Universidade de São Paulo
Instituto de Matemática e Estatística
Bacharelado em Matemática

Representações Modulares de Grupos Finitos

Ricardo Felipe Rosada Canesin

Trabalho de Conclusão de Curso
MAT0148 – Introdução ao Trabalho Científico

Comissão Julgadora: Lucia Satie Ikemoto Murakami – IME-USP (Orientadora)
Felipe Yukihide Yasumura – IME-USP
Vitor de Oliveira Ferreira – IME-USP

São Paulo
2021

Agradecimentos

Este trabalho é a culminação de toda a minha a trajetória ao longo do curso de Bacharelado em Matemática no IME. Por isso, estes agradecimentos se destinam não só àqueles que me ajudaram diretamente com este projeto, mas também àqueles que contribuíram para o meu crescimento e que fizeram parte desses incríveis últimos quatro anos.

Primeiramente, agradeço à minha família. Ela sempre esteve ao meu lado e tudo só pôde começar e se desenvolver por conta dela. Além de me apoiar e me incentivar a dar o meu melhor, ela me deu ótimas condições para que eu pudesse focar nos meus estudos. Também agradeço a Poli, que me estimulou a seguir aquilo que eu mais gostava e que me fez muito boa companhia, tanto de modo virtual quanto de modo presencial, especialmente quando estávamos em São Paulo.

Os meus orientadores, Lucia e Vitor, também foram fundamentais nessa minha jornada e não posso deixar de agradecê-los. Eles me acompanharam desde o começo e me apresentaram a diversos assuntos interessantes. Através de conversas, conselhos e sugestões, também me ajudaram em outros contextos além do acadêmico. O zelo que eles têm pelos seus alunos é admirável. Mais especificamente a respeito deste trabalho, fiquei feliz quando aceitaram e apoiaram o projeto proposto, mesmo sendo em um tema não muito familiar. Também agradeço à sua paciência, em especial para a correção deste longo texto. Nesse sentido, também devo agradecer a Felipe, o terceiro membro da comissão julgadora, por concordar em revisar a monografia.

Eu tive a sorte de ter encontrado pessoas muito especiais ao longo desses anos. Por meio de discussões, jogos, encontros, viagens e muita matemática, eu pude vivenciar com elas momentos inesquecíveis. Espero que as amizades estabelecidas durem mesmo depois de nos formarmos. Sou muito grato a todas elas, mas não vou listar todos os nomes para não correr o risco de esquecer alguém. Ao invés disso, vou destacar aqueles que de alguma forma estiveram mais próximos do desenvolvimento deste projeto: Diogo Souza, Gabriel Bassan, Lorenzo Andreaus, Lucas Seidy e Thiago Landim.

A todos vocês, o meu sincero obrigado!

Resumo

Canesin, R. Representações modulares de grupos finitos. Monografia (Bacharelado em Matemática). *Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo,* 2021.

Esta monografia é uma introdução às representações modulares de grupos finitos. Ao invés de estudar representações sobre o corpo dos números complexos, como de costume, as definimos sobre corpos de característica positiva. Elas possuem um comportamento muito diferente e exigem novas ferramentas para serem abordadas. Após introduzir algumas técnicas da teoria de representações de álgebras associativas e apresentar como elas se especializam no caso de álgebras de grupo, tratamos de conceitos e resultados importantes da teoria de vértices e fontes e da teoria dos blocos, como a Correspondência de Green e os três Teoremas Principais de Brauer. Para concluir o estudo, aplicamos o que foi desenvolvido para demonstrar um profundo teorema que descreve as representações de um bloco com grupo de defeito cíclico. Por fim, em um apêndice, compilamos uma série de exercícios resolvidos sobre o assunto.

Palavras-chave: representações de grupos finitos, representações modulares, Correspondência de Green, teoria dos blocos, blocos com grupo de defeito cíclico.

Abstract

Canesin, R. Modular representations of finite groups. Undergraduate thesis (Bachelor's degree in Mathematics). *Institute of Mathematics and Statistics, University of São Paulo, São Paulo,* 2021.

This undergraduate thesis is an introduction to modular representations of finite groups. Instead of studying representations over the field of complex numbers, as usual, we define them over fields of positive characteristic. They possess a very different behavior and require new tools to be approached. After introducing some techniques from the the representation theory of associative algebras and presenting how they specialize in the case of group algebras, we deal with important concepts and results from the theory of vertices and sources and from block theory, such as Green's Correspondence and Brauer's three Main Theorems. To conclude the study, we apply what has been developed to prove a profound theorem describing the representations of a block with a cyclic defect group. At last, in an appendix, we compile a series of solved exercises about the subject.

Keywords: representations of finite groups, modular representations, Green's Correspondence, block theory, blocks with a cyclic defect group.

Sumário

Notações

Principais símbolos utilizados ao longo do texto

$\lvert X\rvert$	cardinalidade do conjunto X
$X \setminus Y$	diferença entre o conjunto X e o conjunto Y
$X \subseteq Y$	relação de continência entre conjuntos
id_X	função identidade do conjunto X
$\mathbb{Z}$	anel dos números inteiros
$\mathbb{R}$	corpo dos números reais
$\mathbb{C}$	corpo dos números complexos
$\mathbb{F}_q$	corpo finito de q elementos
$m \mid n$	indica que o inteiro m é um divisor do inteiro n
n_p	maior potência do primo p que divide o inteiro positivo n (quando fizer sentido)
$k^\times$	grupo de unidades do corpo k
$\mathrm{char}(k)$	característica do corpo k
C_n	grupo cíclico de n elementos
D_n	grupo diedral de $2n$ elementos
S_n	grupo simétrico em n símbolos
sgn	função sinal do grupo simétrico S_n
$\mathrm{SL}_2(p)$	grupo das matrizes 2×2 de determinante 1 com entradas em $\mathbb{F}_p$
$O_p(G)$	maior p-subgrupo normal do grupo G
$\mathrm{Aut}(G)$	grupo de automorfismos do grupo G
$\mathrm{GL}(U)$	grupo de operadores lineares inversíveis do espaço vetorial U
$\langle g\rangle$	subgrupo gerado pelo elemento g
$[G : H]$	índice do subgrupo H no grupo G
gH	classe lateral à esquerda de H em G contendo o elemento g
$[G/H]$	conjunto de representantes das classes laterais à esquerda de H em G
LgH	classe lateral dupla de H e L em G contendo o elemento g

