Universidade Federal da Bahia
Instituto de Matemática e Estatística
Programa de Pós-Graduação em Matemática

Dissertação de Mestrado

A conjectura de Zassenhaus

Bruna Lima Moreira

Salvador–Bahia

A Conjectura de Zassenhaus

Bruna Lima Moreira

Dissertação de Mestrado apresentada ao Colegiado da Pós-Graduação em Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Nicola Sambonet

Salvador-Bahia

2023

A Conjectura de Zassenhaus

Bruna Lima Moreira

Dissertação apresentada ao Colegiado do Curso de Pós-graduação em Matemática da Universidade Federal da Bahia, como requisito parcial para obtenção do Título de Mestre em Matemática.

Banca examinadora

Prof. Dr. Nicola Sambonet
(UFBA)

Profª. Drª. Manuela da Silva Souza
(UFBA)

Prof. Dr. Martino Garonzi
(UnB)

Aos meus pais, familiares e amigos, como todo amor e carinho.

Ao meu esposo, Fabrício.

Agradecimentos

Primeiramente, agradeço ao meu Pai por esta vitória, pois dele, por Ele e para Ele são todas as coisas e a Ele toda honra e glória para todo sempre, amém!

Agradeço aos meus pais, Francisca e Ronaldo, que por mais que não entendessem minhas escolhas e o caminho que decidi trilhar, nunca me abandonaram e sempre entregaram amor e apoio. Aos meus irmãos David, João Pedro e, especialmente, Matheus, que me aturou mais de perto durante boa parte mestrado, me viu chorar, desesperar e querer desistir constantemente e sempre puxou à realidade, obrigada, irmãos! Ao meu esposo, Fabrício, que embora tenha chegado já perto do final dessa batalha, me viu nos dias mais difíceis e temerosos e sempre me incentivou a continuar firme na minha jornada de todas as formas possíveis, muito, mas muito obrigada por todo apoio, por todo amor, pela compreensão e por sua amizade. Obrigada ainda por ter me dado o maior presente que nosso Senhor poderia ter nos permitido gerar, nossa Maria Cecília . Por ela também me mantive focada na finalização deste trabalho. Muito obrigada, família!

Um agradecimento especial ao professor Nicola, meu orientador. Obrigada por todo tempo, disposição e, principalmente, por não ter desistido de mim. Sei que não fui uma orientanda muito disciplinada, a correria do trabalho no dia a dia acabou me afastando um pouco dos estudos, a rotina não era tão propícia ao estudo. Obrigada por ser compreensivo e sempre tentar me acalmar. Por isso e muito mais, eu te agradeço, Nicola. Não tenho palavras suficientes para descrever o quanto você me ajudou e o quanto sou grata por tudo que você fez por mim.

Agora um agradecimento com imenso amor aos meus irmãos da vida, em especial, Ênio, Rafael, Janara, Jonathas, Eduardo, Juan, Elivan, Sávio, Valéria, Joedson, Taís e Glaene. Pessoal, eu agradeço a Deus pela vida de vocês. Eu também não tenho palavras para agradecer o suficiente por todo apoio, e em todos os âmbitos possíveis e imagináveis, que vocês sempre me deram. Compartilhamos muitos momentos juntos, bons e ruins,

mas eles ainda não foram suficiente. Desejo a presença de cada um de vocês por muitos e muitos anos ainda em minha vida. Muitos churrascos na laje ainda nos aguardam!

Agradeço ainda aos professores Martino Garonzi e Manuela Souza, por terem aceitado o convite para compor minha banca, pelo tempo dedicado à leitura do meu trabalho e, principalmente, por todos os comentários e sugestões feitos a fim de que eu pudesse aperfeiçoar o meu trabalho.

Agradeço aos funcionários do IME-UFBA por terem contribuído de alguma forma. Em particular, um agradecimento especial à secretaria de pós-graduação em matemática da UFBA, e a coordenação do programa de Mestrado em Matemática.

Por fim, agradeço à CAPES pelo apoio financeiro a mim concedido durante todo o Mestrado.

Resumo

Em meados da década de setenta, o matemático alemão Hans J. Zassenhaus, inspirado na tese de Graham Higman e no trabalho desenvolvido por Ian Hughes e Kenneth R. Pearson, formulou algumas conjecturas que impactaram fortemente a pesquisa em anéis de grupos. Muito trabalho foi desenvolvido em torno dessas conjecturas, tanto trazendo resultados positivos para casos particulares, como também apresentando contraexemplos para quase todas elas. Contudo, foi só recentemente que Florian Eisele e Leo Margolis, baseados em um trabalho com Ángel del Río, encontraram contraexemplos para a única conjectura que ainda permanecia em aberto ao longo de todos esses anos, motivando a escrita desta dissertação. Nosso objetivo é primeiramente revisar as noções necessárias para entender as conjecturas, onde se situam na teoria de anéis de grupos, e como se relacionam com a teoria de representação. Em seguida, nós descreveremos os contraexemplos de forma elementar, a fim de simplificar a verificação de algumas informações deixadas ao leitor no artigo original, assim como a construção da tabela dos caracteres. Apesar de não elaborar todos os detalhes, daremos uma indicação das técnicas utilizadas na demonstração que estes grupos contradizem a conjectura.

Palavras-chave: Anéis de grupos, unidades em anéis de grupos, unidades de torção em anéis de grupos integrais, conjecturas de Zassenhaus.

Abstract

In the mid 1960's, the german mathematician Hans J. Zassenhaus, inspired by Gram Higman's thesis and the work of Ian Hughes and Kenneth R. Pearson, stated several conjectures that changed radically the field of research in group rings. Since then many papers have been published about these conjectures, where either an affirmative answer is settled for some specific case, or some counterexamples are determined. Still, it is only very recently that Florian Eisele and Leo Margolis, based on some joint work with Ángel del Río, have found a counterexample for the only conjecture which has been left open. This fact motivated the writing of this dissertation. Our first goal is to revise the notions necessary to understand the conjectures, where they sit in the theory of group rings, and how they relate to representation theory. Then, we describe the counterexamples in an elementary way, in order to simplify the reading of some of their properties. For instance, we determine their character tables. We also point out, still omitting most of the details, which are the techniques involved in the proof that these groups are indeed counterexamples.

Keywords: Group rings, units in group rings, torsion units in integral group rings, Zassenhaus conjectures.

Sumário

Introdução

Um dos grandes problemas da Teoria de Anéis de Grupos é, dado um grupo G, determinar o grupo das unidades $\mathcal{U}(\mathbb{Z}G)$ do anel de grupo integral $\mathbb{Z}G$. Desde o trabalho seminal de G. Higman [17], o alto grau de complexidade para determinar tais grupos ficou evidenciado na década de setenta, quando foi provado que $\mathcal{U}(\mathbb{Z}G)$ geralmente possui subgrupos livres. A existência de subgrupos livres no grupo das unidades de um anel de grupo finito foi estabelecida por B. Hartley e P.F. Pickel sobre os inteiros e por J.Z. Gonçalves sobre corpos. No fim da década de 90, Z. Marciniak e S.K. Sehgal, Gonçalves e D.S. Passman, A. Mandel e M. Shirvani mostraram como gerar grupos livres a partir de unidades razoavelmente bem conhecidas. Para determinadas famílias de grupos é possível descrever explicitamente o grupo das unidades, ou pelo menos obter informações sobre sua estrutura, por exemplo, determinando subgrupos de índice finito. Uma técnica útil para descrever o grupo das unidades seria determinar uma família de geradores que seja finita, porém, até o momento, é somente para um número pequeno de casos que foi encontrado um conjunto finito de geradores de $\mathcal{U}(RG)$. Por exemplo, as unidades cíclicas foram introduzidas por H. Bass, e utilizadas por ele e J. Milnor para mostrar que elas geram um subgrupo de índice finito no anel $\mathcal{U}(\mathbb{Z}A)$, onde A é um grupo abeliano. No caso não abeliano é necessário introduzir novas unidades, as unidades bicíclicas, denominadas assim por J. Ritter e Sehgal, embora nem sempre estas duas famílias de unidades sejam suficientes para gerar subgrupos de índices finitos. Numa série de artigos, E. Jespers, G. Leal e M. M. Parmenter caracterizaram completamente o grupo das unidades de $\mathcal{U}(\mathbb{Z}G)$, quando G é um grupo não abeliano de ordem menor ou igual a 16. As ferramentas principais para estudar este problema chegam da Teoria de Representações e da Teoria dos Números Algébricos. Essas informações podem ser encontradas de forma detalhada, por exemplo, na monografia de Sehgal [39].

Os resultados fundamentais de Higman em [17], sobre as unidades de torção de anéis de grupo integrais de grupos abelianos finitos, não podem ser generalizados, principalmente porque, se um grupo finito G não é abeliano, os conjugados das unidades triviais $\pm G$ em $\mathbb{Z}G$ são, sim, unidades de torção, mas, em geral, podem ser não triviais. Um palpite natural é que todas as unidades de torção no anel de grupo integral de um grupo finito são dessa forma, ou equivalentemente, cada unidade de torção normalizada é conjugada a um elemento do grupo G. Já havia sido observado por Higman que o conjunto das unidades normalizadas $\mathcal{U}_1(\mathbb{Z}S_3)$, a saber, as unidades de aumento 1 do anel de grupo integral sobre o grupo simétrico S_3, contém unidades de torção que não são conjugadas a quaisquer unidades triviais em $\mathcal{U}(\mathbb{Z}S_3)$. Como a tese de Higman ainda não era popular, ela não foi acolhida de imediato por I. Hughes e K. Pearson. Contudo, eles observaram que todos os elementos de torção de $\mathcal{U}_1(\mathbb{Z}S_3)$ são conjugados a elementos de S_3 em $\mathcal{U}(\mathbb{Q}S_3)$. Para maiores detalhes, veja [19] e [34].

Motivado por estes exemplos, e por outros resultados de Higman, no início da década de setenta, Hans Zassenhaus formulou diversas conjecturas sobre as unidades e os isomorfismos de um anel de grupo. Em particular, fez fortes conjecturas a respeito dos subgrupos finitos das unidades do anel de grupo integral, para grupos finitos. Essas conjecturas, chamadas de primeira, segunda e terceira conjectura de Zassanhaus, causaram grande impacto na pesquisa em anéis de grupos. Seguem abaixo tais conjecturas bem como são conhecidas.

(ZC1) Para toda unidade de torção $u \in \mathcal{U}(\mathbb{Z}G)$, existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $u^\alpha \in \pm G$.

(ZC2) Para todo subgrupo finito H de $\mathcal{U}_1(\mathbb{Z}G)$ com $|H| = |G|$, existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $H^\alpha = G$.

(ZC3) Para todo subgrupo finito H de $\mathcal{U}_1(\mathbb{Z}G)$, existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $H^\alpha \subseteq G$.

Um entre os resultados fundamentais da teoria garante que toda unidade de torção u de $\mathbb{Z}G$ satisfaz $u^n = 1$ onde $n = |G|$. Mais em geral, a ordem $|H|$ de qualquer subgrupo finito H de $\mathcal{U}_1(\mathbb{Z}G)$ divide n (por exemplo, veja-se [39, Lema 37.3]); deste ponto de vista as três conjecturas parecem mais que razoáveis. Além disso, (ZC2) resolve o mais famoso *problema de isomorfismo*

$$\mathbb{Z}G \simeq \mathbb{Z}H \stackrel{?}{\Rightarrow} G \simeq H$$

no sentido que uma solução positiva para (ZC2) implica uma solução positiva também para este problema, conforme [39, pág. 197]: se $\varphi : \mathbb{Z}H \to \mathbb{Z}G$ é um homomorfismo de anéis de grupos, definindo $\psi(\sum a_h h) = \sum a_h \varepsilon(\varphi(h))^{-1}\varphi(h)$, obtemos um isomorfismo normalizado $\psi : \mathbb{Z}H \to \mathbb{Z}G$, isto é, tal que $\varepsilon(\psi(h)) = 1$ para todos $h \in H$. Em particular, se $\mathbb{Z}H \simeq \mathbb{Z}G$, existe um isomorfismo normalizado $\psi : \mathbb{Z}H \to \mathbb{Z}G$, assim $\psi(H) \leq \mathcal{U}_1(\mathbb{Z}G)$, e obviamente vale $|H| = |\psi(H)| = |G|$. Portanto, se G satisfaz ZC2, necessariamente $H \simeq \psi(H) = G^\alpha \simeq G$ para algum $\alpha \in \mathcal{U}\mathbb{Q}G$. Um questionamento natural que poderia ser feito é sobre o motivo pelo qual as conjecturas de Zassenhaus são feitas sobre $\mathbb{Q}G$ ao invés de serem sobre $\mathbb{C}G$. Na verdade isso é indiferente, pois se dois subgrupos finitos de $\mathbb{Q}G$ são conjugados em $\mathbb{C}G$, eles já são conjugados em $\mathbb{Q}G$ [39, Lema 37.5].

No decorrer dos anos, pesquisadores conseguiram provar tais conjecturas em casos particulares e outros conseguiram apresentar contraexemplos para a segunda e para a terceira conjectura. Em destaque, K.W. Roggerkamp e L.L. Scott responderam afirmativamente à (ZC2) para grupos nilpotentes e descobriram um contraexemplo metabeliano para a mesma conjectura. Ainda na classe dos grupos nilpotentes, A. Weiss demonstrou (ZC3), pelo menos uma versão forte dela, a (p-ádico)-(ZC3), o que foi um destaque no estudo [42]:

(p-ádico)-(ZC3) Seja $\mathcal{U}_1 = \mathcal{U}_1(\mathbb{Z}_pP)$ o grupo das unidades normalizadas do anel de grupo integral p-ádico $\mathbb{Z}_pP$ do p-grupo finito P. Se H é um p-subgrupo finito de $\mathcal{U}_1$, então $uHu^{-1} \subseteq P$, para algum $u \in \mathcal{U}_1$.

Tempos se passaram e a primeira conjectura ainda permanecia intacta. Devido ao fato de ser a única cujo contraexemplo ainda não havia sido descoberto, ela passou a ser chamada de A conjectura de Zassenhaus. Ela recebeu muita atenção nas últimas décadas e foi comprovada para uma série de grupos solúveis, por exemplo, para grupos que possuem um subgrupo de Sylow normal com complemento abeliano, por M. Hertweck [14], ou grupos cíclicos por abelianos, por M. Caicedo, L. Margolis e A. del Río [7]. Finalmente, contraexemplos para A conjectura, na classe de grupos metabelianos, foram descobertos recentemente por Eisele e Margolis em [12], trabalho este que nos referimos, ao longo do texto, como artigo principal, motivando a escrita desta dissertação.

O objetivo principal deste trabalho é apresentar um pouco dos resultados que já foram desenvolvidos em torno das conjecturas de Zassenhaus, principalmente soluções positivas, mas damos especial atenção ao contraexemplo apresentado por Eisele e Margolis

para A conjectura de Zassenhaus.

No primeiro capítulo, relembramos resultados básicos de boa parte das estruturas algébricas envolvidas no artigo principal, como elementos das teorias de grupos, anéis, módulos, anéis de grupos, e representações. Já no segundo capítulo, apresentamos o conceito de unidades de um anel de grupo, bem como algumas das construções que servem como base para descrever explicitamente as unidades. Já no terceiro capítulo, apresentamos as conjecturas, bem como são conhecidas, trazemos informações sobre o andamento da pesquisa em torno das conjecturas, apresentando algumas das principais soluções positivas já encontradas e só então direcionamos nossa atenção para a construção do contraexemplo. No quarto capítulo elaboramos a tabela dos caracteres dos contraexemplos. Já no quinto e último capítulo, apresentamos um pouco das técnicas utilizadas na demonstração do contraexemplo.

Esperamos que este trabalho possa despertar o interesse dos leitores para os problemas em aberto em anéis de grupo e, quiçá, atrair novos pesquisadores para esta área da matemática.

Capítulo 1

Fundamentos

Neste capítulo, relembraremos resultados importantes das Teorias de Grupos, Anéis e Módulos, de Representações e Caracteres, Ordens e representações integrais e Anéis de Grupos.

1.1 Grupos

Para começar, serão apresentados resultados da Teoria de Grupos que são fundamentais para compreensão dos capítulos seguintes. As possíveis demonstrações necessárias dos resultados aqui apresentados serão, em sua maioria, omitidas, mas podem ser facilmente encontradas em [36], por exemplo.

Um *grupo* é um conjunto não vazio G munido de uma operação binária

$$\cdot : G \times G \to G$$

tal que, dados $a, b, c \in G$, arbitrários, valem:

i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

ii) Existe um elemento, denotado por $1 \in G$, tal que $a \cdot 1 = 1 \cdot a = a$,

iii) Existe um elemento $a^{-1} \in G$, tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Se, além dos itens acima, os elementos do grupo obedecem a propriedade comutativa, isto é, vale $a \cdot b = b \cdot a$ para todo a e b em G, dizemos que tal grupo é *abeliano*. A cardinalidade de um grupo é chamada de *ordem*. Se a cardinalidade de um grupo G for finita, dizemos

simplesmente que G é grupo finito, caso contrário, G é grupo infinito. Dado um elemento $g \in G$, a *ordem* de g é o menor número inteiro positivo n tal que $g^n = 1$ e a denotamos por $o(g)$. Aqui trazemos alguns exemplos de grupos importantes e que são bem conhecidos:

i) Seja X um conjunto não vazio. Denotamos por $\mathrm{Sym}(X)$ ou S_X o conjunto de todas as bijeções de X em si mesmo. Estas bijeções em X também são chamadas de permutações. Munido da operação composição, o conjunto $\mathrm{Sym}(X)$ é chamado de grupo simétrico em X. Se X for finito contendo n elementos, temos o grupo simétrico de grau n, S_n.

ii) Seja $\mathbb{F}$ um corpo qualquer. O conjunto $\mathrm{GL}(n, \mathbb{F}) = \{\alpha \in M_n(\mathbb{F}) : \det \alpha \neq 0\}$ munido com a operação multiplicação usual de matrizes é conhecido como grupo linear geral de grau n sobre $\mathbb{F}$.

iii) O conjunto $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, um conjunto com oito elementos, o munido com a operação de multiplicação satisfazendo

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j,$$

onde 1 é o elemento neutro e valem

$$(-1)^2 = 1,\ (-1)i = -i, \quad \text{e } (-i)j = -(ij) = i(-j)$$

é conhecido como grupo dos quatérnios.

Um subconjunto não vazio H de um grupo G é chamado de *subgrupo* se, munido da mesma operação de G, H é também um grupo e denotamos da seguinte forma $H \leq G$. Note que, sendo H não vazio, $h \in H$, $h^{-1} \in H$ e assim $1 = hh^{-1} \in H$. Da definição acima, podemos dizer, resumidamente, que um subconjunto não vazio H de G é um subgrupo de G se, e somente se, para quaisquer elementos $g, h \in H$ temos que $gh^{-1} \in H$. Um resultado de simples demonstração, sendo esta encontrada em qualquer livro de introdução à álgebra. Seguem alguns exemplos de subgrupos:

i) Dado um qualquer elemento g de um grupo G, temos um subgrupo

$$\langle g \rangle = \{\ g^i\ :\ i \in \mathbb{Z}\ \} \leq G$$

conhecido como subgrupo cíclico gerado por g. Em particular, observamos que a ordem de g e a ordem de $\langle g \rangle$ coincidem.

ii) O subconjunto A_n de S_n, de todas as permutações que podem ser escritas como produto de um número par de transposições, é um subgrupo chamado de grupo alternado. Lembramos que uma transposição é uma permutação (ij), onde $i \neq j$.

iii) $SL(n, \mathbb{F}) = \{\alpha \in M_n(\mathbb{F}) : \det \alpha = 1\} \leq \mathrm{GL}(n, \mathbb{F})$, conhecido como grupo especial linear de grau n sobre $\mathbb{F}$.

É possível também definir subgrupos por meio de identidades a serem satisfeitas, por exemplo, o *centro* de um grupo G é definido por meio da propriedade de comutação.

Definição 1.1. *O centro de um grupo G é o subgrupo*

$$Z(G) = \{\ g \in G\ :\ gx = xg,\ \forall\ x \in G\ \}.$$

Perceba que $Z(G)$ é um grupo abeliano e que G é abeliano se, e somente se, o mesmo coincide com seu centro, isto é, $G = Z(G)$.

Dado um subgrupo H de G, podemos usá-lo para definir uma partição de G, isto é, podemos encontrar subconjuntos disjuntos tais que podem cobrir G.

Definição 1.2. *Seja H um subgrupo de G. Dado um elemento $a \in G$, os subconjuntos das formas*

$$aH = \{ah\ :\ h \in H\} \quad , \quad Ha = \{ha\ :\ h \in H\}$$

são chamados de classe lateral, ou coclasse, respectivamente à esquerda ou à direita, determinadas por a.

Observe que, se definirmos uma aplicação para os elementos h por $h \mapsto ah$, tal aplicação é uma bijeção de H em aH. Assim, se H é um conjunto finito, o lateral aH também o é e ambos possuem a mesma quantidade de elementos.

Definição 1.3. *Seja H um subgrupo de G. O número de coclasses à direita (ou à esquerda) de H em G é chamado de índice de H em G e é denotado por $|G : H|$.*

Como os laterais formam a partição de um grupo, temos o seguinte resultado:

Teorema 1.4 (Lagrange)**.** *Seja H um subgrupo do grupo finito G. Então a ordem de H divide a ordem de G. Precisamente, temos que*

$$|G| = |G : H| \cdot |H|\ .$$

É importante ressaltar que, em geral, podemos ter $gH \neq Hg$. Por exemplo, considere $G = S_3$ e $H = \{1, (12)\}$. Perceba que:

$$(13)H = \{(13), (123)\} \neq \{(13), (132)\} = H(13).$$

Assim, temos que $gH = Hg$ se, e somente se, $H = g^{-1}Hg$.

Definição 1.5. *Seja H um subconjunto não vazio de G. Definimos o normalizador de H em G por*

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

O normalizador $N_G(H)$ é um subgrupo de G, para todo subconjunto $H \subseteq G$. Para ver isso, primeiramente observe que $1 \in N_G(H)$ e que $g^{-1}Hg = H$ se, e somente se, $H = gHg^{-1}$, sendo que uma equação pode ser obtida da outra multiplicando por g e g^{-1} nos dois lados. Logo, $g \in N_G(H)$ equivale a $g^{-1} \in N_G(H)$. Em seguida, para arbitrários $x, y \in N_G(H)$, perceba então que $(xy)^{-1}H(xy) = y^{-1}(x^{-1}Hx)y^{-1} = y^{-1}Hy = H$. Assim, temos $xy \in N_G(H)$ e, portanto, $N_G(H) \leq G$. Além disso, se $H \leq G$, temos $H \leq N_G(H) \leq G$.

Definição 1.6. *Dizemos que H é* normal *em G, e escrevemos $H \trianglelefteq G$, se $N_G(H) = G$, ou seja, se vale $g^{-1}Hg = H$ para todo $g \in G$.*

Para qualquer subgrupo H de G, temos $H \trianglelefteq N_G(H)$, isto é, todo subgrupo é normal no seu normalizador. Se $H \trianglelefteq G$, denotamos por G/H o conjunto dos laterais de H em G. Sendo H normal em G, o produto entre subconjuntos nos dá

$$aH \cdot bH = ab \cdot b^{-1}Hb \cdot H = abHH = abH$$

Ou seja, em G/H está bem definindo o produto entre os elementos por meio da igualdade

$$aH \cdot bH = abH\ .$$

De fato, tal operação determina uma estrutura de grupo em G/H, que chamamos de *grupo quociente* de G por H. Nesta situação, considere a aplicação

$$\omega : G \to G/H \quad , \quad a \mapsto \omega(a) = \bar{a} = aH\ .$$

Perceba que ω é um epimorfismo, conhecido como *homomorfismo canônico* de G para G/H, e é tal que $\omega(1) = 1H = H$ e $Ker(\omega) = H$. Isto mostra particularmente que todo subgrupo normal H de G é o núcleo de algum homomorfismo.

Considere $x, y \in G$. Denotamos o comutador de x e y por $[x, y] = x^{-1}y^{-1}xy$. Perceba que $[x, y] = 1$ se, e somente se x e y comutam. Ainda, se $H, K \subseteq G$ são subgrupos de G, escrevemos $[H, K]$ para denotar o subgrupo de G gerado pelo conjunto $\{[h, k] \mid h \in H,\ k \in K\}$. Assim, o subgrupo gerado por todos os comutadores em G é chamado de subgrupo comutador ou de subgrupo derivado e é denotado por $G' = [G, G]$.

Lema 1.7. *Seja $N \trianglelefteq G$. Então G/N é abeliano se, e somente se $G' \subseteq N$.*

De fato, seja $\varphi : G \to G/N$ o homomorfismo canônico. Se $x, y \in G$, então $[\varphi(x), \varphi(y)] = \varphi([x, y])$ e, portanto, $\varphi(x)$ e $\varphi(y)$ comutam se, e somente se $\varphi([x, y]) = 1$. Como tal fato acontece se, e somente se, $[x, y] \in N$, segue que G/N é abeliano se, e somente se, $[x, y] \in N$, para todos $x, y \in G$. Por outro lado, sendo G' gerado por todos comutadores, tem-se $[x, y] \in N,\ \forall x, y \in G$ se, e somente se, $G' \leq N$.

Agora, seja G um grupo e Ω um conjunto não vazio. Admita que, para cada $g \in G$ e $\alpha \in \Omega$, existe um único elemento definido $\alpha \cdot g \in \Omega$. Considere as seguintes condições:

i) $\alpha \cdot 1 = \alpha$, para todo $\alpha \in \Omega$;

ii) $(\alpha \cdot g) \cdot h = \alpha \cdot (gh)$, para todos $\alpha \in \Omega$ e $g, h \in G$.

Neste caso, dizemos que G age sobre Ω ou que $\cdot$ é uma ação de G em Ω. Toda ação equivale a um homomorfismo $\varphi : G \to \mathrm{Sym}\ \Omega$ onde $\alpha \cdot g = \varphi(g)(\alpha) = \alpha \cdot g$. Dizemos que a ação é transitiva se, para quaisquer elementos $x, y \in \Omega$ existir $g \in G$ tal que $x \cdot g = y$. Dados dois elementos $x, y \in \Omega$, dizemos que x é G-equivalente a y se existe um elemento $g \in G$ tal que $x \cdot g = y$. As classes de equivalência de Ω sob esta relação são chamadas de órbitas de Ω pela ação de G.

