $g(x) = g_0 + g_1 x + \cdots + g_{r-1}x^{r-1} + g_r x^r$ é o polinômio gerador de um código C, então

$$\begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{r-1} & 1 & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_{r-1} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & & & \\ 0 & \cdots & 0 & g_0 & \cdots & & \cdots & \cdots & g_{r-1} & 1 \end{pmatrix}$$

é uma matriz geradora de C. Mostra-se ainda mais, que todo divisor de $x^n - 1$ é um gerador de algum código cíclico. De fato, temos o próximo resultado.

Teorema 2.32. *O polinômio gerador de um código cíclico $C \subset F^n$ divide $x^n - 1$ e, além disso, qualquer divisor de $x^n - 1$ é um polinômio gerador de algum código cíclico.*

Demonstração. Seja $g(x)$ o polinômio gerador de C. Pelo Algoritmo da Divisão em $F[x]$, temos $x^n - 1 = a(x)g(x) + r(x)$, onde $r(x) = 0$ ou $\deg(r(x)) < \deg(g(x))$. Assim, $r(x) \in C$ e pela minimalidade do grau do polinômio gerador, $r(x) = 0$.

Suponha agora que $g(x)$ divide $x^n - 1$. Considere o ideal gerado por $g(x)$ módulo $x^n - 1$, ou seja, todos os múltiplos de $g(x)$ módulo $x^n - 1$. Suponha que existe neste ideal um polinômio $b(x)$ com grau menor que o grau de $g(x)$. Então, em $F[x]$, temos

$$b(x) = a(x)g(x) + (x^n - 1)d(x),$$

para determinados polinômios $a(x)$, $d(x)$. Como $g(x)$ divide $x^n - 1$, segue que $g(x)$ divide $b(x)$, o que é impossível, já que $b(x)$ possui grau menor. Ou seja, este ideal é gerado por $g(x)$. □

2.3.3 Códigos de grupo

A noção de código de grupo surge como a generalização do fato de que todo código cíclico de comprimento n sobre um corpo F poder identificar-se com um ideal do anel de grupo FC_n, onde C_n é o grupo cíclico de ordem n.

Denotaremos por $E = \{e_1, \ldots, e_n\}$ a base canônica de F^n.

Definição 2.33. *Sejam G um grupo de ordem n e $C \subset F^n$ um código linear. Dizemos que C é um G-código (à esquerda, à direita) se existir uma bijeção $\phi : E \to G$ tal que sua extensão por linearidade a um isomorfismo de F-espaços vetoriais, $\phi : F^n \to FG$, cumpre que $\phi(C)$ é um ideal bilateral (à esquerda, à direita) de FG.*

Dizemos que um código linear é um código de grupo (à esquerda, à direita) se for um G-código (à esquerda, à direita) para algum grupo finito G.

Proposição 2.34. *Se $C \subset F^n$ é um G-código à esquerda para um certo grupo finito G, então C também é um G-código à direita.*

Demonstração. Se $C \subset F^n$ é um G-código à esquerda para um certo grupo finito G, então existe um bijeção $\phi : E \to G$ tal que sua extensão por linearidade a um isomorfismo de F-espaços vetoriais é tal que que $\phi(C)$ é um ideal à esquerda de FG. Tomamos o isomorfismo de grupos $\rho : G \to G$ dado por $\rho(g) = g^{-1}$. Então, afirmamos que $\rho \circ \phi : E \to G$ é uma bijeção tal que sua extensão por linearidade cumpre que $\rho \circ \phi(C)$ é um ideal à direita de FG, de onde decorre que C é um G-código à direita. De fato, dados $a = \sum a_g g \in FG$ e

$b = \sum b_h h \in \phi(C)$, representemos por $b' = \sum b_{h^{-1}} h^{-1} = \rho(b)$ e $a' = \sum a_{g^{-1}} g^{-1} = \rho(a)$. Assim,

$$b'a = \rho(a'b) \in \rho \circ \phi(C),$$

pois $a'b \in \phi(C)$, uma vez que este é ideal à esquerda. □

Observação: Note que este fato, no entanto, não implica que todo código de grupo à esquerda ou à direita seja um código de grupo.

Existe uma ação natural do grupo simétrico S_n sobre F^n, definida por

$$\sigma(a_1, a_2, \ldots, a_n) = (a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)}),$$

para cada $(a_1, a_2, \ldots, a_n) \in F^n$.

Definição 2.35. *Dois códigos $C_1, C_2 \subset F^n$ se dizem equivalentes por permutação se existir $\sigma \in S_n$ tal que $C_2 = \sigma(C_1)$.*

Segue da definição acima que, dado um grupo G de ordem n e uma bijeção $\phi : E \to G$, os G-códigos (à esquerda, à direita) sobre F são os códigos lineares contidos em F^n que são equivalentes por permutação a algum código $\phi^{-1}(I)$, onde I é um ideal bilateral (à esquerda, à direita) de FG e ϕ denota também a extensão por linearidade a $F^n \to FG$.

Definição 2.36. *O grupo de automorfismos de permutação de um código C é definido por*

$$\mathrm{PAut}(C) = \{\sigma \in S_n \mid \sigma(C) = C\}.$$

O próximo resultado, cuja prova pode ser vista na tese de doutorado de J. J. Bernal, mostra que um código linear e seu código dual gozam da mesma estrutura de código de grupo.

Proposição 2.37. *Seja G um grupo de ordem n. Então $C \subset F^n$ é G-código (à esquerda, à direita) se, e somente se, $C^\perp$ é G-código (à esquerda, à direita).*

Definição 2.38. *Um código de grupo é dito um código abeliano se é um A-código para um grupo abeliano A.*

Observação. Mostra-se sem muito esforço que um A-código à esquerda (à direita) é na verdade um A-código, quando A é um grupo abeliano.

3 CÓDIGOS DE GRUPO SOBRE GRUPOS NÃO ABELIANOS

Neste capítulo aparecem os resultados principais do trabalho. Salientamos que para representar a ordem de um grupo G, escrevemos $|G|$.

O seguinte resultado é amplamente conhecido e terá sua demonstração omitida em vista disso.

Lema 3.1. *Sejam A, B subgrupos de um grupo G. Então vale a seguinte igualdade*

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

A definição a seguir é muito importante, pois define uma propriedade que será objeto central em vários dos resultados que seguem.

Definição 3.2. *Dizemos que um grupo G admite (possui) uma decomposição abeliana se existirem subgrupos abelianos A, B de G, tais que $G = AB$.*

Lema 3.3. *Suponha que um grupo G possua dois subgrupos abelianos A e B tais que $|G| = |A||B|$ e $|A|$, $|B|$ são primos entre si. Então G possui decomposição abeliana.*

Demonstração. Claramente AB é um subconjunto de G. Além disso, $A \cap B$ é um subgrupo de A e de B, de onde pelo Teorema de Lagrange, $|A \cap B| \mid |A|$ e $|A \cap B| \mid |B|$. em vista de que $|A|$ e $|B|$ são primos entre si, tem-se que $|A \cap B| = 1$. Finalmente, aplicando o lema anterior, temos que

$$|AB| = \frac{|A||B|}{|A \cap B|} = |A||B| = |G|,$$

de onde $G = AB$. □

Lema 3.4. *Suponha que G possua um subgrupo abeliano N tal que G/N é um grupo cíclico. Então G admite decomposição abeliana.*

Demonstração. Se $N = G$, então $G = \{e\}G$. Suponhamos então o contrário. Como G/N é cíclico, existe $a \in G \setminus N$ tal que $G/N = \langle aN \rangle$. Dado $g \in G$, temos que

$$gN = a^n N \Rightarrow g = a^n h,$$

onde $h \in N$ e $a^n \in \langle a \rangle$. Isto mostra que $G = \langle a \rangle N$. Como $\langle a \rangle$ é subgrupo abeliano de G, já que é cíclico, tem-se que esta é uma decomposição abeliana de G. □

Definição 3.5. *Dizemos que um subgrupo H de S_n é regular se $|H| = n$ e $\sigma(j) \neq j$, para qualquer $\sigma \in H \setminus \{e\}$ e para qualquer $j \in \mathbb{N}_n = \{1, 2, \ldots, n\}$.*

Definição 3.6. *Dizemos que um subgrupo H de S_n é transitivo se para quaisquer $i, j \in \mathbb{N}_n$, com $i \neq j$, existe $\sigma \in H$ tal que $\sigma(i) = j$.*

Observação. Sabe-se que um subgrupo de S_n é regular se, e somente se, tem ordem n e é transitivo.

Lema 3.7. *Sejam H um subgrupo regular de S_n e $i_0 \in \mathbb{N}_n$ um elemento fixado. Seja $\psi : H \to \mathbb{N}_n$ a bijeção dada por $\psi(h) = h(i_0)$. Então, existe um anti-isomorfismo $\sigma : H \to C_{S_n}(H)$, levando h em σ_h e dado por*

$$\sigma(h) = \sigma_h(i) = \psi^{-1}(i)(h(i_0)) \ (i \in \mathbb{N}_n).$$

Além disso, $\sigma_h = h$ para todo $h \in Z(H)$ e portanto $Z(H) = Z(C_{S_n}(H))$.

Demonstração. Verifiquemos inicialmente que ψ é uma bijeção. Para isto, já que ψ é, em particular, uma função entre conjuntos finitos de mesma cardinalidade, é suficiente provar que ψ é injetiva. Sejam g e h elementos arbitrários de H. Se $\psi(h) = \psi(g)$, então $h(i_0) = g(i_0)$, o que implica $g^{-1}h(i_0) = i_0$. Sendo H regular, tem-se $g^{-1}h = 1$, o que implica $h = g$.

As seguintes igualdades são de verificação imediata e irão aparecer várias vezes no decorrer da demonstração:

$$\psi^{-1}(i)(i_0) = i, \ \forall \ i \in \mathbb{N}_n \tag{1}$$

$$\psi^{-1}(h(i_0)) = h, \ \forall \ h \in H. \tag{2}$$

Provemos que σ leva H em $C_{S_n}(H)$. De fato, dados $h, k \in H$, tendo em vista a definição de σ_h, temos

$$\sigma_h k(i) \overset{(1)}{=} \sigma_h(k(\psi^{-1}(i)(i_0)) = \psi^{-1}([k\psi^{-1}(i)](i_0))(h(i_0)) \overset{(2)}{=} [k\psi^{-1}(i)](h(i_0)) = k\sigma_h(i).$$

Vejamos que σ é um antihomomorfismo. Nas igualdades que seguem, escreveremos $*$ para indicar que determinada igualdade é justificada pela definição de σ e $**$ para indicar se justifica a partir da igualdade $\psi^{-1}(i)h = \psi^{-1}(\psi^{-1}(i)h(i_0))$, já que $\psi(\psi^{-1}(i)h) = \psi^{-1}(i)h(i_0)$ e ψ é bijeção. Se $h, k \in H$ e $i \in \mathbb{N}_n$, então

$$\begin{aligned} \sigma_{hk}(i) &\overset{*}{=} \psi^{-1}(i)hk(i_0) = (\psi^{-1}(i)h)k(i_0) \overset{**}{=} \psi^{-1}(\psi^{-1}(i)h(i_0))k(i_0) \\ &\overset{*}{=} \sigma_k(\psi^{-1}(i)h(i_0)) \overset{*}{=} \sigma_k(\sigma_h(i)) = \sigma_k\sigma_h(i). \end{aligned}$$

Provemos agora que σ é injetivo. Com efeito, se $\sigma(h) = \sigma_h = 1$, então $\sigma_h(i) = \psi^{-1}(i)(h(i_0)) =$

$(\psi^{-1}(i)h)(i_0) = i \overset{(1)}{=} \psi^{-1}(i)(i_0)$, para todo $i \in \mathbb{N}_n$. Assim, $\psi^{-1}(i) = \psi^{-1}h$, o que implica $h = e$. Finalmente mostremos que σ é sobrejetiva, ou seja, que $\sigma(H) = C_{S_n}(H)$. Dado $x \in C_{S_n}(H) = C$, seja $h = \psi^{-1}(x(i_0)) \in H$. Temos

$$h(i_0) = \psi(h) = x(i_0) \overset{(1)}{=} x((\psi^{-1}(i))^{-1}(i)) \overset{x\in C}{=} (\psi^{-1})^{-1}x(i),\ \forall\, i \in \mathbb{N}_n.$$

Assim, $x(i) = \psi^{-1}(i)(h(i_0)) = \sigma(h)$. Além disso, isto mostra que se $x \in Z(H) = H \cap C_{S_n}(H)$, então $h = x = \sigma_h$. Portanto, como $Z(H) \subset C_{S_n}(H)$, podemos concluir que $Z(C_{S_n}(H)) \subseteq Z(Z(H)) = Z(H)$. A outra inclusão é óbvia a partir das definições de cada um dos conjuntos envolvidos. Portanto, $Z(H) = Z(C_{S_n}(H))$. □

Antes de provarmos o próximo resultado façamos inicialmente considerações gerais, que serão usadas logo mais de modo mais contextualizado com as hipóteses deste. Sejam $E = \{e_1, \ldots, e_n\}$ a base canônica de F^n e $\phi : E \to G$ uma bijeção. Relembremos que também usaremos ϕ para nos referir a extensão por linearidade ao isomorfismo de F-álgebras $\phi : F^n \to FG$. Definimos $f = f_\phi : G \to S_n$ tal que, para $g \in G$, $f(g)$ satisfaz

$$e_{f(g)(i)} = \phi^{-1}(g\phi(e_i)),\ \forall\, i \in \mathbb{N}_n. \tag{3}$$

Notemos que f é um homomorfismo de grupos. De fato, dados $g, h \in G$, pela definição de f e por ϕ ser bijeção, valem as seguintes igualdades

$$\begin{aligned} e_{f(g)f(h)(i)} &= e_{f(g)(f(h)(i))} = \phi^{-1}(g\phi(e_{f(h)(i)})) = \phi^{-1}(g\phi(\phi^{-1}(h\phi(e_i)))) \\ &= \phi^{-1}(gh\phi(e_i)) = e_{f(gh)(i)},\ \forall\, i \in \mathbb{N}_n, \end{aligned}$$

de onde $f(g)f(h) = f(gh)$. Note também que f é injetivo, pois para qualquer $i \in \mathbb{N}_n$,

$$f(g)(i) = i \Leftrightarrow e_i = \phi^{-1}(g\phi(e_i)) \Leftrightarrow \phi(e_i) = g\phi(e_i) \Leftrightarrow g = e.$$

Além disso, isto mostra que $f(G) = H$ é um subgrupo regular de S_n.

Se fixarmos $e_{i_0} = \phi^{-1}(e)$, então, aplicando o lema anterior, temos um anti-isomorfismo $\sigma : H \to C_{S_n}(H)$, dado por $\sigma_h(i) = \psi^{-1}(i)h(i_0)$, $i \in \mathbb{N}_n$, onde $\psi : H \to \mathbb{N}_n$ é a bijeção definida por $\psi(h) = h(i_0)$. De posse destes fatos, para cada $i \in \mathbb{N}_n$, temos

$$e_i \overset{(1)}{=} e_{\psi^{-1}(i)(i_0)} = e_{f(f^{-1}(\psi^{-1}(i)))(i_0)} = \phi^{-1}(f^{-1}(\psi^{-1}(i))\phi(e_{i_0})) \overset{\phi(e_{i_0})=e}{=} \phi^{-1}f^{-1}\psi^{-1}(i).$$

De modo geral, temos

$$e_i = \phi^{-1}f^{-1}\psi^{-1}(i),\ \forall\, i \in \mathbb{N}_n. \tag{4}$$

Além desta última igualdade, usaremos também a igualdade (1) que apareceu no lema anterior e inclusive foi usada acima para obter (4). De posse disto, do fato de que f :

$G \to H$ é um isomorfismo (em particular f^{-1} é homomorfismo), escrevendo $*$ para indicar que determinada igualdade é justificada pela definição de σ e $**$ para indicar se esta se justifica a partir da igualdade $\psi^{-1}(i)h = \psi^{-1}(\psi^{-1}(i)h(i_0))$, como feito na demonstração do Lema anterior, para todo $h \in H$, obtém-se

$$\begin{aligned}\sigma_h(e_i) &= e_{\sigma_h(i)} \overset{*}{=} e_{(\psi^{-1}(i)h)(i_0)} \overset{(4)}{=} \phi^{-1}f^{-1}\psi^{-1}((\psi^{-1}(i)h)(i_0)) \overset{**}{=} \phi^{-1}f^{-1}(\psi^{-1}(i)h) \\ &= \phi^{-1}(f^{-1}(\psi^{-1}(i))f^{-1}(h)) \overset{(4)}{=} \phi^{-1}(\phi(e_i)f^{-1}(h)).\end{aligned}$$

Deste modo, dado $x = \sum_{i=1}^{n} a_i e_i \in F^n$, tem-se

$$\begin{aligned}\sigma_h(x) &= \sigma_h(\sum_{i=1}^{n} a_i e_i) = \sum_{i=1}^{n} a_i \sigma_h(e_i) = \sum_{i=1}^{n} a_i \phi^{-1}(\phi(e_i)f^{-1}(h)) \\ &= \phi^{-1}(\sum_{i=1}^{n} a_i \phi(e_i)f^{-1}(h)) = \phi^{-1}(\phi(x)f^{-1}(h)).\end{aligned}$$

Nestas últimas igualdades usamos a igualdade $\sigma_h(e_i) = \phi^{-1}(\phi(e_i)f^{-1}(h))$ e o fato de ϕ ser isomorfismo de F-álgebras.