$[L\backslash G/H]$	conjunto de representantes das classes laterais duplas de H e L em G
$N_G(H)$	normalizador de H em G
$C_G(H)$	centralizador de H em G
$R \subseteq_G \mathscr{H}$	indica que algum conjugado de R em G está contido em algum elemento da família de subgrupos $\mathscr{H}$
kG	álgebra de grupo do grupo G sobre o corpo k
IG	ideal de aumento da álgebra de grupo kG
$M_n(A)$	álgebra de matrizes $n \times n$ com entradas em A
$T_n(A)$	álgebra de matrizes triangulares inferiores $n \times n$ com entradas em A
$\det(X)$	determinante da matriz X
$\mathrm{tr}(X)$	traço da matriz X
δ_{ij}	delta de Kronecker
e_{ij}	matriz elementar com entrada não nula na coordenada (i, j)
$k[x_1, \ldots, x_r]$	álgebra de polinômios em r variáveis sobre k
$Z(A)$	centro da álgebra A
$[A, A]$	subespaço de comutadores da álgebra A
A^{op}	álgebra oposta de A
$A_1 \times A_2$	produto direto das álgebras (ou dos grupos) A_1 e A_2
${}_AA$	o A-módulo regular (à esquerda)
$\dim_k U$	dimensão do k-espaço vetorial U
$l(U)$	comprimento do módulo U
$V \leq U$	indica que V é um submódulo (ou um subgrupo) de U
$U \oplus V$	soma direta dos espaços vetoriais (ou dos módulos) U e V
U^n	soma direta de n cópias do espaço vetorial (ou do módulo) U
$U \mid V$	indica que U é (isomorfo a) um somando direto de V
$\ker \varphi$	núcleo do homomorfismo φ
$\mathrm{im}\, \varphi$, $\varphi(U)$	imagem da função $\varphi : U \to V$
$\mathrm{Hom}_A(U, V)$	espaço dos homomorfismos do A-módulo U para o A-módulo V
$\mathrm{End}_A(U)$	álgebra de endomorfismos do A-módulo U
$\mathrm{rad}(U)$	radical do módulo (ou da álgebra) U
$\mathrm{rad}^n(U)$	n-ésimo termo da série radical do módulo U
$\mathrm{soc}(U)$	soco do módulo U

$\mathrm{soc}^n(U)$	n-ésimo termo da série de socos do módulo U
$U \otimes V$	produto tensorial entre os espaços vetoriais (ou os kG-módulos) U e V
$U^{\otimes n}$	produto tensorial de n cópias do espaço vetorial (ou do kG-módulo) U
$\varphi \otimes \psi$	produto tensorial das transformações lineares φ e ψ
$S^n(V)$	n-ésima potência simétrica do kG-módulo V
U^*	dual do espaço vetorial (ou do kG-módulo) U
f^*	transposta da transformação linear f
$V^\perp$	anulador do submódulo V de um kG-módulo U
U_H	restrição do kG-módulo U ao subgrupo H
V^G	indução do kH-módulo V a um grupo G contendo H
$kG \otimes_{kH} V$	produto tensorial sobre kH entre kG e um kH-módulo V, onde $H \leq G$
α^G	único homomorfismo de V_1^G em V_2^G que estende o homomorfismo $\alpha : V_1 \to V_2$
${}^gV$	conjugação de um kH-módulo V por $g \in G$, onde $H \leq G$
$\overline{\mathrm{Hom}}_{kG}(M, N)$	quociente de $\mathrm{Hom}_{kG}(M, N)$ pelo subespaço dos homomorfismos de M em N que se fatoram por um kG-módulo projetivo
$\mathrm{Hom}_{kG,\mathscr{H}}(M, N)$	espaço dos homomorfismos $\mathscr{H}$-projetivos de M em N
$\overline{\mathrm{Hom}}^{\mathscr{H}}_{kG}(M, N)$	quociente de $\mathrm{Hom}_{kG}(M, N)$ por $\mathrm{Hom}_{kG,\mathscr{H}}(M, N)$
c_{ST}	invariante de Cartan associado aos módulos simples S e T
C_A	matriz de Cartan da álgebra A
$b_0(G)$	bloco principal de kG
b^G	bloco de kG que corresponde ao bloco b de kH, onde $H \leq G$
$\mathrm{Stab}(b)$	estabilizador em G do bloco b de kN, onde N é subgrupo normal de G
$(R, b_R) \lhd (Q, b_Q)$	relação de normalidade entre subpares
$(R, b_R) \subseteq (Q, b_Q)$	relação de continência entre subpares
PU	cobertura projetiva do kG-módulo U
π_U	epimorfismo essencial de PU em U, onde U é um kG-módulo
ΩU	operador de Heller aplicado ao kG-módulo U, ou seja, núcleo de π_U
IU	envolvente injetiva do kG-módulo U
λ_U	monomorfismo essencial de U em IU, onde U é um kG-módulo
$\Omega^{-1}U$	conúcleo de λ_U para um kG-módulo U
$\Omega^0 U$	maior somando projetivamente livre do kG-módulo U
$G_0(A)$	grupo de Grothendieck da álgebra A

$[U]$	classe do A-módulo U no grupo de Grothendieck $G_0(A)$
$K_0(A)$	subgrupo de $G_0(A)$ gerado pelos elementos da forma $[P]$ onde P é um A-módulo projetivo
$\overline{G_0}(A)$	quociente de $G_0(A)$ por $K_0(A)$

Convenções para algumas letras

k	um corpo qualquer
p	característica de k, que é sempre positiva a partir da Seção 3.2
A	uma álgebra associativa não nula, com unidade e de dimensão finita sobre k
G	um grupo finito qualquer
H	um subgrupo de G qualquer
Q	ao lidarmos com a Correspondência de Green, geralmente denota um p-subgrupo qualquer de G
L	ao lidarmos com a Correspondência de Green, geralmente denota um subgrupo de G contendo $N_G(Q)$
$\mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}$	famílias de subgrupos que aparecem na Correspondência de Green
δ	mapa diagonal de G em $G \times G$ (quando fizer sentido)