Definição 1.8. *Dado um elemento $x \in \Omega$, o conjunto abaixo*

$$xG = \{xg :\ g \in G\}$$

é chamado de órbita de x pela ação de G. Já o conjunto

$$G_x = \{g \in G :\ xg = x\}$$

é um subgrupo de G chamado de estabilizador de x.

Por exemplo, todo grupo G age sobre si mesmo por meio da ação regular

$$G \to \mathrm{Sym}(G) \ , \ g \mapsto \{x \mapsto xg\} \ .$$

Neste caso, existe uma única orbita, e todo ponto $x \in G$ possui estabilizador trivial $G_x = \{1\}$. Em geral, se H é um subgrupo de G, então G age sobre o conjunto G/H dos laterais de H em G, por meio de

$$G \to \mathrm{Sym}(G/H) \ , \ g \mapsto \{Hx \mapsto Hxg\} \ .$$

Também neste caso existe uma única orbita, e tem-se $G_{Hx} = H^x$ para todo $x \in G$. De uma certa forma estas são as ações fundamentais, sendo que vale o seguinte:

Teorema 1.9. *Um grupo G aja sobre um conjunto Ω, e seja $x \in \Omega$. Então a aplicação $xg \mapsto G_x g$ define uma bijeção entre a orbita xG e o conjunto G/G_x dos laterais do estabilizador G_x. Em particular, a cardinalidade de uma órbita é igual ao índice do estabilizador de um representante da órbita, isto é $|xG| = |G : G_x|$. Além disso, tem-se $G_{xg} = (G_x)^g$ para todo $x \in \Omega$ e $g \in G$.*

Também, dado $N \trianglelefteq G$, então G age sobre N por conjugação

$$\vartheta : G \to \mathrm{Sym}(N) \ , \ g \mapsto \{\vartheta_g : x \mapsto x^g\} \ .$$

Em particular, tomando $N = G$, a *classe de conjugação* de x é a órbita x^G, e o estabilizador de x é conhecido como *centralizador*, e são dados por:

$$x^G = \{ \ x^g \mid x \in G \ \} \qquad , \qquad C_G(x) = \{ \ g \in G \mid x^g = x \ \} \ .$$

Lembramos que $x^g = x$ se, e somente se $xg = gx$. De modo geral, temos a seguinte definição: dado um subconjunto H de um grupo G, definimos o centralizador de H em G por

$$C_G(H) = \{ \ g \in G \mid gh = hg, \ \forall h \in H \ \}.$$

O centralizador $C_G(H)$ é um subgrupo de G que está contido no normalizador $N_G(H)$. Mais do que isso, $C_G(H) \trianglelefteq N_G(H)$, sendo que $N_G(H)$ age por conjugação sobre H, e $C_G(H) = \ker \varphi$ é o núcleo da ação $\varphi : N_G(H) \to \mathrm{Sym}(H)$.

A situação típica da ação por conjugação de um grupo sobre um subgrupo normal é generalizada da forma seguinte. Se um grupo G age sobre de um grupo N por meio do homomorfismo $G \to \mathrm{Sym}(N)$, $g \mapsto \{n \mapsto n^g\}$, supondo que vale

$$(hk)^g = h^g k^g \ , \ \forall \ h, k \in N \ , \ g \in G$$

dizemos então que G age por automorfismos sobre N. A escolha da notação n^g no lugar de $n \cdot g$ é motivada em analogia com a conjugação e, de fato, toda ação por autormorfismos pode ser associada com uma ação de conjugação como segue.

Definição 1.10. *Sejam N e H grupos, onde H age sobre N por automorfismos. Então o produto semidireto $G = N \rtimes H$ é o conjunto $N \times H$ junto á operação*

$$(n, h) \cdot (m, k) = (nm^{h^{-1}}, hk)$$

para todos $n, m \in N$ e $h, k \in H$.

O produto semidireto $G = N \rtimes H$ é um grupo, que possui um subgrupo normal $\dot{N} = N \times \{1_H\}$ isomorfo com N, e um subgrupo complementar $\dot{H} = \{1_N\} \times H$, isso é, $G = \dot{N}\dot{H}$ e $\dot{N} \cap \dot{H} = \{1_G\}$, e a ação de $\dot{H}$ por conjugação sobre $\dot{N}$ corresponde a ação original de H sobre N, sendo que vale $(n, 1)^{(1,h)} = (n^h, 1)$ para todos $n \in N$ e $h \in H$. No caso em que H age trivialmente sobre N, obtemos o *produto direto* $N \times H$.

Um grupo finito G diz-se um p-grupo se sua ordem é uma potência de p, com p primo, e um elemento $g \in G$ diz-se um p-elemento se $o(g)$ é uma potência de p. Note então que num p-grupo, todo elemento é um p-elemento, este fato segue diretamente do Teorema de Lagrange, visto que a ordem de um elemento coincide com a ordem do subgrupo cíclico por ele gerado. Se a ordem de um elemento não é divisível por p, então trata-se de um p'-elemento. Seja G um grupo finito de ordem $|G| = p^n m$, onde $p \nmid m$. Um subgrupo de G de ordem p^n chama-se um p-subgrupo de Sylow de G. Apresentamos abaixo o famoso Teorema de Sylow, porém, omitiremos sua demonstração.

Teorema 1.11. *Seja G um grupo finito de ordem $|G| = p^n m$, onde p é um primo que não divide m. Então:*

i) G sempre contém p-subgrupos de Sylow.

ii) Todo p-subgrupo de G está contido num p-subgrupo de Sylow de G.

iii) Todos os p-subgrupos de Sylow de G são conjugados em G.

iv) Se n_p denota o número de p-subgrupos de Sylow de G, então

$$n_p \equiv 1 \mod p \quad e \quad n_p | m.$$

Um grupo G é chamado de *nilpotente* se contém uma série de subgrupos

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

tal que cada subgrupo G_{i-1} é normal em G e cada grupo quociente G_i/G_{i-1} está contido no centro de G/G_{i-1}, $1 \leq i \leq n$. Uma série de subgrupos de G com esta propriedade é chamada de série central de G.

Proposição 1.12. *Seja G um grupo.*

i) Se G é nilpotente, $H \leq G$ e $N \triangleleft G$, então H e G/N são nilpotentes.

ii) Se G é nilpotente, então $Z(G) \neq 1$.

iii) G é nilpotente se, e somente se $G/Z(G)$ é nilpotente.

iv) Se G e H são nilpotentes, então $G \times H$ é nilpotente.

Seja G um grupo abeliano. Desta forma, como segue que $Z(G) = G$, temos que a série trivial $\{1\} = G_0 \subseteq G_1 = G$ satisfaz as condições de nilpotência. Assim, concluímos que todo grupo abeliano é nilpotente. Temos também que todo p-grupo finito é nilpotente. Tal fato segue por indução pela ordem de G. Claro que a afirmação é verdadeira para grupos de ordem p ou p^2, agora suponha que vale para grupos de ordem menor que p^n e seja G um grupo de ordem p^n. Pode ser demonstrado que $Z(G) \neq 1$, então segue que $|G/Z(G)| < p^n$ e, portanto, $G/Z(G)$ é nilpotente. Segue pela proposição anterior que G é portanto nilpotente.

Teorema 1.13. *Seja G um grupo finito. Então as seguintes condições são equivalentes.*

i) G é nilpotente,

ii) G tem a propriedade do normalizador, isto é, todo subgrupo próprio de G está estritamente contido no seu normalizador,

iii) Todo subgrupo de Sylow de G é normal em G,

iv) G é o produto direto dos seus subgrupos de Sylow.

Note que do Teorema acima, se G é nilpotente de ordem $|G| = p_1^{n_1} \cdots p_t^{n_t}$, denotando por S_i, $1 \leq i \leq n$ os p_i-subgrupos de Sylow correspondentes, temos que

$$G = S_1 \times \cdots \times S_n \ .$$

Ao lado dos grupos nilpotentes temos a seguinte noção. Um grupo G é *solúvel* se existe uma coleção de subgrupos normais $G_0, G_1, \ldots, G_n$, tais que

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

e o quociente G_{i+1}/G_i é abeliano, para todo $0 \leq i \leq n$. Perceba então que todo grupo nilpotente é solúvel, em particular todo p-grupo finito.

Teorema 1.14. *Seja G finito e solúvel e considere π um conjunto qualquer de números primos. Então existe um subgrupo $H \subseteq G$ cuja ordem é divisível apenas pelos primos em π e tal que o índice não é divisível por qualquer um dos primos em π.*

Um subgrupo H satisfazendo o teorema acima é chamado de *π-subgrupo de Hall* de G. Perceba que, se $\pi = \{p\}$, isto é, contém apenas um primo, então o π-subgrupo de Hall é um p-subgrupo de Sylow. Ainda, denotamos por π' o conjunto de números primos que não estão em π. A condição de solubilidade é necessária no resultado ácima, por exemplo, o grupo A_5 não possui um π-subgrupo de Hall, para $\pi = \{2, 5\}$, isto é, $\mathrm{Hall}_\pi(A_5) = \emptyset$. De fato, suponhamos, por absurdo, que exista $H \in \mathrm{Hall}_\pi(A_5)$. Como $|A_5| = 60$, temos que $|H| = 20$. Então A_5/H consiste de 3 classes laterais, digamos $\{H, Ha, Hb\}$ e como A_5 age sobre este conjunto, temos um homomorfismo não trivial para $\mathrm{Sym}(A_5/H) \simeq S_3$. Mas isso não é possivel sendo que A_5 é simples e $|S_3| = 6$.

Um grupo G é *metabeliano* se este possui um subgrupo H normal e abeliano tal que G/H é também abeliano. Por exemplo, o grupo dihedral D_8 é metabeliano, sendo que $D_8/Z(D_8)$ possui ordem 4 e portanto é abeliano. Também, o grupo simétrico S_3 é metabeliano. De fato, tomando $A_3 = \langle (123) \rangle \leq S_3$, A_3 é abeliano e S_3/A_3 também é abeliano, visto que $|S_3/A_3| = 2$. De outro lado, S_3 não é nilpotente pois $Z(S_3) = \{1\}$.

Vale lembrar ainda que um grupo abeliano finito G diz-se *abeliano elementar* se existe um primo p tal que todos os elementos diferentes da unidade são de ordem p. Neste caso, G é decomponivel como produto direto de grupos cíclicos de ordem p. De outro lado, um grupo abeliano é dito *livre* se é produto direto de grupos cíclicos infinitos. Chamamos a quantidade de fatores diretos de *posto*. Em geral, se G é um grupo abeliano, então o subgrupo

$$T(G) = \{\ g \in G \mid o(g) < \infty\ \}$$

é chamado de *subgrupo de torção* de G, e se $T(G) = \{1\}$, então dizemos que G é sem torção. Todo grupo abeliano, finitamente gerado, e livre de torção, é livre.

1.2 Anéis e Módulos

A estrutura algébrica que conhecemos como anel teve sua origem, na verdade, de várias fontes, no século XX. A teoria moderna dos anéis teve como base os resultados de R. Dedekind, em seu trabalho de 1871, onde introduziu a noção de ideal, e no trabalho de D. Hilbert, E. Lasker e F. Macaulay, mas o matemático que mais desenvolveu o ponto de vista abstrato da teoria foi E. Noether, em seu elegante trabalho de 1921, onde seu tratamento axiomático constituiu uma novidade na época.

Definição 1.15. *Um anel (mais precisamente, anel associativo com unidade) é um conjunto não vazio R munido de duas operações binárias, $+$ e $\cdot$, chamadas de adição e multiplicação, respectivamente, satisfazendo os seguintes axiomas:*

i) $(R, +)$ *é grupo abeliano,*

ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

iii) $(a + b) \cdot c = a \cdot c + b \cdot c$,

iv) $a \cdot (b + c) = a \cdot b + a \cdot c$.

v) Existe $1 \in R$ *tal que* $1 \cdot a = a \cdot 1 = a$,

para todo $a, b, c \in R$. *Se vale ainda a propriedade*

vi) $a \cdot b = b \cdot a$,

dizemos que o anel é comutativo.

Por exemplo

I) O conjunto dos números inteiros, munido das operações de soma e multiplicação usuais, $(\mathbb{Z}, +, \cdot)$ é anel. Assim como $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$.

II) $\mathrm{End}_K(V)$, o conjunto dos endomorfismos de um K-espaço vetorial V, com as operações de soma

$$v(\alpha + \beta) = v\alpha + v\beta$$

e composição

$$(v)\alpha\beta = (v\alpha)\beta$$

onde $v \in V$ e $\alpha, \beta \in \mathrm{End}_K(V)$ é um anel.

III) Se R é anel comutativo, o conjunto $M_n(R)$ das matrizes quadradas $n \times n$ com coeficientes em R, junto ás operações usuais de soma e produto de matrizes, é anel.

Seja A um subconjunto não vazio do anel R. Dizemos que A é *subanel* (mais precisamente, subanel unitário) de R se $1_R \in A$ e A é fechado pelas operações de R, isto é, A munido das mesmas operações que R é um anel. É bem conhecido que subconjunto não vazio $A \subset R$ é um subanel de R se, e somente se, as seguintes propriedades são válidas:

i) Dados $x, y \in A$, segue que $x - y \in A$,

ii) Dados $x, y \in A$, segue que $xy \in A$,

iii) $1_R \in A$.

Definição 1.16. *Dado um anel R, dizemos que um elemento $a \in R$ é invertível se existe algum elemento $b \in R$ tal que $a \cdot b = b \cdot a = 1$. Neste caso, dizemos que tal elemento é o inverso de a e o denotamos por a^{-1}. O conjunto*

$$\mathcal{U}(R) = \{a \in R \ : \ a \text{ é invertível}\}$$

é chamado de grupo das unidades de R. É fácil verificar que $\mathcal{U}(R)$ é de fato um grupo.

Por exemplo $\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$, $\mathcal{U}(\mathbb{Q}) = \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ e, se R é anel comutativo,

$$\mathcal{U}(M_n(R)) = \mathrm{GL}_n(R) = \{ \ \alpha \in M_n(R) \mid \det \alpha \in \mathcal{U}(R) \ \} \ .$$

Um anel D satisfazendo $\mathcal{U}(D) = D - \{0\}$ é chamado anel com divisão, portanto, um corpo é um anel com divisão comutativo.

Definição 1.17. *Um subconjunto não vazio A do anel R é dito ideal à direita de R se valem:*

i) Dados $a_1, a_2 \in A$ então $a_1 - a_2 \in A$,

ii) Se $a \in A$ e $r \in R$, então $ar \in A$.

Definimos, de modo análogo, o ideal à esquerda de R. Se um ideal A é ideal à direita e à esquerda, dizemos que A é ideal bilateral de R, ou apenas que A é um ideal de R. Ideais gerados por um único elemento são chamados de ideais principais.

A noção de módulos bem como a conhecemos, e apresentamos adiante, apareceu explicitamente nos trabalhos de Dedekind em teoria dos números. Porém, seu estudo começou no trabalho clássico de Noether, de 1929, que foi muito importante para o desenvolvimento da teoria de anéis de grupos e contem os dados básicos desta teoria, [24].

Definição 1.18. *Seja R um anel. Um grupo aditivo abeliano M é chamado de R-módulo à direita se, para cada $r \in R$ e cada $m \in M$, está definido $mr \in M$, satisfazendo*

i) $m(r_1 + r_2) = mr_1 + mr_2$,

ii) $(m_1 + m_2)r = m_1r + m_2r$,

iii) $(mr_1)r_2 = m(r_1r_2)$,

iv) $m1 = m$,

para todos $r_1, r_2 \in R$ e $m, m_1, m_2 \in M$. Analogamente definimos o R-módulo à esquerda. Quando M é, ao mesmo tempo, um R-módulo à esquerda e à direita, dizemos que M é um R-módulo bilateral.

Podemos assim dizer que, a partir da definição, se K é um corpo, então o conceito de K-módulo coincide com a noção de espaço vetorial sobre o corpo K. Assim, uma *base* S para um R-módulo M segue no mesmo sentido de uma base para um espaço vetorial, isto é, M é R-módulo gerado por S, ou seja, para todo $m \in M$ tem-se $m = s_1r_1 + \ldots + s_lr_l$ com $s_i \in S$ e $r_i \in R$, e S é um conjunto linearmente independente sobre R. Um R-módulo M é dito *livre* se possui uma base. Se M é um R-módulo no qual $mr = m$ para todos $m \in M$ e $r \in R$, então dizemos que M é *trivial*. De outro lado, considerando o grupo aditivo de R junto à aplicação $(r, s) \mapsto rs$, obtemos o *R-módulo regular*. Mais geralmente, se I é um ideal à direita de um anel R, o produto de elementos de I por elementos de R define uma estrutura de R-módulo sobre I. De forma analoga às ações de grupos, todo R-módulo M corresponde à uma aplicação

$$R \to \mathrm{End}(M) = \{\ \varphi : M \to M \mid (m+n)\varphi = m\varphi + n\varphi,\ \forall\ m, n \in M\ \}\ .$$

Define-se

$$\mathrm{End}_R(M) = \{\ \varphi \in \mathrm{End}(M) \mid (mr)\varphi = (m\varphi)r,\ \forall\ m \in M,\ \forall\ r \in R\ \}$$

como o *anel dos R-endomorfismos* de M. De fato, $\mathrm{End}_R(M)$ é anel com as operações de soma e composição e, assim, M também é $\mathrm{End}_R(M)$-módulo.

Seja M um módulo sobre o anel R. Um subconjunto não vazio $N \subset M$ é chamado de *submódulo* de M se valem as seguintes condições:

i) Para todos $x, y \in N$, vale $x + y \in N$,

ii) Para todos $r \in R$ e $n \in N$, vale $rn \in N$.

Por exemplo, os ideais são exatamente os submódulos do módulo regular. Todo módulo M possui, no mínimo, dois submódulos: (0) e M. Todos os outros submódulos são *próprios*. Caso um módulo não nulo não possua submódulos próprios, ele é chamado de *simples* ou *irredutível*.

Sejam G um grupo, não necessariamente finito, e R um anel com unidade. Denotaremos por RG o conjunto de todos os elementos da forma

$$\alpha = \sum_{g \in G} a_g g$$

onde $a_g \in R$ e $a_g \neq 0$ apenas para uma quantidade finita de elementos de G. Segue da definição que, dados $\alpha = \sum a_g g$ e $\beta = \sum b_g g \in RG$, temos $\alpha = \beta$ se, e somente se, $a_g = b_g$ para todo $g \in G$. Dado $\alpha = \sum a_g g \in RG$, chamamos de *suporte* de α o conjunto dos elementos de G cujo coeficiente correspondente é não nulo, isto é,

$$\mathrm{Supp}(\alpha) = \{\ g \in G \mid a_g \neq 0\ \}\ .$$

Além disso, dados $\alpha = \sum a_g g$ e $\beta = \sum b_g g \in RG$, definamos soma e multiplicação entre elementos de RG como segue abaixo

$$\alpha + \beta = \left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g$$

e

$$\alpha\beta = \left(\sum_{g \in G} a_g g\right)\left(\sum_{h \in G} b_h h\right) = \sum_{g,h \in G} (a_g b_h) gh = \sum_{g \in G} \left(\sum_{h \in G} a_{gh^{-1}} b_h\right) g\ .$$

Com as operações acima, RG é um anel cuja unidade é dada pelo elemento $1 = \sum c_g g$, onde o coeficiente correspondente a unidade do grupo é $c_1 = 1$ e para os demais elementos de G tem-se $c_g = 0$.

Definição 1.19. *O conjunto RG, com as operações definidas acima, é chamado de anel de grupo de G sobre R.*

Podemos definir também o produto entre elementos de RG e R, como segue

$$\gamma\alpha = \gamma\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G}(\gamma a_g)g, \quad \forall\ \gamma \in R\ .$$

Desta forma, vemos que o anel de grupo RG é um R-módulo livre, gerado por G. Para anéis de grupos temos a seguinte definição:

Definição 1.20. *Sejam V um R-módulo e G um grupo. Dizemos que V é um RG-módulo se a multiplicação $vg,\ v \in V, g \in G$, está bem definida e satisfaz as seguintes condições:*

i) $vg \in V$,

ii) $v(gh) = (vg)h$,

iii) $v1 = v$,

iv) $(rv)g = r(vg)$,

v) $(v_1 + v_2)g = v_1 g + v_2 g$,

para todos $v_1, v_2 \in V,\ r \in R,\ g, h \in G$.

Pode-se verificar que esta definição é compativel com a definição geral de módulo sobre um anel. Além disso, um RG-módulo V é trivial se

$$vg = v\ , \forall\ v \in V,\ g \in G.$$

Por outro lado, V é fiel se a identidade do grupo G é o único elemento para o qual vale

$$vg = v,\ \forall\ v \in V\ .$$

Definição 1.21. *O homomorfismo $\varepsilon : RG \to R$ dado por*

$$\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$$

é chamado de aplicação de aumento de RG e seu núcleo, que é denotado por $\Delta(G)$, é um R-módulo chamado de ideal de aumento de RG.

Note que, dado $\alpha \in \Delta(G)$, temos $\varepsilon(\alpha) = 0$ e, daí, podemos escrever

$$\alpha = \alpha - \varepsilon(\alpha) = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\neq 1\in G} a_g(g-1)\ .$$

Dessa forma, $\Delta(G)$ é gerado como R-módulo pelos elementos da forma $g-1$ ao variar de g em G, ou seja

$$\Delta(G) = \langle\, g-1 \mid g \in G \,\rangle_R \,.$$

No caso em que $R = K$ é corpo, dizemos que KG é a *álgebra de grupo* de G sobre K, de acordo a seguinte definição:

Definição 1.22. *Seja K um corpo. Uma K-álgebra é um anel A que é também um K-espaço vetorial de dimensão finita, tal que,*

$$r(m_1m_2) = (rm_1)m_2 = m_1(rm_2),$$

para todos $r \in R$ e $m_1, m_2 \in M$.

1.3 Representações e Caracteres

A representação de um grupo G é uma ferramenta muito utilizada e que nos permite enxergar tal grupo como uma estrutura algébrica relativamente mais simples, porém, com boas propriedades e com axiomas bem definidos, tais como matrizes, permutações, transformações lineares, entre outros. Nesta seção serão apresentados conceitos básicos de representações de grupos e caracteres. O leitor que desejar aprofundar os conhecimentos acerca destes conceitos poderá fazê-lo em [22], por exemplo.

Definição 1.23. *Sejam G grupo, K um corpo, e V um K-espaço vetorial de dimensão finita n. Uma representação de G em V é um homomorfismo $\varphi : G \to \mathrm{GL}(V)$. O grau da representação é o inteiro n.*

Por definição, uma aplicação φ de G em $\mathrm{GL}(V)$ é uma representação de G se, e somente se, valem as propriedades

i) $\varphi(1) = \mathrm{id}_V$,

ii) $\varphi(gh) = \varphi(g)\varphi(h)$,

iii) $\varphi(g)^{-1} = \varphi(g^{-1})$.

para todos g e h em G. Observe que todo grupo G pode ser representado sobre um K-espaço vetorial V por meio da *representação trivial* $g \mapsto \mathrm{id}_V$. Mais em geral, se um grupo

G age por permutação sobre um conjunto finito Ω, é possível estender por K-linearidade a ação de G sobre $K\Omega$, sendo esse o K-espaço vetorial com base Ω. Neste sentido, as ações são um caso particular de representações sobre um corpo qualquer K.

Definição 1.24. *Se $\varphi : G \to \mathrm{GL}(V)$ é uma representação de grupo finito G sobre um K-espaço vetorial V de dimensão finita, dizemos que V é um KG-*módulo.

Assim, um espaço vetorial V é um KG-módulo se está definida uma ação de G sobre V por meio de transformações K-lineares. Ou seja, de forma explicita, existe uma aplicação $\cdot : G \times V \to V$, $(g, v) \mapsto g \cdot v$ satisfazendo as seguintes propriedades:

i) $1 \cdot v = v$;

ii) $g \cdot (\lambda v_1 + \lambda' v_2) = \lambda(g \cdot v_1) + \lambda'(g \cdot v_2)$;

iii) $g_1 \cdot (g_2 v) = (g_1 g_2) \cdot v$,

para todos $g, g_1, g_2 \in G, v, v_1, v_2 \in V, \lambda, \lambda' \in K$. Logo, dada uma representação φ, a ação sobre V está definida por meio da relação $g \cdot v = \varphi(g)v$, e reciprocamente, se V é KG-módulo, então a aplicação $\varphi : G \to \mathrm{GL}(V)$ definida por $\varphi(g)v = g \cdot v$ é uma representação de G. Além disso, considerando o anel de grupo KG, é possível estender toda representação $\varphi : G \to \mathrm{GL}(V)$ a um homomorfismo de anéis $\varphi : KG \to \mathrm{End}(V)$, definindo

$$\varphi(\sum_{g \in G} k_g g) = \sum_{g \in G} k_g \varphi(g) \ .$$

Assim, um KG-módulo é de fato um módulo do anel de grupo KG.

Lembramos que, se V é um K-espaço vetorial de dimensão n, toda escolha de uma base de V determina um isomorfismo $\mathrm{GL}(V) \simeq \mathrm{GL}(n, K)$. Assim, podemos identificar uma representação como um homomorfismo $\varphi : G \to \mathrm{GL}(n, K)$. Por exemplo, em $\mathrm{GL}(2, \mathbb{C})$, as matrizes

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \ , \ J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \ , \ K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

satisfazem as relações $I^2 = J^2 = K^2 = IJK = -1$, portanto, temos uma representação do grupo dos quatérnios $\varphi : Q_8 \to \mathrm{GL}(2, \mathbb{C})$, tal que $\varphi(i) = I$, $\varphi(j) = J$, e $\varphi(k) = K$. Recordamos ainda que, uma mudança da base de V corresponde a conjugação por alguma matriz em $\mathrm{GL}(n, K)$. Portanto, é de interesse considerar a seguinte relação de equivalência

entre representações por matrizes. Por sua vez, esta relação corresponde a noção de isomorfismo de KG-módulos.

Definição 1.25. *Dizemos que duas representações $\varphi, \psi : G \to \mathrm{GL}(n, K)$ são* similares *se existe $P \in \mathrm{GL}(n, K)$ tal que*

$$\varphi(g) = P^{-1}\psi(g)P.$$

para todo $g \in G$.