Teorema 3.8. *Seja $C \subset F^n$ um código linear e G um grupo de ordem n.*

(1) C é um G-código à esquerda se, e somente se, G é isomorfo a um subgrupo transitivo de S_n contido em $\mathrm{PAut}(C)$.

(2) C é um G-código se, e somente se, G é isomorfo a um subgrupo transitivo H de S_n tal que $H \cup C_{S_n}(H) \subseteq \mathrm{PAut}(C)$.

Demonstração. Assuma que C seja um G-código à esquerda e considere $\phi : E \to G$ a bijeção tal que $\phi(C)$ é um ideal à esquerda de FG. Seja $f = f_\phi$ como anteriormente. Assim, $H = f(G)$ é um subgrupo transitivo de S_n. Ademais, pela definição de f, como $h = f(f^{-1}(h))$ e ϕ é isomorfismo de F-álgebras, se $h \in H$ e $x = \sum a_i e_i$, então

$$h(x) = \sum a_i e_{h(i)} = \sum a_i \phi^{-1}(f^{-1}(h)\phi(e_i)) = \phi^{-1}(f^{-1}(h)\phi(x)).$$

Por isso, de posse do fato de que $g\phi(C) = \phi(C)$, para qualquer $g \in G$ (a inclusão $g\phi(C) \subset \phi(C)$ decorre de $\phi(C)$ ser ideal. Para provar que $\phi(C) \subset g\phi(C)$, basta ver que se $c \in \phi(C)$, então, em FG, podemos escrever $c = g(g^{-1}c)$. Como $g^{-1}c \in \phi(C)$, segue que $c \in g\phi(C)$) decorre que

$$h(C) = \phi^{-1}(f^{-1}(h)\phi(C) = \phi^{-1}(\phi(C)) = C,$$

isto é, $H \subseteq \mathrm{PAut}(C)$. Se, além disso, $\phi(C)$ for um ideal bilateral de FG e $x \in C_{S_n}(H)$, então pelo lema anterior, existe $h \in H$ tal que $\sigma_h = x$. Então, levando em conta a igualdade $\phi(C) = \phi(C)g$, $\forall g \in G$, uma vez que $\phi(C)$ é, em particular, ideal à direita,

temos

$$x(C) = \sigma_h(C) = \phi^{-1}(\phi(C)f^{-1}(h)) = \phi^{-1}(\phi(C)) = C.$$

Reciprocamente, assuma agora que G é isomorfo a um subgrupo transitivo (neste caso regular) H de S_n contido em $\mathrm{PAut}(C)$. Podemos supor, sem perda de generalidade, que $G = H$. Seja $\phi : E \to G$ a bijeção dada por $\phi(e_i) = g$, tal que $g(1) = i$, ou seja, $\phi^{-1}(g) = e_{g(1)}$. Para quaisquer $g, hinG$, temos

$$h\phi(e_{g(1)}) = hg = \phi(e_{(hg)(1)}) = \phi(h(e_{g(1)})).$$

Por isso, uma vez que G é transitivo, para qualquer $i \in \mathbb{N}_n$, vale

$$h\phi(e_i) = \phi(h(e_i)).$$

Assim, usando a linearidade de ϕ, temos

$$h\phi(C) = \phi(h(C)) = \phi(C),$$

pois $h \in G \subset \mathrm{PAut}(C)$. Como por hipótese C é um código linear, segue que, para mostrarmos que $\phi(C)$ é ideal à esquerda, basta mostrar que dado $a = \sum a_i x_i \in FG$, onde $x_i = \phi(e_i)$, vale $a\phi(C) = \phi(C)$. Ora, vimos logo acima que $h\phi(C) = \phi(C)$, $\forall h \in G$, daí

$$a\phi(C) = \sum_{i=1}^{n} a_i x_i \phi(C) = \sum_{i=1}^{n} a_i \phi(C) = \phi(C),$$

já que ϕ é isomorfismo linear de F-álgebras. Logo, $\phi(C)$ é um ideal à esquerda de FG. Assuma, adicionalmente, que $C_{S_n}(G) \subseteq \mathrm{PAut}(C)$ e como antes, seja $f = f_\phi$. Se $g \in G$, então levando em conta a definição de ϕ (em particular, que $\phi(e_i)(1) = g(1) = i$), vale que

$$f(g)(e_i) = e_{f(g)(i)} \overset{(3)}{=} \phi^{-1}(g\phi(e_i)) = e_{g\phi(e_i)(1)} = g(e_{\phi(e_i)(1)}) = g(e_i).$$

Isto nos permite concluir que $f(g) = g$, $\forall g \in G$. Como vimos acima, neste caso, $\phi(\sigma_g(C)) = \phi(C)f^{-1}(g)$, tem-se

$$\phi(C)g = \phi(C)f^{-1}(g) = \phi(\sigma_g(C)) = \phi(C),$$

para todo $g \in G$, já que $\sigma_g \in C_{S_n}(G) \subseteq \mathrm{PAut}(C)$. Logo $\phi(C)$ é também ideal bilateral de FG, o que conclui a prova do teorema. □

Corolário 3.9. *Um código linear $C \subset F^n$ é um código abeliano se, e somente se, existe um subgrupo regular abeliano de S_n que está contido em* $\mathrm{PAut}(C)$.

Demonstração. Demonstração imediata a partir do Teorema acima, (1), uma vez que as

noções código de grupo à esquerda e código de grupo coincidem para grupos abelianos. □

Teorema 3.10. *Seja G um grupo finito. Assuma que G possui dois subgrupos abelianos A e B tais que $G = AB$. Então, todo G-código é um código de grupo abeliano.*

Demonstração. Queremos mostrar que existe um grupo abeliano K tal que C seja um K-código de grupo. Assuma que $C \subset F^n$ é um G-código. Pelo Teorema 3.8, G é isomorfo a um subgrupo regular H de S_n tal que $H \cup C_{S_n}(H) \subset \mathrm{PAut}(C)$. Podemos assumir, sem perda de generalidade, que $G = AB = H$. Seja $\sigma : G \to C_{S_n}(G)$ o anti-isomorfismo definido no Lema 3.7 com relação a algum $i_0 \in \mathbb{N}_n$ e a bijeção $\psi : G \to \mathbb{N}_n$ dada por $\psi(g) = g(i_0)$. Consideremos os conjuntos

$$A_1 = \sigma(A) \text{ e } B_1 = \sigma(B).$$

Como σ é um anti-isomorfismo, segue que A_1 e B_1 são abelianos e satisfazem $C_{S_n}(G) = B_1A_1$. Agora consideremos $K = \langle A, B_1\rangle \leq \langle G, C_{S_n}(G)\rangle \leq \mathrm{PAut}(C)$. Como $A \subset G$ e $B_1 \subset C_{S_n}(G)$, os geradores de K comutam, de onde este é abeliano. Note que, para estarmos nas condições do Teorema 3.8 e assim concluirmos a prova, resta-nos mostrar que K é um subgrupo regular de S_n, ou seja, que $|K| = n$ e se $k \in K$ verifica $k(i) = i$, para algum $i \in \mathbb{N}_n$, então $k = Id$. Para mostrarmos que $|K| = n$, é suficiente mostrar que $[K : A] = [G : A]$, uma vez que $|G| = [G : A]|A|$ e $|K| = [K : A]|A|$. Para provar isto, repare que pelo Lema 3.7,

$$B \cap Z(G) = \sigma(B \cap Z(G)) = B_1 \cap Z(G) = B_1 \cap Z(C_{S_n}(H)).$$

Daí,

$$[B : B \cap Z(G)] = [B_1 : B_1 \cap Z(C_{S_n}(H))]$$

e como $A \cap B \subset Z(G)$, segue também que

$$[B \cap Z(G) : B \cap A] = [B_1 \cap Z(C_{S_n}(G)) : B \cap A].$$

Além disso, usando o fato de que $|B| = [B : A \cap B]|A \cap B|$, $|B_1| = [B_1 : B_1 \cap A]|A \cap B|$ e o Lema 3.1, concluimos que

$$[B : B \cap A] = [AB : A] \text{ e } [B_1 : B_1 \cap A] = [AB_1 : A].$$

Logo,

$$[G : A] = [AB : A] = [B : B \cap A] = [B_1 : B_1 \cap A] = [AB_1 : A] = [K : A].$$

Finalmente, seja $k \in K$ tal $k(i) = i$, para algum $i \in \mathbb{N}_n$. Vale que $k = a\beta$,

para certos $a \in A$ e $\beta = \sigma_b$, com $b \in B$. Além do mais, como ψ é bijeção, existe um único $g \in G$ tal que $g(i_0) = i$. Por isso,

$$g(i_0) = i = k(i) = a\beta g(i_0) = a\sigma_b(\psi(g)) = a\psi^{-1}(\psi(g))(b(i_0)) = agb(i_0).$$

Como $agb \in G$ e G é regular, segue que $agb = g$. Escrevamos $g = a'b'$, com $a' \in A$ e $b' \in B$. Então, temos

$$a'abb' = aa'b'b = agb = g = a'b' \Rightarrow ab = Id \Rightarrow b^{-1} = a \in A \cap B \subset Z(G).$$

Observe que na primeira igualdade acima foi usado o fato de que A e B são abelianos. Assim, mais uma vez pelo Lema 3.7, segue que $\sigma_b = b = \beta$ e por isso

$$k = a\beta = ab = Id,$$

o que completa a prova. □

O Teorema anterior dá sentido ao estudo que será desenvolvido adiante, uma vez que apresenta uma condição importante sobre um grupo para que este determine um código de grupo abeliano.

3.1 Grupos de ordem p^3 e p^4

Lema 3.11. *Sejam G um grupo, $Z(G)$ seu centro e $a, b, c \in G$. Se $[a, c] \in Z(G)$, então, para qualquer $n \geq 1$, vale a fórmula*

$$[a^n b, c] = [a, c]^n [b, c].$$

Demonstração. Provemos por indução em n. Para $n = 1$ temos

$$[a, c][b, c] = (a^{-1}c^{-1}ac)(b^{-1}c^{-1}bc) = b^{-1}(a^{-1}c^{-1}ac)c^{-1}bc = b^{-1}a^{-1}c^{-1}abc = [ab, c].$$

Na segunda igualdade acima usamos o fato de $[a, c]$ pertencer a Z. Suponhamos agora que o resultado é válido para $n \geq 1$ e vamos provar que se mantém verdadeiro para $n+1$. De fato,

$$[a^{n+1}b, c] = [a^n(ab), c] = [a, c]^n[ab, c] = [a, c]^n[a, c][b, c] = [a, c]^{n+1}[b, c],$$

onde na segunda igualdade usamos a hipótese de indução e na terceira usamos o que provamos no caso $n = 1$. □

Proposição 3.12. *Se p é um número primo, então qualquer grupo de ordem p^4 admite decomposição abeliana.*

Demonstração. Seja G um grupo tal que $|G| = p^4$, onde p é um número primo, e seja $Z = Z(G)$ o centro de G. Pelo teorema de Lagrange, temos que $|Z| \in \{p, p^2, p^3, p^4\}$. Mostraremos a veracidade do resultado para cada uma dessas possibilidades, concluindo assim a demonstração.

Caso 1: $|Z| = p^4$: Ora, neste caso temos $Z = G$, de onde G é abeliano e portanto, $G = \{e\}G$.

Caso 2: $|Z| = p^3$: Neste caso teríamos G abeliano, de onde G admitiria a decomposição abeliana trivial.

Caso 3: $|Z| = p^2$: Neste caso, tomemos $a \in G \setminus Z$. Observe que

$$A = \langle a, Z\rangle = \{a_1 a_2 \cdots a_k \mid a_i \in Z \cup \{a\}, k \in \mathbb{Z}\} = \{a^m a_1 a_2 \cdots a_n \mid a_i \in Z, m, n \in \mathbb{Z}\},$$

onde a penúltima igualdade decorre do fato de Z ser o centro de G e portanto, seus elementos comutarem, em particular, com a. Assim, $A = \langle a\rangle Z$ e consequentemente, $|A| = |\langle a\rangle||Z|$. Além disso, A é abeliano. Como $|\langle a\rangle| \mid |G|$ e $a \neq e$, segue que $|A| > p^2$, de onde $|A| = p^3$ ou $|A| = p^4$. Por um lado, se $|A| = p^3$, temos que G/A tem ordem p e portanto, é cíclico. Já que A é abeliano, podemos aplicar 3.4 novamente. Por outro lado, see $|A| = p^4$, então $G = A = \langle a\rangle Z$ e o resultado é válido.

Caso 4: $|Z| = p$: Consideremos o grupo $\overline{G} = G/Z$ de ordem p^3. Caso 4.1: Se existir $\overline{g} \in \overline{G}$ de ordem p^3, então $\overline{G}$ é cíclico e estamos nas condições do Lema 3.4, de onde G admite decomposição abeliana.
Caso 4.2: Se existir $\overline{g} \in \overline{G}$ de ordem p^2, então $\overline{g}^{p^2} = \overline{e}$, o que implica que $g^{p^2} \in Z$. Como $g \notin Z$, pois caso contrário a ordem de $\overline{g}$ seria 1, temos que $g^{p^2} = e$. Pelo Teorema de Lagrange, a ordem g deve ser, em vista do que vimos, p ou p^2. Porém, se $o(g) = p$, então $o(\overline{g}) \leq p$, o que é uma contradição. Logo, podemos concluir que $o(g) = p^2$. Deste modo, $|\langle g, Z\rangle| \geq p^3$, e pelo Caso 3 acima, G admite decomposição abeliana.
Caso 4.3: Por último, consideremos o caso onde para todo $\overline{g} \in \overline{G}$ vale $\overline{g}^p = \overline{e}$. Notemos que, em particular, isto implica que para todo $g \in G \setminus Z$, $o(g) = p$ ou $o(g) = p^2$, já que $|Z| = p$ e $g^p \in Z$. Agora, tomando $\overline{c} \in Z(\overline{G})$, com $\overline{c} \neq \overline{e}$, temos que $c \notin Z$, porém $[a, c] \in Z$, para todo $a \in G$. De fato, nas condições acima, vale que $caZ = acZ \Rightarrow cac^{-1}a^{-1} = z$, para algum $z \in Z$, de onde $c^{-1}a^{-1}ca = a^{-1}c^{-1}zca = z$, logo $[c, a] \in Z \Rightarrow [a, c] = [c, a]^{-1} \in Z$. Seja $C = \langle c, Z\rangle$. Note que podemos escrever $C = \langle c\rangle Z$, de onde C é abeliano. Ademais, C é subgrupo normal de G, já que dados $g \in G$ e $c^m z \in C$, temos $gc^m z = c^m wg$, onde

$z, w \in Z$, uma vez que $[c, g] \in Z$. Isto implica que $gC = Cg$, para qualquer $g \in G$. Não obstante, podemos supor que $|C| = p^2$. Com efeito, pelo Lema 3.1,

$$|C| = \frac{|\langle c\rangle||Z|}{|\langle c\rangle \cap Z|}.$$

Assim, como $\langle c\rangle \cap Z$ é subgrupo de Z, a ordem deste é 1 ou p. Se $|\langle c\rangle \cap Z| = 1$ e $o(c) = p$, segue que $|C| = p^2$. Se $|\langle c\rangle \cap Z| = 1$ e $o(c) = p^2$, teremos que C é um subgrupo normal abeliano de G tal que G/C é cíclico, de onde pelo Lema 3.4 G admitiria decomposição abeliana. Por outro lado, se $|\langle c\rangle \cap Z| = p$, temos $Z = \langle c\rangle \cap Z \subset \langle c\rangle$, de onde devemos ter necessariamente $o(c) = p^2$, pois se fosse $o(c) = p$, valeria $Z = \langle c\rangle$ e por isso, $c \in Z$, absurdo.