Notações e hipóteses específicas do Capítulo 5

k	corpo algebricamente fechado
p	característica de k, que é positiva
B	bloco de kG com grupo de defeito cíclico e não trivial
D	grupo de defeito de B, que é cíclico
q	ordem de D
n	defeito de B, ou seja, vale $q = p^n$
e	índice inercial de B
D_1	único subgrupo de D de ordem p
N	normalizador $N_G(D)$ de D em G
N_1	normalizador $N_G(D_1)$ de D_1 em G
C	centralizador $C_G(D)$ de D em G
C_1	centralizador $C_G(D_1)$ de D_1 em G
b	correspondente de Brauer de B em kN
β	bloco de kC coberto por b

b_1	bloco b^{N_1} de kN_1
β_1	bloco de kC_1 coberto por b_1 e com grupo de defeito D
I_1	estabilizador $\mathrm{Stab}(\beta_1)$ de β_1 em N_1
V_i	i-ésimo b_1-módulo simples, seguindo a ordenação da árvore de Brauer (essa notação e as seguintes são válidas a partir da Seção 5.4)
V_{is}	b_1-módulo indecomponível de quociente radical V_i e comprimento s
S_i	i-ésimo B-módulo simples
T_i	correspondente de Green de S_i, cujo quociente radical é V_i
π	permutação de $\{0, 1, \ldots, e-1\}$ caracterizada por $\mathrm{soc}(T_i) \cong V_{\pi(i)}$
ρ	inversa da permutação π
σ	permutação de $\{0, 1, \ldots, e-1\}$ caracterizada por $\sigma(i) \equiv \pi(i) + 1 \pmod{e}$
$a \ \ (= a(i))$	maior inteiro não negativo tal que $l(T_i) + l(T_{\rho(i)}) + \cdots + l(T_{\rho^a(i)}) > aq$
$b \ \ (= b(i))$	maior inteiro não negativo tal que $l(T_i) + l(T_{\sigma(i)}) + \cdots + l(T_{\sigma^b(i)}) < q$ (não confundir com o correspondente de Brauer de B, que possui a mesma notação)
U_i^ρ	B-módulo unisseriado de comprimento $a+1$ e fatores de composição $S_i, S_{\rho(i)}, \ldots, S_{\rho^a(i)}$, nessa ordem
U_i^σ	B-módulo unisseriado de comprimento $b+1$ e fatores de composição $S_i, S_{\sigma(i)}, \ldots, S_{\sigma^b(i)}$, nessa ordem
W_i^ρ	radical de U_i^ρ
W_i^σ	radical de U_i^σ
P_i	cobertura projetiva de S_i, que satisfaz $\mathrm{rad}(P_i)/\mathrm{soc}(P_i) \cong W_i^\rho \oplus W_i^\sigma$
m	multiplicidade do vértice excepcional da árvore de Brauer de B

Introdução

O conceito de grupo é importantíssimo para a Matemática e está presente nas suas mais diversas áreas. Ele busca abstrair a nossa noção intuitiva do que é simetria e nos permite estudá-la sistematicamente. Porém, olhar apenas para um grupo não é suficiente para descrever todas as nuances dessa intuição. É preciso entender também como o grupo *age* no objeto a ser analisado. Essa ação, em geral, surge naturalmente. Por exemplo, os grupos simétricos finitos, que são centrais para a teoria e foram um de seus principais motivadores, são definidos a partir de permutações em certos conjuntos e, consequentemente, já vêm equipados com uma ação canônica. Além disso, resultados sobre grupos, tais como os Teoremas de Sylow, podem ser demonstrados mais facilmente através de ações.

Existe um tipo especial de ação de grupo: as representações. Elas aparecem quando "linearizamos" o conceito de ação. Formalmente, uma representação de um grupo G é um homomorfismo de G no grupo de operadores lineares inversíveis de um espaço vetorial. Seu estudo se iniciou na última década do século XIX, com os trabalhos do matemático Ferdinand Frobenius sobre a recém-criada teoria de caracteres. Com essas novas ferramentas, Frobenius descobriu resultados surpreendentes e mostrou como as representações de grupos possuem uma teoria muito rica.

Por outro lado, ainda havia incertezas se a introdução da álgebra linear realmente aprimoraria o estudo de grupos e suas ações. Um dos matemáticos que não estavam muito otimistas nesse sentido era William Burnside. Em 1897, Burnside publicou o seu influente tratado *Theory of Groups of Finite Order* e, no prefácio, explicou não ter mencionado representações de grupos pois considerava difícil encontrar um resultado que pudesse ser obtido mais facilmente através delas. Entretanto, sua visão rapidamente mudou. Foi nesse período que começaram a aparecer os primeiros resultados de Frobenius e, logo em seguida, Burnside adentrou esse novo mundo, provando importantes teoremas. No prefácio da segunda edição de seu tratado, publicada em 1911, ele dessa vez escreveu o seguinte a respeito das representações de grupos: "... the reason given in the original preface for omitting any account of it no longer holds good. In fact, it is more true to say that for further advances in the abstract theory one must look largely to the representation of a group by linear substitutions." Ele estava certo! Por exemplo, a teoria de representações foi essencial para se iniciar a classificação dos grupos simples finitos, aparecendo como ingrediente principal em algumas demonstrações, como a do célebre Teorema de Feit-Thompson acerca da solubilidade de grupos finitos de ordem ímpar.

Há um detalhe a ser apontado: as representações de grupos consideradas na história contada até agora eram definidas a partir de espaços vetoriais complexos. A aparição do corpo dos números complexos é natural, já que esse é o primeiro corpo algebricamente fechado que vem à nossa mente. Mas, se quisermos entender todas as formas das quais um grupo pode agir, não devemos considerar também espaços vetoriais definidos sobre outros corpos? A resposta é sim e, nesse sentido, a característica do corpo é o fator mais determinante no comportamento das representações. Na primeira década do século XX, Leonard Dickson foi o primeiro a apontar que a teoria não se comporta da mesma maneira quando a característica é positiva e divide a ordem do grupo. Essas representações *modulares*, como Dickson as chamou, são mais complicadas porque, em uma linguagem mais moderna, elas vêm de álgebras que não são mais semissimples. Talvez tenha sido essa dificuldade que tornou o território modular praticamente inexplorado por um bom

tempo após os trabalhos de Dickson.