Se V é um KG-módulo e W é um subespaço vetorial de V, dizemos que W é *φ-invariante* se $\varphi(g)(W) \subseteq W$, para todo $g \in G$. Como $\varphi(g)$ é automorfismo, então $\varphi(g)|_W$ é também automorfismo, o que nos permite definir $\varphi_W : G \to \mathrm{GL}(W)$, portanto, W é KG-submódulo de V.

Definição 1.26. *Um KG-módulo V é irredutível se seus únicos submódulos são $\{0\}$ e V. Caso contrário, V é redutível.*

Em termos de uma representação por matrizes, se existe um subespaço invariante W, de dimensão $1 < k < n$, podemos completar uma base de W para obter uma base $B = \{w_1, \ldots, w_k, v_{k+1}, \ldots, v_n\}$ de V, assim que

$$\varphi(g)^P = \begin{pmatrix} \alpha(g) & \beta(g) \\ 0 & \gamma(g) \end{pmatrix}$$

onde $\alpha : G \to \mathrm{GL}(k, K)$, $\gamma : G \to \mathrm{GL}(n-k, K)$, $\beta : G \to M_{k,n-k}(K)$, para algum $P \in \mathrm{GL}(n, K)$. Aqui, α é a representação matricial associada ao submódulo W, e P é a matriz de mudança de base.

Definição 1.27. *Um KG-módulo V é completamente redutível se, para todo submódulo W de V, existe um submódulo complementar U para W em V, ou seja, tal que $V = U \oplus W$, isto é, $V = U + W$ e $U \cap W = \{0\}$.*

Por exemplo, considere o grupo cíclico $G = \langle g \rangle$ com 2 elementos e o corpo $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Obtemos uma representação por

$$\varphi : G \to \mathrm{GL}(2, \mathbb{F}_2) \quad , \quad \varphi(g) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} .$$

Vemos que o módulo $V = \mathbb{F}_p^2$ é redutível, sendo $W = \langle (1, 0) \rangle$ um submódulo não trivial mas, de outro lado, V não é completamente redutível, sendo que W não possui complementar em V. De fato, é possível verificar que um KG-módulo V é completamente redutível

se, e somente se, é soma direta de irredutíveis. Além disso, em termos de matrizes, cada soma direta de submódulos corresponde a ter uma representação em blocos diagonais. Um dos teoremas fundamentais em teoria da representação afirma que a situação acima é típica do caso no qual char K não divide $|G|$.

Teorema 1.28. *(Maschke) Sejam G um grupo finito e K um corpo cuja característica não divide $|G|$. Então todo KG-módulo é completamente redutível.*

O Teorema de Maschke afirma que, se char K não divide $|G|$, então KG é uma álgebra semissimples. Uma álgebra A é chamada *semissimples* se seu módulo regular é completamente redutível. Em tal caso, todo módulo é isomorfo com um submódulo do módulo regular. Reportamos alguns dos resultados fundamentais sobre as álgebras semissimples, conforme [20, §1].

Teorema 1.29 (Duplo centralizador)**.** *Sejam A uma álgebra semissimples e V um A-módulo irredutível, e seja $D = \mathrm{End}_A(V)$, então $\mathrm{End}_D(V) = \{\ v \mapsto vx \mid x \in A\ \}$.*

Teorema 1.30 (Wedderburn)**.** *Sejam A uma álgebra semissimples, $V_1, \ldots, V_r$ representantes pelas classes de isomorfismo dos A-módulos irredutíveis, $D_i = \mathrm{End}_A(V)$, e denotamos por W_i a soma de todos os submódulos de A isomorfos com V_i. Então*

i) Todo W_i é um ideal bilateral minimal de A, e $A = W_1 \oplus \ldots \oplus W_r$

ii) Tem-se $V_i W_j = 0$ toda vez que $i \neq j$.

iii) A aplicação $x \mapsto \{v \mapsto vx\}$ define um isomorfismo $W_i \to \mathrm{End}_{D_i}(V_i)$.

Lema 1.31 (Schur)**.** *Se U e V são A-módulos irredutíveis, então todo homomorfismo não nulo em $\mathrm{Hom}_A(U, V)$ possui um inverso em $\mathrm{Hom}_A(V, U)$. Portanto, $\mathrm{End}_A(V)$ é uma álgebra com divisão. Além disso, se K é algebricamente fechado, então $\mathrm{End}_A(V) = K$.*

Juntando este resultado ao teorema de Wedderburn temos a seguinte caracterização estrutural da álgebra de grupo $\mathbb{C}G$:

Corolário 1.32. *A álgebra de grupo $\mathbb{C}G$ é uma soma direta $\mathbb{C}G = W_1 \oplus \ldots \oplus W_r$, onde $W_i \simeq \mathrm{End}_{\mathbb{C}}(V_i)$. Logo, $\mathbb{C}G \simeq M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_r}(\mathbb{C})$ é uma soma direta de álgebras de matrizes, onde $n_i = \dim_{\mathbb{C}}(V_i)$.*

Assim, o grupo das unidades de $\mathbb{C}G$ é dado por

$$\mathcal{U}(\mathbb{C}G) \simeq \mathrm{GL}_{n_1}(\mathbb{C}) \oplus \ldots \oplus \mathrm{GL}_{n_r}(\mathbb{C}) \ .$$

Mais ainda, em $\mathrm{GL}_{n_i}(\mathbb{C})$, toda matriz de torção é similar com uma matriz diagonal, cujas entradas são raizes da unidade. Considerando a representação $\varphi_i : G \to \mathrm{GL}_{n_i}(\mathbb{C})$, para cada $g \in G$, tem-se $\varphi_i(g) \sim \mathrm{diag}(\varepsilon_{i1}, \ldots, \varepsilon_{in_i})$, onde $\varepsilon_i^{o(g)} = 1$. Logo

$$\{\ u \in \mathcal{U}(\mathbb{C}G) \mid u \sim g\ \} = \{\ u \in \mathbb{C}G \mid \varphi(u) \sim \mathrm{diag}(\varepsilon_{11}, \ldots, \varepsilon_{1n_1}, \ldots, \varepsilon_{1n_r}, \ldots \varepsilon_{rn_r})\ \} \ .$$

Vemos que em $\mathbb{C}G$ as unidades conjugadas com os elementos de G são completamente determinadas pela decomposição de Wedderburn. De outro lado, como já foi mencionado na introdução, dois subgrupos finitos de $\mathbb{Q}G$ conjugados em $\mathbb{C}G$, são já conjugados em $\mathbb{Q}G$, em vista do seguinte resultado [39, Lema 37.5].

Lema 1.33. *Sejam $k \leq K$ corpos infinitos e G um grupo finito. Sejam H_1 e H_2 dois subgrupos finitos do grupo das unidades em kG. Então*

$$H_1 \sim H_2 \text{ em } KG \implies H_1 \sim H_2 \text{ em } kG$$

.

Junto a representações, é interessante considerar os caracteres. Lembramos que o *traço* de uma matriz quadrada é a soma dos coeficientes da diagonal:

$$A = (a_{ij}) \in M_n(K) \quad , \quad \mathrm{tr}\ A = \sum_{i=1}^{n} a_{ii} \ .$$

É fácil ver que a função $\mathrm{tr} : M_n(K) \to K$ satisfaz $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ para todo A e B. Consequentemente,

$$\mathrm{tr}(A^P) = \mathrm{tr}(P^{-1}AP) = \mathrm{tr}(A)$$

sempre que $P \in \mathrm{GL}(n, K)$.

Definição 1.34. *Seja $\varphi : G \to \mathrm{GL}(V)$ uma representação do grupo G, onde V tem dimensão finita. Chamamos de caractere da representação a seguinte função*

$$\chi : G \to K \quad , \quad g \mapsto \mathrm{tr}(\varphi(g))$$

Dizemos que χ é irredutível se φ é tal. Denotamos por $\mathrm{Irr}(G, K)$ o conjunto dos caracteres associados com as representações irredutíveis sobre K-espaços vetoriais. No caso em que $K = \mathbb{C}$, escrevemos simplesmente $\mathrm{Irr}(G) = \mathrm{Irr}(G, \mathbb{C})$.

O caractere da representação trivial $G \to \mathbb{C}$ é chamado *caractere principal*, ele é a função constante $\mathbf{1}_G : g \mapsto 1$, $\forall\ g \in G$. Mais em geral, caracteres associados com módulos de dimensão 1 são chamados *lineares*, e correspondem aos homomorfismos de G em $\mathbb{C}^\times$. Representações similares possuem o mesmo caractere, sendo que, dada uma representação $\varphi : G \to \mathrm{GL}(n, K)$ e uma matriz $P \in \mathrm{GL}(n, K)$, tem-se tr $(\varphi(g)^P) =$ tr $(\varphi(g))$ para todo $g \in G$. Além disso, os caracteres são funções constantes sobre as classes de conjugação, sendo tr $(\varphi(g)^{\varphi(h)}) =$ tr $(\varphi(g^h))$ para todo $g, h \in G$. Portanto, geralmente os caracteres irredutíveis são apresentados em forma de tabela $X = (\chi_i(g_j))_{ij}$, onde $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_r\}$, e $\mathrm{Cl}(G) = \{\ g_j^G \mid j = 1, \ldots, r\}$ são as classes de conjugação em G. Por exemplo (veja [20, p.288]), a tabela dos caracteres irredutíveis comlexos de A_5 é dada por

	1	(12)	(123)	(12345)	(12354)
χ_1	1	1	1	1	1
χ_2	3	-1	0	α	β
χ_3	3	-1	0	β	α
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

onde

$$\alpha = \frac{1-\sqrt{5}}{2}\ ,\ \beta = \frac{1+\sqrt{5}}{2}\ .$$

No caso dos $\mathbb{C}$-caracteres, $\mathrm{Irr}(G)$ é uma base do espaço vetorial das funções de classe, e de fato é ortonormal, ou seja, vale a relação $[\chi, \psi] = \delta_{\chi\psi}$ para todos $\chi, \psi \in \mathrm{Irr}(G)$. A respeito do produto interno temos

$$[\alpha, \beta] = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}$$

definido para quaisquer funções de classes α e β com valores em $\mathbb{C}$ [20, §2]. O grande interesse em estudar os caracteres no lugar de trabalhar diretamente com as representações é evidenciado pelo seguinte teorema.

Teorema 1.35. *Se* char K *não divide* $|G|$ *então duas representações são similares se, e somente se, possuem o mesmo caractere.*

Este resultado é bem conhecido se $K = \overline{K}$. O caso geral é demonstrado utilizando a noção de corpo de decomposição de um grupo [20, Teorema 9.21, Corolário 9.22]. Em

particular, para $K = \mathbb{Q}$, pode-se mostrar que $\mathrm{Irr}(G, \mathbb{Q})$ está em bijeção com o conjunto das órbitas em $\mathrm{Irr}(G)$ do grupo de Galois $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}[\chi]/\mathbb{Q})$, onde $\mathbb{Q}[\chi] = \mathbb{Q}[\chi(g)|g \in G]$ é um subcorpo da extensão ciclotômica $\mathbb{Q}[\varepsilon]$ de $\mathbb{Q}$, sendo ε uma raiz primitiva n-ésima da unidade em $\mathbb{C}$, para $n = \exp G$. Nesta correspondência, todo $\xi \in \mathrm{Irr}(G, \mathbb{Q})$ escreve-se como $\xi = m \sum \chi^{\mathcal{G}}$, onde $\chi^{\mathcal{G}} = \{\chi^\sigma\}_\sigma$ é a órbita de $\chi \in \mathrm{Irr}(G)$ pela ação de $\mathcal{G}$, e m é um inteiro positivo.

Dado um subgrupo H de um grupo G, toda representação de G define uma representação de H simplesmente por restrição. Assim, em termos de caracteres, temos uma função $\cdot\downarrow_H$ que leva caracteres de G em caracteres de H. De outro lado, toda representação de H determina uma representação de G por meio da indução [20, §5]. Em termos de módulos, a indução é a aplicação que leva o KH-módulo V no KG-módulo $V\uparrow^G = V \otimes_{KH} KG$. Focando no caso ordinário de representações complexas, isso corresponde a uma aplicação $\vartheta \mapsto \vartheta^G$, onde ϑ é um caractere de H, por meio da formula

$$\vartheta\uparrow^G(g) = \frac{1}{|H|}\sum_{x\in G}\vartheta^\circ(g^x)$$

onde $\vartheta^\circ\downarrow_H = \vartheta$ e $\vartheta^\circ\downarrow_{G\setminus H} = 0$. Mais ainda, por meio desta fórmula a indução pode ser generalizada a todas as funções de classes de H. Restrição e indução estão relacionadas por meio do produto interno.

Teorema 1.36 (Reciprocidade de Frobenius)**.** *Dado $H \leq G$, sejam ϑ e χ funções de classes de H e G com valores em $\mathbb{C}$, respectivamente. Então $[\vartheta\uparrow^G, \chi] = [\vartheta, \chi\downarrow_H]$.*

A teoria que relaciona os caracteres de um grupo com aqueles de um subgrupo normal é devida a Clifford [20, §6]. Dado $H \trianglelefteq G$, então G age sobre $\mathrm{Irr}(H)$ por meio da relação $\vartheta^g(x) = \vartheta(x^{g^{-1}})$. Para $\vartheta \in \mathrm{Irr}(H)$, definimos o *subgrupo de inércia* de ϑ em G como o estabilizador

$$G_\vartheta = \{g \in G \mid \vartheta^g = \vartheta\}\ .$$

Em particular, se $\vartheta^G = \{\vartheta = \vartheta_1, \vartheta_2, \ldots, \vartheta_t\}$ é a orbita de ϑ em $\mathrm{Irr}(H)$ sob a ação de G, tem-se $t = |\vartheta^G| = |G : G_\vartheta|$. Além disso, denotamos por $\mathrm{Irr}(G|\vartheta)$ o conjunto dos caracteres $\chi \in \mathrm{Irr}(G)$ cuja restrição a H possui ϑ como constituinte irredutível.

Teorema 1.37 (Clifford)**.** *Sejam $H \trianglelefteq G$. Dado $\chi \in \mathrm{Irr}(G)$, se $\vartheta \in \mathrm{Irr}(H)$ é tal que $\chi \in \mathrm{Irr}(G|\vartheta)$, vale $\chi\downarrow_H = e\sum\vartheta^G$ por algum inteiro positivo e. De outro lado, fixado $\vartheta \in \mathrm{Irr}(H)$, então a indução $\cdot\uparrow^G\colon \mathrm{Irr}(G_\vartheta|\vartheta) \to \mathrm{Irr}(G|\vartheta)$ é uma bijeção.*

Enfim, reportamos um resultado que descreve os caracteres de um produto direto [20, Teorema 4.21]. Se $G = H \times K$ é produto direto de dois grupos H e K, para duas funções $\alpha : H \to \mathbb{C}$ e $\beta : K \to \mathbb{C}$, obtemos uma função $\alpha\beta : hk \mapsto \alpha(h)\beta(k)$.

Teorema 1.38. *Seja $G = H \times K$. Então as funções $\eta\vartheta$, onde $\eta \in \mathrm{Irr}(H)$ e $\vartheta \in \mathrm{Irr}(K)$ são exatamente os caracteres irredutíveis de G, isto é $\mathrm{Irr}(G) = \mathrm{Irr}(H) \times \mathrm{Irr}(K)$.*

1.4 Ordens

Considerando um anel de grupo integral $\mathbb{Z}G$, por meio das inclusões $\mathbb{Z}G \leq \mathbb{Q}G \leq \mathbb{C}G$, podem ser utilizados os resultados de teoria das representações. De outro lado, é necessário explorar também a relação que liga o anel $\mathbb{Z}G$ com a álgebra $\mathbb{Q}G$, sendo a mesma dada por meio da noção de ordem.

Definição 1.39. *Sejam A uma $\mathbb{Q}$-álgebra e R um subanel de A. Dizemos que R é uma ordem em A, se R é finitamente gerado como $\mathbb{Z}$-módulo e $\mathbb{Q}R = A$.*

A notação aqui utilizada é a seguinte: dado um subconjunto não vazio X de uma $\mathbb{Q}$-álgebra A, denotamos por $\mathbb{Q}X$ o subespaço de A gerado por X. Assim, se R é uma ordem, tem-se

$$\mathbb{Q}R = \left\{ \sum_{i=1}^{m} q_i r_i \mid q_i \in \mathbb{Q}, \forall\ i = 1, \ldots, m \right\}$$

onde $\{r_1, \ldots, r_m\}$ é um conjunto gerador do $\mathbb{Z}$-módulo R. Como já antecipado, o anel de grupo inteiro $\mathbb{Z}G$ de um grupo finito G é uma ordem em $\mathbb{Q}G$. Um outro exemplo fundamental é o anel O_K dos inteiros de um corpo algébrico K, que é uma ordem em K. Mais ainda, $O_K G$ é uma ordem em KG. Reportamos alguns dos resultados básicos que serão utilizados em seguida, conforme [39].

Lema 1.40. *Seja A uma $\mathbb{Q}$-álgebra.*

i) Sejam R_1 e R_2 ordens em A. Então $R_1 \cap R_2$ é também uma ordem em A.

ii) Seja $R \subset A$ subanel finitamente gerado como $\mathbb{Z}$-módulo. Se R_1 é uma ordem em A e $R_1 \subset R$, então R é também ordem em A.

Demonstração. i) Sejam R_1 e R_2 ordens em A. Por definição $\mathbb{Q}R_1 = A$, assim, como $R_2 \subseteq A$, $\forall s \in R_2$, tem-se $s = \sum q_i r_i$, onde $q_i \in \mathbb{Q}$ e $r_i \in R_1$. Logo $\exists z \in \mathbb{N} : zs \in R_1 \cap R_2$.

Tome $\{s_1, \ldots, s_m\}$ como geradores de R_2. Então $\exists z_1, \ldots, z_m$ tais que $\{z_1 s_1, \ldots, z_m s_m\} \subseteq R_1 \cap R_2$, o que implica que $\mathbb{Q}(R_1 \cap R_2) \supseteq \mathbb{Q}\{z_1 s_1, \ldots, z_m s_m\} = \mathbb{Q}\{s_1, \ldots, s_m\} = \mathbb{Q}R_2 = A$.
ii) Claro que $\mathbb{Q}R \subset A$. Agora, note que $A = \mathbb{Q}R_1 \subset \mathbb{Q}R$, isto é, $A \subset \mathbb{Q}R$. O resultado segue. □

Lema 1.41. *Sejam $R_1 \subseteq R_2$ ordens em A, $\mathbb{Q}$-álgebra. Então existe um inteiro d tal que $dR_2 \subseteq R_1$. Além disso, considerando R_1 e R_2 como grupos aditivos, tem se que $|R_1 : dR_2| < \infty$.*

Demonstração. Por definição, R_1 e R_2 são finitamente gerados como $\mathbb{Z}$-módulos. Assim, considere $\{r_1, \ldots, r_m\}$ e $\{s_1, \cdots, s_n\}$ conjuntos de geradores de R_1 e R_2, respectivamente. Como $A = \mathbb{Q}R_1$, podemos escrever cada elemento $s_i \in A$ da seguinte forma:

$$s_i = \sum_{i,j} q_{ij} r_j.$$

Então existe $d_i \in \mathbb{N}$ tal que $d_i q_{ij} \in \mathbb{Z}$, $\forall j$, logo $d_i s_i \in R_1 \cap R_2$. Seja $d =$ m.m.c $(d_1, \ldots, d_n)$. Assim $dR_2 \subseteq R_1 \cap R_2 \subseteq R_1$, isto é, $dR_2 \subseteq R_1$.

Como $R_2 \supseteq R_1 \supseteq dR_2$, pelo Teorema do Isomorfismo temos

$$\frac{R_2}{R_1} \simeq \frac{R_2/dR_2}{R_1/dR_2} \text{ e } \frac{R_2}{dR_2} \simeq (\mathbb{Z}_d)^n.$$

Desta forma $|R_1 : dR_2| < |R_2 : dR_2| < \infty$, como queríamos.

□

Lema 1.42. *Sejam $R_1 \subset R_2$ ordens em uma $\mathbb{Q}$-álgebra A. Então:*

i) Se $\mathcal{U}(R_1)$ e $\mathcal{U}(R_2)$ são os grupos das unidades de R_1 e R_2, respectivamente, então o índice $|\mathcal{U}(R_2) : \mathcal{U}(R_1)|$, como grupos multiplicativos, é finito.

ii) Se $u \in R_1$ é invertível em R_2, então $u^{-1} \in R_1$.

Demonstração. i) De acordo com o lema anterior, existe um inteiro d tal que $dR_2 \subset R_1$ e, quando tomamos R_1 e dR_2 como grupos aditivos, $|R_1 : dR_2| < \infty$. Consideremos então os grupos multiplicativos $\mathcal{U}(R_1)$ e $\mathcal{U}(R_2)$ e os elementos $x, y \in \mathcal{U}(R_2)$ tais que $x + dR_2 = y + dR_2$. Temos então que $xy^{-1} \in 1 + dR_2 \subseteq R_1$ e $yx^{-1} \in 1 + dR_2 \subset R_1$, pois $1 \in R_1$ e $dR_2 \in R_1$. Similarmente $y^{-1}x \in R_1$, o que implica que $xy^{-1} \in \mathcal{U}(R_1)$, ou seja $x\mathcal{U}(R_1) = y\mathcal{U}(R_1)$. Portanto $|\mathcal{U}(R_2) : \mathcal{U}(R_1)| \leq |R_2 : R_1| \leq |R_2 : dR_2| < \infty$.

ii) Seja $u \in R_1 \cap \mathcal{U}(R_2)$. Sendo $u \in \mathcal{U}(R_2)$, tem-se

$$ur + uR_2 = us + uR_2 \iff r + R_2 = s + R_2.$$

Logo, se $\{s_1, \ldots, s_n\}$ é uma transversal para R_2 em R_1, então $us_1, \ldots, us_n$ é uma transversal para uR_2 em R_1. Daí $|R_2 : R_1| = |R_2 : uR_1|$. Sendo $u \in R$, tem-se que $uR \subseteq R_1$, portanto, $uR_1 = R_1$. Como $1 \in R_1$, tem–se $u \in \mathcal{U}(R_1)$. □

Capítulo 2

Unidades em Anéis de Grupos

Os anéis de grupos surgiram pela primeira vez de forma natural no estudo de representações de grupos como matrizes sobre corpos ou, mais geralmente, como endomorfismos de módulos. Um dos principais problemas deste campo é descrever os subgrupos de $\mathcal{U}(RG)$ e, em particular, os elementos de torção. Desde o trabalho seminal de G. Higman [17], o alto grau de complexidade para determinar tais grupos ficou evidenciado na década de setenta, quando foi provado que $\mathcal{U}(\mathbb{Z}G)$ geralmente possui subgrupos livres. Tal problema, especialmente no caso de anéis de grupos integrais de grupos finitos, acabaram por produzir muitos resultados importantes e que combinam várias áreas da matemática. Embora o grupo de unidades de anéis de grupo tenha tenha sido alvo de pesquisa por décadas, relativamente pouco avanço foi feito, no sentido de descriminar explicitamente tais grupos, visto que, até o presente momento, isto só é possível para poucas classes de anéis de grupo. Neste capítulo, falaremos brevemente sobre o conceito de unidades de um anel de grupo e apresentaremos algumas unidades bem conhecidas, tais como unidades unipotentes, bicíclicas, unidades cíclicas de Bass, unidades triviais e unidades de torção. Também demonstraremos algumas propriedades e teoremas importantes.

Seja RG o anel de grupo de G sobre R. Denotamos por $\mathcal{U}(RG)$ o conjunto das unidades de RG, isto é

$$\mathcal{U}(RG) = \{\alpha \in RG : \ \alpha\beta = \beta\alpha = 1, \ \text{ para algum } \beta \in RG\}.$$

Considere a aplicação de aumento

$$\varepsilon : RG \longrightarrow R \quad , \quad \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g \ .$$

Como ε é um homomorfismo, segue que $\varepsilon(\alpha) \in \mathcal{U}(R),\ \forall \alpha \in \mathcal{U}(RG)$. Denotamos por $\mathcal{U}_1(RG)$ o subgrupo das unidades de aumento 1, também chamado de subgrupo das unidades normalizadas, em $\mathcal{U}(RG)$, isto é

$$\mathcal{U}_1(RG) = \{\alpha \in \mathcal{U}(RG) : \varepsilon(\alpha) = 1\}.$$

Se u é uma unidade de $\mathbb{Z}G$, temos que $\varepsilon(u) = \pm 1$ e, portanto,

$$\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G).$$

Analogamente, dado um anel arbitrário R, temos que

$$\mathcal{U}(RG) = \mathcal{U}(R) \times \mathcal{U}_1(RG).$$

Dado $rg \in RG$, onde $r \in \mathcal{U}(R)$ e $g \in G$, note que $r^{-1}g^{-1}$ é seu inverso em RG. Elementos dessa forma são chamados de unidades triviais de RG. Por exemplo, elementos da forma $\pm g$ são as unidades triviais em $\mathbb{Z}G$. Se K é um corpo qualquer, os elementos da forma kg, onde $k \in K,\ k \neq 0$ e $g \in G$ são as unidades triviais de KG.

2.1 Algumas classes de unidades

Uma técnica útil para descrever o grupo das unidades seria determinar uma família de geradores que seja finita, porém, até o momento, é somente para um número pequeno de casos que foi encontrado um conjunto finito de geradores de $\mathcal{U}(RG)$. Por exemplo, as unidades cíclicas foram introduzidas por H. Bass, e utilizadas por ele e J. Milnor para mostrar que elas geram um subgrupo de índice finito no anel $\mathcal{U}(\mathbb{Z}A)$, onde A é um grupo abeliano. No caso não abeliano é necessário introduzir novas unidades, as unidades bicíclicas, denominadas assim por J. Ritter e Sehgal, embora nem sempre estas duas famílias de unidades sejam suficientes para gerar subgrupos de índices finitos.