Se G/C for cíclico, então mais uma vez pelo Lema 3.4, G admite decomposição abeliana. Devido a ordem de G/C, sabemos que este é abeliano. Além disso, tomando $aC, bC \in G/C$ com $aC \neq eC$ e $bC \neq eC$, temos que $\langle aC, bC\rangle = \langle aC\rangle\langle bC\rangle$ e a ordem deste último é p^2, logo $G/C = \langle aC, bC\rangle$. Pelo que vimos acima, temos que $[a, c] = z$ e $[b, c] = w$ estão ambos em Z. Se um dos elementos z, w for igual a e, digamos $z = e$, então $\langle a, C\rangle = \langle a\rangle C$ é um subgrupo abeliano (já que C é abeliano e $\overline{c} \in Z(\overline{G})$) de ordem p^3, de onde o quociente de G por este é cíclico por ter ordem p, o que nos deixa novamente nas condições do Lema 3.4. Suponhamos então que ambos, z e w são diferentes de e. Repare que Z é um grupo cíclico e deste modo, temos, por exemplo, $Z = \langle z\rangle$, de onde existe $0 \leq k < p$ tal que $w^{-1} = z^k$. Usando o fato de $[a, c], [b, c]$ estarem em Z e o Lema acima, temos que para $1 \leq n$, vale

$$[a^n b, c] = [a, c]^n [b, c].$$

Em particular, para $n = k$ segue que

$$[a^k b, c] = [a, c]^k [b, c] = z^k w = ww^{-1} = e.$$

Isto nos mostra que $(a^k b)^{-1} c^{-1} a^k bc = e \Rightarrow a^k bc = ca^k b$. Podemos então concluir que

$$B = \langle a^k b, c, Z\rangle = \langle a^k b\rangle\langle c\rangle Z = \langle a^k b\rangle C.$$

Como $a^k b \notin C$ (caso contrário, teríamos, para cada $0 < n < p$, $e = [a^k b, c] = [a, c]^k [b, c]$, o que violaria a unicidade do inverso de $[b, c]$), em particular $a^k b \notin Z$ e por isso $o(a^k b) = p$ ou $o(a^k b) = p^2$. Já sabemos que B é abeliano e temos que ordem de B é p^3 ou p^4. Não obstante, na pior das hipóteses ($|B| = p^3$ de onde B é necessariamente normal, assim como mostrado no Corolário 4.2.2 de HALL (1976)), aplica-se mais uma vez o Lema 3.4 para concluirmos a demonstração. □

Corolário 3.13. *Se p é um número primo, então qualquer grupo de ordem p^3 admite*

decomposição abeliana.

Demonstração. Seja G um grupo cuja ordem é p^3. Considere $H = C_p$, o grupo cíclico multiplicativo de ordem p. Note que $G \times H$, que denota o produto direto de G por H, tem ordem p^4. Pela Proposição 3.12, segue que existem subgrupos abelianos A, B de $G \times H$ tais que $G \times H = AB$. Agora, seja $f : G \times H \to G$ o homomorfismo de grupos dado por $f(g, h) = g$. Uma vez que f é homomorfismo, vale que

$$f(G \times H) = f(AB) = f(A)f(B) = G,$$

onde $f(A)$ e $f(B)$ são subgrupos abelianos de G, logo G admite decomposição abeliana. □

Proposição 3.14. *Seja G um grupo de ordem $p^i q^j$, onde p e q são primos distintos e $0 < i, j < 3$. Então G possui uma decomposição abeliana.*

Demonstração. Seja $|G| = p^i q^j$. Aplicando o Primeiro Teorema de Sylow para p e para q, sabemos que existem um p-subgrupo de Sylow A e um q-subgrupo de Sylow B tais que $A \cap B = \{e\}$ de $G = AB$. Como as ordens destes subgrupos são no máximo p^2 e q^2, respectivamente, segue que são ambos abelianos. □

Corolário 3.15. *Seja G um grupo de ordem $p^i q^j$, onde p e q são primos (não necessariamente distintos) e $0 < i, j < 3$. Então G admite decomposição abeliana.*

Demonstração. Pelas Proposições 3.14, 3.12 e o Corolário 3.13, o resultado segue. □

3.2 Resultados Principais

Corolário 3.16. *Para $1 \leq n \leq 23$, qualquer grupo de ordem n admite uma decomposição abeliana.*

Demonstração. Se $n \in \{1, 2, 3, 4, 5, 7, 9, 11, 13, 17, 19, 23\}$, então qualquer grupo de ordem n é abeliano, já que nestes casos sua ordem é prima ou é quadrado de um primo. Se $n \in \{6, 10, 12, 14, 15, 18, 20, 21, 22\}$, então qualquer grupo de ordem n está nas condições da Proposição 3.14. Se $n \in \{8, 16\}$, então qualquer grupo de ordem n está nas condições do Corolário 3.13 ou da Proposição 3.12. □

Proposição 3.17. *O grupo simétrico S_4 não possui decomposição abeliana.*

Demonstração. Sobre o grupo simétrico, sabemos que qualquer permutação, com exceção da identidade, pode ser escrita como produto de ciclos disjuntos, além disso, salvo o caso de uma permutação e seu inverso, duas permutações comutam se, e somente se, são

disjuntas. De posse disto, seja A um subgrupo abeliano do grupo simétrico S_4. Vejamos as possibilidades para a quantidade de elementos de A. Se existir um 4-ciclo (ou um 3-ciclo) σ em A, necessariamente devemos ter $A = \{Id, \sigma, \sigma^2, \sigma^3\}$ (ou $A = \{Id, \sigma, \sigma^2\}$). Resta então analisar o caso em que A possui apenas transposições e produtos disjuntos destas. As transposições de S_4 são $(1\,2), (1\,3), (1\,4), (2\,3), (2\,4)$ e $(3\,4)$, de onde

$$A = \{Id, (1\,2), (3\,4), (1\,2)(3\,4)\}$$

ou

$$A = \{Id, (1\,4), (2\,3), (1\,4)(2\,3)\}$$

ou

$$A = \{Id, (1\,3), (2\,4), (1\,3)(2\,4)\}.$$

Além de $A = \{Id, \sigma\}$, onde σ é uma transposição. Logo, qualquer subgrupo abeliano de S_4 possui no máximo 4 elementos, e deste modo, o produto de dois subgrupos abelianos de S_4 possui no máximo 16 elementos, de onde S_4 não admite decomposição abeliana. □

Agora sabemos que 24 é a menor ordem para um grupo não possuir decomposição abeliana.

Por suas boas propriedades de solubilidade e nilpotência, espera-se que seja mais interessante trabalhar com p-grupos e por isso, um questionamento é determinar qual a menor ordem de um p-grupo para que este não admita decomposição abeliana.

Uma possível maneira de encontrar p-grupos finitos que não possuam decomposição abeliana é baseada na contrução de OL'SHANSKII (1978). Para um primo fixado p, seja $F(n)$ a função definida pela seguinte condição: $p^{F(n)}$ é a maior ordem possível de um p-grupo para que este não possua subgrupo abeliano de ordem maior que p^n. O Teorema 2 de OL'SHANSKII (1978) afirma que para qualquer primo p,

$$F(n) \geq \frac{n^2 + 4n - 8}{8}.$$

Além disso, a demonstração deste teorema inclui uma construção na qual dados n, p, um grupo G tal que $|G| = p^m$ com G não possuindo subgrupos abelianos de ordem maior que p^n, vale

$$m = \left[\frac{n^2 - 1}{8}\right] + \frac{n}{2},$$

se n for par, e

$$m = \left[\frac{n^2 - 2}{8}\right] + \frac{n + 1}{2},$$

se n for ímpar.

Diante disso, temos o seguinte resultado.

Proposição 3.18. *Dados um primo p e um número natural n, se G é um grupo de ordem p^m, com $m > 2n-1$ e G não possui subgrupos abelianos com ordem maior que p^n, então G não possui decomposição abeliana.*

Demonstração. Suponhamos que $G = AB$ para certos subgrupos abelianos A e B. Podemos assumir que o centro Z de G está contido em $A \cap B$, já que caso contrário, bastava tomar $\overline{A} = AZ$ e $\overline{B} = ZB$ e teríamos que $G = \overline{A}\,\overline{B}$ seria uma decomposição abeliana nessas condições. Como $|Z| \geq p$, temos que $|A \cap B| \geq p$, de onde, aplicando o Lema 3.1, usando a hipótese e a desigualdade encontrada, temos

$$|G| = |AB| = \frac{|A||B|}{|A \cap B|} \leq \frac{p^n p^n}{p} = p^{2n-1} < p^m = |G|,$$

o que é uma contradição. □

Tomando $n = 13$, obtemos que $m = 27 > 2 \cdot 13 - 1$, de onde G, com $|G| = 2^{27}$, não possui decomposição abeliana, pela proposição anterior, desde que G não possua subgrupo abeliano com ordem maior que p^n. Em ALPERIN (1965) é dado um exemplo de um grupo de ordem 2^{50} que não possui decomposição abeliana. Claramente, os grupos obtidos desta forma são muito grandes. Tentaremos melhorar estes resultados provando que existem grupos de ordem 64 que não admitem decomposição abeliana. No caso em que p é um primo ímpar, os resultados para p-grupos, vistos anteriormente, não podem ser estendidos.

Com o intuito de provar o próximo resultado, enunciaremos o Teorema de Schreier, cuja demonstração está em HALL (1976).

Teorema 3.19. ***(Teorema de Schreier)*** *Dados um grupo G com subgrupo normal N e um grupo quociente $H = G/N$, se escolhermos representantes $\overline{u} \in G$ das classes $\overline{u}N = u \in H$, sendo $\overline{e} = e$, os automorfismos e um conjunto quociente (para $h_1, h_2 \in H, (h_1, h_2) \in N$ é o elemento tal que $\overline{h_1}\,\overline{h_2} = \overline{h_1 h_2}(h_1, h_2)$) são determinados satisfazendo*

$$(a^u)^v = (u,v)^{-1}(a^{uv})(u,v),\ a,(u,v) \in N,\ u,v \in H \tag{5}$$

$$(uv,w)(u,v)^w = (u,vw)(v,w),\ (e,e) = e. \tag{6}$$

Reciprocamente, se para cada $u \in H$ é associado um automorfismo $a \rightleftharpoons a^u$ de N e para estes automorfismos e o conjunto quociente $\{(u,v) \in N \mid u,v \in H\}$ as condições (4) e (5) valerem, então $G = \{\overline{u}a \mid u \in H, a \in N\}$ com a operação $\overline{u}a \cdot \overline{v}b = \overline{uv}(u,v)a^u b$ é um grupo com subgrupo normal N e tal que $G/N \cong H$.

Teorema 3.20. *Para qualquer número primo ímpar p existe um grupo de ordem p^5 que não possui decomposição abeliana.*

Demonstração. Consideremos dois p-grupos abelianos elementares, N gerado por u, z_1,

z_2 e H gerado por $\overline{x}$, $\overline{y}$. Queremos construir uma extensão G de N por H, ou seja, um grupo G tal que $N \lhd G$ e $G/N \cong H$. Para isto escolhamos imagens inversas x, y de $\overline{x}$, $\overline{y}$, respectivamente, tais que as seguintes relações sejam satisfeitas:

$$x^p = y^p = e, \quad [x, y] = u, \quad [x, u] = z_1, \quad [y, u] = z_2, \tag{7}$$

$$[x, z_1] = [y, z_1] = [x, z_2] = [y, z_2] = e. \tag{8}$$

Vejamos que isto nos permite estar nas condições do Teorema de Schreier. De fato, das equações acima temos

$$u^{\overline{x}} = uz_1^{-1}, \quad u^{\overline{y}} = uz_2^{-1}, \quad z_1^{\overline{x}} = z_1^{\overline{y}} = z_1, \quad z_2^{\overline{x}} = z_2^{\overline{y}} = z_2.$$

Os automorfismos requeridos em 3.19 são determinados pelas igualdades acima, enquanto que o conjunto quociente pode ser determinado usando (7) e (8). O cálculo para determinar o conjunto quociente é longo , mas direto, por isso descrevemos apenas a fórmula resultante que o determina

$$\left(\overline{x}^k\overline{y}^l, \overline{x}^r\overline{y}^s\right) = u^{-rl} z_1^{\frac{lr(l-1)}{2}} z_2^{rls+\frac{rl(l-1)}{2}}, \ \forall\, k, l, r, s \geq 0.$$

Para este conjunto quociente e os automorfismos acima citados, as condições do Teorema de Schreier são satisfeitas, restando-nos apenas averiguar a validade da equação acima, no sentido de que, quando somamos p a algum dos números k, l, m, n, o resultado não se altera. Isto só não ocorre quando $p = 2$, portanto, p deve estar nas condições de nossa hipótese. Agora, seja G a extensão garantida por 3.19.

Inicialmente, note que $|G| = p^5$, uma vez que $|H| = p^2$ e $|N| = p^3$. Além disso, provaremos que G não possui subgrupo abeliano de ordem p^4. De fato, se tivéssemos um tal subgrupo A, por HALL (1976), Corolário 4.2.2, este seria normal. Como $|G/A| = p$, teríamos G/A abeliano e consequentemente $A \supset G' \supset N$, já que os geradores de N são comutadores. Como A tem mais elementos que N, podemos tomar $a \in A \setminus N$. Sem perda de generalidade, podemos supor que $a = x^k y^l$, onde nem k nem l são múltiplos de p. Do fato de A ser abeliano e $a, u \in A$, temos que $[u, a] = 1$, o que implica

$$u = a^{-1}ua = y^{-l}x^{-k}ux^k y^l = y^{-l}u^{\overline{x}^k}y^l = (uz_1^{-k})^{\overline{y}^l} = u^{\overline{y}^l}z_1^{-k} = uz_1^{-k}z_2^{-l} \neq u,$$

uma contradição.

Finalizando, suponhamos que existam subgrupos abelianos A e B de G tais que $G = AB$. Podemos supor que tanto A quanto B contêm o centro $Z(G) = \langle z_1, z_2 \rangle$

de G, já que $AZ(G)$ e $BZ(G)$ seriam novamente subgrupos abelianos tais que $G = AB$. Neste caso, $|A \cap B| \geq |Z(G)| = p^2$, de onde $|AB| \leq p^3 p^3/p^2 = p^4$, um absurdo. □

Antes de provarmos os próximos resultados relembremos algumas definições e resultados que serão bastante usados. A primeira definição e não menos importante é a de grupo nilpotente. O que está descrito abaixo pode ser encontrado em MILIES and SEHGAL (2002).

Definição 3.21. *Um grupo G diz-se nilpotente se ele contém uma série de subgrupos:*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

tais que cada subgrupo G_{i-1} é normal em G_i e em G, e cada quociente G_i/G_{i-1} está contido em $Z(G/G_{i-1})$, $1 \leq i \leq n$. A série de subgrupos de G com esta propriedade é chamada de série central de G.

Observação. Prova-se, por exemplo, na página 28 de MILIES and SEHGAL, 2002, que todo p-grupo finito é nilpotente.