O matemático Richard Brauer foi o primeiro a de fato estudar as representações modulares sistematicamente, elevando a teoria a um novo patamar. Brauer acreditava que essa área poderia fornecer novos métodos e novas técnicas para atacar a teoria de grupos, em especial a classificação dos grupos simples finitos. Ele obteve êxito nesse sentido e, para isso, precisou desenvolver diversas ideias, dentre elas, a teoria dos blocos. Se G é um grupo finito e k é um corpo de característica $p > 0$, podemos decompor a álgebra de grupo kG como uma soma direta de ideais bilaterais indecomponíveis, os chamados *blocos* de G. Brauer associou um p-subgrupo de G a cada bloco, o seu *grupo de defeito*. A decomposição de kG em blocos particiona a coleção de caracteres irredutíveis de um modo especial, e propriedades do grupo de defeito de um bloco refletem propriedades dos caracteres associados. Esses conceitos foram fundamentais em boa parte do trabalho de Brauer e de outros matemáticos que levaram as suas ideias adiante.

A presente monografia se encaixa nesse contexto[1] e tem como objetivo principal introduzir a teoria das representações modulares de grupos finitos. Diferentemente de Brauer, que focou no uso de caracteres, a nossa abordagem será dada através da teoria de módulos, visão esta que teve como pioneiros Emmy Noether e, mais especificamente no caso modular, James A. Green. Sob essa ótica, desenvolveremos o básico da teoria dos blocos de Brauer e concluiremos com o seguinte profundo teorema que descreve a estrutura das representações de um bloco com grupo de defeito cíclico:

Teorema. Seja G um grupo finito e seja k um corpo algebricamente fechado cuja característica é positiva e divide a ordem de G. Se B é um bloco de kG e possui um grupo de defeito D não trivial e cíclico, então B é uma álgebra de Brauer. Além disso, o número de arestas da árvore de Brauer associada é igual ao índice inercial e de B e a multiplicidade de seu vértice excepcional é $(|D| - 1)/e$.

De certa forma, quase todos os conceitos e resultados que serão introduzido neste material visam explicar o enunciado acima e a sua demonstração.

Como todo texto de Matemática, alguns pré-requisitos são exigidos do leitor. De teoria de grupos, assumimos desde as propriedades básicas dos grupos finitos até os Teoremas de Sylow. Em alguns momentos, conhecer algumas propriedades de p-grupos também ajudará. Em relação à teoria de anéis e de corpos, pouco é necessário, mas é preciso conhecer a definição de álgebra associativa e alguns exemplos. De álgebra linear, além do básico, requeremos que o leitor tenha alguma familiaridade com a decomposição de Jordan de um operador linear e com produtos tensoriais de espaços vetoriais. Por fim, é necessário saber um tanto de teoria de módulos. Essencialmente, utilizamos o linguajar inicial, como as definições de submódulo, quociente, soma direta, homomorfismo e os teoremas correlatos, mas também precisamos de alguma noção sobre sequências exatas e de algumas propriedades de módulos simples, especialmente do Teorema de Jordan-Hölder.

A seguir, damos mais detalhes a respeito dos capítulos deste texto.

Os Capítulos 1 e 2 lidam, em sua maior parte, com um contexto mais geral, introduzindo os conceitos para álgebras de dimensão finita quaisquer. Essas técnicas da teoria de representações de álgebras associativas formam a base para o que se segue e, pouco a pouco, vamos nos especializando no caso das álgebras de grupo. O Capítulo 1 apresenta resultados iniciais sobre módulos simples e semissimples. Após introduzir os conceitos de radical e de soco e de provar o Teorema de Wedderburn, são demonstrados alguns resultados sobre representações de grupos, já voltados para o caso modular. Em seguida, o Capítulo 2 foca no entendimento dos módulos indecomponíveis, em especial daqueles que também são projetivos. As principais propriedades são mostradas e então abordamos duas ferramentas especiais presentes nas representações de grupos: a dualidade e o produto tensorial. Até esse ponto, já conseguimos obter propriedades interessantes das representações.

[1] Se quiser conhecer mais sobre essa introdução histórica, consulte [8], por exemplo.

A partir do Capítulo 3, utilizamos mais fortemente a teoria de grupos. A ideia é relacionar as representações de um grupo com as de seus subgrupos. Para esse propósito, é imprescindível estudar mais a fundo a restrição e a indução de representações, que compõem essa ponte associando os subgrupos. Como forma de estender as técnicas do Capítulo 2, é considerado o conceito de projetividade relativa e naturalmente somos levados às definições de vértices e fontes de módulos indecomponíveis. É nesse momento que os p-subgrupos (com p um número primo) e os seus normalizadores e centralizadores começam a adquirir maior importância. O capítulo se encerra após um extenso tratamento acerca da Correspondência de Green e de suas propriedades. Ela pode ser considerada o maior "lema" de toda esta exposição, uma vez que essa correspondência é peça-chave dos principais teoremas que se seguem.

Finalmente, chegamos na teoria dos blocos propriamente dita. O Capítulo 4 traz as propriedades básicas dos blocos e logo após é dada uma das possíveis definições para um grupo de defeito. Ao longo do capítulo, a ideia por trás desse conceito se clarifica e, caracterizando os blocos com grupo de defeito trivial, começamos a visualizar como os grupos de defeito influenciam a estrutura das representações. O outro ponto alto deste capítulo é a demonstração dos três Teoremas Principais de Brauer, que relacionam os blocos de um grupo e de seus subgrupos na mesma filosofia do Capítulo 3. Em alguns casos, em especial no estudo da Correspondência de Brauer, nos aprofundamos na teoria e estendemos alguns resultados para uso posterior ou apenas a título de curiosidade.

Concluímos com uma descrição detalhada dos blocos com grupo de defeito cíclico. No Capítulo 5, vemos que esses são exatamente os blocos com um número finito de módulos indecomponíveis e, por isso, imaginamos haver mais chance de conseguir classificá-los. No entanto, essa classificação é longa e nada fácil. Precisaremos aplicar basicamente tudo o que desenvolvemos até então. Em termos históricos, o próprio Brauer já havia conseguido uma boa descrição, mas apenas quando o grupo de defeito possui ordem prima. Uma descrição do caso geral só foi obtida na década de 1960 pelo matemático Everett Dade. Como estamos seguindo outra abordagem, atacaremos o problema por outra direção, seguindo, em especial, os trabalhos de Jonathan Alperin (vide o último capítulo de [1]) e de Richard Peacock (vide [18]).