Unidades unipotentes

Sejam R um anel arbitrário e $\eta \in R$ tal que $\eta^2 = 0$. Note que $1 - \eta^2 = 1$, isto é, $(1+\eta)(1-\eta) = 1$ e desta forma $1 \pm \eta \in \mathcal{U}(R)$. Analogamente, se $\eta \in R$ é tal que $\eta^n = 0$, para algum inteiro positivo n, então

$$(1-\eta)(1+\eta+\cdots+\eta^{n-1}) = 1 - \eta^n = 1,$$

$$(1+\eta)(1-\eta+\eta^2\cdots\pm\eta^{n-1}) = 1 \pm \eta^n = 1.$$

Portanto $1 \pm \eta \in \mathcal{U}(R)$ e estes elementos são chamados de *unidades unipotentes* de R. Por exemplo, se R possui característica $p > 0$ e $g \in G$ é um elemento de ordem p^n, isto é, $g^{p^n} = 1$, temos que $0 = (1 - g^{p^n}) = (1 - g)^{p^n}$ e, então, $\eta = 1 - g \in RG$ é nilpotente. Claramente, $1 - \eta = g$ é uma unidade trivial em RG, porém $1 + \eta = 2 - g$ é uma unidade não trivial, se $char(R) \neq 2$.

Unidades bicíclicas

Sejam $\mathbb{Z}G$ um anel de grupo inteiro e $g \in G$ um elemento de ordem finita n. Note que, como $g^n = 1$, então $g^n - 1 = 0$, donde segue que $(g-1)(1+g+\cdots+g^{n-1}) = 0$. Tomando $h \in G$, podemos construir uma unidade:

$$\mu_{g,h} = 1 + (1-g)h\hat{g}, \quad \text{onde } \hat{g} = 1 + g + \cdots + g^{n-1}.$$

Note que $((1-g)h\hat{g})^2 = 0$, ou seja, $(1-g)h\hat{g}$ é um elemento nilpotente em G e, portanto, como construído acima, segue que $\mu_{g,h}$ é uma unidade em $\mathbb{Z}G$.

Definição 2.1. *Sejam $g \in G$ um elemento de ordem $n < \infty$ e h um elemento qualquer em G. A unidade $\mu_{g,h}$ construída acima é chamada de unidade bicíclica do anel de grupo $\mathbb{Z}G$.*

Denotamos por B_2 o subgrupo de $\mathcal{U}(\mathbb{Z}G)$ gerado por todas as unidades bicíclicas de $\mathbb{Z}G$. Observe que todas as unidades bicíclicas são unidades normalizadas. De fato, $\varepsilon(1 + (1-g)h\hat{g}) = \varepsilon(1) = 1$. Note ainda que, se g e h comutam, então $\mu_{g,h} = 1$.

Proposição 2.2. *Sejam G um grupo e $g, h \in G$, com $o(g) = n < \infty$. Então $\mu_{g,h}$ é trivial se, e somente se, h normaliza $\langle g \rangle$. Neste caso, $\mu_{g,h} = 1$.*

Demonstração. Suponha que $\mu_{g,h}$ é trivial. Como $\varepsilon(\mu_{g,h}) = 1$, existe um elemento $x \in G$ tal que $\mu_{g,h} = x$. Temos então

$$1 + (1-g)h\hat{g} = x,$$

logo

$$1 + h\hat{g} = x + gh\hat{g}.$$

Se $x = 1$, então $h = ghg^i$, para algum inteiro i. Daí, segue que $h^{-1}gh = g^{-i}$. Se $x \neq 1$, como 1 aparece no lado esquerdo da equação, então deve aparecer no lado direito também.

Desta forma, deve existir $j \in \mathbb{Z}$ tal que $ghg^j = 1$ e daí $h = g^{-(j+1)}$. Note que, assim, $x = 1 + (1-g)g^{-(j+1)}\hat{g} = 1 + (1-g)\hat{g}g^{-(j+1)} = 1$, contradição. Portanto h normaliza $\langle g \rangle$ e $\mu_{g,h} = 1$. Reciprocamente, suponha que $h^{-1}gh = g^i$, para algum $i \in \mathbb{Z}$. Então $gh = hg^i$ e, como $g^i\hat{g} = \hat{g}$, segue que $gh\hat{g} = h\hat{g}$. Daí $\mu_{g,h} = 1 + (1-g)h$. □

Segue diretamente que:

Proposição 2.3. *Seja G um grupo finito. O grupo B_2 é trivial se, e somente se, cada subgrupo de G é normal.*

Proposição 2.4. *Toda unidade bicíclica $\mu_{g,h} \neq 1$ de $\mathbb{Z}G$ tem ordem infinita.*

Demonstração. Seja $\mu_{g,h} = 1 + (1-g)h\hat{g}$ uma unidade bicíclica de $\mathbb{Z}G$. Note que

$$\mu_{g,h}^t = (1 + (1-g)h\hat{g})^t = 1 + t(1-g)h\hat{g}, \quad t \in \mathbb{Z}.$$

portanto, para $t \neq 0$, $\mu_{g,h}^t = 1$ se, somente se $(1-g)h\hat{g} = 0$, o que acontece se, e somente se, $\mu_{g,h} = 1$. Se $t = 0$, o resultado é imediato □

Unidades cíclicas de Bass

Consideremos agora $G = \langle g \rangle$ um grupo cíclico de ordem n. Pelos teoremas de Maschke e Wedderburn podemos escrever

$$\mathbb{Q}G \simeq \oplus_{d|n}\mathbb{Q}(\zeta^d)$$

onde ζ é uma raiz n-ésima primitiva da unidade, d é divisor de n, e o isomorfismo é dado da forma abaixo:

$$g \mapsto (1, \ldots, \zeta^d, \ldots, \zeta) \ .$$

Seja $i \in \mathbb{Z}$, $1 < i < n-1$ e $(i,n) = 1$. Considerando $\zeta \neq 1$, note que $\frac{\zeta^i - 1}{\zeta - 1}$ é inversível em $\mathbb{Z}[\zeta]$ e tem inversa $\frac{\zeta - 1}{\zeta^i - 1} = \frac{\zeta^{ik} - 1}{\zeta^i - 1} = \sum_{j=1}^{k} \zeta^{i(j-1)}$, onde $k \in \mathbb{Z}$ e $ik \equiv 1 (\text{mod } n)$. Analogamente, tomemos $x = 1 + \cdots + g^{i-1}$. Note que a projeção de x na primeira componente é i e, portanto, x não é inversível em $\mathbb{Z}G$. Tendo em mente a escolha de i como descrito acima, temos, pelo Teorema de Euler, que $i^{\phi(n)} \equiv 1 (\text{mod } n)$, isto é $i^{\phi(n)} = 1 + kn$, onde $k \in \mathbb{Z}$ e $\phi(n)$ é a função de Euler. Considere agora $y = (1 + \cdots + g^{i-1})^{\phi(n)} - k(1 + \cdots + g^{n-1})$. Como a projeção de $(1 + \cdots + g^{n-1})$ em qualquer outra componente diferente de $\mathbb{Q}$ é 0, segue que a sua projeção em $\mathbb{Q}[\zeta]$ é $(1 + \cdots + \zeta^{i-1})^{\phi(n)} - k(1 + \cdots + \zeta^{n-1}) = (1 + \cdots + \zeta^{i-1})^{\phi(n)}$, que é inversível em $\mathbb{Z}[\zeta]$, e sua projeção em $\mathbb{Q}$ é $i^{\phi(n)} - kn = 1$. Logo y

é unidade em $\mathbb{Z}G$. Além disso, $\varepsilon(y) = 1$ e, portanto, $y \in \mathcal{U}_1(\mathbb{Z}G) \subseteq \mathcal{U}(\mathbb{Z}G)$ é uma unidade normalizada, chamada de *unidade cíclica de Bass*.

Proposição 2.5. *Sejam $g \in G$ um elemento de ordem finita n e $i \in \mathbb{Z}$ tal que $1 < i < n-1$ e $(i, n) = 1$. Então a unidade cíclica de Bass*

$$\mu_i = (1 + \cdots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\hat{g}$$

é de ordem infinita.

2.2 Unidades triviais

Vimos anteriormente que, dados R, anel comutativo com unidade, e G, grupo, uma unidade trivial do anel de grupo RG é um elemento da forma rg, onde $r \in \mathcal{U}(R)$. Nesta seção, vamos abordar resultados importantes nos anéis de grupos integrais utilizando tais unidades, bem como vamos demonstrar o Teorema de Higman.

Proposição 2.6. *Seja $G^* = G \times \langle x \rangle$, tal que $x^2 = 1$. Então*

$$\mathcal{U}(\mathbb{Z}G) = \pm G \implies \mathcal{U}(\mathbb{Z}G^*) = \pm G^*.$$

Demonstração. Consideremos $\alpha, \beta, \gamma, \lambda \in \mathbb{Z}G$ tais que $(\alpha + \beta x)(\gamma + \lambda x) = 1$, isto é, de tal forma que $\alpha + \beta x$ e $\gamma + \lambda x \in \mathcal{U}(\mathbb{Z}G^*)$. Queremos mostrar que, se α e β são unidades triviais em $\mathbb{Z}G$, então $\alpha + \beta x$ é uma unidade trivial em $\mathbb{Z}G^*$. Como $(\alpha + \beta x)(\gamma + \lambda x) = 1$, temos

$$(\alpha\gamma + \beta\lambda) + (\alpha\lambda + \beta\gamma)x = 1,$$

donde segue que $\alpha\gamma + \beta\lambda = 1$ e $\alpha\lambda + \beta\gamma = 0$. Somando e subtraindo estas equações, temos, respectivamente, as seguintes igualdades

$$(\alpha + \beta)(\gamma + \lambda) = 1 \text{ e } (\alpha - \beta)(\gamma - \lambda) = 1.$$

Segue, particularmente, que $\alpha + \beta$ e $\alpha - \beta \in \mathcal{U}(\mathbb{Z}G)$. Como, por hipótese, as unidades $\mathbb{Z}G$ são triviais, vem que

$$\alpha + \beta = \pm g \text{ e } \alpha - \beta = \pm g', \quad g, g' \in G$$

Somando-se novamente as equações acima, temos $2\alpha = \pm g \pm g'$. Como as únicas maneiras onde o coeficiente do elemento $\pm g \pm g'$ seja par é quando $g = \pm g'$, concluímos então que $\alpha = 0$ ou $\beta = 0$ e, portanto a unidade $\alpha + \beta x$ é trivial. □

Proposição 2.7. *Seja Q_8 o grupo dos Quatérnios de ordem 8. Então $\mathcal{U}(\mathbb{Z}Q_8) = \pm Q_8$.*

Demonstração. Seja $Q_8 = \langle x, y \mid x^4 = 1 = y^4,\ x^2 = y^2,\ yx = x^{-1}y\rangle$. Tomando $z = xy$ e $\alpha = (a_0 + a_1x + a_2y + a_3z) + (b_0 + b_1x + b_2y + b_3z)x^2$ uma unidade de $\mathbb{Z}Q_8$, considere o homomorfismo $\psi : \mathbb{Z}Q_8 \longrightarrow \mathbb{Z}[i,j,k]$ tal que $x \mapsto i, y \mapsto j, z \mapsto k$, onde $\mathbb{Z}[i,j,k] = \{a_0 + a_1i + a_2j + a_3k : a_i \in \mathbb{Z}, i = 0,1,2,3\}$ é o anel dos quatérnios integral. Temos que a imagem de α é $(a_0 - b_0) + (a_1 - b_1)i + (a_2 - b_2)j + (a_3 - b_3)k$. Como as unidades de $\mathbb{Z}[i,j,k]$ são $\pm 1, \pm i, \pm j, \pm k$, segue que

$$a_p - b_p = \pm 1, \quad p = 0,1,2,3 \ \text{ e } \ a_q - b_q = 0, \quad \text{se } q \neq p. \tag{2.2.1}$$

Considere agora o grupo $H = \langle x'\rangle \times \langle y'\rangle$ e um homomorfismo $\psi' : \mathbb{Z}Q_8 \longrightarrow \mathbb{Z}H$ tal que $x \mapsto x', y \mapsto y'$. Note que a imagem de α pela ψ' é $(a_0 + b_0) + (a_1 + b_1)x' + (a_2 + b_2)y' + (a_3 + b_3)x'y'$. Como as unidades de $\mathbb{Z}H$ são triviais, segue da proposição anterior que

$$a_m + b_m = \pm 1, \quad m = 0,1,2,3 \ \text{ e } \ a_n + b_n = 0, \quad \text{se } m \neq n. \tag{2.2.2}$$

Seque de (2.2.1) e (2.2.2) que $p = m$ e

$$a_m = \pm 1, b_m = 0,\ m = 1,2,3 \text{ e } a_n = b_n = 0 \text{ se } n \neq m$$

ou

$$a_m = 0, b_m = \pm 1,\ m = 1,2,3 \text{ e } a_n = b_n = 0 \text{ se } n \neq m,$$

Procedendo analogamente ao que foi feito na demonstração da proposição anterior, concluímos que α é uma unidade trivial e o resultado segue. □

Corolário 2.8. *Seja $G = E \times Q_8$, onde E é um 2-grupo abeliano elementar e Q_8 é o grupo dos Quatérnios de ordem 8. Então $\mathcal{U}(\mathbb{Z}G) = \pm G$.*

Demonstração. Segue das proposições (2.7) e (2.6). □

Proposição 2.9. *Seja $\langle g\rangle$ um grupo cíclico de ordem n. Seja ζ_d uma d-ésima raiz primitiva da unidade, onde d é divisor de n. Então existe um isomorfismo*

$$\theta : \mathbb{Q}\langle g\rangle \longrightarrow \oplus_{d|n}\mathbb{Q}(\zeta_d) \quad e \quad \theta(\mathbb{Z}\langle g\rangle) \subseteq \oplus_{d|n}\mathbb{Z}[\zeta_d].$$

Demonstração. Considere $\zeta_n = \zeta$ e a aplicação $\theta : \mathbb{Q}\langle g\rangle \longrightarrow \oplus_{d|n}\mathbb{Q}(\zeta_d)$ tal que $q_ig^i \mapsto q_i + \cdots + q_i\zeta_d^i + \cdots + q_i\zeta^i$. Como $dim_{\mathbb{Q}}(\oplus_{d|n}\mathbb{Q}(\zeta_d)) = \sum_{d|n}\phi(d) = n$, para mostrar que

θ é um isomorfismo, basta verificar que tal aplicação é injetora. Suponha então que $\theta\left(\sum_i q_i g^i\right) = 0$. Logo $q_i + \cdots + q_i\zeta_d^i + \cdots + q_i\zeta^i = 0$. Como $\{1, \cdots, \zeta_d^i, \cdots \zeta^i\}$, $d|n$, é um conjunto linearmente independente, segue que $q_i = 0, \forall\ i$ e, portanto, θ é isomorfismo. Além disso, se $z_i \in \mathbb{Z}$, $\theta(z_i g^i) = z_i + \cdots + z_i\zeta_d^i + \cdots + z_i\zeta^i$. Logo $\theta(\mathbb{Z}\langle g\rangle) \subseteq \oplus_{d|n}\mathbb{Z}[\zeta_d]$. □

Proposição 2.10. *Seja R subanel de $\mathbb{Q}G$ contendo $\mathbb{Z}G$. Suponha que R é finitamente gerado como $\mathbb{Z}$-módulo. Então $(\mathcal{U}(R) : \mathcal{U}(\mathbb{Z}G)) < \infty$.*

Demonstração. Segue do item i. do Lema (1.42) Como $\mathbb{Z}G \subseteq R$ são ordens em $\mathbb{Q}G$ vale que $(\mathcal{U}(R) : \mathcal{U}(\mathbb{Z}G)) < \infty$. □

Lema 2.11. *Todas as unidades de $\mathbb{Z}\langle a\rangle$ são triviais se, e somente se, $o(a) = 1, 2, 3, 4$ ou 6.*

Demonstração. ($\Rightarrow$) Seja $n = o(a)$. Suponha, por absurdo, que $n = 5$ ou $n > 6$. Como $\phi(n) > 2$, teríamos então a existência de unidades cíclicas de Bass não triviais em $\mathcal{U}(\mathbb{Z}\langle a\rangle)$, contradizendo a hipótese. Portanto $n = 1, 2, 3, 4$ ou 6.

($\Leftarrow$) Para o caso em que $n = 1$ ou 2 o resultado segue. Para os demais casos, considere um isomorfismo $\psi : \mathbb{Z}\langle a\rangle \longrightarrow \mathbb{Z}[\zeta_d], a^i \mapsto \zeta_d^i,\ i = 1, \cdots, n$. Afirmamos que, se ζ_d é uma raiz da unidade de ordem 3 ou 4, então as unidades do anel $\mathbb{Z}[\zeta_d]$ são triviais. O resultado segue. Se $\alpha = x_0 + x_a + \cdots + x_n a^n \in \mathcal{U}(\mathbb{Z}\langle a\rangle)$, então $\psi(\alpha) = x_0 + x_1\zeta_d + x_n\zeta_d^n \in \mathcal{U}(\mathbb{Z}[\zeta_d])$ e como $\mathcal{U}(\mathbb{Z}[\zeta_d]) = \{\pm\zeta_d^i\}$, segue que α também é trivial. □

Lembramos que, se G é um grupo abeliano, então todos os seus subgrupos são normais, mas a recíproca não é verdadeira. Se G é um grupo não comutativo cujos subgrupos são todos normais, chamamos tal G de grupo Hamiltoniano e pode-se provar que ele é da forma $G = Q \times A \times E$, onde Q é o grupo dos quatérnios de ordem 8, E é um 2-grupo abeliano elementar e A é um grupo abeliano cujos elementos são de ordem ímpar (veja [36]; Teorema 1.8.5).

Teorema 2.12. ***(Higman)*** *Seja G grupo finito. As unidades de $\mathbb{Z}G$ são triviais se, e somente se, G é abeliano de expoente 2, 3, 4 ou 6 ou $G = E \times Q$, onde E é um 2-grupo abeliano elementar e Q é o grupo dos quatérnios de ordem 8.*

Demonstração. ($\Leftarrow$) Segue do Corolário 2.8 e do Lema 2.11. ($\Rightarrow$) Seja G grupo finito tal que $\mathcal{U}(\mathbb{Z}G) = \pm G$. Desta forma, considere então a unidade bicíclica $1 + (1 - g)h\hat{g} = x,\ x \in G$. Temos que $1 + h\hat{g} = gh\hat{g} + x$ e assim $h = ghg^i$. Consequentemente $g^{-i} = h^{-1}gh$ e, portanto, $\langle g\rangle \trianglelefteq G,\ \forall g \in G$. Temos então que G é um grupo abeliano ou Hamiltoniano.

No caso em que G é abeliano, suponha, por absurdo, que G tem expoente $n = 5$ ou $n > 6$. Em ambos os casos, note que $\phi(n) > 2$ e portanto $\mathbb{Z}G$ teria uma unidade cíclica de Bass não trivial. Absurdo, visto que G é grupo finito. No caso em que G é Hamiltoniano, lembrando que $G = Q \times A \times E$, suponha, por absurdo, que G não é um 2-grupo. Deve existir então $x \in A$ de ordem $p > 2$ tal que $g = kx,\ g \in G$ e $o(g) = 4p$, onde k é um dos geradores de Q de ordem 4. Assim, $\phi(n) > 2$ e portanto $\mathbb{Z}G$ possui uma unidade cíclica de Bass não trivial, contradição. □

2.3 Unidades de Torção

Sejam G grupo e R um anel. Dizemos que $\alpha \in \mathcal{U}(RG)$ é uma unidade de torção se existe um inteiro positivo $n \in \mathbb{Z}$ tal que $\alpha^n = 1$.

Teorema 2.13. *Seja* $\alpha = \sum_{g \in G} a_g g \in \mathbb{Z}G$ *tal que* $\alpha^n = 1$, *para algum inteiro positivo* n. *Se o coeficiente do elemento neutro de* α *é não nulo, isto é,* $a_1 \neq 0$, *então* $\alpha = \pm 1$.

Demonstração. Para cada $x \in \mathbb{Q}G$ vamos considerar a representação regular de $\mathbb{Q}G$ dada por

$$L_x : \mathbb{Q}G \to \mathbb{Q}G$$
$$y \mapsto xy$$

Represente L_x por uma matriz em relação à base $\{g_1, g_2, \ldots, g_m\}$ de $\mathbb{Q}G$ formada pelos elementos de G, onde $m = |G|$. Para $g \in G$, $L_g(g_i) = g_i$ se, e somente se, $g = 1$. Portanto, para $g \in G$, traço de L_g, trL_g, é dado por

$$trL_g = \begin{cases} 0 & \text{se} \quad g \neq 1 \\ |G| & \text{se} \quad g = 1 \end{cases}$$

Como $\alpha^n = 1$, então $(L_\alpha)^n = I_m$, onde I_m representa a matriz identidade de ordem m. Podemos então diagonalizar L_α. Seus autovalores são raízes n-ésimas da unidade $\zeta_i, 1 \leq i \leq m$. Portanto, temos

$$\sum_{i=1}^{m} \zeta_i = trL_g \ = \ \sum_g \alpha_g trL_g = \alpha_1 |G|$$

Como $\alpha_1 \neq 0$ é inteiro, temos que $|\alpha_1| \geq 1$. Além disso, $|\zeta_i| = 1$. Assim obtemos

$$|\sum_i \zeta_i| \leq \sum_i |\zeta_i| = m = |G|$$

e

$$|\alpha_1|G|| \geq |G|$$

Pelas três equações acima segue que $|\sum_1^m \zeta_i| = \sum_1^m |\zeta_i| = |G|$. Portanto $\zeta_i = \zeta, \forall i$. Segue que $L_\alpha = \zeta I_m$, e, assim, $\alpha = \zeta \cdot 1$. Como $\alpha \in \mathbb{Z}G$, temos que $\zeta = \pm 1$. □

Proposição 2.14. *Seja R um anel comutativo. A aplicação $^* : RG \to RG$ definida por*

$$(\sum_{g\in G} a_g g)^* \mapsto \sum_{g\in G} a_g g^{-1}$$

satisfaz as seguintes propriedades:

i) $(\alpha + \beta)^* = \alpha^* + \beta^*$,

ii) $(\alpha\beta)^* = \beta^*\alpha^*$,

iii) $(\alpha^*)^* = \alpha$.

Demonstração. De fato, sejam $\alpha = \sum_g a_g g$, $\beta = \sum_h b_h h$ e a aplicação * como definida acima. Temos então que:

i) $(\alpha + \beta)^* = \Big((\sum_g a_g g) + (\sum_h b_h h)\Big)^* = \Big(\sum_g (a_g + b_g) g\Big)^* = \sum_g (a_g + b_g) g^{-1} =$
$= \sum_g a_g g^{-1} + \sum_h b_h h^{-1} = \alpha^* + \beta^*$;

ii) $(\alpha \cdot \beta)^* = \Big((\sum_g a_g g) \cdot (\sum_h b_h h)\Big)^* = \Big(\sum_{g\cdot h} (a_g b_h) gh\Big)^* = \sum_{g\cdot h} (a_g b_h)(gh)^* =$
$= \sum_{g\cdot h} (a_g b_h)(h^{-1} g^{-1}) = \sum_g (b_h a_g) h^{-1} g^{-1} = (\sum_h b_h h^{-1})(\sum_g a_g g^{-1}) = \beta^*\alpha^*$;

iii) $(\alpha^*)^* = \Big((\sum_g a_g g)^*\Big)^* = (\sum_g a_g g^{-1})^* = \sum_g a_g (g^{-1})^{-1} = \sum_g a_g g$.

Perceba que a antepenúltima igualdade do item ii) acima só é válida pois R é anel comutativo. □

Corolário 2.15. *Suponha que exista $\alpha \in \mathbb{Z}G$ tal que α e α^* comutam. Se α é uma unidade de torção, então $\alpha = \pm g$ para algum $g \in G$.*

Demonstração. Sejam $\alpha = \sum_{g\in G} a_g g$ e, consequentemente $\alpha^* = \sum_{g\in G} a_g g^{-1}$. Suponha que α seja uma unidade de torção. Então $\exists n \in \mathbb{Z}$ tal que $\alpha^n = 1$. Como α e α^* comutam, segue que $(\alpha\alpha^*)^n = 1$. Perceba que $(\alpha\alpha^*)_1 = \sum_{g\in G} a_g^2 \neq 0$, isto é, o coeficiente do elemento neutro de $\alpha\alpha^*$ é não nulo. Pelo teorema anterior, segue que $\alpha\alpha^* = 1$ e como $a_g \in \mathbb{Z}$, so pode ser que $\alpha = \pm g$. □

Do corolário acima, os resultados a seguir seguem imediatamente.

Corolário 2.16. *Todas as unidades de torção centrais em $\mathbb{Z}G$ são triviais.*

Teorema 2.17. *Seja A um grupo abeliano finito. Então o grupo das unidades de torção do anel de grupo inteiro $\mathbb{Z}A$ é $\pm A$.*

Capítulo 3

As Conjecturas de Zassenhaus

Em sua tese, Higman apresentou resultados importantes que implicam que o Problema do Isomorfismo, em anéis de grupos integrais, possui solução positiva caso o grupo em questão seja abeliano finito. Especificamente, ele mostrou que se G é abeliano finito, então todas as unidades de torção em $\mathcal{U}(\mathbb{Z}G)$ são triviais. Contudo, tal resultado não pode ser estendido ao caso de grupos não abelianos, visto que conjugado de unidades triviais são unidades de torção, geralmente não triviais. Higman também observou que $\mathcal{U}_1(\mathbb{Z}S_3)$ contém unidades de torção que não são trivialmente conjugadas em $\mathcal{U}(\mathbb{Z}S_3)$, porém, algum tempo depois, Pearson e Hughes mostraram que o mesmo não ocorrem em se tratando de $\mathbb{Q}S_3$, isto é, as unidades de torção em $\mathcal{U}_1(\mathbb{Z}S_3)$ são sim conjugadas em $\mathbb{Q}S_3$ a elementos de S_3. Baseado em ambos os resultados aqui apresentados, Zassenhaus formulou as três conjecturas que apresentamos um pouco mais abaixo. Neste último capítulo, apresentamos um breve levantamento dos trabalhos já desenvolvidos em torno das conjecturas, com ênfase no recente trabalho desenvolvido por Eisele e Margolis [12], onde foram apresentados contraexemplos para ZC1, a última das conjecturas que permanecia sem solução negativa até o momento.

Como mencionado acima, foi motivado fortemente pelos resultados oriundos da tese de Higman que Hans Zassenhaus fez fortes conjecturas a respeito dos subgrupos finitos das unidades do anel de grupo integral, para grupos finitos. Essas conjecturas, chamadas de primeira, segunda e terceira conjectura de Zassenhaus, causaram grande impacto na pesquisa em anéis de grupos. Seguem abaixo tais conjecturas bem como são conhecidas.