Definição 3.22. *Dado um grupo G, definimos indutivamente as seguintes séries de subgrupos:*

$$G^{(1)} = G,\ G^{(2)} = G' \text{ e } G^{(i)} = \left[G, G^{(i-1)}\right]$$

$$Z_0(G) = \{1\},\ Z_1(G) = Z(G) \text{ e } Z_i(G)$$

é o único subgrupo de G tal que $Z_i(G)/Z_{i-1}(G) = Z\left(G/Z_{i-1}(G)\right)$. O grupo $Z_i(G)$ é chamado o i-ésimo centro de G. Estas séries, que verificam

$$G^{(1)} = G \supsetneq G^{(2)} \supsetneq \cdots \supset G^{(n)} \supsetneq \cdots$$

$$\{1\} = Z_0(G) \subsetneq Z_1(G) \subsetneq \cdots \subsetneq Z_n(G) \subset \cdots,$$

são claramente centrais e são chamadas, respectivamente, de série central inferior e série central superior.

Os dois próximos lemas podem ser provados usando indução e são demonstrados na referência citada anteriormente. Eles permitem entender, de modo mais significativo, o por quê de as séries centrais acima definidas serem chamadas de inferior e superior, respectivamente.

Lema 3.23. *Seja*

$$G = A_0 \supset A_1 \supset \cdots \supset A_n \supset \cdots$$

uma série central descendente. Então $G^{(n)} \subset A_{n-1}$, para qualquer n.

Lema 3.24. *Seja*

$$\{1\} = A_0 \subset A_1 \subset \cdots \subset A_n \subset \cdots$$

uma série central ascendente. Então $A_n \subset Z_n(G)$ para todo n.

Os lemas acima nos permitem dar a seguinte definição para comprimento nilpotente de um grupo, já que mostram que no caso de um grupo com série central inferior ou superior finitas, estas têm o mesmo comprimento.

Definição 3.25. *Dado um grupo nilpotente finito G, definimos seu comprimento nilpotente como sendo o comprimento de sua série central superior (inferior).*

Os próximos lemas constituem as partes da demonstração do Teorema seguinte. Também vale ressaltar que, alguns argumentos usados nas demonstrações destes serão explicados com detalhes uma única vez, para não tornar o texto repetitivo. Assim, os mesmos argumentos podem ser usados adiante nas demonstrações dos demais lemas, sem que se faça menção explícita a estes.

Relembremos que dado um grupo abeliano $(G, +)$ e subgrupos A, B de G, tais que $G = A + B$ e $A \cap B = \{e\}$, mostra-se, assim como feito em LANG (2002), que a aplicação

$$A \times B \to G$$

dada por $(x, y) \mapsto x + y$ é um isomorfismo. Neste caso, escrevemos $G = A \oplus B$ para expressar que cada elemento de G se escreve de forma única como soma de elementos de A e B. Não obstante, podemos generalizar este fato para uma quantidade finita de subgrupos. É importante ressaltar que apesar de escrevermos $G = A_1 \oplus \cdots \oplus A_n$, nos referiremos à escrita de um elemento de G através da notação multiplicativa, mais especificamente, escreveremos para cada $g \in G$,

$$g = a_1 \cdots a_n$$

ao invés de

$$g = a_1 + \cdots + a_n,$$

com $a_i \in A_i$, pois consideraremos $(G, \cdot)$.

Escreveremos também C_n para denotar um subgrupo de G isomorfo a $\mathbb{Z}_n$. Ademais, usaremos as seguintes propriedades de comutadores de um grupo. Seja G um grupo e x, y, z elementos de G. Tendo em vista que $x^y = y^{-1}xy$, vale que:

(*i*) $[xy, z] = [x, z]^y [y, z]$

(*ii*) $[x, yz] = [x, z] [x, y]^z$

(*iii*) Se $[x, y] = z \in Z(G)$, então, para qualquer inteiro m, existe um certo inteiro n, tal que $(xy)^m = x^m y^m z^n$.

Lema 3.26. *Se G é um grupo de ordem 32 com comprimento nilpotente igual a 2, então G admite decomposição abeliana.*

Demonstração. Pela definição de comprimento nilpotente, temos que a série central superior de G é

$$\{1\} = Z_0(G) \subsetneq Z(G) = Z_1(G) \subsetneq G = Z_2(G).$$

Além disso, $G/Z(G) = Z\left(G/Z(G)\right)$, de onde $G/Z(G)$ é abeliano. Olhando também para a série central inferior de G, neste caso, teremos

$$\{1\} = G^{(3)} \subset G' = G^{(2)} \subset G^{(1)} = G.$$

Pelo Lema 3.23, temos que $G' = G^{(2)} \subset Z(G) = Z_1(G)$. Em vista disto, do Teorema de Lagrange e do fato de que o centro de um p-grupo, p primo, é não trivial, temos que as possíveis ordens para $Z(G)$ são $2, 4, 8$ e 16. Mas, note que se $|Z(G)| = 16$, então estaríamos nas condições do Lema 3.4, de onde o resultado segue. Resta portanto, analisarmos cada um dos demais casos.

(a) $|Z(G)| = 2$: Escrevamos $Z(G) = \langle z \rangle$. Vale que $|G/Z(G)| = 16$, de onde pela Classificação dos Grupos Abelianos Finitamente Gerados, temos as seguintes possibilidades para $G/Z(G)$:

$$C_{16},\ C_2 \oplus C_8,\ C_4 \oplus C_4,\ C_2 \oplus C_2 \oplus C_4,\ C_2 \oplus C_2 \oplus C_2 \oplus C_2.$$

Repare que se $G/Z(G) = C_{16}$, estaríamos mais uma vez nas condições do Lema 3.4. Foquemos nos demais casos.

(i) $G/Z(G) = C_2 \oplus C_8$: Consideremos $C_2 \oplus C_8 = \langle \overline{a} \rangle \oplus \left\langle \overline{b} \right\rangle$, com $o(\overline{a}) = 2$ e $o(\overline{b}) = 8$. Assim, tomando $A = \langle a \rangle$ e $B = \langle b \rangle\, Z(G)$, teremos $G = AB$. De fato, pelo que discutimos exatamente antes deste lema, temos, para cada $\overline{g} \in G/Z(G)$, $\overline{g} = \overline{a}^m \overline{b}^n$, para certos m, n inteiros. Donde $g = a^m b^n w$, para $w \in Z(G)$. Mas esta é precisamente a forma de um elemento de AB, de onde $G \subset AB$ e consequentemente a igualdade vale. O caso $C_4 \oplus C_4$ é análogo.

(ii) $G/Z(G) = C_2 \oplus C_2 \oplus C_4$: Admitindo que $C_2 \oplus C_2 \oplus C_4 = \langle \overline{a} \rangle \oplus \left\langle \overline{b} \right\rangle \oplus \langle \overline{c} \rangle$, de $G' \subset Z(G)$ segue que $[a, c], [b, c] \in Z(G) = \langle z \rangle = \{1, z\}$. Se $[a, c] = z = [b, c]$, então

$$[ab, c] = [a, c]^b\, [b, c] = z^b z = b^{-1} z b z = z^2 = 1.$$

Logo, tomando $A = \langle ab, c \rangle$ e $B = \langle a \rangle\, Z(G)$, teremos dois subgrupos abelianos tais que $G = AB$. Com efeito, já sabemos que dado $g \in G$ existem inteiros l, m, n tais que $g = a^l b^m c^n w$, onde $w \in Z(G)$. Além disso, um elemento de AB tem a seguinte forma

$$(ab)^r c^s a^t w_0 = a^r b^r w' c^s a^t w_0 = a^r b^r c^s a^t w' w_0 = a^r a^t b^r c^s w'' w' w_0 = a^{r+t} b^r c^s w,$$

onde $w_0, w^{'}, w^{''} \in Z(G)$, $w = w_0 w^{'} w^{''}$ e usamos o fato de $[a,b], [b,c] \in Z(G)$ para comutar as potências de tais elementos. Tomando $l = r + t$, $m = r$ e $n = s$, temos a igualdade pretendida. Se $[a,c] = 1$ (ou analogamente $[b,c] = 1$), então $G = AB$, onde $A = \langle a, c \rangle$ e $B = \langle b \rangle Z(G)$ são abelianos.

(iii) $G/Z(G) = C_2 \oplus C_2 \oplus C_2 \oplus C_2$: Considerando

$$C_2 \oplus C_2 \oplus C_2 \oplus C_2 = \langle \overline{a} \rangle \oplus \langle \overline{b} \rangle \oplus \langle \overline{c} \rangle \oplus \langle \overline{d} \rangle$$

e sabendo que $G^{'} \subset Z(G)$, segue que se $[a,b] = z = [a,c]$, então $[a,bc] = [a,c]\,[a,b]^c = z^2 = 1$. Assim como $[b,c] = z = [b,d]$ implica $[b,cd] = 1$. Deste modo, tomando os subgrupos abelianos $A = \langle a, bc \rangle$ e $B = \langle b, cd \rangle Z(G)$, teremos $G = AB$. A prova da igualdade é completamente análoga as discutidas acima. Portanto, podemos supor, sem perda de generalidade, que $[a,b] = 1$. Se $[a,c] = 1 = [b,c]$, então $A = \langle a, b, c \rangle$ e $B = \langle d \rangle Z(G)$ são subgrupos abelianos tais que $G = AB$. Assim, podemos supor que $[a,c] = z$. Se $[c,d] = 1$, então $A = \langle a, b \rangle$ e $B = \langle c, d \rangle Z(G)$ são os subgrupos desejados. Finalmente, se $[c,d] = z = [a,c]$, então $[c, ad] = 1$, de onde $A = \langle a, b \rangle$ e $B = \langle c, ad \rangle$ são os subgrupos abelianos requeridos. Isto encerra a prova deste caso.

(b) $|Z(G)| = 4$: Aqui temos $|G/Z(G)| = 8$, de onde as possibilidades para $G/Z(G)$ são:

$$C_8,\ C_2 \oplus C_4,\ C_2 \oplus C_2 \oplus C_2.$$

Mais uma vez, veja que se $G/Z(G) = C_8$, o resultado decorre do Lema 3.4. Além disso, o caso $G/Z(G) = C_2 \oplus C_4$ é análogo ao caso $(a)(i)$. Portanto, somente falta analisar o caso em que $G/Z(G) = C_2 \oplus C_2 \oplus C_2 = \langle \overline{a} \rangle \oplus \langle \overline{b} \rangle \oplus \langle \overline{c} \rangle$. Note também que $Z(G)$ é um subgrupo abeliano de ordem 4, de onde podemos ter:

(i) $Z(G) = \langle z \rangle = C_4$: Aqui, temos $[a,b], [a,c], [b,c] \in Z(G) = \{1, z, z^2, z^3\}$. Se $[a,b] = 1$, então $A = \langle a, b \rangle$ e $B = \langle c \rangle Z(G)$ resolvem. Um raciocínio análogo pode ser aplicado caso em que algum dos demais comutadores citados seja igual a 1. Assim, suponhamos que todos sejam diferentes de 1. Se algum destes for igual a z, digamos $[a,b] = z$, então, como $a^2 \in Z(G)$, pois $\overline{a}^2 = 1$, vale que

$$1 = \left[a^2, b\right] = [a,b]^a\,[a,b] = z^a z = z^2,$$

pois $[a^2, b] \subset [Z(G), b] = \{1\}$, o que contradiz a ordem de z ser 4. Como $o(z^3) = 4$, o mesmo raciocínio pode ser aplicado se um destes três comutadores for igual a z^3. Finalmente, nestas condições teremos necessariamente dois destes iguais a z^2, digamos $[a,b] = z^2 = [a,c]$. Não obstante, da propriedade de comutadores, decorre que $[a,bc] = 1$

e portanto $A = \langle a, bc\rangle$ e $B = \langle c\rangle\, Z(G)$ são os subgrupos abelianos procurados.

(ii) $Z(G) = C_2 \oplus C_2 = \langle z_1\rangle \oplus \langle z_2\rangle$: Claro que $z_1^2 = z_2^2 = 1$. Não obstante, temos $[a,b], [a,c], [b,c] \in Z(G) = \{1, z_1, z_2, z_1z_2\}$. Se $[a,b] = 1$ (um raciocínio análogo se aplica aos demais), então $A = \langle a, b\rangle$ e $B = \langle c\rangle\, Z(G)$ resolvem. Como $o(z_1) = o(z_2) = o(z_1z_2) = 2$, se dois dos comutadores acima forem iguais a z_1 (ou z_2, ou z_1z_2), aplicamos o mesmo raciocínio feito em $(b)(i)$ para quando dois comutadores eram iguais a z^2. Resta portanto o caso em que $[a,b] = z_1$, $[a,c] = z_2$ e $[b,c] = z_1z_2$ (a menos de trocarmos essa ordem). Então

$$[ab,c] = [a,c]^b\,[b,c] = z_2^b z_1 z_2 = z_2^2 z_1 = z_1 = z_1^b = [a,b]^b\,[b,b] = [ab,b].$$

Assim,

$$[ab,bc] = [ab,c]\,[ab,b]^b = z_1 z_1^b = z_1^2 = 1.$$

Logo, $A = \langle ab, bc\rangle$ e $B = \langle c\rangle\, Z(G)$ são subgrupos abelianos tais que $G = AB$.

(c) $|Z(G)| = 8$: Neste caso, $|G/Z(G)| = 4$. Por um lado, se $G/Z(G) \cong C_4$, o resultado segue do Lema 3.4. Por outro lado, se $G/Z(G) \cong C_2 \oplus C_2$, podemos proceder como em $(a)(i)$. □

Lema 3.27. *Seja G um grupo de ordem 32 com comprimento nilpotente igual a 3, então G admite decomposição abeliana.*

Demonstração. Sejam

$$\{1\} = Z_0(G) \subsetneq Z(G) = Z_1(G) \subsetneq Z_2(G) \subsetneq Z_3(G) = G$$

e

$$\{1\} = G^{(4)} \subsetneq G^{(3)} \subsetneq G' = G^{(2)} \subsetneq G^{(1)} = G$$

as respectivas séries centrais superior e inferior. Pelo Lema 3.23 segue que $G^{(3)} \subset Z(G) = Z_1(G)$. Além disso, da definição de série central superior, $G/Z_2(G) = Z(G/Z_2)$, de onde $G/Z_2(G)$ é abeliano. Pelo Lema 1.5.4 de MILIES and SEHGAL (2002), segue que $G' \subset Z_2(G)$. Como as inclusões que aparecem nas séries centrais são estritas e $|Z(G)| \geq 2$, temos as seguintes possibilidades para a ordem de $Z_2(G)$: 4, 8 e 16. Repare que $|Z_2(G)| = 16$ implica $|G/Z_2(G)| = 2$, de onde $G/Z_2(G)$ é cíclico. Assim,

$$\frac{G/Z_1(G)}{Z(G/Z_1(G))} = \frac{G/Z_1(G)}{Z_2(G)/Z_1(G)} \cong G/Z_2(G),$$

de onde temos que $G/Z_1(G)$ é abeliano (pois o quociente deste por seu centro é cíclico) e, por isso, $Z_2(G)/Z_1(G) = Z(G/Z_1(G)) = G/Z_1(G)$, o que implica $Z_2(G) \cong G$, o que é uma contradição. Esta contradição nos permite excluir os casos em que $G/Z_2(G)$ é cíclico.

Usaremos este argumento mais vezes no decorrer desta demonstração, assim como na demonstração dos dois lemas seguintes.

Restam os outros dois casos.

(a) $|Z_2(G)| = 4$: Aqui temos $|G/Z_2(G)| = 8$, de onde temos as seguintes possibilidades para $G/Z_2(G)$:

$$C_2 \oplus C_4,\ C_2 \oplus C_2 \oplus C_2.$$

Inicialmente é importante observar que, em qualquer um dos casos acima, $|Z(G)| = 2$, já que $Z(G) \subsetneq Z_2(G)$. Daí, escrevamos $Z(G) = Z_1(G) = \langle z \rangle$ e $Z_2(G)/Z_1(G) = \langle \overline{u} \rangle = C_2$.