A estruturação dos capítulos como acima é fortemente baseada no livro [1], a nossa principal referência. Esta monografia pode ser pensada como uma versão estendida desse livro. Acrescentamos comentários, alteramos alguns argumentos e explicamos melhor algumas demonstrações que, para nós, não estavam muito claras[1]. Ademais, resultados e exemplos de outras fontes também foram apresentados para complementar a linha de raciocínio seguida. Nesse sentido, as principais referências auxiliares foram os livros [7] e [22]. Finalmente, em um apêndice, compilamos uma série de exercícios e soluções para cada capítulo do texto, incluindo as soluções de todos os exercícios de [1]. Alguns desses exercícios são utilizados durante texto, mas, em geral, são observações simples que não encaixam no meio das demonstrações. De qualquer forma, sempre aparece indicado o exercício correspondente caso seja necessário recorrer à solução.

[1] Destacamos, em especial, as demonstrações dos Teoremas 5.4.12 e 5.5.1.

Capítulo 1

Semissimplicidade

Como veremos, estudar as representações de um grupo G sobre um corpo k é equivalente a estudar os módulos sobre a álgebra de grupo kG. Desse modo, podemos utilizar todo o arsenal de teoria de módulos a nosso favor. Este capítulo inicial dá os primeiros passos nessa direção, fornecendo resultados sobre a classe de módulos mais facilmente tratável: os módulos semissimples. Essa facilidade reside essencialmente no fato de que, conhecidos os fatores de composição de um módulo semissimples, sabemos como juntá-los para recuperar o nosso módulo.

A primeira seção do capítulo aborda as propriedades dos módulos semissimples sobre álgebras de dimensão finita quaisquer, mas esse não é o seu foco principal. No futuro, lidaremos muito mais com módulos que não são semissimples, então apresentamos algumas formas de como "quebrar" um módulo qualquer em camadas semissimples. Isso é feito através dos conceitos de radical e de soco de um módulo. Para ilustrar as definições, calculamos como elas se especializam para o caso de uma álgebra de matrizes triangulares.

Em seguida, nos dedicamos à prova do Teorema de Wedderburn. Ele nos mostra como construir todas as álgebras semissimples a partir de álgebras de divisão e suas álgebras de matrizes. Não demonstramos esse resultado apenas por sua beleza, mas também porque, quando estivermos investigando as álgebras de grupo, aparecerão algumas álgebras semissimples e essa caracterização será útil.

Com isso em mãos, iniciamos o estudo das representações de grupos. Os teoremas provados nessa seção dão uma ideia de como são os módulos simples e semissimples sobre uma álgebra de grupo e conectam certas propriedades de grupos a certas propriedades desses módulos. Também apresentamos diversos exemplos e destacamos, em especial, as representações de grupos cíclicos e do grupo $\mathrm{SL}_2(p)$, que serão constantemente aprofundadas ao longo do restante do texto. Para concluir o capítulo, é provado o Teorema de Brauer a respeito do número de classes de isomorfismo de módulos simples de uma álgebra de grupo.

1.1 Definições e propriedades iniciais

Notação 1.1.1. Daqui em diante, denotaremos por A uma álgebra associativa não nula, com unidade e de dimensão finita sobre um corpo k. Um A-módulo U será entendido como um A-módulo *à esquerda*. A princípio, lidaremos apenas com álgebras e módulos de dimensão finita sobre k e, portanto, deixaremos esse fato implícito.

Para estudar módulos sobre A, começamos entendendo aqueles que têm uma estrutura menos complicada. No nosso caso, um A-módulo U é **simples** se $U \neq 0$ e os únicos submódulos de U são os triviais. Note que qualquer elemento não nulo é um gerador de U e, portanto, segue que U é um quociente de A, visto como A-módulo por multiplicação à esquerda[1]. Por isso, U é um fator

[1] Esse é o **A-módulo regular**. Às vezes o denotaremos por ${}_AA$ para diferenciá-lo da álgebra A, mas, em geral, o representaremos apenas por A para não sobrecarregar a notação.

de composição de ${}_AA$ e, consequentemente, há apenas um número finito de módulos simples.

O primeiro passo da seção será introduzir a próxima classe de módulos mais fácil de estudar: os módulos que são soma direta de módulos simples. Chamaremos tais módulos de **semissimples**.

Observação 1.1.2. É conveniente considerar que o módulo nulo é semissimples. Pode-se pensar que ele é a soma "vazia" de módulos simples.

Começamos com uma caracterização:

Proposição 1.1.3. Se U é um A-módulo, então U é semissimples se e somente se todo submódulo de U é um somando direto.

Demonstração: ($\Longrightarrow$) Se U é semissimples, escreva[1] $U = S_1 \oplus \cdots \oplus S_n$, onde cada S_i é um submódulo simples. Seja V um submódulo qualquer de U. Vamos construir um complemento para V somando alguns dos S_i's. Seja $I \subseteq \{1, \ldots, n\}$ maximal com a propriedade de que a soma

$$V + \sum_{i \in I} S_i$$

é direta (talvez I possa ser o conjunto vazio). Afirmamos que a soma acima é igual a U, de modo que V é um somando direto. De fato, caso isso não acontecesse, existiria algum S_j não contido nessa soma. Sendo S_j simples, S_j intersectaria trivialmente a soma em questão e, assim, a soma

$$V + S_j + \sum_{i \in I} S_i$$

seria direta, contradizendo a maximalidade de I.

($\Longleftarrow$) Primeiramente, vejamos que U é soma (não necessariamente direta) de submódulos simples. Seja W a soma de todos os submódulos simples de U. Provemos que $W = U$. Como W é somando direto de U, existe um submódulo W' tal que $U = W \oplus W'$. Se W' fosse não nulo, então W' conteria um submódulo simples (por questões de dimensão). Mas tal submódulo simples deveria estar em W, por construção. Sendo a soma direta, deve valer $W' = 0$ e $U = W$, como preciso. Como U tem dimensão finita, U é a soma de um número finito de submódulos simples. Para concluir, podemos imitar a prova em ($\Longrightarrow$) considerando $V = 0$, de onde obtemos que U é a soma direta de alguns submódulos simples. □

Observe que a segunda parte da demonstração acima prova que, se um módulo é soma (não necessariamente direta) de submódulos simples, então ele é semissimples. Essa é uma outra caracterização de semissimplicidade.