(ZC1) Para toda unidade de torção $u \in \mathcal{U}(\mathbb{Z}G)$, existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $u^\alpha \in \pm G$.

(ZC2) Para todo subgrupo finito H de $\mathcal{U}_1(\mathbb{Z}G)$ com $|H| = |G|$, existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $H^\alpha = G$.

(ZC3) Para todo subgrupo finito H de $\mathcal{U}_1(\mathbb{Z}G)$, existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $H^\alpha \subseteq G$.

Um certo suporte para estas conjecturas também vem dos seguintes resultados: Se H é um subgrupo finito de $\mathcal{U}_1(\mathbb{Z}G)$ então sua ordem divide a ordem de G [44] e seus elementos são linearmente independentes sobre $\mathbb{Q}$ [18]. Os expoentes de G e $\mathcal{U}_1(\mathbb{Z}G)$ coincidem e isto ainda é verdade caso troque $\mathbb{Z}$ por qualquer anel de inteiros algébricos [8].

As conjecturas de Zassenhaus têm sido alvo de intensa pesquisa desde a época de sua formulação. Claramente, ZC3 implica ZC2 e ZC1, assim é a mais forte das três conjecturas. Em geral, grupos nilpotentes fornecem solução positiva para todas as três conjecturas e a demonstração dada por Weiss, em [42], para ZC3 trouxe grande impacto na pesquisa pela sua sofisticação e complexidade. A terceira conjectura é ainda válida para os casos em que:

- $G = \langle x \rangle \times \langle y \rangle$ tal que $(o(x), o(y)) = 1$,
- $G = S_4$ (M. Dokuchaev e S.O. Juriaans, [10]),
- $G = D_8$ (Polcino, [37]),
- $G = S_5$, A_5 e $SL(2,5)$ (Dokuchaev, Juriaans e Polcino, [11]),
- $|G| = p^2q$, onde p e q são primos (J. H. Liu, [25]),
- Grupos G tais que todos os seus subgrupos de Sylow são cíclicos (Juriaans e Polcino ,[23]).

Já para ZC2, entre as soluções positivas temos os seguintes grupos:

- Todo grupo simples finito que possua 2-subgrupos de Sylow abelianos e também para todo grupo de tipo Lie de posto 1 ou 2, de modo que não são isomorfos aos grupos unitários $PSU(4, q^2)$ ou $PSU(5, q^2)$ (F.M. Bleher, [4]),
- Grupos simétricos (Peterson, [38]),

- Grupos finitos que possuam p-subgrupos de Sylow normais N tais que o centralizador de N em G está contido em G (Hertwek e Kimmerle, [16]),

- Grupos Coxeter (Bleher e Geck, [5]).

Em 1972, Hughes e Pearson mostraram que vale ZC1 para o caso em que $G = S_3$, além de descreverem explicitamente a estrutura de $\mathcal{U}(\mathbb{Z}S_3)$ em [19]. Pouco tempo depois, no ano de 1973, utilizando método similar ao usado no trabalho supracitado, Polcino também apresentou resposta positiva para ZC1 no caso onde $G = D_8$. A primeira conjectura já foi validada ainda, por I. Luthar e A. Bhandari, para grupos metacíclicos da forma $G = \langle x, y : x^p = y^q = 1\rangle$, onde p e q são primos, $p \equiv 1 \bmod q$, $j^q \equiv 1 \bmod p$, $j \not\equiv 1 \bmod p$, expressando $\mathcal{U}_1(\mathbb{Z}G)$ e $\mathcal{U}_1(\mathbb{Q}G)$ como produto semidireto de grupos de matrizes de ordem q. Polcino, J. Ritter e Sehgal mostraram que grupos metacíclicos da forma $G = \langle x\rangle \rtimes \langle y\rangle$, onde $(o(x), o(y)) = 1$ também fornecem solução verdadeira para ZC1. No mais, ainda oferecem resposta positiva para a primeira conjectura de Zassenhaus os seguintes grupos:

- S_4 (N. Fernandes, [13]),

- A_5 (Luthar e Passi, [26]),

- A_6 (Hertweck, [15]),

- $\mathrm{GL}(2, 5)$ (Bovdi e Hertweck, [6]),

- S_5 (Luthar e P. Trama, [29]),

- para o caso $G = \langle x\rangle \rtimes H$, onde H é abeliano e $(o(x), |H|) = 1$ (Luthar e Trama, [28]),

- $A \rtimes \langle b\rangle$, onde A é abeliano b é elemento de ordem menor que qualquer divisor primo de $|A|$ (Marciniak, Ritter, Sehgal e Weiss, [30]),

- Grupos com subgrupo normal abeliano de índice 2 (Luthar, Sehgal, [27]),

- Grupos cíclico por abeliano (Caicedo, Margolis e del Río, [7]),

- Grupos de Frobenius de ordem $p^a q^b$, onde p e q são primos (O. Juriaans e Polcino, [23]),

- $A \times F$, onde A é abeliano e F grupo de Frobenius com complemento de ordem ímpar (A. Bächle, W. Kimmerle e M. Serrano, [1]),
- $P \rtimes A$, onde P é um p-grupo e A um p'-grupo abeliano (Hertweck, [14]),
- $PSL(2,q)$, $q \leq 25$ ou $q \in \{31, 32\}$ (Bächle e Margolis, [2]),
- $PSL(2,p)$, onde p é primo de Mersenne ou de Fermat (Margolis, del Río e Serrano, [31]),
- $SL(2,p)$ ou $SL(2,p^2)$ (del Río e Serrano, [9]), entre outros.

Ao longo dos anos foram surgindo soluções negativas para a segunda e terceira conjectura, porém, nenhum contraexemplo para ZC1 fora encontrado até então, por isso ela passou a ser tratada como A Conjectura de Zassenhaus.

Olhando para os vários resultados positivos encontrados ao longo dos anos na classe de grupos metabelianos para outros problemas que, inclusive, têm certa ligação com as conjecturas, parece que tais grupos teriam sido o próximo passo lógico para uma solução positiva e, certamente, vários pesquisadores da área tentaram provar as conjecturas de Zassenhaus para tais grupos, mas sem sucesso. Grupos metabelianos foram uma das primeiras classes de grupos para os quais o problema de isomorfismo em anéis de grupo integrais eram conhecidos por terem uma resposta positiva (veja [12]). Por outro lado, essa classe de grupos proporcionou o contraexemplo de E. Dade à pergunta de R. Brauer, que questionou se, $KG \simeq KH$, para todo corpo K, implica que G e H são isomorfos. Foi na classe de grupos metabelianos super solúveis onde encontraram-se os primeiros contraexemplos para ZC2 e, em particular ZC3, construídos por Roggenkamp e Scott para serem, a princípio, uma solução negativa para o problema do automorfismo (AUT), que apresentamos brevemente abaixo:

(AUT) Será que todos os automorfismo normalizados de $\mathbb{Z}G$ são a composição da extensão linear de um automorfismo de G e a restrição a $\mathbb{Z}G$ de um automorfismo interno de $\mathbb{Q}G$?

Tendo este último ponto em vista, já que contraexemplos para ZC2 foram encontrados, nada mais natural do que enfraquecer a conjectura e testá-la. Por exemplo, apresentamos abaixo uma versão de ZC2 que também continua em aberto:

(p-ZC) Seja H um subgrupo de $\mathcal{U}_1(\mathbb{Z}G)$ que é um p–grupo finito. Então existe uma unidade $\alpha \in \mathbb{Q}G$ tal que $H^\alpha \subset G$?

A validade desse caso já foi demonstrada para grupos que são do tipo nilpotente por nilpotente, grupos solúveis cujas ordens não são divisíveis pela quarta potência de um primo e grupos solúveis tais que todo p-subgrupo de Sylow é abeliano ou quatérnio generalizado (Dokuchaev e Juriaans, [10]). Também é uma solução verdadeira para p-ZC o caso de grupos de Frobenius em geral, quando $p > 2$, e para grupos de Frobenius que não têm imagem homomorfa isomorfa a S_5, quando $p = 2$ (Dokuchaev, Juriaans e Polcino, [11]).

3.1 A construção do contraexemplo

A ideia que grupos como aqueles apresentados no artigo de Eisele–Margolis [12] podem ser bons candidatos a contraexemplos para a conjectura de Zassenhaus foi observada em [33], na tentativa de criar algoritmos para estudar uma versão restringida da conjectura, conhecido como 35º Problema de Sehgal. Como podemos ver na lista acima, muitos dos grupos para os quais a conjectura já foi provada possuem um subgrupo normal N tal que, tanto N quanto G/N possuem boas propriedades, tais como, são abelianos, cíclicos, nilpotentes, entre outras, e o 35° Problema de Sehgal está focado nesta situação.

Dado um subgrupo normal N de um grupo G, temos um homomorfismo

$$\omega_N : \mathbb{Z}G \to \mathbb{Z}(G/N) \quad , \quad \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g Ng$$

ou seja, ω_N é a extensão linear do homomorfismo canônico $G \to G/N$. Definimos então

$$V(\mathbb{Z}G, N) = \{\ u \in \mathcal{U}_1(\mathbb{Z}G) \mid \omega_N(u) = 1\ \} \ ,$$

e observamos que, sendo $\omega_N(x) = \varepsilon(x) \cdot 1 \in \mathbb{Z}(G/N)$ para todo $x \in \mathbb{Z}N$, vale

$$\mathcal{U}_1(\mathbb{Z}N) \subseteq V(\mathbb{Z}G, N) \ .$$

Supondo que ZC1 possui solução afirmativa para N, é natural perguntar se este resultado estende-se às unidades de torção em $V(\mathbb{Z}G, N)$. Em particular, sabendo que grupos nilpotentes satisfazem a afirmação de ZC1, temos o seguinte:

35º Problema de Sehgal. *Sejam G um grupo finito e N um subgrupo normal nilpotente de G. Considere $u \in V(\mathbb{Z}G, N)$ um elemento de torção. Então u é conjugado a um elemento de G em $\mathcal{U}(\mathbb{Q}G)$?*

Ángel del Rio e Margolis demostram a solução afirmativa no caso em que N possui no máximo um subgrupo de Sylow não cíclico [32, Corolário 5.4]. Em seguida, os mesmos autores escrevem alguns algoritmos capazes de resolver o $35^{\underline{o}}$ Problema de Sehgal assumindo alguma restrição adicional sobre a estrutura de N [33]. Os algoritmos são desenhados para retornar o valor `true` em caso de resposta afirmativa e, em caso contrario, os aumentos parciais das unidades de torção que não são racionalmente conjugadas com as unidades triviais. Depois de obter vários resultados afirmativos, os autores focam no caso metabeliano, que já forneceu contraexemplos para ZC2 e ZC3. Em vista do resultado acima e assumindo que ambos N e G/N são abelianos, é natural analisar em primeiro lugar o caso mínimo, no qual

$$N \simeq (C_p \times C_p) \times (C_q \times C_q)$$

onde p e q são primos distintos. Contudo, os algoritmos não podiam resolver completamente este caso, sendo assim, Eisele e Margolis decidiram estudar a fundo alguns dos grupos para os quais o novo método não funcionava [12]. Precisamente, por meio da identificação de N com o grupo aditivo $\mathbb{F}_{p^2} \times \mathbb{F}_{q^2}$, os contraexemplos encontram-se entre subgrupos de um produto direto de grupos afins.

Seja p um número primo, e considere o corpo com p^2 elementos $\mathbb{F}_{p^2}$. Lembramos que uma forma de representar $\mathbb{F}_{p^2}$ é considerar o corpo de decomposição do polinômio $f(X) = X^{p^2} - X$ sobre $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ou, alternativamente, considerar um polinômio irredutível $g(X)$ de grau 2 em $\mathbb{F}_p[X]$ e identificar $\mathbb{F}_{p^2}$ com o quociente $\mathbb{F}_p[X]/I$ do anel de polinômios $\mathbb{F}_p[X]$ sobre o ideal $I = (g(X))$. Assim, o grupo aditivo $N = (\mathbb{F}_{p^2}, +)$ é produto direto de dois grupos cíclicos de ordem p, sendo que $I + aX + b = (I + aX) + (I + b)$ com $a, b \in \mathbb{F}_p$, para todo elemento de N. Por sua vez, é bem conhecido que o grupo multiplicativo $L = (\mathbb{F}_{p^2}^{\times}, \cdot\ )$ é cíclico de ordem $p^2 - 1$, e seus geradores são chamados de *elementos primitivos*. Por definição, tais elementos existem sempre, apesar da dificuldade que pode surgir na tarefa de calcular explicitamente quais as classes laterais $I + aX + b$ correspondem a elementos primitivos em $\mathbb{F}_{p^2}$. O grupo L age por multiplicação sobre N, assim pode-se considerar o produto semidireto $N \rtimes L$. Este grupo é também conhecido como *grupo afim* $\mathrm{GA}_1(\mathbb{F}_{p^2})$ de posto 1 sobre $\mathbb{F}_{p^2}$, sendo em geral $\mathrm{GA}_d(\mathbb{F}) = \mathbb{F}^d \rtimes \mathrm{GL}_d(\mathbb{F})$ para qualquer inteiro positivo d e qualquer corpo $\mathbb{F}$. Agora, fixados dois primos p e q, formamos o produto direto

$$\Gamma = \mathrm{GA}_1(\mathbb{F}_{p^2}) \times \mathrm{GA}_1(\mathbb{F}_{q^2})\ .$$

Podemos descrever este grupo considerando desta vez o grupo aditivo $N = \mathbb{F}_{p^2} \times \mathbb{F}_{q^2}$, sobre o qual o grupo multiplicativo $L = \mathbb{F}_{p^2}^{\times} \times \mathbb{F}_{q^2}^{\times}$ age da seguinte forma

$$\forall\ v = (x, y) \in \mathbb{F}_{p^2} \times \mathbb{F}_{q^2}\ ,\ \lambda = (s, t) \in \mathbb{F}_{p^2}^{\times} \times \mathbb{F}_{q^2}^{\times} \quad :\quad v^{\lambda} = (x, y)^{(s,t)} = (sx, ty)\ ,$$

e obtemos uma decomposição em produto semidireto $\Gamma = N \rtimes L$. Portanto, dado um subgrupo qualquer A de L obtemos um grupo metabeliano $G = N \rtimes A$, onde podemos testar o $35^{\underline{o}}$ de Sehgal para $V(\mathbb{Z}G, N)$.

Em particular, supondo haver um divisor comum d de $p^2 - 1$ e $q^2 - 1$ e fixados elementos primitivos $\alpha \in \mathbb{F}_{p^2}$ e $\beta \in \mathbb{F}_{q^2}$, Eisele e Margolis consideram o subgrupo A de L gerado pelos elementos $a = (\alpha^d, 1)$, $b = (1, \beta^d)$, e $c = (\alpha, \beta)$. Observando que $o(a) = o(\alpha^d) = \frac{o(\alpha)}{d} = \frac{p^2-1}{d}$, $o(b) = \frac{q^2-1}{d}$ e $c^d = ab$, os autores obtêm uma apresentação para A, chegando à definição [12]:

Definição 3.1. *Sejam p e q primos distintos, d um divisor comum de $p^2 - 1$ e $q^2 - 1$, porém, que não divide $p + 1$ nem $q + 1$, e sejam α e β elementos primitivos de $\mathbb{F}_{p^2}$ e $\mathbb{F}_{q^2}$, respectivamente. Considere o grupo aditivo $N = \mathbb{F}_{p^2} \times \mathbb{F}_{q^2}$, e o grupo abeliano*

$$A = \langle\ a, b, c \mid [a, b] = [a, c] = [b, c] = a^{\frac{p^2-1}{d}} = b^{\frac{q^2-1}{d}} = 1\ ,\ c^d = ab\ \rangle\ ,$$

junto a uma ação de A sobre N é determinada pelas relações

$$(u, v)^a = (\alpha^d u, v) \quad , \quad (u, v)^b = (u, \beta^d v) \quad , \quad (u, v)^c = (\alpha u, \beta v)\ .$$

Então o produto semidireto $G = N \rtimes A$ é o grupo $G = G(p, q; d; \alpha, \beta)$.

Observe que a descrição de G como subgrupo de Γ nos permite de verificar com facilidade algumas das propriedades de G, por exemplo, temos que todo elemento de A escreve-se de forma única como $a^r \cdot b^s \cdot c^t = (\alpha^{dr+t}, \beta^{ds+t})$ onde $r \in \{1, \ldots, (p^2 - 1)/d\}$, $s \in \{1, \ldots, (q^2 - 1)/d\}$, e $t \in \{0, \ldots, d - 1\}$, em particular temos

$$|A| = \frac{(p^2 - 1)(q^2 - 1)}{d} \quad , \quad |G| = \frac{p^2(p^2 - 1)q^2(q^2 - 1)}{d}\ .$$

Consequentemente, o foco principal do trabalho de Eisele e Margolis é a demonstração dos Teoremas A e B que seguem:

Teorema A. *Seja $G = G(7, 19; 3; \alpha, \beta)$, onde α é uma raiz do polinômio $x^2 - x + 3$ sobre $\mathbb{F}_7$ e β é uma raiz do polinômio $x^2 - x + 2$ sobre $\mathbb{F}_{19}$. Então existe uma unidade $u \in \mathcal{U}(\mathbb{Z}G)$ de ordem $7 \cdot 19$ tal que u não é conjugada em $\mathbb{Q}G$ a qualquer elemento da forma $\pm g$ com $g \in G$. Em particular, a conjectura de Zassenhaus não é válida para G.*

Assim, o primeiro contraexemplo $G = G(7, 19; 3; \alpha, \beta)$ para ZC1 é um grupo metabeliano de ordem $2^7 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 19^2$ cujo anel de grupo integral possui unidade de ordem $7 \cdot 19$ que não é racionalmente conjugado a nenhuma unidade trivial. Além deste resultado de grande relevância, Eisele e Margolis demonstram a existência de uma quantidade ilimitada de contraexemplos, por meio da seguinte generalização:

Teorema B. *Sejam d um inteiro positivo ímpar e $n \in \mathbb{N}$ arbitrário. Então existem infinitos pares de primos p e q tais que, para qualquer escolha de α, β, para $G = G(p, q; d; \alpha, \beta)$, existem $u_1, \cdots u_n \in \mathcal{U}(\mathbb{Z}G)$, cada uma de ordem pq, tal que nenhum dos u_i é conjugado em $\mathcal{U}(\mathbb{Q}G)$ a algum elemento da forma $\pm g$, onde $g \in G$ ou a qualquer outro $u_j, j \neq i$. Em particular, a conjectura de Zassenhaus não é válida para tal grupo G.*

Várias décadas após sua formulação, finalmente foram encontrados contraexemplos para A conjectura de Zassenhaus. Como todas as três conjecturas já são demonstradamente não verdadeiras de modo geral, nada mais natural do que estudar as versões mais fracas delas. É importante reiterar que as três conjecturas são válidas para uma grande classes de grupos e também que continuam em aberto para muitos casos particulares. Por exemplo, enquanto ZC1 ainda estava aberta, vários casos fracos da conjectura foram propostos. O primeiro e mais forte deles é o Problema de Kimmerle:

(KP) Seja G um grupo finito e u um elemento de torção em $\mathcal{U}_1(\mathbb{Z}G)$. Existe algum grupo H que contém G tal que u é conjugado em $\mathbb{Q}H$ a um elemento de G?

Como A conjectura ainda era o alvo principal de estudo, o Problema de Kimmerle até então não foi muito trabalhado em si, assim como diversos outros casos particulares das conjecturas em geral.

Capítulo 4

A tabela de caracteres dos contraexemplos

Uma vez definido o candidato $G = G(p, q; d; \alpha, \beta)$ a ser um contraexemplo para a conjectura de Zassenhaus, para mostrar que alguma unidade de torção $u \in \mathcal{U}_1(\mathbb{Z}G)$ não é conjugada com as unidades triviais de G, é suficiente determinar um $\mathbb{C}G$-módulo V junto ao seu caractere χ, e observar que o valor $\chi(u)$ não pertence ao conjunto dos valores $\{\ \chi(g) \mid g \in G\ \}$. Em detalhes, lembramos que toda representação $\varphi : G \to \mathrm{GL}(V)$ estende-se por linearidade a um homomorfismo de álgebras $\varphi : \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(V)$, assim todo caractere pode ser considerado como uma função $\chi : \mathbb{C}G \to \mathbb{C}$, e sendo $\chi(u) = \chi(u^z)$ para todos $u \in \mathbb{C}G$ e $z \in \mathcal{U}(\mathbb{C}G)$, se vale $u^z = g \in G$, tem que ser $\chi(u) = \chi(g)$. Alem disso, sendo que todo caractere é combinação linear com coeficientes inteiros de caracteres irredutíveis, é de fundamental interesse conhecer $\mathrm{Irr}(G)$. De fato, os caracteres irredutíveis de $G(p, q; d; \alpha, \beta)$ são brevemente apresentados em [12, Teorema 7.6], contudo, a apresentação não é completa, no sentido que não aparece a descrição explicita da tabela dos caracteres. Daremos esta descrição nesse capitúlo.

4.1 Grupos afins gerais de posto 1

Sejam p um primo e a um inteiro positivo. Denotamos por $V = \mathbb{F}_{p^a}$ e $H = \mathbb{F}_{p^a}^{\times}$ os grupos aditivo e multiplicativo do corpo $\mathbb{F}_{p^a}$, respectivamente. Então H age por multiplicação em V e temos um grupo $\Gamma = V \rtimes H$. Denotamos por γ_V o elemento de Γ que corresponde a $\gamma \in \mathbb{F}_{p^a}$, e por δ_H o elemento de Γ que corresponde a $\delta \in \mathbb{F}_{p^a}^{\times}$. Logo, todo elemento de

Γ escreve–se unicamente como $\gamma_V\delta_H$, onde $\gamma, \delta \in \mathbb{F}_{p^a}$ e $\delta \neq 0$, e escrevemos $1 = 0_H 1_V$, $\delta_V = \delta_V 1_H$, e $\gamma_H = 0_V\gamma_H$. As regras que descrevem a multiplicação e a conjugação em Γ são dadas por

$$\gamma_V\delta_H \cdot \gamma'_V\delta'_V = (\gamma + \delta^{-1}\gamma')_V(\delta\delta')_H, \qquad (\gamma_V\delta_H)^{\gamma'_V\delta'_H} = (\delta'(\gamma - \gamma') + \delta'\delta^{-1}\gamma')_V\delta_H \ .$$

Assim, sendo $(1_V)^{\gamma'_V\delta'_H} = \delta'_V$, a classe de conjugação $(1_V)^G$ contem todos os elementos γ_V ao variar de γ em $\mathbb{F}_{p^2}^{\times}$. De outro lado, sendo $(\delta_H)^{\gamma'_V\delta'_H} = ((1-\delta^{-1})\delta'\gamma')_V\delta_H$, para $\delta \neq 1$, a classe de conjugação $(\delta_H)^\Gamma$ contem todos os elementos $\gamma_V\delta_H$ ao variar de γ em $\mathbb{F}_{p^2}$. Portanto, as classes de conjugação de Γ são

$$1^\Gamma = \{\ 1\ \}\ ,\ (1_V)^\Gamma = \{\ \delta_V \mid \delta \in \mathbb{F}_p^{\times}\ \}\ ,\ (\delta_H)^\Gamma = \{\ \gamma_V\delta_H \mid \gamma \in \mathbb{F}_{p^a}\ :\ \delta \in \mathbb{F}_{p^a}^{\times}\}.$$

Além disso, fixado um elemento primitivo α de $\mathbb{F}_{p^a}$, vale $\mathbb{F}_{p^a} = \{0\} \cup \{1, \alpha, \ldots, \alpha^{p^a-2}\}$, assim as classes de conjugação de Γ são

$$1^\Gamma = \{\ 1\ \}\ ,\ (1_V)^\Gamma = \{\ \alpha_V^k \mid 0 \leq k < p^a{-}1\ \}\ ,\ (\alpha_H^k)^\Gamma = \{\ \gamma_V\alpha_H^k \mid \gamma \in \mathbb{F}_{p^a}\ :\ 0 < k < p^a{-}1\ \}.$$

Agora, identificamos $\mathrm{Irr}(H)$ com $\mathrm{Irr}(\Gamma/V)$, sendo estes todos os caracteres lineares de Γ. Como V é um p-grupo abeliano elementar de posto a e H age transitivamente em $V \setminus \{0\}$, então $V \setminus \{0\} = v^\Gamma$ para qualquer $v \in V \setminus \{0\}$. Agora, seja ϑ um caractere linear de V que não seja um caractere principal. Então existe $x \in V$ tal que, denotando $P = \langle x \rangle$, temos $\vartheta(x^k) = \varepsilon^k$ para $k = 0, \ldots, p-1$, onde ε é uma p-ésima raiz primitiva da unidade em $\mathbb{C}$, e $V = P \times U$ onde $U = \ker\vartheta$. Mais ainda, $U = P^{g_2} \times \ldots \times P^{g_a}$ para determinados $g_2, \ldots, g_a \in H$. Considere o caractere induzido $\sigma = \vartheta \uparrow^\Gamma$. Por definição de caractere induzido, temos que

$$\sigma(g) = \frac{1}{|V|}\sum_{x\in G}\vartheta^\circ(g^x)$$

onde $\vartheta^\circ(h) = \vartheta(h)$ se $h \in V$, e $\vartheta^\circ(h) = 0$ para $h \in \Gamma \setminus V$. Em particular, $\sigma(1) = |\Gamma : V| = p^a - 1$ e, como $V \trianglelefteq \Gamma$, então $\sigma(g) = 0$ para todo $g \in \Gamma \setminus V$. Além disso, temos que

$$\sigma(v) = \frac{1}{|V|}\sum_{x\in G}\vartheta(v^x) = \frac{|C_\Gamma(v)|}{|V|}\sum_{k=1}^{p}\vartheta(v^k) = \sum_{k=1}^{p}\varepsilon^k = -1$$

uma vez que $C_\Gamma(v) = V$, o único ponto de V fixado por H é 0_H. Portanto

$$\sigma(g) = \begin{cases} p^a - 1, & g = 1 \\ -1, & g \in V \setminus \{0\} \\ 0, & g \in \Gamma \setminus V\ . \end{cases}$$

Além disso, como

$$[\sigma,\sigma] = \frac{1}{|\Gamma|}\sum_{g\in G}|\sigma(g)|^2 = \frac{1}{p^a(p^a-1)}\left((p^a-1)^2+(p^a-1)(-1)^2\right) = 1$$

temos que $\sigma \in \mathrm{Irr}(\Gamma)$. Daí, segue que

$$\mathrm{Irr}(H)\cup\{\sigma\} \subseteq \mathrm{Irr}(\Gamma)$$

Por outro lado, pela fórmula do grau

$$\sum_{\chi\in\mathrm{Irr}(\Gamma)}\chi(1)^2 = |\Gamma|$$

e pela equação

$$\sum_{\vartheta\in\mathrm{Irr}(H)}\vartheta(1)^2+\chi(1)^2 = |H|+\sigma(1)^2 = p^a-1+(p^a-1)^2 = p^a(p^a-1) = |\Gamma|$$

concluímos que

$$\mathrm{Irr}(\Gamma) = \mathrm{Irr}(H)\cup\{\sigma\}\ .$$

Particularmente, vemos que σ é o único caractere irredutível de Γ que é não linear, e também que $\mathrm{Irr}(H) = \mathrm{Irr}(\Gamma/V)$ são todos os caracteres lineares de Γ, para $V = [\Gamma,\Gamma]$. Portanto, a tabela de caracteres de Γ é

	1	1_V	α_H	α_H^2	$\ldots$	$\alpha_H^{p^a-2}$
1	1	1	1	1	$\ldots$	1
λ	1	1	ϵ	ϵ^2	$\ldots$	ϵ^{p^a-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
λ^l	1	1	ϵ^l	ϵ^{2l}	$\ldots$	$\epsilon^{(p^a-2)l}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
λ^{p^a-2}	1	1	ϵ^{p^a-2}	$\epsilon^{2(p^a-2)}$	$\ldots$	$\epsilon^{(p^a-2)^2}$
σ	p^a-1	-1	0	0	$\ldots$	0

onde ϵ é uma (p^a-1)–ésima raiz primitiva da unidade em $\mathbb{C}$.