(i) $G/Z_2(G) = C_2 \oplus C_4 = \langle \overline{a} \rangle \oplus \left\langle \overline{b} \right\rangle$: Observe que $Z_2(G)/Z_1(G) = Z(G/Z_1(G))$, de onde

$$h \in Z_2(G) \Leftrightarrow (hZ_1(G))(gZ_1(G)) = (gZ_1(G))(hZ_1(G)),\ \forall\, g \in G \Leftrightarrow [h, g] \in Z_1(G),\ \forall\, g \in G.$$

Em particular, $[a, u], [b, u] \in Z_1(G) = \{1, z\}$. Se $[a, u] = 1$ (ou se $[b, u] = 1$), então $A = \langle a \rangle Z_2(G)$ e $B = \langle b \rangle$ (respectivamente $A = \langle a \rangle$ e $B = \langle b \rangle Z_2(G)$) são subgrupos abelianos tais que $G = AB$. A (respectivamente B) é de fato abeliano, pois $Z_2(G) = \langle u \rangle Z_1(G)$ e a, u comutam (respectivamente, b e u comutam). Se $[a, u] = z = [b, u]$, então $[ab, u] = [a, u]^b [b, u] = z^2 = 1$. Portanto $A = \langle ab \rangle Z_2(G)$ e $B = \langle b \rangle$ são subgrupos abelianos tais que $G = AB$.

(ii) $G/Z_2(G) = C_2 \oplus C_2 \oplus C_2 = \langle \overline{a} \rangle \oplus \left\langle \overline{b} \right\rangle \oplus \langle \overline{c} \rangle$: Assim como discutido no item anterior, $[a, u], [b, u], [c, u] \in Z_1(G) = \{1, z\}$. Se $[a, u] = [b, u] = [c, u] = z$, então $[ab, u] = 1 = [bc, u]$, de onde a menos de trocar $[a, u]$ por $[ab, u]$ e $[b, u]$ por $[bc, u]$, podemos supor que $[a, u] = 1 = [b, u]$ e $[c, u] = z$. Agora, olharemos para $[a, b], [a, c], [b, c] \in G' \subset Z_2(G) = \{1, z, u, zu\}$.

1. Se $[a, b] = 1$, então $A = \langle a, b \rangle Z_2(G)$ e $B = \langle c \rangle$ são abelianos tais que $G = AB$.
2. Se $[a, b] = u$, então do fato de $o(\overline{a}) = 2$, vem que $a^2 \in Z_2(G)$, de onde $[a^2, b] \in [Z_2(G), b] = \{1\}$, já que b comuta com u. Assim, $[a^2, b] = 1$. Porém,

$$1 = \left[a^2, b\right] = [a, b]^a [a, b] = u^a u = u^2,$$

uma vez que a comuta com u. Logo, $o(u) = 2$ e por isso $Z_2(G) = C_2 \oplus C_2$. Daqui decorre que $u^{-1} = u$ e $z^{-1} = z$, portanto, para qualquer comutador $[g, h]$ em $Z_2(G)$ valerá que $[g, h] = [g, h]^{-1} = [h, g]$.

2.1 Se $[a, c] = u$, então $[a, cb] = [a, b] [a, c]^b = uu^b = u^2 = 1$. Consequentemente, $A = \langle a, cb, z \rangle$ e $B = \langle b, u \rangle$ são abelianos tais que $G = AB$.

2.2 Se $[a,c] = z = [b,c]$, então $[c,ba] = 1$, de onde $A = \langle c, ba, z\rangle$ e $B = \langle a, u\rangle$ são abelianos tais que $G = AB$.

2.3 Se $[a,c] = z$ e $[b,c] = uz$, então $[c,ab] = [c,b]\,[c,a]^b = uzz = u$, ou seja, $[ab,c] = u$. Repare também que $[ab,b] = [a,b]^b\,[b,b] = u^b = u$. Portanto,

$$[ab,cb] = [ab,b]\,[ab,c]^b = uu^b = u^2 = 1.$$

Logo, $A = \langle ab, cb, z\rangle$ e $B = \langle b, u\rangle$ são abelianos tais que $G = AB$.

2.4 Os casos em que $[a,c] = uz$ e $[b,c] = z$ e $[a,c] = uz$ e $[b,c] = uz$ são similares aos dois casos anteriores e terão a demonstração omitida.

3. Seja $[a,b] = z$. Se $[a,c] = z$, então $[a,bc] = [a,c]^b\,[a,b] = z^2 = 1$ e portanto $A = \langle a, bc\rangle$ e $B = \langle b\rangle\, Z_2(G)$ são abelianos tais que $G = AB$. Se $[a,c] = uz$, então $[a,bc] = u$, mas assim

$$[ab,cb] = [a,cb]^b\,[b,cb] = u\,[b,cb] = u\,[b,c]^b\,.$$

O caso em que $[b,c] = z$ é análogo a quando $[a,c] = z$. Se $[b,c] = u$, então $[ab,cb] = 1$ e assim $A = \langle ab, cb\rangle$ e $B = \langle b\rangle\, Z_2(G)$ resolvem. Se $[b,c] = uz$, então $[b,ac] = u$ e o resultado segue de modo análogo a 2., trocando a por ac. Deste modo podemos supor, sem perda de generalidade, que $[a,c] = u$. $o(\overline{c}) = 2$ implica que $c^2 \in Z_2(G)$, de onde $[a,c^2] \in [a, Z_2(G)] = \{1\}$. Então

$$1 = \left[a,c^2\right] = [a,c]\,[a,c]^c = uu^c.$$

Não obstante, $u^c = c^{-1}uc = u\,[u,c] = uz$, o que implica

$$1 = uu^c = uuz = u^2z \Rightarrow u^2 = z.$$

Logo, $Z_2(G) = C_4 = \langle u\rangle$. Nestas condições, se $[b,c] = u = [a,c]$, então $[ab,c] = [a,c]^b\,[b,c] = u^bu = u^2 = z$, o que implica, $[ab,bc] = [ab,c]\,[ab,b]^c = zz^c = z^2 = 1$. Portanto $A = \langle a\rangle\, Z_2(G)$ e $B = \langle ab, bc\rangle$ são abelianos tais que $G = AB$. Se $[b,c] = z$, então $[ac,b] = 1$ e o resultado segue. Finalmente, se $[b,c] = uz = u^3$, então $[ab,c] = [a,c]^b\,[b,c] = u^bu^3 = u^4 = 1$, de onde $A = \langle ab, c\rangle$ e $B = \langle b\rangle\, Z_2(G)$ são abelianos tais que $G = AB$.

4. Seja $[a,b] = uz$. Analogamente ao caso 2., teremos $o(uz) = 2$, o que implica $o(u) = 2$, de onde $Z_2(G) = C_2 \oplus C_2$ e, de modo similar a 2. teremos o pretendido.

(b) $|Z_2(G)| = 8$: Vale que $|G/Z_2(G)| = 4$. Então $G/Z_2(G) = C_2 \oplus C_2$. Já $Z_2(G)$ pode ser C_8, $C_4 \oplus C_2$, $C_2 \oplus C_2 \oplus C_2$, Q_8 ou D_4. Analisaremos cada um destes casos.

(i) $Z_2(G) = C_8 = \langle v \rangle$: Como $Z(G) \subsetneq Z_2(G)$, segue que $|Z(G)| = 2$ ou $|Z(G)| = 4$. Assim, temos as seguintes possibilidades:

1. Seja $Z(G) = \langle v^2 \rangle \cong C_4$. Do fato de $G' \subset Z_2(G)$, vem que $[a, b] \in Z_2(G)$. Além disso, $o(\overline{a}) = 2$ implica que $a^2 \in Z_2(G)$, de onde $[a^2, b] \in Z(G) = \{1, v^2, v^4, v^6\}$. Escrevamos $[a^2, b] = v^j$, onde $j \in \{0, 2, 4, 6\}$. Escrevendo $[a, b] = v^i$, vale que

$$v^j = \left[a^2, b\right] = [a, b]^a [a, b] = a^{-1} v^i a v^i.$$

   Se $v^i \in Z(G)$, ou seja, $i = 0, 2, 4, 6$, então $[a^2, b] = v^{2i}$, de onde $i \in \{0, 2\}$. Se $i = 0$, então $A = \langle a, b \rangle$ e $B = Z_2(G)$ são abelianos tais que $G = AB$. Portanto estamos no caso em que $i \in \{1, 2, 3, 5, 7\}$. Suponhamos, por absurdo, que $a^2 \in Z(G)$, deste modo $1 = [a^2, b] = a^{-1} v^i a v^i$, de onde $[a, v^i] = v^{2i}$ e portanto, como $v^{2i} \in Z(G)$, temos

$$1 = \left[a, v^{2i}\right] = \left[a, v^i\right] \left[a, v^i\right]^{v^i} = (v^{2i})^2 = v^{4i}.$$

   Como a ordem de v é 8, temos uma contradição para qualquer $i \in \{1, 2, 3, 5, 7\}$. Logo, $a^2 \notin Z(G)$ (de modo análogo $b^2 \notin Z(G)$) , assim $A = \langle a \rangle Z_2(G)$ e $B = \langle b \rangle$, por 3.1, são subgrupos abelianos tais que $G = AB$.

   Observe que teríamos usado o mesmo raciocínio e abreviado a conta se supuséssemos inicialmente que $[a, b] = v$. Chamamos atenção para este fato porque o usaremos adiante sem explicar novamente o motivo.
2. Se $Z(G) = \langle v^4 \rangle = C_2$, então $[a, v], [b, v] \in Z(G) = \{1, v^4\}$. Se um deste for igual a 1, digamos $[a, v] = 1$, então $A = \langle a \rangle Z_2(G)$ e $B = \langle b \rangle$ são abelianos tais que $G = AB$. Resta portanto analisar o caso em que $[a, v] = v^4 = [b, v]$. Neste caso, $[ab, v] = 1$ e assim $A = \langle ab \rangle Z_2(G)$ e $B = \langle b \rangle$ são abelianos tais que $G = AB$.

Isto encerra este caso.

(ii) $Z_2(G) = C_2 \oplus C_4 = \langle u \rangle \oplus \langle v \rangle$: Aqui temos quatro diferentes possibilidades para $Z(G)$: $\langle u \rangle$, $\langle v^2 \rangle$, $\langle v \rangle$ e $\langle u \rangle \times \langle v^2 \rangle$ (os casos $\langle uv^2 \rangle$ e $\langle uv \rangle$ são análogos a $\langle u \rangle$ e $\langle v \rangle$, respectivamente).

1. $Z(G) = \langle u \rangle$: Temos $[a, v], [b, v] \in Z(G) = \{1, u\}$. Procede-se como em $(b)(i)2$.
2. $Z(G) = \langle v^2 \rangle$: Temos que $[a, v], [b, v], [a, u], [b, u] \in Z(G) = \{1, v^2\}$. A menos de trocarmos $[a, u]$ por $[ab, u]$ e $[a, v]$ por $[ab, v]$, podemos supor que $[a, u] = [a, v] = 1$, de onde $A = \langle a, u, v \rangle$ e $B = \langle b \rangle$ são abelianos tais que $G = AB$, ou $[a, u] = 1 = [b, v]$, de onde $A = \langle a, u \rangle$ e $B = \langle b, v \rangle$ são abelianos e $G = AB$.
3. $Z(G) = \langle v \rangle$: Note $[a, u] \in Z(G)$ e como $u^2 = 1$, segue que $1 = [a, u^2] = [a, u]^2$, o que implica que $[a, u] = 1$ ou $[a, u] = v^2$. Analogamente se mostra que $[b, u] = 1$ ou $[b, u] = v^2$. Como $[a, u] = v^2 = [b, u]$ implica $[ab, u] = 1$, podemos supor, a menos de trocar $[a, u]$ por $[ab, u]$, que $[a, u] = 1$. Assim, $A = \langle a, u \rangle$ e $B = \langle b, v \rangle$ são abelianos tais que $G = AB$.

4. $Z(G) = \langle u \rangle \times \langle v^2 \rangle$: Como observado em $(b)(i)1$, suporemos que $[a,b] = v$. Veja que $[a,v], [b,v] \in Z(G) = \{1, u, v^2, uv^2\}$. Se $[a,v] = 1$ (similarmente $[b,v] = 1$), então $A = \langle a \rangle Z_2(G)$ é abeliano e $G = A\langle b \rangle$. Se $[a,v] = [b,v] = u$ (ou qualquer outro elemento de ordem 2), então $[ab,v] = 1$ e portanto $G = \langle ab \rangle Z_2(G) \langle b \rangle$. Será suficiente analisar o caso em que $[a,v] = u$ e $[b,v] = v^2$. Suponhamos, por absurdo, que $a^2 \in Z(G)$, então

$$1 = \left[a^2, b\right] = [a,b]^a [a,b] = a^{-1}vav = vv^{-1}a^{-1}vav = v[v,a]v = v^2u,$$

o que é uma contradição. Portanto $a^2 \notin Z(G)$ e analogamente, $b^2 \notin Z(G)$. Logo, pelo Lema 3.1, $G = A\langle b \rangle$, onde $A = \langle a \rangle Z(G)$.

O que encerra este caso.

(iii) $Z_2(G) = C_2 \oplus C_2 \oplus C_2$: Neste caso temos $Z(G) = C_2$ ou $Z(G) = C_2 \oplus C_2$.

1. $Z(G) = C_2 \oplus C_2 = \langle z_1 \rangle \oplus \langle z_2 \rangle$: Escrevamos $Z_2(G) = \langle u \rangle \oplus \langle z_1 \rangle \oplus \langle z_2 \rangle$. Podemos assumir que $[a,b] = u$, já que $a^2 \in Z_2(G)$. Temos que $[a,u] \in Z(G)$. Se $[a,u] = 1$, então $G = A\langle b \rangle$, onde $A = \langle a \rangle Z_2(G)$ é abeliano. Seja $[a,u] \neq 1$. Se $a^2 \in Z(G)$, então, como $u^2 = 1$, segue que $u = u^{-1}$ e assim

$$\left[a^2, b\right] = [a,b]^a [a,b] = u^a u = a^{-1}u^{-1}au = [a,u],$$

o que é uma contradição. Logo $a^2 \notin Z(G)$ e pelo Lema 3.1, $G = A\langle b \rangle$, onde $A = \langle a \rangle Z(G)$ é abeliano.

2. $Z(G) = C_2 = \langle z \rangle$: Escrevamos $Z_2(G) = \langle u \rangle \oplus \langle v \rangle \oplus \langle z$. Podemos supor, sem perda de generalidade, que $[a,b] = u$. Veja que $[a,u], [b,u], [a,v], [b,v] \in Z(G) = \{1, z\}$. A menos de trocarmos $[a,u]$ por $[ab,u]$, caso $[a,u] = z = [b,u]$ e $[a,v]$ ou $[b,v]$ por $[ab,v]$, caso $[a,v] = z = [b,v]$, será suficiente considerarmos os casos em que $[a,u] = 1$ e ou $[a,v] = 1$, ou $[b,v] = 1$. Se $[a,v] = 1$, então $A = \langle a \rangle Z_2(G)$ é abeliano e $G = A\langle b \rangle$. Se $[b,v] = 1$ e $[a,v] = z$, então $A = \langle a,u,z \rangle$ e $B = \langle b,v \rangle$ são abelianos tais que $G = AB$.

Como pretendíamos.

(iv) $Z_2(G) = Q_8 = \langle u, v \mid u^4 = 1, u^2 = v^2 = z, u^v = u^{-1} \rangle$: Neste caso, $Z(G) = Z(Q_8) = \langle z \rangle$. Sem perda de generalidade, suponhamos que $[a,b] = u$. Se $[a,u] = z = [b,u]$, então $[ab,u] = 1$, de onde podemos supor que $[a,u] = 1$. Seja $[b,u] = z$. Se $[b,v] = z$, então $[b,uv] = 1$ e uv cumpre o mesmo papel de v, assim podemos supor que $[b,v] = 1$. Por isso, $A = \langle a,u \rangle$ e $B = \langle b,v \rangle$ são abelianos tais que $G = AB$. Se tivermos $[b,u] = 1$ e $[b,v] = z = [a,v]$, então $[ab,v] = 1$ e $A = \langle a,u \rangle$ e $B = \langle ab,v \rangle$ são abelianos tais que $G = AB$.