Vejamos algumas propriedades dos módulos semissimples:

Proposição 1.1.4. Somas (não necessariamente diretas) de módulos semissimples, submódulos de módulos semissimples e quocientes de módulos semissimples são todos novamente semissimples.

Demonstração: A propriedade da soma é imediata da definição inicial de semissimplicidade. Note que a soma não precisa ser direta em vista da observação logo acima do enunciado.

Agora, sejam U um A-módulo semissimples e V um submódulo de U. Se $W \leq V$, então, pela Proposição 1.1.3 (que passaremos a usar sem avisar!), existe $W' \leq U$ tal que $U = W \oplus W'$. Não é difícil verificar que $V = W \oplus (W' \cap V)$. Desse modo, todo submódulo de V é somando direto, ou seja, V é semissimples também.

Por fim, mostremos que se U é semissimples e $V \leq U$ então U/V é semissimples. De fato, como V possui um complemento V' em U, vemos que $U/V \cong V'$ e a afirmação segue do parágrafo anterior. □

[1] Lembre que estamos supondo que U tem dimensão finita, logo há um número finito de termos na soma direta. Se U for de dimensão qualquer, não é difícil adaptar o argumento dado (e outros que aparecem depois), mas precisamos do Lema de Zorn em alguns momentos.

Por álgebra linear, sabemos que todos os módulos sobre um corpo (mais geralmente, sobre um anel/álgebra de divisão) são semissimples. Relacionando com representações de grupos, repare que o enunciado usual do Teorema de Maschke[1] diz que todo módulo sobre a álgebra de grupo kG é semissimples se o grupo G for finito e $\text{char}(k)$ não dividir $|G|$. Nesses exemplos, note que *todos* os módulos são semissimples.

Definição 1.1.5. Se todos os A-módulos são semissimples, dizemos que A é uma **álgebra semissimples**.

Observação 1.1.6. Para verificar que A é semissimples, basta verificar que o A-módulo regular ${}_AA$ é semissimples. Isso segue da Proposição 1.1.4 e do fato de que todo A-módulo é quociente de uma soma direta de cópias do módulo regular.

No âmbito das representações modulares de grupos finitos, ou seja, quando $\text{char}(k)$ divide $|G|$, não vale mais que kG é semissimples e, por isso, desenvolveremos métodos para estudar álgebras e módulos que não são semissimples. A ideia é tentar construir os módulos através de "camadas" de semissimples, como veremos daqui a pouco.

Definição 1.1.7. Definimos o **radical de** A (ou **radical de Jacobson** de A), denotado por $\text{rad}(A)$, como a interseção dos anuladores de todos os A-módulos *simples*.

Por anulador de um A-módulo U queremos dizer o subconjunto de A dos elementos que anulam U. É fácil provar que esse anulador é um ideal (bilateral). Em particular, $\text{rad}(A)$ é um ideal de A.

Mas qual a relação do radical com módulos semissimples? De imediato, podemos ver que $\text{rad}(A)$ consiste dos elementos que anulam módulos semissimples. Também temos as seguintes caracterizações:

Teorema 1.1.8. O radical de A coincide com cada um dos seguintes módulos:

(1) O menor submódulo de ${}_AA$ cujo quociente correspondente é semissimples.

(2) A interseção de todos os submódulos maximais de ${}_AA$.

(3) O maior ideal nilpotente de A.

Note que os submódulos de ${}_AA$ são exatamente os ideais à esquerda de A. Além disso, diremos que um ideal N de A é **nilpotente** se existir um inteiro positivo n tal que[2] $N^n = 0$ ou, equivalentemente, tal que $x_1x_2\cdots x_n = 0$ para todos $x_1, \ldots, x_n \in N$.

Demonstração: Comecemos provando que (1) e (2) são o mesmo submódulo. Seja I a interseção de todos os submódulos maximais do módulo regular A (denotaremos assim para simplificar a notação). Como A tem dimensão finita, I é a interseção de um número finito de submódulos maximais, digamos $M_1, \ldots, M_r$. Somando as projeções de A a A/M_i, obtemos um mapa

$$A \to A/M_1 \oplus A/M_2 \oplus \cdots \oplus A/M_r$$

cujo núcleo é I. Logo, A/I é isomorfo a um submódulo da soma acima, que é semissimples pois cada A/M_i é simples. Por isso, A/I é semissimples. Vejamos que I é o menor submódulo com essa propriedade. Seja $J \leq A$ tal que A/J é semissimples e escreva

$$A/J = J_1/J \oplus \cdots \oplus J_s/J$$

[1] Se você não conhece esse teorema, aguarde um pouco que já chegaremos nele!

[2] Se I é um ideal de A e U é um A-módulo, IU denota o submódulo de U gerado pelos produtos xy com $x \in I$ e $y \in U$. Para ideais de A, faz sentido iterar esse procedimento e podemos definir de modo natural o ideal I^n para qualquer inteiro positivo n.

onde $J \leq J_i \leq A$ e cada J_i/J é simples. Se N_i é a soma de todos os J_j com $j \neq i$, então

$$\frac{A}{N_i} \cong \frac{A/J}{N_i/J} \cong \frac{J_i}{J}$$

é simples e N_i é submódulo maximal. Como $J = N_1 \cap \cdots \cap N_s$, segue que J é a interseção de alguns submódulos maximais e, por isso, $I \subseteq J$.

Vamos mostrar que $I = \operatorname{rad}(A)$. Como A/I é semissimples, $\operatorname{rad}(A)$ anula esse quociente e então $\operatorname{rad}(A) \subseteq I$. Para provar a inclusão contrária, seja $x \in I$ e mostremos que $xS = 0$ para todo módulo simples S. Da simplicidade de S, dado $s \in S$ não nulo, s gera S. Logo, o homomorfismo de módulos $A \to S$ dado por $a \mapsto as$ é sobrejetor e, novamente da simplicidade de S, seu núcleo M_s é um submódulo maximal de A. Como $x \in I$, vale que $x \in M_s$ e então $xs = 0$. Como s era arbitrário, segue que $xS = 0$ como preciso. Disso, concluímos que $x \in \operatorname{rad}(A)$ e $I \subseteq \operatorname{rad}(A)$.