4.2 Subgrupos dos grupos afins de posto 1

Descreveremos os caracteres irredutíveis de certos subgrupos dos grupos afins $\Gamma = V\rtimes H$ construídos acima. Em particular, para qualquer divisor fixado d de $p-1$, definimos

$$\Delta = V\rtimes H^d \quad , \quad H^d = \langle\alpha_H^d\rangle = \left\{\ \alpha_H^{id} \mid 0\le i < \frac{p^a-1}{d}\ \right\}\ .$$

Ainda para este grupo, tomamos um caractere não principal ϑ de V e consideramos o caractere induzido $\sigma = \vartheta \uparrow^{\Delta}$. Temos que

$$\sigma(1) = |\Delta : V| \cdot \vartheta(1) = \frac{p^a - 1}{d}$$

e $\sigma(g) = 0$ para todo $g \in \Delta \setminus V$. Por outro lado, para $v \in V \setminus \{0\}$, temos

$$\sigma(v) = \frac{1}{|V|} \sum_{g \in \Delta} \vartheta(v^g) = \sum_{h \in H^d} \vartheta(v^h) \ .$$

Denotamos por φ_V o elemento de V que corresponde a φ em $\mathbb{F}_{p^a}$, e por φ_H o elemento de H que corresponde a φ em $\mathbb{F}_{p^a}^{\times}$. Lembramos que a ação de H^d sobre V é dada por

$$(\alpha_V^k)^{\alpha_H^{id}} = \alpha^{id} \alpha_V^k = \alpha_V^{id+k}$$

assim, as classes de conjugação não triviais de Δ em V são

$$(\alpha_V^k)^{\Delta} = \left\{ \ \alpha_V^j \mid 0 \leq j < p^a - 1 \ , \ j \equiv k \mod d \ \right\} \quad : \quad 0 \leq k < d \ .$$

Portanto, calculando

$$\sigma(1_V) \ , \ \sigma(\alpha_V) \ , \ \ldots \ , \ \sigma(\alpha_V^{d-1})$$

e, sabendo que

$$\sigma(\alpha_V^k) = \sum_{i=0}^{\frac{p^a-1}{d}-1} \vartheta(\alpha_V^{id+k})$$

queremos encontrar uma fórmula explícita de algum caractere ϑ. Para isso, observamos que cada elemento de $\mathbb{F}_{p^a}$ pode ser escrito unicamente como $u_0 + u_1\alpha + \ldots + u_{a-1}\alpha^{a-1}$ onde $u_0, \ldots, u_{a-1} \in \mathbb{F}_p$, então

$$\alpha^k = u_{0,k} + u_{1,k}\alpha + \ldots + u_{a-1,k}\alpha^{a-1} \ .$$

Os coeficientes $u_{i,k}$'s podem ser calculados usando recursivamente a equação abaixo

$$\alpha^a = r_0 + r_1\alpha + \ldots + r_{a-1}\alpha^{a-1}$$

a qual é obtida pelo polinômio mínimo

$$f(X) = X^a - r_{a-1}X^{a-1} - \ldots - r_1X - r_0$$

de α sobre $\mathbb{F}_p$. Além disso, escolhendo

$$t = \frac{p^a - 1}{p - 1} = p^{a-1} + \ldots + p + 1$$

temos que

$$\pi = \alpha^t$$

é um elemento primitivo de $\mathbb{F}_p$, daí $\alpha^{lt+j} = \pi^l \alpha^j$ para todo j, l, e então

$$u_{i,lt+j} = \pi^l u_{i,j} \ .$$

Portanto, considerando o caractere irredutível

$$\vartheta_1 \in \mathrm{Irr}(V) \quad , \quad \vartheta_1(u_0 1_V + u_1 \alpha_V + \ldots + u_{a-1}\alpha_V^{a-1}) = \varepsilon^{u_0}$$

onde ε é uma fixada p-ésima raiz da unidade em $\mathbb{C}$, a fórmula acima para um σ genérico especifica

$$\sigma_1(\alpha_V^k) = \sum_{i=0}^{\frac{p^a-1}{d}-1} \varepsilon^{u_{0,id+k}} \ .$$

Mais ainda, se $m_{r,k}$ denota a multiplicidade de r no conjunto $\{\ u_{0,j} \mid j \equiv k \mod d\ \}$, então

$$m_{r,k} = |\ \{\ j \mid 0 \leq j < p^a - 1\ ,\ j \equiv k \mod d\ ,\ u_{0,j} = r\ \}\ | \ ,$$

e temos

$$\sigma_1(\alpha_V^k) = \sum_{r=0}^{p-1} m_{r,k} \cdot \varepsilon^r \ .$$

Ainda, como $\alpha^{-1} = \alpha^{p^2-2}$, segue que

$$\delta = u_{0,p^2-2} \quad : \quad m_{r,k} = m_{\delta^{-k}r,0} \quad , \quad \forall\ r, k \ .$$

Em breve daremos exemplos concretos de tal caractere σ_1, porém, antes disso, vamos provar que $\sigma_1 \in \mathrm{Irr}(\Delta)$, e também mostraremos como ele pode determinar todo o $\mathrm{Irr}(\Delta)$. A ação de H sobre $V \setminus \{0_V\}$ é livre de pontos fixos e, como V é abeliano, tal é a ação sobre $\mathrm{Irr}(V) \setminus \{\mathbf{1}_V\}$. Em particular, para todo $\vartheta \in \mathrm{Irr}(V) \setminus \{\mathbf{1}_V\}$, o subgrupo de inércia de ϑ em Γ é $\Gamma_\vartheta = V$, assim $\Delta_\vartheta = V$. Pelo t Teorema de Clifford, temos que $\sigma = \vartheta \uparrow^\Delta \in \mathrm{Irr}(\Delta)$ e ainda, se $\{\vartheta_1, \ldots, \vartheta_b\}$ são os representantes para as órbitas de H^d, denotando $\sigma_i = \vartheta_i \uparrow^\Delta$, temos que $\sigma_i \neq \sigma_j$ para $i \neq j$. Por isso, se determinarmos os ϑ_i's, obtemos um subconjunto linearmente independente $\{\sigma_1, \ldots, \sigma_b\}$ de $\mathrm{Irr}(\Delta)$. Restrinjamos ao caso em que d e t são coprimos. Observe que esta condição é satisfeita sob a hipótese de Eisele e Margolis, onde d é um primo ímpar e $a = 2$, daí $t = \frac{p^2-1}{p-1} = p + 1$ não é divisível por d. Como H age transitivamente nos elementos de$V \setminus \{0_V\}$, o mesmo acontece com os subgrupos de V cuja ordem é p. Como $\alpha^i \in \mathbb{F}_p$ se, e somente se, t divide i, temos que $H_P = \langle \alpha_H^t \rangle$ é o

estabilizador de $P = \langle 1_V \rangle$ em H, e a quantidade de órbitas é $|H : H_P| = t$. Por restrição, temos uma ação de H^d tal que $H_P^d = H^d \cap H_P = \langle \alpha_H^{dt} \rangle$, já que d e t são coprimos. Particularmente, $|H^d : H_P^d| = |H : H_P| = t$, e daí H^d também age transitivamente. Segue então que o conjunto de representantes para as órbitas de H^d em $\mathrm{Irr}(V) \setminus \{\mathbf{1}_V\}$ pode ser encontrado em $\{\vartheta_1, \ldots, \vartheta_{p-1}\}$ onde $\vartheta_k = \vartheta_1^k$. De fato, temos que $(\vartheta_k)^{H_P^d} = \{\ \vartheta_{id+k} \mid 0 \leq i \leq \frac{p-1}{d}\ \}$ para todo $k = 1, \ldots, p-1$, então $\{\vartheta_1, \ldots, \vartheta_d\}$ é um conjunto completo de representantes das órbitas de Δ em $\mathrm{Irr}(V) \setminus \{\mathbf{1}_V\}$. Consequentemente

$$\mathrm{Irr}(\Delta) = \mathrm{Irr}(H^d) \cup \{\sigma_1, \ldots, \sigma_d\}\ ,$$

onde

$$\sigma_l(\alpha_V^k) = \sum_{r=0}^{p-1} m_{r,k} \cdot \varepsilon^{rl}$$

para todo $0 \leq k < d-1$. Além do mais, observamos que $\Delta \trianglelefteq \Gamma$ daí Γ age em $\mathrm{Irr}(\Delta)$ de forma que $\varphi^g(x) = \varphi(x^{g^{-1}})$ para $g \in \Gamma$ e $x \in \Delta$ e, portanto, a ação preserva o grau, então Γ permuta $\{\sigma_1, \ldots, \sigma_d\}$. Como, particularmente, $\sigma_1^{\alpha_H^k}(\alpha_V^l) = \sigma_1(\alpha_V^{l-k})$ para todo l, k, segue que

$$\sigma_1^{\alpha_H^k} = \sigma_l \iff \sigma_l(\alpha_V^k) = \sigma_1(1_V)$$

descreve a ação de $H = \langle \alpha \rangle$ em $\{\sigma_1, \ldots, \sigma_d\}$.

4.3 O caso p=7, a=2, e d=3

Sejam $p = 7$ e $a = 2$, assim $p^2 = 49$. Então

$$f(X) = X^2 - X - 4 \in \mathbb{F}_7[X]$$

é um polinômio primitivo, e $\mathbb{F}_{49} \simeq \mathbb{F}_7[X]/(f(X))$. Seja α uma raiz de f em $\mathbb{F}_{49}$, daí

$$\mathbb{F}_{49} = \mathbb{F}_7[\alpha] = \{\ u_0 + u_1\alpha \mid u_0, u_1 \in \mathbb{F}_7\ \}\ ,\quad \alpha^2 = 4 + \alpha\ .$$

Segue então que $\sigma_1 \in \mathrm{Irr}(\Delta)$ possui grau

$$\sigma_1(1) = \sigma_1(0_V) = \frac{p^2-1}{d} = \frac{49-1}{3} = 16\ .$$

Calculamos $\alpha^i = u_{0,i} + u_{1,i}\alpha$, para $0 \leq i < t$, onde

$$u_{0,i}, u_{1,i} \in \mathbb{F}_p = \mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}\ ,\ t = \frac{p^2-1}{p-1} = p + 1 = 8\ .$$

Por exemplo,

$$\alpha^3 = \alpha^2 \cdot \alpha = (4+\alpha)\alpha = 4\alpha + \alpha^2 = 4\alpha + (4+\alpha) = 4 + 5\alpha$$
$$\alpha^4 = \alpha^3 \cdot \alpha = (4+5\alpha)\alpha = 4\alpha + 5\alpha^2 = 4\alpha + 5(4+\alpha) = 20 + 9\alpha = 6 + 2\alpha \ ,$$

e assim por diante. Uma vez que obtemos todos os valores de α^i, $u_{0,i}$ e $u_{1,i}$ ao variar de $i = 0, \ldots, 7$, podemos colocar os mesmos em uma tabela, conforme abaixo:

i	0	1	2	3	4	5	6	7
α^i	1	α	$4+\alpha$	$4+5\alpha$	$6+2\alpha$	$1+\alpha$	$4+2\alpha$	$1+6\alpha$
$u_{0,i}$	1	0	4	4	6	1	4	1
$u_{1,i}$	0	1	1	5	2	1	2	6

Mais ainda, sendo

$$\pi = \alpha^{p+1} = \alpha^8 = (1+6\alpha)\alpha = \alpha + 6\alpha^2 = \alpha + 6(4+\alpha) = 24 = 3 \ ,$$

e portatnto $u_{0,8l+i} = \pi^l u_{0,i} = 3^l u_{0,i}$ para todo i, l, podemos calcular os valores de todos os coeficientes $\{\ u_{0,k}\ \}_{k=0}^{47}$, assim como aparecem na tabela:

i	0	1	2	3	4	5	6	7
$u_{0,i}$	1	0	4	4	6	1	4	1
$u_{0,8+i}$	3	0	5	5	4	3	5	3
$u_{0,16+i}$	2	0	1	1	5	2	1	2
$u_{0,24+i}$	6	0	3	3	1	6	3	6
$u_{0,32+i}$	4	0	2	2	3	4	2	4
$u_{0,40+i}$	5	0	6	6	2	5	6	5

Observe que cada linha é simplesmente obtida multiplicando por 3 a linha anterior, e tomando as classes de resto módulo 7. Em seguida, para $k = 0, 1, 2$, verificaremos a multiplicidade $m_{r,k}$ de todo coeficiente $r \in \mathbb{F}_7$ no conjunto

$$\{\ u_{0,j} \mid 0 \leq j < 48\ ,\ j \equiv k \mod 3\ \}\ .$$

Por exemplo, tomando $k = 0$, precisamos selecionar os coeficientes $u_{0,j}$ para $j \equiv 0 \mod 3$, que evidenciamos na tabela acima pela diferente coloração:

	0	1	2	3	4	5	6	7
$u_{0,i}$	1	0	4	4	6	1	4	1
$u_{0,8+i}$	3	0	5	5	4	3	5	3
$u_{0,16+i}$	2	0	1	1	5	2	1	2
$u_{0,24+i}$	6	0	3	3	1	6	3	6
$u_{0,32+i}$	4	0	2	2	3	4	2	4
$u_{0,40+i}$	5	0	6	6	2	5	6	5

assim, a multiplicidade de $r = 1$ é $m_{1,0} = 2$, a multiplicidade de $r = 2$ é $m_{2,0} = 1$, e assim por diante. Contando assim, para todo $k = 0, 1, 2$ e $r \in \mathbb{F}_7$ temos

	0	1	2	3	4	5	6
$m_{r,0}$	2	2	1	4	4	1	2
$m_{r,1}$	2	4	2	1	1	2	4
$m_{r,2}$	2	1	4	2	2	4	1

Portanto, segue que

$$\begin{aligned}
\sigma_1(1_V) &= 2 + 2\varepsilon + \varepsilon^2 + 4\varepsilon^3 + 4\varepsilon^4 + \varepsilon^5 + 2\varepsilon^6 \\
\sigma_1(\alpha_V) &= 2 + 4\varepsilon + 2\varepsilon^2 + \varepsilon^3 + \varepsilon^4 + 2\varepsilon^5 + 4\varepsilon^6 \\
\sigma_1(\alpha_V^2) &= 2 + \varepsilon + 4\varepsilon^2 + 2\varepsilon^3 + 2\varepsilon^4 + 4\varepsilon^5 + \varepsilon^6
\end{aligned}$$

e, sendo $\sum_{i=0}^{6} \varepsilon^i = 0$, temos que

$$\begin{aligned}
\sigma_1(1_V) &= -\varepsilon^2 + 2\varepsilon^3 + 2\varepsilon^4 - \varepsilon^5 \\
\sigma_1(\alpha_V) &= 2\varepsilon - \varepsilon^3 - \varepsilon^4 + 2\varepsilon^6 \\
\sigma_1(\alpha_V^2) &= -\varepsilon + 2\varepsilon^2 + 2\varepsilon^5 - \varepsilon^6 \ .
\end{aligned}$$

Para calcular σ_2 e σ_3, é suficiente substituir ε por ε^2 e ε^3, respectivamente, nas equações acima. Por exemplo,

$$\sigma_2(1_V) = \sigma_1(1_V)^\tau = -\varepsilon^4 + 2\varepsilon^6 + 2\varepsilon - \varepsilon^3 \quad , \quad \tau = (\varepsilon, \varepsilon^2) \ .$$

Portanto, a tabela de caractere de Δ é

	1	1_V	α_V	α_V^2	α_H^3	$\dots$	α_H^{45}
$\mathbf{1}_\Delta$	1	1	1	1	1	$\cdots$	1
λ^k	1	1	1	1	ι^k	$\cdots$	ι^{15k}
σ_1	16	a	b	c	0	$\cdots$	0
σ_2	16	b	c	a	0	$\cdots$	0
σ_3	16	c	a	b	0	$\cdots$	0

onde $1 \leq k < 16$, e os coeficientes irracionais são

$$\begin{aligned}
\iota &= e_{16} \\
\varepsilon &= e_7 \\
a &= -\varepsilon^2 + 2\varepsilon^3 + 2\varepsilon^4 - \varepsilon^5 \\
b &= 2\varepsilon - \varepsilon^3 - \varepsilon^4 + 2\varepsilon^6 \\
c &= -\varepsilon + 2\varepsilon^2 + 2\varepsilon^5 - \varepsilon^6
\end{aligned}$$

onde e_n denota uma n-ésima raiz primitiva da unidade em $\mathbb{C}$. Além disso, lembrando que $\sigma_1^{\alpha^k} = \sigma_l$ se, e somente se $\sigma_l(\alpha_V^k) = \sigma_1(1_V)$, temos que

$$\sigma_1^\alpha = \sigma_3 \quad , \quad \sigma_3^\alpha = \sigma_2 \quad , \quad \sigma_2^\alpha = \sigma_1$$

descreve a ação de $H = \langle \alpha_H \rangle$ no conjunto $\{\sigma_1, \sigma_2, \sigma_3\}$.

4.4 O caso q=19, a=2, e d=3

Considere o primo $q = 19$ e o expoente $a = 2$, assim $q^2 = 361$. Então

$$f(X) = X^2 - X - 17 \in \mathbb{F}_{19}[X]$$

é um polinômio primitivo e $\mathbb{F}_{361} \simeq \mathbb{F}_{19}[X]/(f(X))$. Seja β uma raiz de f em $\mathbb{F}_{361}$. Desta forma

$$\mathbb{F}_{361} = \mathbb{F}_{19}[\beta] = \{\ u_0 + u_1\beta \mid u_1, u_2 \in \mathbb{F}_{19}\ \}\ ,\ \beta^2 = \beta + 17\ .$$

Sejam $d = 3$ e $\Lambda = W \rtimes K^3$, onde $K = \mathbb{F}_{361}^\times$ age por multiplicação em $W = \mathbb{F}_{361}$. Considere ainda $\vartheta \in \mathrm{Irr}(W)$, definida por $\vartheta(u_0 1_W + u_1\beta_V) = \omega^{u_0}$, onde ω é uma 19-ésima raiz primitiva da unidade em $\mathbb{C}$. Então $\tau_1 = \vartheta_1 \uparrow^\Lambda$ possui grau

$$\tau_1(1) = \tau_1(0_W) = \frac{p^2 - 1}{d} = \frac{361 - 1}{3} = 120$$

Calculamos $\beta^i = u_{0,i} + u_{1,i}\beta$ para $0 \leq i < t$, onde

$$t = \frac{p^2 - 1}{p - 1} = p + 1 = 20$$

Donde segue

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$u_{0,i}$	1	0	17	17	2	6	2	9	5	6	15	3	11	5	2	11	7	4	9	1
$u_{1,i}$	0	1	1	18	16	18	5	7	16	2	8	4	7	18	4	6	17	5	9	18

e

$$\pi = \beta^{20} = 2 \ .$$

Como $u_{0,20l+i} = 2^l u_{0,i}$ temos que

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$u_{0,0+k}$	1	0	17	17	2	6	2	9	5	6	15	3	11	5	2	11	7	4	9	1
$u_{0,20+k}$	2	0	15	15	4	12	4	18	10	12	11	6	3	10	4	3	14	8	18	2
$u_{0,40+k}$	4	0	11	11	8	5	8	17	1	5	3	12	6	1	8	6	9	16	17	4
$u_{0,60+k}$	8	0	3	3	16	10	16	15	2	10	6	5	12	2	16	12	18	13	15	8
$u_{0,80+k}$	16	0	6	6	13	1	13	11	4	1	12	10	5	4	13	5	17	7	11	16
$u_{0,100+k}$	13	0	12	12	7	2	7	3	8	2	5	1	10	8	7	10	15	14	3	13
$u_{0,120+k}$	7	0	5	5	14	4	14	6	16	4	10	2	1	16	14	1	11	9	6	7
$u_{0,140+k}$	14	0	10	10	9	8	9	12	13	8	1	4	2	13	9	2	3	18	12	14
$u_{0,160+k}$	9	0	1	1	18	16	18	5	7	16	2	8	4	7	18	4	6	17	5	9
$u_{0,180+k}$	18	0	2	2	17	13	17	10	14	13	4	16	8	14	17	8	12	15	10	18
$u_{0,200+k}$	17	0	4	4	15	7	15	1	9	7	8	13	16	9	15	16	5	11	1	17
$u_{0,220+k}$	15	0	8	8	11	14	11	2	18	14	16	7	13	18	11	13	10	3	2	15
$u_{0,240+k}$	11	0	16	16	3	9	3	4	17	9	13	14	7	17	3	7	1	6	4	11
$u_{0,260+k}$	3	0	13	13	6	18	6	8	15	18	7	9	14	15	6	14	2	12	8	3
$u_{0,280+k}$	6	0	7	7	12	17	12	16	11	17	14	18	9	11	12	9	4	5	16	6
$u_{0,300+k}$	12	0	14	14	5	15	5	13	3	15	9	17	18	3	5	18	8	10	13	12
$u_{0,320+k}$	5	0	9	9	10	11	10	7	6	11	18	15	17	6	10	17	16	1	7	5
$u_{0,340+k}$	10	0	18	18	1	3	1	14	12	3	17	11	15	12	1	15	13	2	14	10

Verificando a multiplicidade $m_{r,k}$ de r no conjunto $\{\ u_{0,j} \mid j \equiv k \mod 3\ \}$ tem-se

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$m_{r,0}$	6	9	6	6	4	6	4	9	9	4	4	9	9	4	6	4	6	6	9
$m_{r,1}$	6	6	4	4	9	4	9	6	6	9	9	6	6	9	4	9	4	4	6
$m_{r,2}$	6	4	9	9	6	9	6	4	4	6	6	4	4	6	9	6	9	9	4

Portanto

$$\begin{aligned}
\tau(1_W) &= 6 + 9\omega + 6\omega^2 + 6\omega^3 + 4\omega^4 + 6\omega^5 + 4\omega^6 + 9\omega^7 + 9\omega^8 + 4\omega^9 \\
&\quad + 4\omega^{10} + 9\omega^{11} + 9\omega^{12} + 4\omega^{13} + 6\omega^{14} + 4\omega^{15} + 6\omega^{16} + 6\omega^{17} + 9\omega^{18} \\
\tau(\beta_W) &= 6 + 6\omega + 4\omega^2 + 4\omega^3 + 9\omega^4 + 4\omega^5 + 9\omega^6 + 6\omega^7 + 6\omega^8 + 9\omega^9 \\
&\quad + 9\omega^{10} + 6\omega^{11} + 6\omega^{12} + 9\omega^{13} + 4\omega^{14} + 9\omega^{15} + 4\omega^{16} + 4\omega^{17} + 6\omega^{18} \\
\tau(\beta_W^2) &= 6 + 4\omega + 9\omega^2 + 9\omega^3 + 6\omega^4 + 9\omega^5 + 6\omega^6 + 4\omega^7 + 4\omega^8 + 6\omega^9 \\
&\quad + 6\omega^{10} + 4\omega^{11} + 4\omega^{12} + 6\omega^{13} + 9\omega^{14} + 6\omega^{15} + 9\omega^{16} + 9\omega^{17} + 4\omega^{18}
\end{aligned}$$

e, como $\sum_{i=0}^{18} \omega^i = 0$, temos que

$$\begin{aligned}
\tau(1_W) =& 3(\omega + \omega^7 + \omega^8 + \omega^{11} + \omega^{12} + \omega^{18}) - 2(\omega^4 + \omega^6 + \omega^9 + \omega^{10} + \omega^{13} + \omega^{15}) \\
\tau(\beta_W) =& 3(\omega^4 + \omega^6 + \omega^9 + \omega^{10} + \omega^{13} + \omega^{15}) - 2(\omega^2 + \omega^3 + \omega^5 + \omega^{14} + \omega^{16} + \omega^{17}) \\
\tau(\beta_W^2) =& 3(\omega^2 + \omega^3 + \omega^5 + \omega^{14} + \omega^{16} + \omega^{17}) - 2(\omega + \omega^7 + \omega^8 + \omega^{11} + \omega^{12} + \omega^{18}).
\end{aligned}$$

Concluímos então que a tabela de caractere de Λ é

	1	1_W	β_W	β_W^2	β_K^3	$\ldots$	β_K^{357}
$\mathbf{1}_\Lambda$	1	1	1	1	1	$\cdots$	1
μ^l	1	1	1	1	ν^l	$\cdots$	ν^{119l}
τ_1	120	e	f	g	0	$\cdots$	0
τ_2	120	g	e	f	0	$\cdots$	0
τ_3	120	f	g	e	0	$\cdots$	0

onde $1 \leq l < 120$, e os coeficientes irracionais são

$$\begin{aligned}
\nu =& e_{120} \quad , \\
\omega =& e_{19} \\
e =& 3(\omega + \omega^7 + \omega^8 + \omega^{11} + \omega^{12} + \omega^{18}) - 2(\omega^4 + \omega^6 + \omega^9 + \omega^{10} + \omega^{13} + \omega^{15}) \\
f =& 3(\omega^4 + \omega^6 + \omega^9 + \omega^{10} + \omega^{13} + \omega^{15}) - 2(\omega^2 + \omega^3 + \omega^5 + \omega^{14} + \omega^{16} + \omega^{17}) \\
g =& 3(\omega^2 + \omega^3 + \omega^5 + \omega^{14} + \omega^{16} + \omega^{17}) - 2(\omega + \omega^7 + \omega^8 + \omega^{11} + \omega^{12} + \omega^{18}).
\end{aligned}$$

Mais ainda,

$$\tau_1^\beta = \tau_2 \quad , \quad \tau_2^\beta = \tau_3 \quad , \quad \tau_3^\beta = \tau_1$$

descreve a ação de $K = \langle \beta \rangle$ no conjunto $\{\tau_1, \tau_2, \tau_3\}$.