(v) $Z_2(G) = D_4 = \langle u, v \mid u^4 = 1 = v^2, vuv = u^{-1} \rangle$: Observe que $Z(G) = Z(D_4) = \langle u^2 = z \rangle$. Como $[a,u], [b,u], [ab,u], [a,v], [b,v], [ab,v] \in Z(G) = \{1, z\}$, podemos assumir sem perda de generalidade que $[a,u] = 1$ e um dos elementos $[a,v]$, $[b,v]$ é igual a 1. Se $[b,v] = 1$, então $A = \langle a,u \rangle$ e $B = \langle b,v \rangle$ são abelianos e $G = AB$. Basta considerar os casos: se $[a,v] = 1 = [a,u]$ e $[b,v] = z$, podemos assumir que $[b,u] = z$ (caso contrário, se $[b,u] = 1$, então $G = AB$ para $A = \langle a,v \rangle$ e $B = \langle b,u \rangle$). Então $[b,uv] = 1$ e $G = AB$, onde $A = \langle a,u \rangle$ e $B = \langle b,uv \rangle$ são abelianos. □

Lema 3.28. *Seja G um grupo de ordem 32 com comprimento nilpotente igual a 4, então G admite decomposição abeliana.*

Demonstração. Sejam

$$\{1\} = Z_0(G) \subsetneq Z(G) = Z_1(G) \subsetneq Z_2(G) \subsetneq Z_3(G) \subsetneq Z_4(G) = G$$

e

$$\{1\} = G^{(5)} \subsetneq G^{(4)} \subsetneq G^{(3)} \subsetneq G' = G^{(2)} \subsetneq G^{(1)} = G$$

as respectivas séries centrais superior e inferior. Repare que pelos Lemas 3.23 e 3.24 temos $G^{(2)} = Z_3(G)$, $G^{(3)} = Z_2(G)$ e $G^{(4)} = Z_1(G)$. Do Teorema de Lagrange e o do fato de as inclusões serem estritas, temos que

$$Z_1(G) = \langle z \rangle,\ Z_2(G) = \langle v \rangle Z_1(G),\ Z_3(G) = \langle u \rangle Z_2(G) \text{ e } G/Z_3(G) = \langle \overline{a} \rangle \oplus \langle \overline{b} \rangle.$$

Mais explicitamente, além disso, temos

$$Z_1(G) \cong C_2,\ Z_2(G)/Z_1(G) = \langle v \rangle \cong C_2,\ Z_3(G)/Z_2(G) = \langle u \rangle \cong C_2 \text{ e } G/Z_3(G) \cong C_2 \oplus C_2.$$

Repare que usamos o fato de $G/Z_3(G)$ ser o centro de um grupo e portanto abeliano. Note também que não é preciso considerarmos o caso em que $G/Z_3(G)$ é cíclico, pois isto levaria a mesma contradição citada na demonstração do lema anterior. Não obstante, resta o caso em que $|Z_3(G)| = 8$, de onde da classificação dos grupos de ordem 8, devemos considerar cinco possibilidades para $Z_3(G)$. Analisaremos cada uma delas.

Antes de começarmos a tratar especificamente de cada possível estrutura para $Z_3(G)$, façamos algumas considerações gerais. Inicialmente, note que devido a $Z_1(G)$ e $Z_2(G)$ estarem contidos em $Z_3(G)$, ao determinarmos a estrutura deste último, determinamos também a dos dois primeiros. Observe também que podemos supor, sem perda de generalidade, que $[a,b] = u$. Usaremos inúmeras vezes o fato de que $h \in Z_{i+1}(G)$ se, e somente se, $[g,h] \in Z_i(G)$, para qualquer $g \in G$. Como $[a,v], [b,v] \in Z_1(G) = \{1, z\}$, temos que se $[a,v] = z = [b,v]$, então $[ab,v] = 1$, portanto, também podemos assumir,

sem perda de generalidade, que $[a, v] = 1$.

Sendo $[a, v] = 1$, $[a, Z_2(G)] = \{1\}$, e por isso $A = \langle a\rangle Z_2(G)$ é abeliano. Se $a^2 \notin Z_2(G)$, então $|A| = 16$ e $G = AB$ (onde $B = \langle b\rangle$). Deste modo, recapitulando, assumiremos daqui em diante que

$$a^2 \in Z_2(G) = \langle z, v\rangle = G^{(3)},\ [a, b] = u,\ [a, v] = 1.$$

(*a*) $Z_3(G) \cong D_4$: Neste caso, temos duas possibilidades para $Z_2(G)$ dependendo da estrutura de $Z_3(G)$, a saber

$$(1):\ Z_3(G) = \langle u, v \mid u^4 = 1 = v^2, u^2 = z, [u, v] = z\rangle$$

ou

$$(2):\ Z_3(G) = \langle u, v \mid v^4 = 1 = u^2, v^2 = z, v^u = v^{-1}\rangle.$$

Veja que em qualquer dos casos acima, vale que $u^2 \in Z_1(G)$. Temos que $[a, u], [b, u] \in Z_2(G) = \{1, z, v, zv\}$. Se $[a, u] = 1$ (ou $[b, u] = 1$), então $G = \langle a, v, u\rangle\langle b, z\rangle$ (ou $G = \langle a, v, z\rangle\langle b, u\rangle$). Se $[a, u] = z = [b, u]$, então $[ab, u] = 1$ e $G = \langle ab, v, u\rangle\langle b, z\rangle$. Assim, se $[a, u] = z$ basta considerar $[b, u] \neq z$. Estamos assumindo que $a^2 \in Z_2(G)$, portanto $[a^2, b] \in Z_1(G)$ e

$$\left[a^2, b\right] = [a, b]^a [a, b] = a^{-1}uau = \begin{cases} a^{-1}u^{-1}ua = [a, u] \\ a^{-1}uzzua = za^{-1}u^{-1}ua = z[a, u] \end{cases}$$

Acima consideramos os casos (1) e (2), onde em (1) temos $u = u^{-1}$ e em (2) temos $u^{-1} = uz$. De todo modo, segue $[a, u] \in Z(G)$, portanto teremos que $[b, u] \in \{v, zv\}$. Mas

$$1 = \left[b, u^2\right] = [b, u]\,[b, u]^u = vv^u \Rightarrow v^u = v^{-1}.$$

Logo, devemos ter necessariamente $Z_3(G)$ do tipo (2). Porém, vejamos que isto também leva a um absurdo. Se $b^2 \in Z_2(G)$, então $[a, b^2] \in Z(G)$ e por isso $[a, b^2] = uu^b = u^{-1}b^{-1}ub = [u, b]$, uma contradição, já que $[b, u] \notin Z_1(G)$. Por isso, $b^2 \notin Z_2(G)$. Assumamos, portanto, que $b^2 = u$. Daí, por um lado, $[a, b^2] = [a, u] \in Z_1(G)$. Por outro lado, $[a, b^2] = uu^b = [u, b] \notin Z_1(G)$, uma contradição. concluímos que não podemos ter $Z_3(G) \cong D_4$.

(*b*) $Z_3(G) \cong Q_8 = \langle u, v \mid u^4 = 1, v^2 = u^2 = z, [v, u] = z\rangle$: Fazendo contas análogas as feitas acima quando consideramos o caso (2), vemos que do fato de $[a^2, b] \in Z_1(G)$ vem que $[a, u] \in Z_1(G) = \{1, z\}$. Como $Z_3(G) = G^{(2)} = \langle v\rangle$, podemos supor que $[b, u] = v$. Se $b^2 \in Z_2(G)$, então $[a, b^2] \in Z_1(G)$ e assim como antes

$[a, b^2] = uu^b = uzzu^b = zu^{-1}b^{-1}ub = z\,[u, b] = zv^{-1} \notin Z_1(G)$, contradição. Então, $b^2 \notin Z_2(G)$, isto é, $b^2 \in \{u, u^{-1}, uv, u^{-1}v\}$. Uma vez que $[b, u] = v \neq 1$, concluímos que $b^2 = uv$ ou $b^2 = u^{-1}v$ e $G = AB$, onde $A = \langle a\rangle Z_2(G)$ e $B = \langle b\rangle$ são abelianos.

(*c*) $Z_3(G) = \langle u\rangle \cong C_8, v = u^2, z = u^4$: Como $u^2 = v$ e $[a, v] = 1$, temos que

$$1 = \left[a, u^2\right] = [a, u]\,[a, u]^u = [a, u]^2.$$

Como $[a, u] \in Z_2(G) = \{1, u^2, u^4, u^6\}$, segue que $[a, u] \in \{1, u^4\}$. Se $[a, u] = 1$, então $A = \langle a\rangle Z_3(G)$ é abeliano e $G = A\langle b\rangle$. Assim, resta analisar o caso em que $[a, u] = u^4$. Mas isto implica que $u^a = a^{-1}ua = u\,[u, a] = uu^4 = u^5$. Por outro lado,

$$\left[a^2, b\right] = u^a u = u^5 u = u^6 \notin Z_1(G),$$

o que é uma contradição, pois $[a^2, b] \in Z_1(G)$.

(*d*) $Z_3(G) = \langle u\rangle \oplus \langle v\rangle \oplus \langle z\rangle \cong C_2 \oplus C_2 \oplus C_2$: Temos que $[b, v] \in Z_1(G) = \{1, z\}$, de onde podemos supor que $[b, v] = z$ (POR QUÊ? $[b, v] = 1$ não resolve e não dá o absurdo pretendido). Além disso, $[a^2, b] \in Z_1(G)$ e $[a^2, b] = u^a u = [a, u]$, já que $u^2 = 1$. Assim, se $[a, u] = 1$, então $A = \langle a\rangle Z_3(G)$ é abeliano e $G = A\langle b\rangle$. Se $[a, u] = z$, podemos supor que $[b, u] = v$ (o caso $[b, u] = zv$ daria na mesma, a justificativa é dada em (*a*)). Repare também que $o(\overline{b}) = 2$ implica que $b^2 \in Z_3(G)$ (que é abeliano), logo

$$1 = \left[b^2, u\right] = [b, u]^b\,[b, u] = v^b v = [b, v] = z,$$

o que é uma contradição.

(*e*) Seja

$$C_4 \oplus C_2 \cong Z_3(G) = \begin{cases} \langle u\rangle \oplus \langle z\rangle,\ u^2 = v\ (1) \\ \langle u\rangle \oplus \langle v\rangle,\ u^2 = z\ (2) \\ \langle v\rangle \oplus \langle u\rangle,\ v^2 = z\ (3) \end{cases}$$

Temos, assim como nos casos anteriores, que $[a^2, b] \in Z_1(G)$ e $[a^2, b] = u^a u$. No caso (2), $u^{-1} = uz$ e por isso $[a^2, b] = ua^{-1}ua = zuza^{-1}ua = z\,[u, a]$, de onde $[a, u] = [u, a]^{-1} \in Z_1(G)$. No caso (3), vale que $u^{-1} = u$ e por isso $[a^2, b] = [a, u] \in Z_1(G)$. Nestes dois casos, $[a, u] = 1$ ou $[a, u] = z$. Podemos assumir que $[b, u] = v$ e $[b, v] = z$. Se $[a, u] = 1$, então $G = \langle a, u, v\rangle\langle b, z\rangle$. Seja $[a, u] = z$. Como $b^2 \in Z_3(G)$ (que é abeliano), $1 = [b^2, u] = [b, u]^b\,[b, u] = v^b v$. Se $o(v) = 2$, então $1 = v^b v = [b, v] = z$, uma contradição. Portanto, $o(v) = 4$ e devemos ter $Z_3(G)$ do tipo (3).
Assim como em (*a*), $b^2 \notin Z_2(G)$, pois se $b^2 \in Z_2(G)$ teríamos $[b, u] = v \in Z_1(G)$. Além disso, podemos supor que $b^2 = u$, daí $[a, u] = [a, b^2] = u^b u = [u, b] = v^{-1}$, uma

contradição, pois $[a,u] \in Z_1(G)$.

Agora vejamos o caso em que $[a,u] \notin Z_1(G)$ e como vimos anteriormente, isto implica que $Z_3(G)$ é do tipo (1). Podemos assumir que $[a,u] = v$ e $[b,v] = z$ (as contas seriam análogas nos demais casos). Se $[b,u] = 1$, então $G = (\langle a \rangle Z_2(G)) \langle b,u \rangle$. Se $[b,u] = z$, então $[b,vu] = [b,u]\,[b,v]^u = zz^u = z^2 = 1$, de onde $G = AB$ onde $A = \langle a \rangle Z_2(G)$ e $B = \langle b, vu \rangle$. Se $[b,u] = v$, então $[ab,u] = [a,u]^b\,[b,u] = v^b v = b^{-1}vbv = b^{-1}bvzv = v^2 z = z^2 = 1$. Logo, $G = (\langle a \rangle Z_2(G)) \langle ab,u \rangle$. O caso em que $[b,u] = vz$ é imediato dos feitos acima.

□

Lema 3.29. *Sejam G um grupo nilpotente e p um número primo tal que ordem de G é $p^m \geq p^2$. Então:*

1. *O comprimento nilpotente de G é no máximo $m-1$.*
2. *Se G tem comprimento nilpotente n então $(G : Z_{n-1}(G)) \geq p^2$.*
3. *$(G : G') \geq p^2$.*

Demonstração. Inicialmente provaremos 2. Seja n o comprimento nilpotente dee G. Suponhamos por absurdo que $(G : Z_{n-1}(G)) = p$. Se $n = 1$ então $(G : Z_0(G)) = p$ e por isso $|G| = |Z_0(G)|(G : Z_{n-1}(G)) = p$, já que $Z_0(G) = e$. Isto é uma contradição com a hipótese quanto a ordem de G, portanto, $n \geq 2$ e

$$\frac{G/Z_{n-2}(G)}{Z(G/Z_{n-2}(G))} = \frac{G/Z_{n-2}(G)}{Z_{n-1}(G)/Z_{n-2}(G)} \cong G/Z_{n-1}(G)$$

é um grupo cíclico, pois possui ordem p. Consequentemente G/Z_{n-2} é abeliano e assim $Z_{n-1}(G)/Z_{n-2}(G) = Z((G/Z_{n-2}(G))) = G/Z_{n-2}(G)$, de onde $Z_{n-1}(G) = G$, o que é uma contradição. Isto conclui a prova de 2. Agora 3 decorre do Lema 3.24, pois $G' \subset Z_{n-1}$. Finalmente, como a série central superior possui n passos, segue que $p^m = |G| \geq p^{n+1}$, de onde $n \leq m-1$ e a condição 1 é satisfeita. □

Teorema 3.30. *Qualquer grupo de ordem* 32 *pode ser escrito como produto de dois grupos abelianos.*

Demonstração. Do Lema 3.29, sabemos que o comprimento nilpotente de um grupo de ordem p^n, $n \geq 2$ e p primo, é um inteiro entre 1 e $n-1$. No caso em questão, entre 1 e 4. Porém, observe que se o comprimento nilpotente de G fosse 1, teríamos $G = Z(G)$, de onde G seria abeliano e admitiria a decomposição abeliana trivial. Deste modo, este resultado decorre dos lemas anteriormente provados. □

Proposição 3.31. *Existe um grupo G tal que $Z(G)$ e $G/Z(G)$ são grupos abelianos elementares de ordem* 8*, mas G não admite decomposição abeliana.*