Para terminar, resta mostrar que $\operatorname{rad}(A)$ é o ideal em (3). Primeiro, vejamos que todo ideal nilpotente N está contido em $\operatorname{rad}(A)$. Dado um A-módulo simples S, vale que $NS = 0$ ou $NS = S$. Se $NS = S$, então $N^n S = S$ para todo $n \geq 1$, contradizendo que N é nilpotente. Por isso, $NS = 0$ e $N \subseteq \operatorname{rad}(A)$. Agora, vamos demonstrar que $\operatorname{rad}(A)$ é nilpotente. Como A tem dimensão finita, existe uma série de composição

$$0 = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_r = A$$

de modo que A_{i+1}/A_i é sempre simples. Mas então $\operatorname{rad}(A)$ anula cada um desses quocientes e vale $\operatorname{rad}(A)A_{i+1} \subseteq A_i$ para todo $1 \leq i \leq r$. Logo

$$\operatorname{rad}(A)^r = \operatorname{rad}(A)^r A_r \subseteq A_0 = 0,$$

como queríamos. □

Corolário 1.1.9. A álgebra A é semissimples se e somente se $\operatorname{rad}(A) = 0$.

Demonstração: Segue imediatamente do Teorema 1.1.8 usando a caracterização (1). □

Observação 1.1.10. Como vimos anteriormente, $\operatorname{rad}(A)$ anula todo A-módulo semissimples e, por isso, podemos ver um A-módulo semissimples como um $(A/\operatorname{rad}(A))$-módulo. Reciprocamente, pelo Teorema 1.1.8, $A/\operatorname{rad}(A)$ é um A-módulo semissimples e é fácil ver que ele continua semissimples como um $(A/\operatorname{rad}(A))$-módulo. Lembrando que $\operatorname{rad}(A)$ é um ideal de A, segue que $A/\operatorname{rad}(A)$ é semissimples como álgebra. Dessa forma, todo $(A/\operatorname{rad}(A))$-módulo é semissimples e, ao restringirmos escalares[1] para A, obtemos um A-módulo semissimples também. Em outras palavras, os módulos semissimples sobre A são precisamente os A-módulos anulados por $\operatorname{rad}(A)$ e, por consequência, estão em correspondência com os módulos sobre $A/\operatorname{rad}(A)$.

Exemplo 1.1.11. Seja $A = T_n(k)$ a álgebra das matrizes triangulares inferiores $n \times n$ com entradas em k. Vamos encontrar o radical de $T_n(k)$. Como $\operatorname{rad}(T_n(k))$ contém os ideais nilpotentes, sabemos que $\operatorname{rad}(T_n(k))$ tem que conter o ideal N de $T_n(k)$ formado pelas matrizes com 0 em toda a diagonal principal (para ver que N é ideal, use a relação do próximo parágrafo, e para provar que N é nilpotente, olhe o Exemplo 1.1.18). Por outro lado, vejamos que $T_n(k)/N$ é semissimples como $T_n(k)$-módulo. Isso implicará que $\operatorname{rad}(T_n(k)) \subseteq N$ e teremos $\operatorname{rad}(T_n(k)) = N$.

Passando a relação

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ * & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ * & b_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & 0 & \cdots & 0 \\ * & a_{22}b_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & a_{nn}b_{nn} \end{pmatrix}$$

[1] Se $\varphi : A \to B$ é um homomorfismo de álgebras e U é um B-módulo, o A-módulo obtido **restringindo escalares** de U tem como estrutura linear subjacente a mesma de U mas com ação $a \cdot_A u := \varphi(a) \cdot_B u$, onde $a \in A$ e $u \in U$. Nesse caso, a restrição é através da projeção $A \to A/\operatorname{rad}(A)$.

ao quociente, podemos ver que o subconjunto S_i de $T_n(k)/N$ dado por

$$S_i = \{M + N \mid M = (a_{ij}) \in T_n(k) \text{ e } a_{jj} = 0 \text{ para } j \neq i\}$$

é um submódulo. Como ele tem dimensão 1, S_i é simples para todo i. Mas é imediato que $T_n(k)/N = S_1 \oplus \cdots \oplus S_n$, provando que $T_n(k)/N$ é semissimples, como preciso.

Observe que cada S_i acima pode ser identificado com k de modo que a ação de $T_n(k)$ em S_i é dada por

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ * & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & a_{nn} \end{pmatrix} b = a_{ii}b,$$

onde a matriz acima pertence a $T_n(k)$ e $b \in k$ é qualquer. Como esses são os módulos simples que constituem $T_n(k)/\operatorname{rad}(T_n(k))$, sabemos que eles consistem de todos os módulos simples sobre $T_n(k)$ pela observação de antes desse exemplo. Note que eles são dois a dois não isomorfos.

O próximo passo será definir o radical para A-módulos quaisquer e ver qual é a relação com $\operatorname{rad}(A)$.

Proposição 1.1.12. Se U é um A-módulo, então os seguintes módulos são iguais:

(1) $\operatorname{rad}(A)U$.

(2) O menor submódulo de U cujo quociente correspondente é semissimples.

(3) A interseção de todos os submódulos maximais de U.

Demonstração: O início da demonstração do Teorema 1.1.8 pode ser adaptado facilmente para mostrar que (2) e (3) definem o mesmo módulo. Vejamos que (1) e (2) também coincidem. Note que $U/\operatorname{rad}(A)U$ é semissimples pela Observação 1.1.10, já que é anulado por $\operatorname{rad}(A)$. Por outro lado, se $V \leq U$ é tal que U/V é semissimples, então $\operatorname{rad}(A)$ anula U/V, ou seja, $\operatorname{rad}(A)U \subseteq V$. Isso mostra que $\operatorname{rad}(A)U$ é o menor submódulo de U cujo quociente é semissimples. □

O submódulo de U dado pela proposição acima também será chamado de **radical** de U e o denotaremos por $\operatorname{rad}(U)$. Veja que para $U = {}_AA$ essa definição coincide com $\operatorname{rad}(A)$. Como $\operatorname{rad}(U)$ é um módulo, podemos aplicar a construção mais uma vez e definir

$$\operatorname{rad}(\operatorname{rad}(U)) = \operatorname{rad}(A)(\operatorname{rad}(A)U) = \operatorname{rad}(A)^2U.$$