4.5 Os contraexemplos de Eisele–Margolis

Sejam p e q primos distintos e α e β elementos primitivos de $\mathbb{F}_{p^2}$ e $\mathbb{F}_{q^2}$, respectivamente. Considere

$$\begin{aligned}
V &= \{\ a_0 1_V + a_1 \alpha_V \mid a_0, a_1 \in \mathbb{F}_p\ \} \simeq \mathbb{F}_{p^2} \\
W &= \{\ b_0 1_W + b_1 \beta_W \mid b_0, b_1 \in \mathbb{F}_q\ \} \simeq \mathbb{F}_{q^2} \\
H &= \{\ \alpha_H^i \mid 0 \leq i \leq p^2 - 1\} \simeq \mathbb{F}_{p^2}^\times \\
K &= \{\ \beta_K^j \mid 0 \leq j \leq q^2 - 1\} \simeq \mathbb{F}_{q^2}^\times
\end{aligned}$$

assim, temos os grupos afins $\Gamma = V \rtimes H$ e $\Xi = W \rtimes K$. Ainda, defina $E = \Gamma \times \Xi$. Fixando um primo ímpar d, divisor de $(p^2 - 1, q^2 - 1)$, consideramos $\Delta = V \rtimes H^d$, $\Lambda = W \rtimes K^d$, e $D = \Delta \times \Lambda$, assim $\Delta \trianglelefteq \Gamma$, $\Lambda \trianglelefteq \Xi$, e $D \trianglelefteq E$. Sejam $N = V \times W$, $A = \langle \alpha_H^d, \beta_H^d, \alpha_H \beta_H \rangle$, e $G = N \rtimes A$. Observe que $D \trianglelefteq G$, $G = D\langle \alpha_H \beta_K \rangle$, em particular $|G : D| = d$, e $G \trianglelefteq E$. Identificamos $\mathrm{Irr}(A)$ com os caracteres irredutíveis de $\mathrm{Irr}(G/N)$. Como D é um produto direto, temos que

$$\mathrm{Irr}(D) = \mathrm{Irr}(\Delta) \times \mathrm{Irr}(\Lambda)\ .$$

Já que d não divide $\frac{p^2-1}{p-1} = p + 1$, vimos que

$$\mathrm{Irr}(\Delta) = \mathrm{Irr}(\Delta/V) \cup \{\sigma_1, \ldots, \sigma_d\}$$

onde $\mathrm{Irr}(\Delta/V)$ é identificado com

$$\mathrm{Irr}(H^d) = \left\{\ \lambda^i \mid 0 \leq i < \frac{p^2 - 1}{d}\ \right\} \quad , \quad \lambda(\alpha_H^{kd}) = \iota^k \quad \left(\ = \lambda(\alpha_V^r \alpha_H^{kd})\ ,\ \forall\ 0 \leq r < p^2 - 1\ \right)$$

onde ι é uma raiz primitiva $\frac{p^2-1}{d}$-ésima da unidade em $\mathbb{C}$, e, para todo $1 \leq l \leq d$, temos

$$\sigma_l(1) = \frac{p^2-1}{d} \quad , \quad \sigma_l(\alpha_V^k) = \sum_{r=0}^{p-1} m_{r,k} \cdot \varepsilon^{rl} \quad , \quad \sigma_l(x) = 0 \ \ \forall\, x \in \Delta \setminus V$$

onde ε é uma raiz primitiva p-ésima da unidade em $\mathbb{C}$, para adequados coeficientes $m_{r,k}$ em $\mathbb{N}$. Similarmente, como d não divide $\frac{q^2-1}{q-1} = q+1$, temos que

$$\mathrm{Irr}(\Lambda) = \mathrm{Irr}(\Lambda/W) \cup \{\tau_1, \ldots, \tau_d\}$$

onde $\mathrm{Irr}(\Lambda/W)$ é identificado com

$$\mathrm{Irr}(K^d) = \left\{ \ \mu^j \mid 0 \leq j < \frac{q^2-1}{d} \ \right\} \quad , \quad \mu(\beta_K^{ld}) = \nu^l \quad \left(\equiv \nu(\beta_W^s \beta_K^{ld}) \ \forall\ 0 \leq s < q^2-1 \ \right)$$

sendo ν uma raiz primitiva $\frac{q^2-1}{d}$-ésima da unidade em $\mathbb{C}$, e, para todo $1 \leq l \leq d$, temos

$$\tau_l(1) = \frac{q^2-1}{d} \quad , \quad \tau_l(\beta_W^k) = \sum_{r=0}^{q-1} n_{r,k} \cdot \omega^{rl} \quad , \quad \tau_l(y) = 0 \ \forall\ y \in \Lambda \setminus W$$

sendo ω uma q-ésima raiz primitiva da unidade em $\mathbb{C}$, para adequados coeficientes $n_{r,k}$ em $\mathbb{N}$. Portanto,

$$\mathrm{Irr}(D) = \left\{ \ \lambda^i\mu^j \ , \ \lambda^i\tau_j \ , \sigma_i\mu^j \ , \sigma_i\tau_j \ \right\}_{i,j} \ .$$

Como $H^d \times K^d$ é um subgrupo de um grupo abeliano A, todo $\lambda^i\mu^j$ é extensível a algum caractere de $\mathrm{Irr}(A)$. Por outro lado, tendo $\Gamma_{\sigma_i} = \Delta$ para todo i, e $\Xi_{\tau_j} = \Lambda$ para todo j, como $G = D\langle \alpha_H \beta_K \rangle$, segue que

$$E_{\lambda^i\tau_j} = E_{\sigma_i\mu^j} = E_{\sigma_i\tau_j} = D \ .$$

Pela correspondência de Clifford temos que os caracteres induzidos são irredutíveis e são distintos para distintos representantes das $\langle \alpha_H \beta_K \rangle$-órbitas. Temos que

$$(\lambda^i\tau_j)^{(\alpha_H\beta_K)^k} = \lambda^i\tau_j^{\beta^k} \ ,$$

como $\langle \beta_K \rangle$ age transitivamente sobre $\{\tau_1, \ldots, \tau_d\}$, o mesmo acontece com $\langle \alpha_H \beta_K \rangle$ sobre $\{\lambda^i\tau_1, \ldots, \lambda^i\tau_d\}$. De forma similar, $\langle \alpha_H \beta_K \rangle$ age transitivamente em $\{\sigma_1\mu^j, \ldots, \sigma_d\mu^j\}$. Por sua vez, para todos $1 \leq i, j, k \leq d$ temos que

$$(\sigma_i\tau_j)^{(\alpha\beta)^k} = \sigma_i^{\alpha^k}\tau_j^{\beta^k}$$

para que se tenha uma órbita $\{\sigma_i\tau_j, \sigma_i^{\alpha}\tau_j^{\beta}, \ldots, \sigma_i^{\alpha^{d-1}}\tau_j^{\beta^{d-1}}\}$. Como $\langle\alpha_H\rangle$ é cíclico e age transitivamente em $\{\sigma_1, \ldots, \sigma_d\}$, então existe um único $\sigma_1\tau_l$ na órbita de $\sigma_i\tau_j$. Portanto, dentro de $\mathrm{Irr}(G)$ temos os pares de caracteres distintos

$$\left\{ \lambda^i\tau_j \uparrow^G \mid 0 \leq i < \frac{p^2-1}{d} \right\} \cup \left\{ \sigma_i\mu^j \uparrow^G \mid 0 \leq j < \frac{q^2-1}{d} \right\} \cup \left\{ \sigma_1\tau_j \uparrow^G \mid 1 \leq j \leq d \right\}$$

além dos caracteres lineares, $\mathrm{Irr}(G/N) \equiv \mathrm{Irr}(A)$. Denotando por X o conjunto desses caracteres, como

$$\begin{aligned}
\lambda^i\tau_1 \uparrow^G (1) &= |G:D| \cdot \lambda^i(1) \cdot \tau_1(1) = d \cdot \frac{q^2-1}{d} = q^2-1 \\
\sigma_1\mu^j \uparrow^G (1) &= |G:D| \cdot \sigma_1(1) \cdot \mu^j(1) = d \cdot \frac{p^2-1}{d} = p^2-1 \\
\sigma_1\tau_j \uparrow^G (1) &= |G:D| \cdot \sigma_1(1) \cdot \tau_j(1) = d \cdot \frac{p^2-1}{d} \cdot \frac{q^2-1}{d} = \frac{(p^2-1)(q^2-1)}{d}
\end{aligned}$$

temos que

$$\begin{aligned}
\sum_{\chi\in X} \chi(1)^2 =& \frac{(p^2-1)(q^2-1)}{d} + \frac{p^2-1}{d} \cdot (q^2-1)^2 + \frac{q^2-1}{d} \cdot (p^2-1)^2 \\
&+ d \cdot \frac{(p^2-1)^2(q^2-1)^2}{d^2} \\
=& \frac{(p^2-1)(q^2-1)}{d} \left(1 + (q^2-1) + (p^2-1) + (p^2-1)(q^2-1)\right) \\
=& \frac{(p^2-1)(q^2-1)}{d} \cdot p^2q^2 = |G|
\end{aligned}$$

provando que $X = \mathrm{Irr}(G)$. Além disso, os caracteres acima podem ser descritos explicitamente da forma seguinte. Para $\vartheta_i = \lambda^i\tau_1 \uparrow^G$, temos que

$$\vartheta_i(g) = 0 \quad \forall\ g \in G \setminus D$$

e, por outro lado,

$$\vartheta_i \downarrow_D = \lambda^i \sum_{j=1}^{d} \tau_j = \lambda_i \cdot \tau \downarrow_\Lambda$$

onde τ é o caractere não–linear de Ξ. Isto é,

$$\vartheta_i(g) = \begin{cases} (q^2-1)\iota^{ik} & \text{se } \ g = \alpha_H^{dk} \ \text{ ou } \ g = \alpha_V^r\alpha_H^{dk} \\ -\iota^{ik} & \text{se } \ g = \beta_W^s\alpha_H^{dk} \ \text{ ou } \ g = \alpha_V^r\beta_W^s\alpha_H^{dk} \\ 0 & \text{nos outros casos.} \end{cases}$$

Similarmente, para $\varsigma_j = \sigma_1\mu^j \uparrow^G$, segue que

$$\varsigma_j(g) = \begin{cases} (p^2-1)\nu^{jl} & \text{se } \ g = \beta_K^{dl} \ \text{ ou } \ g = \alpha_V^r\beta_K^{dl} \\ -\nu^{jl} & \text{se } \ g = \beta_W^s\beta_K^{dl} \ \text{ ou } \ g = \alpha_V^r\beta_W^s\beta_K^{dl} \\ 0 & \text{nos outros casos.} \end{cases}$$

Para $\chi_j = \sigma_1\tau_j \uparrow^G$, temos

$$\chi_j \downarrow_N = \sum_{k=1}^{d} \sigma_1^{\alpha^k}\tau_j^{\beta^k} \downarrow_N$$

e

$$\chi_j(g) = 0 \quad \forall\ g \in G \setminus N$$

Enfim, os caracteres $\mathrm{Irr}(G/N) \equiv \mathrm{Irr}(A)$ são todos os caracteres lineares de G e sua descrição completa depende da fatoração de A em produto direto de grupos cíclicos.

4.6 O caso p=7, q=19, a=2, e d=3

Os caracteres ϑ_i e ς_j são totalmente descritos como no caso geral. Para os caracteres χ_i, neste caso, lembramos de §4.3 e §4.4 que

$$\sigma_1^{\alpha} = \sigma_3 \quad , \quad \sigma_1^{\alpha^2} = \sigma_2 \quad , \quad \tau_1^{\beta} = \tau_2 \quad , \quad \tau_1^{\beta^2} = \tau_3$$

assim

$$\begin{aligned}
\chi_1 \downarrow_N &= \sigma_1\tau_1 + \sigma_2\tau_3 + \sigma_3\tau_2 \\
\chi_2 \downarrow_N &= \sigma_1\tau_2 + \sigma_2\tau_1 + \sigma_3\tau_3 \\
\chi_3 \downarrow_N &= \sigma_1\tau_3 + \sigma_2\tau_2 + \sigma_3\tau_1 \ .
\end{aligned}$$

Finalmente, vamos computar os caracteres lineares de G. Lembre que α e β são elementos primitivos de $\mathbb{F}_{49}$ e $\mathbb{F}_{361}$ respectivamente, daí $o(\alpha_H) = 48$ e $o(\beta_K) = 360$. O grupo abeliano

$$A = \langle \alpha_H^3, \beta_K^3, \alpha_H\beta_K \rangle$$

se decompõe como produto direto de grupos cíclicos

$$A = \langle \gamma \rangle \times \langle \delta \rangle \simeq C_8 \times C_{720}$$

onde

$$\gamma = \beta_K^{45} \ , \ \delta = \alpha_H\beta_K \ .$$

De fato, temos que

$$\alpha_H^3 = \gamma\delta^{675} \quad , \quad \beta_K^3 = \gamma^7\delta^{48}$$

e mais geralmente

$$\alpha_H^{3k+m}\beta_K^{3l+m} = \gamma^{k+7l}\delta^{675k+48l+m} \ .$$

Portanto, se ζ denota uma 720-ésima raiz primitiva da unidade em $\mathbb{C}$,então os caracteres de A são

$$\mathrm{Irr}(A) = \{\ \lambda_{ab} \mid 0 \leq a < 8\ ,\ 0 \leq b < 720\ \}$$

onde

$$\lambda_{ab}(\gamma^c\delta^d) = \zeta^{90ac+bd}\ ,$$

isto é

$$\lambda_{ab}(\alpha_H^{3k+m}\beta_K^{3l+m}) = \zeta^{90a(k+7l)+b(675k+48l+m)} = \zeta^{45(2a+15b)k+6(105a+8b)l+bm}\ .$$

Note que ζ^{45} é uma 16-ésima raiz primitiva da unidade em $\mathbb{C}$, e ζ^6 é uma 120-ésima raiz da unidade, exatamente como os números irracionais ι e ν descrevendo os valores dos caracteres ϑ_i e ς_j, assumimos assim que $\iota = \zeta^{45}$ e $\nu = \zeta^6$. A este respeito, o sistema de equações lineares

$$\begin{cases} i = 2a + 15b \\ j = 105a + 8b \end{cases}$$

com coeficientes em $\mathbb{Z}_{720}$, admite a solução

$$\begin{cases} a = 248i + 345j \\ b = 255i + 242j \end{cases}$$

por isso, para $\lambda'_{ij} = \lambda_{248i+345j,255i+242j}$, temos

$$\lambda'_{ij}(\alpha_H^{3k+m}\beta_K^{3l+m}) = \zeta^{45ik+6jl+255im+242jm} = \iota^{ik}\nu^{jl}\zeta^{255im+242jm}\ .$$

Portanto, a tabela de caracteres de $G = G(7, 19; 3; \alpha, \beta)$ é

	1	1_V	1_W	1_V1_W	$1_V\beta_W$	$1_V\beta_W^2$	α_H^{3k}	$1_W\alpha_H^{3k}$	β_K^{3l}	$1_V\beta_K^{3l}$	$\alpha_H^{3k+m}\beta_K^{3l+m}$
$\mathbf{1}_G$	1	1	1	1	1	1	1	1	1	1	1
λ'_{ij}	1	1	1	1	1	1	ι^{ik}	ι^{ik}	ν^{jl}	ν^{jl}	ζ_{klm}
ϑ_i	360	360	-1	-1	-1	-1	$360\iota^{ik}$	$-\iota^{ik}$	0	0	0
ς_j	48	-1	48	-1	-1	-1	0	0	$48\nu^{jl}$	$-\nu^{jl}$	0
χ_1	5760	-120	-16	r	s	t	0	0	0	0	0
χ_2	5760	-120	-16	t	r	s	0	0	0	0	0
χ_3	5760	-120	-16	s	t	r	0	0	0	0	0

onde ζ é uma 720-ésima raiz primitiva da unidade em $\mathbb{C}$, $\iota = \zeta^{45}$, $\nu = \zeta^{6}$, $\zeta_{klm} = \zeta^{45ik+6jl+255im+242jm}$ e

$$r = ae + bf + cg$$
$$s = af + bg + ce$$
$$t = ag + be + cf$$

para os números complexos a, b, c, d, e, f definidos em §4.3 e §4.4 respectivamente. Em particular, r, s, t pertencem à extensão ciclotômica $\mathbb{Q}[e_{133}]$ do corpo dos números racionais $\mathbb{Q}$. Portanto, temos os $|A| = 5760$ caracteres lineares

$$\{\mathbf{1}_G\} \cup \{\ \lambda'_{ij} \mid i, j\ \} = \{\ \lambda_{ab} \mid 0 \leq a < 8\ ,\ 0 \leq b < 720\ \}$$

os 16 caracteres ϑ_i, os 120 caracteres ς_j, e enfim χ_1, χ_2, e χ_3. Por outro lado, temos as 6 classes de conjugação de G contidas em N

$$\begin{aligned}
1^G &= \{\ 1\ \} \\
(1_V)^G &= \{\ \alpha_V^i \mid 0 \leq i < p^2 - 1\ \} \\
(1_W)^G &= \{\ \beta_W^j \mid 0 \leq j < q^2 - 1\ \} \\
(1_V 1_W)^G &= \{\ \alpha_V^i \beta_W^j \mid 0 \leq i < p^2 - 1\ ,\ 0 \leq j < q^2 - 1\ ,\ j - i \equiv 0 \mod 3\ \} \\
(1_V \beta_W)^G &= \{\ \alpha_V^i \beta_W^j \mid 0 \leq i < p^2 - 1\ ,\ 0 \leq j < q^2 - 1\ ,\ j - i \equiv 1 \mod 3\ \} \\
(1_V \beta_W^2)^G &= \{\ \alpha_V^i \beta_W^j \mid 0 \leq i < p^2 - 1\ ,\ 0 \leq j < q^2 - 1\ ,\ j - i \equiv 2 \mod 3\ \}
\end{aligned}$$

em seguida, para $0 < k < 16$, temos as 15 classes

$$(\alpha_H^{3k})^G = \{\ \gamma_V \alpha_H^{3k} \mid \gamma \in \mathbb{F}_{p^2}\ \}$$

junto ás 15 classes

$$(1_W \alpha_H^{3k})^G = \{\ \gamma_V \delta_W \alpha_H^{3k} \mid \gamma \in \mathbb{F}_{p^2}\ ,\ \delta \in \mathbb{F}_{q^2}^{\times}\ \}$$

analogamente, para $0 < l < 120$, temos as 119 classes

$$(\beta_K^{ld})^G = \{\ \delta_W \beta_K^{ld} \mid \delta \in \mathbb{F}_{q^2}\ \}$$

e as 119 classes

$$(1_V \beta_K^{ld})^G = \{\ \gamma_V \delta_W \beta_K^{ld} \mid \gamma \in \mathbb{F}_{p^2}^{\times}\ ,\ \delta \in \mathbb{F}_{q^2}\ \}$$

finalmente, as restantes 5625 classes

$$(\alpha_H^{3k+m} \beta_K^{3l+m})^G = \{\ \gamma_V \delta_W \alpha_H^{3k+m} \beta_K^{3l+m} \mid \gamma \in \mathbb{F}_{p^2}\ ,\ \delta \in \mathbb{F}_{q^2}\ \}$$

para $0 \leq k < 16$, $0 \leq l < 120$, $0 \leq m < 3$, com $(k, l, m) \neq (k, 0, 0), (0, l, 0)$.

Capítulo 5

Sobre a demonstração de Eisele–Margolis

Ao se tratar das conjecturas de Zassenhaus, usualmente utiliza-se a noção de módulos de ação dupla [39]. A ideia fundamental é que a conjugação em $\mathbb{Q}G$ pode ser vista como a relação de equivalência entre $\mathbb{Q}G$-representações por meio da identificação

$$\mathcal{U}(\mathbb{Q}G) \simeq \mathrm{GL}(1, \mathbb{Q}G) \ .$$

Ou seja, dados um grupo finito H, defina um homomorfismo $\varphi : H \to \mathrm{GL}(1, \mathbb{Q}G)$ dado por $h \mapsto \{\ v \mapsto \varphi(h)v \mid \forall v \in \mathbb{Q}G\ \}$. Podemos assim dizer que a $\mathbb{Q}G$-representação φ é similar com qualquer representação obtida por conjugação em $\mathrm{GL}(1, \mathbb{Q}G)$ que, por sua vez, será da forma $h \mapsto \{\ v \mapsto \varphi(h)^u v \mid \forall v \in \mathbb{Q}G\ \}$, para todo $u \in \mathcal{U}(\mathbb{Q}G)$. Portanto, o grupo de unidades $\varphi(H)$ é racionalmente conjugado com um subgrupo de G se, e somente se, a $\mathbb{Q}G$-representação φ é similar com alguma $\mathbb{Q}G$-representação γ com valores em G. Este discurso não teria seguido se não pudéssemos voltar à teoria ordinária de representações, onde o anel dos coeficientes é um corpo. Para este fim, observamos que o $\mathbb{Q}$-espaço vetorial $\mathbb{Q}G$ é um H-módulo à esquerda, por meio de φ, mas também é um G-módulo à direita, precisamente o módulo regular, ou seja, $\mathbb{Q}G$ é um H-G-módulo. Para interpretar a estrutura de módulo sobre uma álgebra de grupo podemos assim considerar o produto direito $G \times H$, para obter ambas as ações do mesmo lado.

Definição 5.1. *Sejam G e H grupos finitos e $\varphi : H \to \mathcal{U}(\mathbb{Q}G)$ um homomorfismo de grupos. O* módulo de ação dupla $(\mathbb{Q}G)_\varphi$ *é o conjunto $\mathbb{Q}G$ com a estrutura de $\mathbb{Q}(G \times H)$-*

módulo dada pela ação definida por

$$(g,h)\cdot v = \varphi(h)vg^{-1} \quad , \quad \forall\ g\in G\ ,\ h\in H\ ,\ v\in \mathbb{Q}G$$

e estendida por $\mathbb{Q}$-linearidade.

Claramente, dados $\varphi,\gamma : H\to \mathcal{U}(\mathbb{Q}G)$, temos que $(\mathbb{Q}G)_\varphi$ e $(\mathbb{Q}G)_\gamma$ são isomorfos como $\mathbb{Q}(G\times H)$-módulos se, e somente se, são isomorfos como H-G-módulos, sendo que, nos dois casos, um isomorfismo f está definido pela identidade

$$\gamma(h)f(v)g^{-1} = f(\varphi(h)vg^{-1}) \quad , \quad \forall\ g\in G\ ,\ h\in H\ ,\ \ v\in \mathbb{Q}G\ .$$

A conexão entre as conjecturas de Zassenhaus e os módulos de ação dupla se baseiam na seguinte proposição (que é um caso particular de [39, Lema 38.8]).