Demonstração. Consideremos um 2-grupo abeliano elementar N gerado por z_1, z_2, z_3 e um 2-grupo abeliano elementar H gerado por $\overline{x}_1$, $\overline{x}_2$ e $\overline{x}_3$. Queremos construir uma extensão G com $N = Z(G) \lhd G$ e $G/N \cong H$, tal que para certas imagens inversas x_1, x_2, x_3 de $\overline{x}_1$, $\overline{x}_2$, $\overline{x}_3$, respectivamente, as seguintes relações sejam satisfeitas:

$$x_i^2 = z_i^2 = e, \;\; i = 1, 2, 3; \;\; [x_i, z_j] = [z_i, z_j] = e, \;\; i, j = 1, 2, 3; \tag{9}$$

$$[x_i, x_j] = z_{i+j-2}, \;\; i \neq j \in \{1, 2, 3\}. \tag{10}$$

Dados os grupos N e H como acima, suponhamos termos feito uma escolha de representantes que satisfaçam as relações acima. Tomando os automorfismos, requeridos nas hipóteses do Teorema 3.19, de N como aplicações identidade e o conjunto quociente definido por:

$$\left(\overline{x}_1^{k_1}\overline{x}_2^{k_2}\overline{x}_3^{k_3}, \overline{x}_1^{r_1}\overline{x}_2^{r_2}\overline{x}_3^{r_3}\right) = z_1^{r_1k_2} z_2^{r_1k_3} z_3^{r_2k_3}, \;\; \forall \; k_i, r_j \in \mathbb{F}_2, \;\; i, j = 1, 2, 3, \tag{11}$$

temos as condições do Teorema de Schreier são satisfeitas. Com efeito, a primeira condição é obviamente satisfeita, já que os automorfismos foram definidos como aplicações identidades. Quanto a segunda condição, sejam $\overline{u} = \overline{x}_1^{k_1}\overline{x}_2^{k_2}\overline{x}_3^{k_3}$, $\overline{v} = \overline{x}_1^{r_1}\overline{x}_2^{r_2}\overline{x}_3^{r_3}$ e $\overline{w} = \overline{x}_1^{s_1}\overline{x}_2^{s_2}\overline{x}_3^{s_3}$. Primeiramente repare que como os geradores de N e os representantes escolhidos comutam, vale que $(\overline{u}, \overline{v})^{\overline{w}} = w^{-1}\,(\overline{u}, \overline{v})\, w = (\overline{u}, \overline{v})$. Portanto, usando (11), temos

$$(\overline{uv}, \overline{w})\,(\overline{u}, \overline{v})^{\overline{w}} = z_1^{s_1(k_2+r_2)+r_1k_2} z_2^{s_1(k_3+r_3)+r_1k_3} z_3^{s_2(k_3+r_3)+r_2k_3}.$$

Por outro lado,

$$(\overline{u}, \overline{vw})\,(\overline{v}, \overline{w}) = z_1^{k_2(r_1+s_1)+s_1r_2} z_2^{k_3(r_1+s_1)+s_1r_3} z_3^{k_3(r_2+s_2)+s_2r_3}.$$

Assim, segue que $(\overline{uv}, \overline{w})\,(\overline{u}, \overline{v})^{\overline{w}} = (\overline{u}, \overline{vw})\,(\overline{v}, \overline{w})$. Portanto, seja G a extensão garantida pelo Teorema de Schreier satisfazendo as condições acima descritas. Mostraremos que G não contém um subgrupo abeliano com mais que $2^4 = 16$ elementos, de onde decorrerá que se $G = AB$, para dois subgrupos abelianos A, B (podemos supor que estes subgrupos contêm o centro de G que possui 2^3 elementos), então $2^6 = |G| = |AB| = |A||B|/|A \cap B| \leq 2^4 2^4/2^3 = 2^5$, o que será uma contradição. De fato, suponhamos que A seja um subgrupo abeliano de G. Podemos supor que $Z(G) \subset A$, a menos de seguirmos na prova com $Z(G)A$. Dados $a, b \in A$, podemos escrever $a = x_1^{k_1}x_2^{k_2}x_3^{k_3}z$, $b = x_1^{r_1}x_2^{r_2}x_3^{r_3}z'$, onde $z, z' \in Z(G)$, $k_i, r_i \in \mathbb{F}_2$, $i = 1, 2, 3$. Além disso, $ab = ba$ é equivalente a $(a, b) = (b, a)$, de onde segue que

$$z_1^{r_1k_2} z_2^{r_1k_3} z_3^{r_2k_3} = z_1^{k_1r_2} z_2^{k_1r_3} z_3^{k_2r_3}.$$

Ora, mas isto significa que todos os determinantes das submatrizes quadradas da matriz

$$\begin{pmatrix} k_1 & k_2 & k_3 \\ r_1 & r_2 & r_3 \end{pmatrix}$$

sobre $\mathbb{F}_2$ são nulos, ou seja, essa matriz possui posto menor que 2. Mas sobre $\mathbb{F}_2$ isto significa que uma das linhas é nula (e neste caso, $a \in Z(G)$ ou $b \in Z(G)$), ou ambas coincidem (o que implica $aZ(G) = bZ(G)$). Note que isto nos garante que $(A : Z(G)) \leq 2$, onde $(A : Z(G))$ denota o índice de $Z(G)$ em A, de onde $|A| = |Z(G)|\,(A : Z(G)) \leq 2^3 2 = 2^4$. □

Existem 19 grupos de ordem 2^6 não possuindo decomposição abeliana, porém escolhemos o grupo descrito na demonstração da proposição acima por suas propriedades interessantes, por exemplo, ele possui comprimento nilpotente 2 e seu expoente é igual a quatro (ambos os valores são os menores possíveis). Este exemplo prova que a recíproca do resultado de Ito não é válida. De fato, este grupo é metabeliano, mas não possui decomposição abeliana.

Note que não segue da Proposição 3.17 que existem S_4-códigos não abelianos sobre algum corpo. Não obstante, forneceremos um exemplo abaixo. Até o fim desta seção fixaremos $F = \mathbb{Z}_5$ e $G = S_4$, visto como grupo das permutação do conjunto $\{0, 1, 2, 3\}$. A conhecida teoria de diagramas de Young (ver, por exemplo, CURTIS and REINER (1966) mostra que o anel de grupo $R = FG$ contém cinco ideais minimais (bilaterais), gerados pelos seguintes elementos centrais:

$$\begin{aligned}
e_0 &= -\sum_{g\in G} g, \quad e_4 = -\sum_{g\in G} (-1)^g g, \\
e_1 &= 2(3e - (0\,1)(2\,3) - (0\,2)(1\,3) - (0\,3)(1\,2) \\
&\quad + (0\,1) + (0\,2) + (0\,3) + (1\,2) + (1\,3) + (2\,3) \\
&\quad -(0\,1\,2\,3) - (0\,2\,1\,3) - (0\,2\,3\,1) \\
&\quad -(0\,3\,2\,1) - (0\,3\,1\,2) - (0\,1\,3\,2)), \\
e_2 &= e + (0\,1)(2\,3) - (0\,2)(1\,3) + (0\,3)(1\,2) \\
&\quad - 3(0\,1\,2) - 3(0\,1\,3) - 3(0\,2\,3) - 3(1\,2\,3) \\
&\quad - 3(0\,2\,1) - 3(0\,3\,1) - 3(0\,3\,2) - 3(1\,3\,2), \\
e_3 &= 2(3e - (0\,1)(2\,3) - (0\,2)(1\,3) - (0\,3)(1\,2) \\
&\quad - (0\,1) - (0\,2) - (0\,3) - (1\,2) - (1\,3) - (2\,3) \\
&\quad + (0\,1\,2\,3) + (0\,2\,1\,3) + (0\,2\,3\,1) \\
&\quad + (0\,3\,2\,1) + (0\,3\,1\,2) + (0\,1\,3\,2)).
\end{aligned}$$

Com base nestes fatos, podemos provar o seguinte resultado.

Teorema 3.32. *Os códigos $K(Re_1)$ e $K(Re_3)$ não são abelianos, enquanto que $K(Re_0)$, $K(Re_2)$ e $K(Re_4)$ são abelianos.*

Demonstração. Provaremos que $K(Re_0)$, $K(Re_2)$ e $K(Re_4)$ são abelianos, porém, a prova de que os demais códigos são não abelianos foi feita computacionalmente e foge do escopo desta dissertação. Os detalhes podem ser encontrados em PILLADO *et al.* (2013).
Inicialmente, note que

$$\begin{aligned}\left(\sum_{h\in G} a_h h\right) e_0 &= \left(\sum_{h\in G} a_h h\right)\left(-\sum_{g\in G} 1g\right) = -\sum_{h,g\in G} a_h hg = -\sum_{x\in G}\left(\sum_{hg=x} a_h\right) x \\ &= \left(\sum_{y\in G} a_y\right)\left(-\sum_{x\in G} 1\cdot x\right) = ae_0,\end{aligned}$$

para $a = \sum_{y\in G} a_y \in F$. Isto mostra que $Re_0 = Fe_0$. De modo análogo, mostra-se que $Re_4 = Fe_4$. Se considerarmos $\sigma \in S_G$ de ordem 24 e tal que σ leva permutações ímpares em pares e vice-versa, teremos que $e_0^\sigma = \sum_{\sigma(g)\in G}\sigma(g) = e_0$ e $e_4^\sigma = -\sum_{\sigma(g)\in G}(-1)^{\sigma(g)}\sigma(g) = -e_4$. Isto, aliado ao fato de σ fixar os elementos de F, mostra que $\sigma \in \mathrm{PAut}(Re_0 = Fe_0)$ e $\sigma \in \mathrm{PAut}(Re_4 = Fe_4)$. Como estes são subgrupos de S_G, segue que $H = \langle\sigma\rangle$ é subconjunto de ambos. De modo a generalizar a definição de subgrupo transitivo, podemos dizer que um subgrupo H de S_G é regular se $|H| = |G|$ e para qualquer $\sigma \in H \setminus \{Id\}$, vale que $\sigma(g) \neq g$, para qualquer $g \in G$. Veja que H é subgrupo regular S_G. De fato, vale que $|H| = |G| = 24$ e $\sigma^i(g) \neq g$, para $1 \leq i \leq 23$, já que $o(\sigma) = 24$. Assim, a partir do Corolário 3.9, temos que os códigos $K(Re_0)$ e $K(Re_4)$ são abelianos.
Para provarmos que $K(Re_2)$ determina um código abeliano, consideremos o subgrupo de Klein $K = V_4 \subset S_4 = G$ e escrevamos G como união das classes laterais módulo K:

$$G = Ka_0 \cup Ka_1 \cup \cdots \cup Ka_5,$$

onde a_i são representantes das classes de modo que $(-1)^{a_i} = (-1)^i$, $i \in \{0,\ldots,5\}$. Seja $\sigma_0 \in S_G$ um elemento de ordem quatro fixado. Consideremos os elementos σ e τ em S_G tais que $\sigma(xa_i) = (xa_i)^\sigma = x^{\sigma_0}a_i$ e $\tau(xa_i) = (xa_i)^\tau = xa_{i(\mathrm{mod}6)}$, para qualquer $x \in K$ e para qualquer $i \in \{0,\ldots,5\}$. Note que $o(\sigma) = 4$, $o(\tau) = 6$ e $\sigma\tau = \tau\sigma$, pois $\sigma\tau(xa_i) = \sigma(xa_{i(mod6)}) = x^{\sigma_0}a_{i(mod6)} = \tau(x^{\sigma_0}a_i) = \tau\sigma(xa_i)$. Deste modo, $H = \langle\sigma,\tau\rangle$ é um subgrupo abeliano de S_G com $|H| = |G| = 24$. Além disso, é imediato ver que se $\alpha \in H\setminus\{Id\}$, então $\alpha(g) = \alpha(xa_i) \neq xa_i = g$, para um certo $x \in K$ e um algum $0 \leq i \leq 5$. Logo, H é um subgrupo regular abeliano de S_G. Foi provado computacionalmente que $H \subset \mathrm{PAut}(Re_2)$, de onde mais uma vez pelo Corolário 3.9, $K(Re_2)$ é um código de grupo

abeliano. □

3.3 Mudança de corpo base

Nesta seção, estudaremos se dados um subcorpo finito F de um corpo finito E e um grupo finito G, e supormos que qualquer G-código sobre E é abeliano, então todo G-código sobre F é abeliano e vice versa, se todo G-código sobre F é abeliano, então todo G-código sobre E é também abeliano. Daremos uma resposta afirmativa a primeira pergunta e parcial a segunda.

O próximo lema afirma que alguns ideais nos anéis de grupo EG e FG possuem os mesmos grupos de automorfismos de permutação.

Lema 3.33. *Se F é um subcorpo do corpo E e I é um ideal do anel de grupo FG, então EI é um ideal em EG e* $\mathrm{PAut}(I) = \mathrm{PAut}(EI)$.

Demonstração. Sejam $B = \{e_1, e_2, \ldots, e_k\}$ uma base de E sobre F e $|G| = n$. Para qualquer ideal I de FG, vale que $EI = \sum_{i=1}^{k} e_i I$. De fato, para provarmos isto escrevamos

$$G = \{g_1 = e, g_2, \ldots, g_n\},$$

e assim, para $a \in FG$, temos $a = \sum_{i=1}^{n} a_i g_i$, com $a_i \in F$. Dados $\sum_{i=1}^{k} b_i e_i \in E$ (aqui usamos o fato de B ser base) onde $b_i \in F$ e $x \in I$, vale que

$$\left(\sum_{i=1}^{k} b_i e_i\right) x = \sum_{i=1}^{k} e_i (b_i x) = \sum_{i=1}^{k} e_i x_i,$$

onde $x_i = b_i x \in I$, já que I é ideal de FG. Além disso, note que EI é ideal de EG, o que decorre diretamente de I ser ideal de FG, e que $EI \cap FG = I$, já que $EI = \sum_{i=1}^{k} e_i I$ e $I \subset FG$. Dado $\sigma \in \mathrm{PAut}(I)$, σ se estende a uma aplicação E-linear em EG. Se $x = \sum_{i=1}^{k} e_i x_i \in EI$, então

$$\sigma(x) = \sum_{i=1}^{k} e_i \sigma(x_i) \in EI,$$

uma vez que $\sigma(x_i) \in I$, onde $i \in \{1, \ldots, k\}$. Isto mostra que $\mathrm{PAut}(I) \subseteq \mathrm{PAut}(EI)$.

Reciprocamente, seja $\tau \in \mathrm{PAut}(EI)$. Novamente consideraremos τ como uma aplicação E-linear sobre EG. Como τ age sobre G, $\tau(FG) = FG$, então

$$\tau(I) = \tau(EI \cap FG) = \tau(EI) \cap \tau(FG) = EI \cap FG = I.$$

Isto mostra que $\mathrm{PAut}(EI) \subseteq \mathrm{PAut}(I)$, de onde $\mathrm{PAut}(I) = \mathrm{PAut}(EI)$. □

Teorema 3.34. *Sejam F um subcorpo de um corpo E e G um grupo. Se todos os G-códigos sobre E são abelianos, então todos os G-códigos sobre F são abelianos.*

Demonstração. Para qualquer ideal I de FG, pelo Lema anterior, $\mathrm{PAut}(I) = \mathrm{PAut}(EI)$, onde EI é ideal de EG. Como $F \subset E$, podemos pensar em um G código sobre F como um G-código sobre E. Supondo que $C \subset F^n \subset E^n$ seja um G-código associado a I e já o identificando com o ideal bilateral EI de EG, temos pelo Corolário 3.9, que $\mathrm{PAut}(EI)$ contém um subgrupo regular abeliano. Do fato de que o mesmo é válido para $\mathrm{PAut}(I) = \mathrm{PAut}(EI)$, pelo Lema anterior, aplicando o Corolário 3.9 uma vez mais, temos que I é um código abeliano. □

O teorema anterior é a resposta afirmativa a primeira questão colocada no início da seção. O próximo teorema dá uma resposta parcial à segunda questão.

Antes de enunciarmos o próximo resultado, relembremos a definição de Produto Tensorial. Sejam R um anel, M um R-módulo à direita, N um R-módulo à esquerda e A um grupo abeliano com operação aditiva. Uma aplicação $f\colon M \times N \to A$ é dita uma *aplicação balanceada* se satisfaz

1. $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$;
2. $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$;
3. $f(m, rn) = f(mr, n)$,

para quaisquer $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $r \in R$. O produto tensorial de módulos é usualmente definido via uma propriedade universal.

Definição 3.35. *Sejam M, N e R como acima. Um grupo abeliano T, juntamente com uma aplicação balanceada $\phi\colon M \times N \to T$ é dito um produto tensorial de M e N se as seguintes propriedades valem:*

(i) Os elementos da forma $\phi(m, n)$, $m \in M$, $n \in N$ geram T (como um grupo aditivo).

(ii) Para qualquer grupo abeliano A e qualquer aplicação balanceada $f\colon M \times N \to A$, existe uma aplicação $f^*\colon T \to A$ tal que $f = f^* \circ \phi$.

Mostra-se, vide MILIES and SEHGAL (2002), que o Produto Tensorial existe e é único. Nas notações acima, escrevemos $T = M \otimes_R N$.