Proposição 5.2. *Dois $\mathbb{Q}(G\times H)$-módulos de ação dupla $(\mathbb{Q}G)_\varphi$ e $(\mathbb{Q}G)_\gamma$ são isomorfos se, e somente se, existe $u\in\mathcal{U}(\mathbb{Q}G)$ tal que $\gamma(h)=\varphi(h)^u$, para todo $h\in H$.*

Demonstração. Primeiramente, supomos existir u tal que $\gamma(h)=\varphi(h)^u$, para todo $h\in H$. A aplicação $\vartheta : (\mathbb{Q}G)_\varphi\to(\mathbb{Q}G)_\gamma$, $v\mapsto u^{-1}v$, satisfaz

$$\vartheta((g,h)\cdot v) = \vartheta(\varphi(h)vg^{-1}) = u^{-1}\varphi(h)vg^{-1} = \varphi(h)^u u^{-1}vg^{-1} = \gamma(h)\vartheta(v)g^{-1}\ ,$$

portanto, é isomorfismo de $\mathbb{Q}(G\times H)$-módulos. De outro lado, seja $\vartheta : (\mathbb{Q}G)_\varphi\to(\mathbb{Q}G)_\gamma$ um isomorfismo de $\mathbb{Q}(G\times H)$-módulos. Para todo $v\in(\mathbb{Q}G)_\varphi$ e $g\in G$, tem-se

$$\vartheta(v)g^{-1} = (g,1)\vartheta(v) = \vartheta((g,1)v) = \vartheta(vg^{-1})\ ,$$

consequentimente, a aplicação ϑ corresponde à multiplicação em $\mathbb{Q}G$ por $x=\vartheta(1)$, e sendo ϑ um isomorfismo, segue que ϑ é injetora, portanto inversível, desta forma, tem que ser $x\in\mathcal{U}(\mathbb{Q}G)$. Agora,

$$x\varphi(h)v = \vartheta(hv) = \vartheta((1,h)v) = (1,h)\vartheta(v) = \gamma(h)\vartheta(v) = \gamma(h)xv$$

para todo $h\in H$ e $v\in V$, e podemos tomar $u=x^{-1}$ para concluir a demonstração. □

Se H é um grupo de unidades normalizadas de $\mathbb{Z}G$, isto é $H\leq\mathcal{U}_1(\mathbb{Z}G)$, a imersão $\varphi : H\hookrightarrow\mathcal{U}(\mathbb{Z}G)$ define um $\mathbb{Q}(G\times H)$-módulo de ação dupla $(\mathbb{Q}G)_\varphi$. Pela Proposição 5.2, mostrar que H é racionalmente conjugado a um subgrupo de G é o mesmo que encontrar um homomorfismo de grupos $\gamma : H\to G$ para o qual $(\mathbb{Q}G)_\varphi$ e $(\mathbb{Q}G)_\gamma$ são isomorfos. Como pela proposição acima dois $\mathbb{Q}(G\times H)$-módulos são isomorfos se, e somente se os caracteres são iguais, segue a importância da relação abaixo:

Lema 5.3. *O caractere χ_φ de um $\mathbb{Q}(G \times H)$-módulo de ação dupla $(RG)_\varphi$, é descrito pela fórmula*

$$\chi_\varphi(g,h) = |C_G(g)| \cdot \varepsilon_{g^G}(\varphi(h)),$$

onde

$$\varepsilon_{g^G} : \mathbb{Q}G \to \mathbb{Q} \quad , \quad \sum_{y\in G} a_y y \mapsto \sum_{z\in g^G} a_z \ .$$

Demonstração. Sendo G uma base de $(\mathbb{Q}G)_\varphi = \mathbb{Q}G$, então, para calcular $\chi_\varphi(g,h)$, que é o traço do endomorfismo $v \mapsto (g,h)v$, precisamos somar ao variar de $y \in G$ o coeficiente de $(g,h)y$ em y. Como $\varphi : H \to \mathcal{U}(\mathbb{Q}G)$, tem-se $\varphi(h) = \sum_{x\in G} a_x x$, onde $a_x \in \mathbb{Q}$, e portanto $(g,h)v = \varphi(h)vg^{-1} = \sum_x a_x xvg^{-1}$, para todo $v \in (\mathbb{Q}G)_\varphi$. Sendo $xyg^{-1} = y$ se, e somente se, $x = g^{y^{-1}}$, obtemos

$$\chi_\varphi(g,h) = \sum_{y\in G}\{a_x \mid xyg^{-1} = y\} = \sum_{y\in G} a_{g^{y^{-1}}} = |C_G(g)| \sum_{z\in g^G} a_z = |C_G(g)| \cdot \varepsilon_{g^G}(\varphi(h))$$

como desejado. □

A aplicação ε_{g^G} é chamada *aumento parcial* em g^G e, claramente, se g e y são conjugados em G, vale $\varepsilon_{g^G} = \varepsilon_{y^G}$. Calculando o caractere χ_γ para um homomorfismo γ de H em G obtemos uma condição de grande interesse ao se tratar das conjecturas de Zassenhaus:

Lema 5.4. *Seja H subgrupo de $\mathcal{U}_1(\mathbb{Z}G)$. São equivalentes:*

i) H é racionalmente conjugado a um subgrupo de G,

ii) Existe um homomorfismo $\gamma : H \to G$ tal que $\forall g \in G, h \in H$ tem-se $\varepsilon_{g^G}(h) \neq 0$ se, e somente se, $g^G = (\gamma(h))^G$.

Demonstração. Primeiramente, observamos que a restrição de ε_{g^G} ao grupo G é simplesmente a função característica da classe g^G. Em particular, se $\gamma : H \to G$ é um homomorfismo, tem-se

$$\varepsilon_{g^G}(\gamma(h)) = \begin{cases} 1 & \text{se } \gamma(h) \in g^G \\ 0 & \text{se } \gamma(h) \notin g^G \end{cases} .$$

Denotamos por $\varphi : H \hookrightarrow \mathcal{U}_1(\mathbb{Q}G)$ a imersão. Lembramos que $i)$ é equivalente a ter $\chi_\varphi = \chi_\gamma$ para algum γ, e, de outro lado, sendo $\varphi(h) = h$, isso é $\varepsilon_{g^G}(h) = \varepsilon_{g^G}(\gamma(h))$ para todo $g \in G$ e $h \in H$. Agora, H é subgrupo das unidades normalizadas $\mathcal{U}_1(\mathbb{Z}G)$, portanto,

tem-se $\sum_{g^G} \varepsilon_{g^G}(h) = \varepsilon(h) = 1$. Assim, assumindo $ii)$, tem que ser $\varepsilon_{g^G}(h) = \varepsilon_{g^G}(\gamma(h)) = 0$ para toda classe $g^G \neq \gamma(h)^G$, o que comporta $\varepsilon_{\gamma(h)^G}(h) = \varepsilon(h) = 1$, ou seja, $\chi_\gamma = \chi_\varphi$. De outro lado, assumindo $i)$, se $\gamma : H \to G$ é um homomorfismo de conjugação em $\mathbb{Q}G$, temos que $\varepsilon_{g^G}(h) = \varepsilon_{g^G}(\gamma(h)) \in \{0, 1\}$, e o valor é não nulo precisamente quando $g \in \gamma(h)^G$. □

Este resultado pode ser, de alguma forma, refinado para obter o seguinte:

Teorema 5.5. *Sejam G um grupo finito de ordem n e u um elemento de torção em $\mathcal{U}_1(\mathbb{Z}G)$. Então u é conjugado, em $\mathbb{Q}G$, a algum elemento de G se, e somente se, para todo divisor d da ordem de G e $\forall g \in G$, tem-se $\varepsilon_{g^G}(u^d) \geq 0$.*

É importante ressaltar que estes resultados têm sido grandes pilares no estudo das Conjecturas de Zassenhaus. Muitos outros resultados já foram desenvolvidos em torno deles e são úteis para encontrar soluções, tanto positivas quanto negativas em casos particulares destas conjecturas.

No artigo de Eisele e Margolis, é apresentada a construção do próprio grupo $G = G(7, 19; 3; \alpha, \beta)$, apresentada em 3.1 e, em seguida, é mostrado que $\mathbb{Z}G$ contem uma unidade de torção que não é racionalmente conjugada a uma unidade trivial [12]. Lembramos que, pelo Teorema 5.5, dado u um elemento de torção em $\mathcal{U}_1(\mathbb{Z}G)$ de ordem n, mostrar que u contradiz a conjectura é equivalente a verificar que o caractere χ_φ do módulo de ação dupla $(\mathbb{Q}G)_\varphi$ assume valores negativos, onde $\varphi : \langle u \rangle \hookrightarrow \mathbb{Q}G$ é induzido pela inclusão. Considerando a construção realizada dos grupos candidatos juntamente com as observações acima, a saída do Algoritmo 1 de [33] é utilizada para obter os aumentos parciais que podem corresponder a contraexemplos pela conjectura, e os autores mostram que tal entendimento é válido. Portanto, o material apresentado caminha justamente na direção das condições necessárias para utilizar os algoritmos previamente descritos. O artigo é dividido basicamente em dois momentos: o primeiro, que abrange as quatro primeiras seções, é a apresentação de alguns dos resultados gerais que serão utilizados no segundo momento, este, por sua vez, que abrange as três últimas seções, é o lugar onde são apresentados gradualmente resultados que, juntos, tornam a demonstração do Teorema A razoavelmente mais simples. Em particular, o resultado sai diretamente como aplicação e computação do Teorema 5.8, que será brevemente apresentado mais a frente [12, Teorema 7.2]. O nosso objetivo é selecionar alguns dos pontos chave da demonstração, para oferecer uma ideia simplificada das técnicas utilizadas. Esperamos que o material aqui apresentado

possa incentivar o leitor a completar o estudo das partes omitidas, referindo-se ao artigo original.

Seja G um grupo finito da forma $G = N \rtimes A$ onde N é grupo abeliano. Considere-se um grupo cíclico $U = \langle u \rangle$ cuja ordem é igual ao expoente de N. O objetivo é descrever os módulos de açaõ dupla $(\mathbb{Q}G)_\varphi$, ao variar de $\varphi : U \to \mathbb{Q}G$, ou seja, classificar os possíveis aumentos parciais. O primeiro passo é provar uma versão local do nosso objetivo, onde, para uma coleção de primos π, é encontrado um módulo sobre $\mathbb{Z}_\pi(G \times U)$, que realiza um determinado aumento parcial. Aqui $\mathbb{Z}_\pi = \cap_{p \in \pi} \mathbb{Z}_{(p)}$, onde $\mathbb{Z}_{(p)}$ é a localização de $\mathbb{Z}$ sobre o ideal maximal (p) (veja por exemplo [21]). Portanto, seja

$$\varepsilon : G \to \mathbb{Z} \quad , \quad g \mapsto \varepsilon_{g^G}$$

uma função de classes que se anula no complementar de N, e defina

$$\chi = \sum_{g^G} \varepsilon_{g^G} \cdot (\mathbf{1}_{(g,u)})^{G \times U}$$

onde $(\mathbf{1}_{(g,u)})^{G \times U}$ é o caractere induzido a $G \times U$ do caractere principal do subgrupo

$$\langle (g, u) \rangle \leq G \times C \ .$$

Assumindo as seguintes condições:

C.1) $\sum_{g^G} \varepsilon_{g^G} = 1$,

C.2) Se $\varepsilon_{n^G} \neq 0$, para algum $n \in N$, então $C_G(n_p) \cap C_G(n_{p'}^g) = N \ \forall g \in G$ e para todo primo p que divide a ordem de N,

C.3) Para cada primo p que divide a ordem de N vale a decomposição

$$\chi|_{N \times U} = \sum_{n \in N_p} \lambda_n \otimes (\mathbf{1}_{(n,u)_p})^{N_p \times U_p}$$

onde λ_n é um caractere próprio de $N_{p'} \times U_{p'}$, para cada $n \in N_p$

é possível mostrar o seguinte [12, Teorema 5.1]:

Teorema 5.6. *Seja π uma coleção finita de primos. Então, sob as condições acima, existe um $\mathbb{Z}_\pi(G \times U)$-módulo, regular como $\mathbb{Z}_\pi G$-módulo, com caractere χ. Mais que isso, o aumento parcial da unidade $u_\pi \in \mathcal{U}(\mathbb{Z}_\pi G)$ é dado por ε.*

O ponto seguinte na demonstração é mostrar que, fazendo suposições mais fortes sobre G e χ, é possível juntar as unidades semi–locais $u_\pi \in \mathcal{U}(\mathbb{Z}_\pi G)$ construídas no teorema acima para voltar ao caso integral $u \in \mathcal{U}(\mathbb{Z}G)$. Em detalhes, temos as seguintes condições:

C.4) G não tem uma imagem epimórfica isomórfica a qualquer um dos seguintes grupos:

a) Um grupo de quatérnio generalizado de ordem $4n$ onde $n \geq 2$,

b) O grupo tetraédrico binário de ordem 24,

c) O grupo octaédrico binário de ordem 48,

d) O grupo binário icosaédrico de ordem 120.

C.5) $[\chi, \eta \otimes \mathbf{1}_U] \neq 0$ para todo $\eta \in \mathrm{Irr}_{\mathbb{C}}(G)$.

e temos o resultado [12, Teorema 6.2]:

Teorema 5.7. *Assuma as condições C.1–C.5 acima. Então existe um $\mathbb{Z}(G \times U)$-módulo, regular como $\mathbb{Z}G$-módulo, cujo caractere é χ. Além disso, o aumento parcial em u é a mesma função de classe ε, ou seja $\varepsilon_{g^G}(u) = \varepsilon(g)$ para todo $g \in G$.*

As demonstrações destes dois últimos teoremas necessitam de alguns resultados mais avançados sobre representações, álgebras, *lattices* e ordens, e por esta razão serão omitidas aqui.

Com as devidas construções realizadas, o próximo passo é reformular as condições sob as quais se produzem unidades semi-locais e globais, respectivamente, em um grupo $G(p, q; d; \alpha, \beta)$. Lembrando que $G = N \rtimes A$, onde $N = \mathbb{F}_{p^2} \times \mathbb{F}_{q^2}$, e $A = \langle a, b, c \rangle$ é identificado com um subgrupo de $\mathbb{F}_{p^2}^\times \times \mathbb{F}_{q^2}^\times$, com ação $(x, y)^a = (\alpha^d x, y)$, $(x, y)^b = (x, \beta^d y)$, e $(x, y)^c = (\alpha x, \beta y)$, definimos o subconjunto

$$K_p = \{(\alpha + x, 0) \mid x \in \mathbb{F}_p\} \subseteq N_p = \mathbb{F}_{p^2} \times \{0\}$$

e ainda, para todo $i \in \mathbb{Z}$, definimos

$$r_i = \left| \left\{ t = 1, \ldots, \frac{p^2 - 1}{d} \ : \ (\alpha^{i+t\cdot d}, 0) \in K_p \right\} \right| .$$

Note que $r_i(p) = r_j(p)$, se $i \equiv j \bmod d$. Vale o seguinte [12, Teorema 7.2]:

Teorema 5.8. *Seja $G = G(p, q; d; \alpha, \beta)$, e seja $\varepsilon : G \to \mathbb{Z}$, $g \mapsto \varepsilon_{g^G}$ uma função de classes tal que*

i) $\sum_{g^G} \varepsilon_{g^G} = 1$,

ii) Se $\varepsilon_{g^G} \neq 0$ *para algum* $g \in G$*, então* g *pertence a* N *e a sua ordem é* pq*,*

iii) Para cada $j \in \{0, \ldots, d-1\}$ *valem as inequações*

$$\sum_{i=1}^{d} r_{j+i}(p) \cdot \varepsilon_{(\alpha^t,1)^G} \geq 0 \quad , \quad \sum_{i=1}^{d} r_{j+i}(q) \cdot \varepsilon_{(1,\beta^t)^G} \geq 0$$

Então existe uma unidade $u \in \mathcal{U}(\mathbb{Z}G)$ *de ordem* pq*, cujo aumento parcial é dado pela função de classes* ε*. Se* $\varepsilon_{(\alpha^t,1)^G} \neq 0$ *para mais de um* $i \in \{1, \ldots, d\}$*, então* u *não é conjugado a um elemento da forma* $\pm g$*, com* $g \in G$*.*

A demonstração deste teorema segue de várias proposições e lemas, cada uma correspondendo, mais ou menos, a uma das condições dos Teoremas 5.6 e 5.7. Porém, algumas considerações a cerca do tal grupo G ainda são necessárias, e são listadas abaixo [12, Proposição 7.5]:

Proposição 5.9. *Seja* $G = G(p, q; d; \alpha, \beta)$*, então:*

1) Se $g \in N$ *possui ordem* pq*, então* $C_G(g) = N$*,*

2) Se $n \in N_p \setminus \{1\}$*, então* $C_G(n) = C_G(N_p)$*,*

3) As classes de conjugação em G *dos elementos de ordem* pq *contidos em* N *são representadas pelos elementos* $(1,1), (\alpha,1), (\alpha^2,1), \ldots, (\alpha^{d-1},1)$*. Mais do que isso, se* $n \in N_q \setminus \{1\}$*, as classes de conjugação em* $C_G(n)$ *dos elementos de ordem* p *pertencentes a* N *são dadas por* $(1,0), (\alpha,0), \ldots, (\alpha^{d-1},0)$*,*

4) G *age (por conjugação) transitivamente no conjunto de subgrupos cíclicos de* N *cuja ordem é* pq*,*

5) $G/C_G(N_p)$ *age regularmente no conjunto das coclasses laterais não triviais de subgrupos cíclicos em* N_p *de ordem* p*, isto é, o conjunto*

$$\{\ nX \mid X \leq N_p \ \ , \ \ |X| = p \ \ , \ \ n \in N_p \setminus X\ \}$$

cuja cardinalidade é $p^2 - 1$*.*

6) $C_A(N_q)$ *age semirregularmente no conjunto do ponto 5.*

7) $C_G(N_q)$ *age transitivamente no conjunto dos subgrupos cíclicos de ordem* p *em* N_p.

Para demonstrar o Teorema 5.8, primeiramente faz-se necessário verificar as condições do Teorema 5.6. A primeira condição C.1 segue direto da definição de ε, para verificar C.2 utiliza-se a proposição acima, e a condição C.3 utiliza o seguinte resultado [12, Lemma 7.8]:

Lema 5.10. *Fixado* $G = G(p, q, d; \alpha, \beta)$*, seja* $\varepsilon : G \to \mathbb{Z}$ *uma função de classes que é não nula somente em elementos de* N *de ordem* pq *tal que*

$$\sum_{g^G} \varepsilon_{g^G} = \sum_{i=1}^{d} \varepsilon_{(\alpha^i,1)^G} = 1$$

seja $U = \langle u \rangle$ *um grupo cíclico de ordem* pq*, e seja* $n = (0, 1) \in N_q$*. Então a função de classe*

$$\xi_n = \sum_{m \in N_p} \varepsilon_{(m \cdot n)^G} \cdot (\mathbf{1}_{(m,u)_p})^{N_p \times U_p}$$

é um caractere de $N_p \times U_p$ *se, e somente se, vale*

$$\begin{pmatrix} r_1 & r_2 & \dots & r_d \\ r_2 & r_3 & \dots & r_1 \\ \vdots & \vdots & \ddots & \vdots \\ r_d & r_1 & \dots & r_{d-1} \end{pmatrix} \begin{pmatrix} \varepsilon_{(\alpha,1)^G} \\ \varepsilon_{(\alpha^2,1)^G} \\ \vdots \\ \varepsilon_{(\alpha^d,1)^G} \end{pmatrix} \geq 0$$

onde $r_i = r_i(p)$ *para* $i = 1, \dots, d$*. Além disso, é possível descrever com detalhes a multiplicidade das componentes irredutíveis de* ξ_n *em* $\mathbb{Q}(N_p \times U_p)$ *(aqui omitido).*

A validade destas condições nos fornecem uma unidade semilocal u_π de ordem pq em $\mathcal{U}_1(\mathbb{Z}_\pi G)$ com o aumento parcial desejado. Após checar também as condições do Teorema 5.7, isto é, C.4 e C.5, temos por fim uma unidade $u \in \mathcal{U}(\mathbb{Z}G)$, que também tem aumento parcial dado por ε. Segue imediatamente do formalismo de ação dupla que se ε é não nula em mais de uma classe de conjugação, então u não é conjugado em $\mathcal{U}(\mathbb{Q}G)$ e algum elemento de G. Uma vez que o Teorema 5.8 é demonstrado, o próximo e último passo é definir bons parâmetros para os valores de p, q e da função de classes ε, assim de reduzir a demonstração do Teorema A basicamente a um cálculo computacional.

De forma parecida, o Teorema B é essencialmente uma aplicação do seguinte corolário do Teorema 5.8 [12, Corolário 7.3]:

Corolário 5.11. *Fixe $M \in \mathbb{N}$ e seja $G = G = G(p, q; d; \alpha, \beta)$. Considere que tanto p quanto q são maiores ou iguais a*

$$\frac{d^4 \cdot M^2}{1 - |\cos(2\pi/d)|}$$

Seja $\varepsilon : G \to \mathbb{Z} : g \mapsto \varepsilon_{g^G}$ uma função de classes tal que

i) $\sum_{g^G} \varepsilon_{g^G} = 1$,

ii) $|\varepsilon_{g^G}| \leq M$ *para todo* $g \in G$,

iii) Se $\varepsilon_{g^G} \neq 0$, *para algum* $g \in G$, *então* $g \in N$ *e a ordem de* g *é* pq.

Então existe uma unidade $u \in \mathcal{U}(\mathbb{Z}G)$ de ordem pq cujo aumento parcial é dado por ε.

Referências

[1] Bächle, A, Kimmerle, W. e Serrano, M. *On the first Zassenhaus conjecture and direct products,* Canad. J. Math. 72 (2020), no. 3, 602–624.

[2] Bächle, A. e Margolis, L. *Rational conjugacy of torsion units in integral group rings of non-solvable groups.* Proc. Edinb. Math. Soc. (2) 60, n. 4, 2017, p. 813–830.

[3] Bhandari, A. K., Luthar, I. S. *Torsion units of integral group rings of metacyclic groups.* J. Number Theory 17, 1983, p. 170–183.

[4] Bleher, F. M. *Finite groups of Lie type of small rank.* Pacific J. Math. 187, n. 2, 1999, 215–239

[5] Bleher,F. M., Geck, M. e Kimmerle, W. *Automorphisms of generic Iwahori-Hecke algebras and integral group rings of finite Coxeter groups.* J. Algebra 197, n. 2, 1997, p. 615–655.

[6] Bovdi, V. A. e Hertweck, M. *Zassenhaus conjecture for central extensions of S5.* J. Group Theory 11, no. 1, 2008, p. 63–74.

[7] Caicedo, M., Margolis, L., del Río, Á. *Zassenhaus conjecture for cyclic-by-abelian groups.* J. Lond. Math. Soc. (2) 88(1), p.65-78, 2013.

[8] Cohn, J. A., Livingstone, D. *On the structure of group algebras, I.* Canad. J. Math. 17 (1965), 583–593.

[9] del Río, Á. e Serrano, M. *Zassenhaus conjecture on torsion units holds for $SL(2,p)$ and $SL(2,p^2)$.* J. Group Theory 22 (2019), no. 5, 953–974.

[10] Dokuchaev, M.A., Juriaans, S.O. *Finite Subgroups in Integral Group Rings.* Canad. J. Math., 48, 1996, p. 1170–1179.

[11] Dokuchaev, M.A., Juriaans, S.O., Milies, C. P. *Integral Group Rings of Frobenius groups and the Conjectures of H.J. Zassenhaus.* Comm. Algebra 25, 1997, 3211–2325.

[12] Eisele, F., Margolis, L. *A counterexample to the first Zassenhaus Conjecture.* Adv. Math. 339, 2018, p. 599–641.

[13] Fernandes,N. *Torsion Units in the integral group ring of* S_4. Bol. Soc. Bras. Mat. 18, 1987, p. 1–10.

[14] Hertweck, M. *On the torsion units of some integral group rings.* Algebra Colloq. 13(2), 2006, p.329–348.

[15] Hertweck, M. *Zassenhaus conjecture for A6.* Proc. Indian Acad. Sci. Math. Sci. 118, no. 2, 2008, p. 189–195.

[16] Hertweck, M. e Kimmerle, W. *On principal blocks of p-constrained groups.* Proc. London Math. Soc. (3) 84, n. 1, 2002, p. 179–193.

[17] Higman, G. *Units in group rings.* Thesis (PhD), Oxford, 1940.

[18] Higman, G. *The units of group-rings.* Proc. London Math. Soc. (2) 46, (1940), p. 231–248.

[19] Hughes, I e Pearson, K.R. *The group of units of the integral group ring* $\mathbb{Z}S_3$. Canad. Math, Bull. n. 15, 1972,p. 529–534.

[20] Isaacs, I. M. *Character theory of finite groups.* Academic Press, New York, 1976.

[21] Isaacs, I. M. *Algebra: A Graduate Course.* Brooks & Cole, New York, 1994.

[22] James, G. and Liebeck, M. *Representation and characters of groups.* CUP, Cambridge, 1993.

[23] Juriaans, S. O e Polcino Milies, C. *Units of integral group rings of Frobenius groups.* J. Group Theory 3, no. 3, 2000, p. 277–284.

[24] Kleiner, I. *A history of Abstract Algebra.* Boston: Birkhauser, 2007.

[25] Liu, J.H. *Zassenhaus conjecture for groups of order* p^2q. Comm. Algebra 36, n. 5, 2008, p; 1671–1674.

[26] Luthar, I. S e . Passi, I. B. S. *Zassenhaus conjecture for A_5*. Proc. Indian Acad. Sci99, 1989, p. 1–5.

[27] Luthar, I. S. e Sehgal, S. K. *Torsion units in matrix group rings.* Comm. Algebra 20, no. 4, 1992, p. 1223–1228.

[28] Luthar,I. S., Trama, P. *Zassenhaus conjecture for certain integral group rings.* J. Indian Math. Soc. n. 55, 1990, p. 199–212.

[29] Luthar,I. S., Trama, P. *Zassenhaus conjecture for S_5*. Comm. Algebra 19, no. 8, 1991, pp.2353–2362.

[30] Marciniak, Z., Ritter, J., Sehgal, S. K. e Weiss, A. *Torsion units in integral group rings of some metabelian groups. II.* J. Number Theory 25, no. 3, 1987, p. 340–352.

[31] Margolis, L., del Río, A. Serrano, . *Zassenhaus conjecture on torsion units holds for $PSL(2,p)$ with p a Fermat or Mersenne prime.* J. Algebra 531 (2019), 320–335.

[32] Margolis, L. del Río, A. *Cliff-Weiss inequalities and the Zassenhaus Conjecture.* J. Algebra 507, 2018, p.292–319.

[33] Margolis, L. del Río, Á. *An algorithm to construct candidates to couterexemples to the Zassenhaus conjecture.* J. Algebra 514, p. 536-558, 2018.

[34] Margolis, L. del Río, Á. *Finite Subgroups of Group Rings: A survey.* Adv. Group Theory Appl, n. 8, 2019, p. 1–37.

[35] Margolis, L. del Río, Á. *Partial augmentations power properthy: A Zassenhaus conjecture related problem.* J. Pure Appl. Algebra 223 (2019), no. 9, 4089–4101.

[36] Miles, C. P, Sehgal, S. K. *An introduction to Group Rings.* Kluwer Academic Publishers, 2002.

[37] Milies, C. P. *The Group of Units of the Integral Group Ring $\mathbb{Z}D_4$*. Bol. Soc. Brasileira de Mat. n. 4, 1973, p. 85–92.

[38] Peterson, G. L. *Automorphisms of the integral group ring of Sn.* Proc. Amer. Math. Soc. 59, no. 1, 1976, p. 14–18.

[39] Sehgal, S. K. *Units in integral group rings.* Longman Scientific & Technical, New York, 1993.

[40] Tent, M. *Emmy Noether: The mother of Modern Algebra.* Wellesley: A K Peters, 2008.

[41] Van der Waerden, B. *A history of Algebra - from Al-Khowarism to Emmy Noether.* Berlim: Springer Verlag, 1985.

[42] Weiss, A. *Rigidity of p-adic p-torsion.* Ann. of Math. (2) 127, 1988, p. 317-332.

[43] Weiss. A. *Torsion units in integral group rings.* J. Reine Angew. Math. 415, 1991, p. 175-187.

[44] Zmud,È. M., Kurennoi, G. C. : *The finite groups of units of an integral group ring.* Vestnik Harkov. Gos. Univ. 1967, no. 26, (1967), p. 20 - 26.

Universidade Federal da Bahia - UFBA

Instituto de Matemática / Programa de pós-graduação em Matemática

---

Av. Milton Santos, s/n, Campus Universitário de Ondina, Salvador - BA

CEP: 40170 -110

<http://www.pgmat.ufba.br>