Lema 3.36. *Sejam R, S anéis com $R \subset S$ e com o mesmo elemento identidade. Se G é um grupo, então $SG \cong S \otimes_R RG$.*

Demonstração. Sejam $S \otimes_R RG$ e $\phi\colon S \times RG \to S \otimes_R RG$ o produto tensorial de S e RG. Definamos $f\colon S \times RG \to SG$ a aplicação dada por $f(s, \sum_{g\in G} r_g g) = \sum_{g\in G}(sr_g)g$. Pela propriedade universal do produto tensorial existe uma aplicação $f^*\colon S \otimes_R RG \to SG$ tal que $f = f^* \circ \phi$. Agora, tomando $\psi\colon SG \to S \otimes_R RG$ dada por $\psi(\sum_{g\in G} s_g g) = \sum_{g\in G}(s_g \otimes 1 \cdot g)$, temos um homomorfismo. Fazendo alguns cálculos vê-se que ψ é inversa

de f^*. Assim, o resultado segue. □

Teorema 3.37. *Sejam F um subcorpo de um corpo E e G um grupo. Suponha, adicionalmente, que* char$F \nmid |G|$ *e*

$$FG \cong \bigoplus_{i=1}^{k} M_{d_i}(F) \quad (*)$$

(a álgebra de grupo FG é uma soma direta de álgebras de matrizes sobre F). Sobre estas condições, se todo G-código sobre F é abeliano, então todo G-código sobre E é abeliano.

Demonstração. De modo análogo ao feito no Lema anterior, se pode mostrar que $E \otimes_F M_n(F) = M_n(E)$, para $n \geq 1$. Tendo em vista este fato, o lema anterior e as hipóteses do Teorema, temos que

$$EG = E \otimes_F FG = E \otimes_F \bigoplus_{i=1}^{k} M_{d_i}(F) = \bigoplus_{i=1}^{k} E \otimes_F M_{d_i}(F) = \bigoplus_{i=1}^{k} M_{d_i}(F).$$

Além disso, como qualquer anel de matrizes sobre um corpo é simples, segue que qualquer ideal J de EG pode ser escrito na forma $J = \bigoplus_{i \in S} M_{d_i}(E)$, onde $S \subset \{1, \cdots, k\}$. Não obstante disto, temos $J = EI$, onde $I = \bigoplus_{i \in S} M_{d_i}(F)$. A partir daqui a prova segue de forma análoga à do teorema anterior. □

Um corpo F satisfazendo a condição $(*)$ diz-se um corpo de decomposição para G. Adicionalmente, mostraremos a seguir que a condição $(*)$ é satisfeita para uma família infinita de corpos F, ou seja, G possui uma infinidade de corpos de decomposição.

Proposição 3.38. *Para qualquer primo p tal que $p \nmid n = |G|$, existe um número m tal que um corpo F, com $|F| = p^l$, satisfaz a condição $(*)$ do Teorema anterior se, e somente se, $m \mid l$.*

Demonstração. Seja $F_0 = \mathbb{Z}_p$ para um primo $p \nmid n = |G|$. Então, pelo Teorema 2.17, $F_0G \cong \bigoplus_{i=1}^{r} M_{d_i}(F_i)$, onde $F_1, \ldots, F_r$ são extensões de corpos de F_0. Como para qualquer corpo F tal que char$F = p$ (em particular para um corpo F onde $|F| = p^l$), encarando F como extensão de F_0, usando o último Lema e considerações similares as usadas na demonstração do Teorema anterior, vale que

$$FG = F \otimes_{F_0} F_0G = \bigoplus_{i=1}^{r} F \otimes_{F_0} M_{d_i}(F_i) = \bigoplus_{i=1}^{r} M_{d_i}(F \otimes_{F_0} F_i),$$

de onde segue que $(*)$ é equivalente a

$$F \otimes_{F_0} F_i \cong F \oplus F \oplus \cdots \oplus F, \ \forall\, i \in \{0, \ldots, r\},$$

onde o número de parcelas isomorfas a F é igual a $dim_{F_0}(F_i)$. O último isomorfismo

é válido se, e somente se, o polinômio minimal de um elemento primitivo em F_i sobre F_0 se decompõe sobre F (vide Exemplo 9.5 em PIERCE (1982)). Seja E o corpo de decomposição do produto dos polinômios minimais dos elementos primitivos de $F_1, \ldots, F_r$ sobre F_0, e $m = \dim_{F_0} E$, isto é, $|E| = p^m$. Então $(*)$ é equivalente a existir um isomorfismo de E para algum subcorpo E' de F, e tal isomorfismo existe se, e somente se, $m \mid l$. □

Agora, novamente ressaltaremos a diferença entre códigos de grupo e códigos de grupo à esquerda. Enquanto é aparentemente difícil determinar se a propriedade "todos G-códigos sobre um corpo F são abelianos" se mantém válida ao trocarmos F por uma extensão E, existe um exemplo mostrando que códigos de grupo à esquerda não possuem esta propriedade.

Proposição 3.39. *Sejam F o corpo $GF(2)$, $E = GF(2^2 = 4)$ sua extensão e $G = Q_8$ o grupo dos quatérnios. Então todos os G-códigos à esquerda sobre F são abelianos, mas existem G-códigos à esquerda sobre E que não são abelianos.*

Demonstração. A segunda parte da afirmação decorre, como mencionado na introdução, de COUSELO *et al.* (2004) tabela 6, onde é mostrado que existem $[8, 3, 5]$-códigos à esquerda em $\mathbb{F}_4 Q_8$ mas não existe um A-código abeliano sobre $\mathbb{F}_4$ com os mesmos parâmetros para qualquer grupo abeliano de ordem 8.

Para provar a primeira parte, ou seja, que todo G-código à esquerda sobre F é abeliano, será suficiente mostrar que todo ideal à esquerda de FG é um ideal bilateral, em vista do Teorema 3.10, já que Q_8 admite decomposição abeliana, pois sua ordem é o cubo de um número primo.

Poderemos considerar apenas ideais principais à esquerda, já que todo ideal à esquerda é uma soma de ideais principais à esquerda. Denotaremos os elementos de Q_8 por

$$e, i, j, k, \epsilon, \epsilon i, \epsilon j, \epsilon k,$$

ao invés da notação tradicional $\epsilon = -1$, para distinguir os elementos do grupo e do corpo. Denotaremos por $H = \{e, \epsilon\}$ o centro do grupo G. Uma vez que qualquer elemento em FG com suporte consistindo de um número ímpar de elementos é invertível em FG, de onde teríamos que o ideal gerado por esse elemento seria todo RG, logo bilateral. Portanto, basta considerarmos apenas os elementos de FG cujo suporte consiste de um número par de elementos de G. Ademais, podemos sempre supor que e pertence ao suporte de um elemento que gera um dado ideal à esquerda de FG, pois se $x \in \mathrm{Supp}(a)$, então $e \in \mathrm{Supp}(x^{-1}a)$.

Se um elemento de FG possui suporte com oito elementos, então, pela Pro-

posição 2.18, segue que este elemento é central e portanto gera um ideal bilateral.

Para os elementos de $FG = R$ com suporte consistindo de dois elementos, primeiramente note que $e+\epsilon$ anula qualquer comutador aditivo de elementos do grupo G, ou seja, $(xy-yx)(e+\epsilon) = 0$ para quaisquer $x, y \in G$. Então, qualquer ideal à esquerda L contido no ideal $R(e+\epsilon)$ é um ideal bilateral. Por outro lado, se L é um ideal à esquerda de R contendo $R(e+\epsilon)$, então pelo Teorema da Correspondência, L é imagem inversa do homomorfismo natural de R para $R/R(e+\epsilon)$. Como G/H é um grupo abeliano, pois $|G/H| = 4$, segue que $F(G/H)$ é um anel comutativo e como $R/R(e+\epsilon) \cong F(G/H)$, temos que L é na verdade a imagem inversa de um ideal bilateral, logo L é ideal bilateral. Considere agora $L = R(e+g)$, onde $g \in G \setminus H$. Então

$$(e+g)^2 = e^2 + 2g + g^2 = e + \epsilon,$$

logo, L contém $R(e+\epsilon)$ e pelo que foi comentado antes, L é um ideal bilateral. Isto encerra o caso cujo suporte contém dois elementos.

Se considerarmos elementos de FG com suporte consistindo de quatro elementos, incluindo e, existem três casos possíveis:

- (I) O suporte de um elemento u consiste de elementos das classes H, gH, onde $g \in G \setminus H$. Então $u = e+\epsilon+g+\epsilon g = (e+g)(e+\epsilon)$, ou seja, $u \in R(e+\epsilon)$ e pelo mesmo argumento comentado antes, Ru é um ideal bilateral de FG.
- (II) O suporte de um elemento u consiste de elementos de duas classes distintas de H. Sem perda de generalidade, podemos assumir que $u = e+\epsilon+i+j$, $(u = i+j+\epsilon i+\epsilon j = i+j+\epsilon(i+j) = (i+j)(e+\epsilon)$ e pelo que comentamos antes, teríamos Ru ideal bilateral) pois para quaisquer dois elementos $a, b \in G$ tais que $a, b, ab^{-1} \in H$ (ou seja, elementos que geram $G = Q_8$ e portanto não estão numa mesma classe) temos um automorfismo $f\colon G \to G$ tal que $f(i) = a$ e $f(j) = b$. Assim, as seguintes igualdades são válidas, como se pode verificar facilmente:

$$\begin{aligned}(e+\epsilon+i+j)i &= (e+j+\epsilon)(e+\epsilon+i+j),\\ (e+\epsilon+i+j)j &= (e+i+\epsilon)(e+\epsilon+i+j),\\ (e+\epsilon+i+j)k &= \epsilon k(e+\epsilon+i+j).\end{aligned}$$

  Isto mostra que dado $a \in R$, vale que $ua = bu \in R$, para algum $b \in R$. Logo Ru é ideal bilateral de R.
- (III) O suporte de um elemento u contém elementos de todas as classes de G módulo H. Devido aos automorfismos que citamos anteriormente, podemos supor que $u =$

$e+i+j+k$ ou $u = e+i+j+\epsilon k$. Mais uma vez, é simples verificar que as seguintes igualdades são válidas:

$$\begin{aligned}
(e+i+j+k)i &= j(e+i+j+k),\\
(e+i+j+k)j &= k(e+i+j+k),\\
(e+i+j+k)k &= i(e+i+j+k),\\
(e+i+j+\epsilon k)i &= \epsilon k(e+i+j+\epsilon k),\\
(e+i+j+\epsilon k)j &= i(e+i+j+\epsilon k),\\
(e+i+j+\epsilon k)k &= \epsilon j(e+i+j+\epsilon k).
\end{aligned}$$

Isto prova que Ru é ideal bilateral de R.

Resta apenas considerar apenas o caso em que um elemento u possui suporte consistindo de seis elementos. Podemos assumir, que $\epsilon \in \mathrm{Supp}(u)$, já que se $x \in \mathrm{Supp}(u)$ então $\epsilon \in \mathrm{Supp}(\epsilon x^{-1}u)$. Assim, estamos supondo que $e, \epsilon \in \mathrm{Supp}(u)$. Pelos automorfismos que citamos em (II), podemos supor sem perda de generalidade que $u = e+\epsilon+i+\epsilon i+j+\epsilon j = (e+i+j)(e+\epsilon)$, de onde temos que $u \in R(e+\epsilon)$ e como vimos anteriormente, isto implica que Ru é ideal bilateral.

Suponhamos agora que $u = x+\gamma$, onde x é um elemento cujo suporte consiste de oito elementos e $\gamma \in \{i+j, \epsilon i+\epsilon j, i+\epsilon j\}$ (sem perda de generalidade, usando os automorfismos supracitados). Observe que $xz = 0$ para qualquer elemento z com suporte consistindo de um número par de elementos, o que implica que $\gamma u = \gamma^2 = (e+\epsilon)g$, para algum $g \in G$. Por isso, $R(e+\epsilon) \subset R\gamma$ e, pelo que foi antes visto, $R\gamma$ é um ideal bilateral de R. Como $x \in Z(R)$, pois possui suporte com 8 elementos, segue que Ru é ideal bilateral de R. $\square$

4 CONCLUSÃO

Uma dos principais propostas desta dissertação era a de responder quando um código de grupo é um código de grupo abeliano. A resposta a esta pergunta para códigos de grupo à esquerda já era conhecida.

Levando em consideração que BERNAL, DEL RÍO, and SIMÓN (2009) provaram que se um grupo admite decomposição abeliana, então este grupo determina um código de grupo abeliano, voltou-se a atenção para o problema de saber quando um grupo admitiria decomposição abeliana. Nesta perspectiva, provamos que a ordem minimal de um grupo para que este não admita decomposição abeliana é 24, uma vez que mostramos que todo grupo de ordem menor que 24 admite decomposição abeliana e que S_4 não admite uma tal decomposição como produto de dois subgrupos abelianos. Não obstante, tendo em vista as vantagens algébricas gozadas por p-grupos, fomos motivados a estender este questionamento a esta classe de grupos. Provamos, portanto, que se p é um número ímpar, todo grupo de ordem p^4 admite decomposição abeliana e, além disso, mostramos que existe um grupo de ordem p^5 que não admite. Quando $p = 2$, mostramos que todo grupo de ordem $2^5 = 32$ admite decomposição abeliana e que existe um grupo de ordem $2^6 = 64$ que não admite. Consequentemente, a ordem minimal de um p-grupo para que não haja decomposição abeliana é 2^6 se p é um primo par e p^6 se p é um primo ímpar.

Uma outra questão do nosso interesse foi a de saber se a propriedade de um G-código ser abeliano dependia somente do grupo G, ou seja, se tal propriedade não dependia do corpo F que determina o anel de grupo FG. Com efeito, provamos que sendo F e E corpos finitos com $F \subset E$ e G um grupo finito, tem-se que o fato de todos os G-códigos sobre E serem abelianos implica que todos os G-códigos sobre F são, também, abelianos. Ademais, se todos os G-códigos sobre F forem abelianos e a álgebra de grupo FG for uma soma direta de álgebras de matrizes sobre F, com $\mathrm{char}F \nmid |G|$, então todos os G códigos sobre E também são abelianos.

REFERÊNCIAS

ALPERIN, J. L. Large abelian subgroups of p-groups. *Transactions of the American Mathematical Society*, v. 117, p. 10–20, 1965.

BERNAL, J. J; DEL RÍO, A; SIMÓN, J. J. An intrinsical description of group codes. *Designs, Codes and Cryptography*, v. 51, n. 3, p. 289–300, 2009.

COUSELO, E.; GONZÁLEZ, S.; MARKOV, V.; NECHAEV, A. Loop codes. *Discr. Math. and Appl*, v. 14, n. 2, p. 163–172, 2004.

CURTIS, C. W.; REINER, IRVING. *Representation theory of finite groups and associative algebras*, v. 356. American Mathematical Soc., 1966.

HALL, MARSHALL. *The theory of groups*, v. 288. American Mathematical Soc., 1976.

HEFEZ, A.; VILLELA, M. L. T. *Códigos corretores de erros*. Instituto de Matematica Pura e Aplicada, 2008.

LANG, SERGE. *Algebra*. Springer, 2002.

MILIES, C. POLCINO; SEHGAL, SUDARSKAN K. *An introduction to group rings*, v. 1. Springer Science & Business Media, 2002.

OL'SHANSKII, A YU. *The number of generators and orders of abelian subgroups of finite p-groups. Mathematical notes of the Academy of Sciences of the USSR, v. 23, n. 3, p. 183–185, 1978.*

PASSMAN, DONALD S. The algebraic structure of group rings. Courier Corporation, 2011.

PIERCE, RICHARD S. The Associative Algebra. Springer, 1982.

PILLADO, C. GARCÍA; GONZALEZ, S.; MARTINEZ, C.; MARKOV, V.; NECHAEV, A. Group codes over non-abelian groups. Journal of Algebra and its Applications, v. 12, n. 07, p. 1350037 (20 pages), 2013.

PILLADO, C. GARCÍA; GONZÁLEZ, SANTOS; MARKOV, V.; MARTINEZ, C.; NECHAEV, ALEXANDR. Group codes which are not abelian group codes. p. 123–127, 2011.