Denotaremos esse módulo por $\operatorname{rad}^2(U)$. Iterando esse processo, definimos analogamente $\operatorname{rad}^n(U) = \operatorname{rad}(A)^nU$ para n inteiro positivo. Por conveniência, impomos $\operatorname{rad}^0(U) = U$. A cadeia descendente

$$U = \operatorname{rad}^0(U) \supseteq \operatorname{rad}^1(U) \supseteq \operatorname{rad}^2(U) \supseteq \cdots$$

é a **série radical** de U, onde cada um dos quocientes (chamados de **camadas radicais**[1] de U) é semissimples pela Proposição 1.1.12. Note que a série eventualmente chega em 0, pois $\operatorname{rad}(A)$ é nilpotente. O primeiro inteiro r tal que $\operatorname{rad}^r(U) = 0$ chama-se **comprimento radical** de U.

Proposição 1.1.13. A série radical de um A-módulo U é a cadeia descendente mais rápida de submódulos de U com quocientes semissimples.

[1] Em alguns momentos, nos referiremos à camada radical $U/\operatorname{rad}(U)$ como sendo o **quociente radical** de U.

Demonstração: Por "mais rápida" queremos dizer o seguinte: se

$$U = U_0 \supseteq U_1 \supseteq U_2 \supseteq \cdots$$

é uma cadeia descendente com quocientes semissimples, então $\mathrm{rad}^i(U) \subseteq U_i$ para todo i. A prova é por indução. Para $i = 0$, vale a igualdade. Suponha agora que $\mathrm{rad}^i(U) \subseteq U_i$ para algum $i \geq 0$. Como U_i/U_{i+1} é semissimples, a Proposição 1.1.12 nos dá que $\mathrm{rad}(U_i) \subseteq U_{i+1}$. Consequentemente,

$$\mathrm{rad}^{i+1}(U) = \mathrm{rad}(\mathrm{rad}^i(U)) \subseteq \mathrm{rad}(U_i) \subseteq U_{i+1},$$

como queríamos. Aqui usamos que o radical preserva inclusões, já que aplicar o "operador rad" é equivalente a multiplicar à esquerda por $\mathrm{rad}(A)$. □

Podemos dualizar a noção de radical de um módulo: ao invés de buscar o menor submódulo de quociente semissimples podemos construir o maior submódulo semissimples, como faremos a seguir.

Proposição 1.1.14. Se U é um A-módulo, então os seguintes módulos são iguais:

(1) O conjunto dos $u \in U$ tais que $\mathrm{rad}(A)u = 0$.

(2) O maior submódulo semissimples de U.

(3) A soma de todos os submódulos simples de U.

Demonstração: Note que o conjunto V em (1) é de fato submódulo de U (aqui usamos que $\mathrm{rad}(A)$ é ideal de A). Além disso, ele é o maior submódulo semissimples de U pois, por construção, $\mathrm{rad}(A)$ anula V e, se $W \leq U$ é semissimples, então $\mathrm{rad}(A)$ anula W e $W \subseteq V$. Isso prova a igualdade entre (1) e (2). Agora, como V é semissimples, V é soma de submódulos simples de U e está contido no módulo descrito em (3). Por outro lado, a soma[1] de todos os submódulos simples de U é semissimples e, pela igualdade entre (1) e (2), tem que estar contida em V. Isso conclui que (1) e (3) determinam o mesmo submódulo, terminando a prova. □

O submódulo de U dado pela proposição acima será chamado de **soco**[2] (pronuncia-se "sóco") de U e o denotaremos por $\mathrm{soc}(U)$. Como no caso do radical, podemos definir $\mathrm{soc}^n(U)$ da seguinte forma. Como $U/\mathrm{soc}(U)$ é um módulo, podemos tomar o seu soco. Nesse caso, $\mathrm{soc}^2(U)$ será o submódulo de U contendo $\mathrm{soc}(U)$ que corresponde a $\mathrm{soc}(U/\mathrm{soc}(U))$. Para obter $\mathrm{soc}^3(U)$, tomamos o soco de $U/\mathrm{soc}^2(U)$ e assim sucessivamente. Definiremos $\mathrm{soc}^0(U)$ como 0. Temos uma caracterização interessante:

Proposição 1.1.15. Se U é um A-módulo, então $\mathrm{soc}^n(U)$ é o conjunto dos $u \in U$ tais que $\mathrm{rad}(A)^n u = 0$.

Demonstração: Provaremos o resultado por indução. Se $n = 0$, então é imediato (considerando que $\mathrm{rad}(A)^0 = A$). Suponha então que, para algum $n \geq 0$, $\mathrm{soc}^n(U)$ seja o conjunto do enunciado e vamos provar que o mesmo vale para $n + 1$. De fato, se $u \in U$, então

$$\begin{aligned}
u \in \mathrm{soc}^{n+1}(U) &\iff u + \mathrm{soc}^n(U) \in \mathrm{soc}(U/\mathrm{soc}^n(U)) \\
&\iff \mathrm{rad}(A)(u + \mathrm{soc}^n(U)) = 0 + \mathrm{soc}^n(U) \\
&\iff \mathrm{rad}(A)u \subseteq \mathrm{soc}^n(U) \\
&\iff \mathrm{rad}(A)^n(\mathrm{rad}(A)u) = 0 \\
&\iff \mathrm{rad}(A)^{n+1}u = 0,
\end{aligned}$$

como preciso. A Proposição 1.1.14 foi utilizada na segunda equivalência e a hipótese de indução foi usada na penúltima. □

[1] Lembre que a soma não precisa ser direta!

[2] Essa palavra vem do termo em inglês "socle", que pode ser traduzido também como "soclo", "supedâneo", "plinto", "peanha" ou, mais simplesmente, "pedestal".

A cadeia ascendente

$$0 = \mathrm{soc}^0(U) \subseteq \mathrm{soc}^1(U) \subseteq \mathrm{soc}^2(U) \subseteq \cdots$$

é a **série de socos** de U. Note que os quocientes (chamados de **camadas de soco**) são semissimples, por serem o soco de algum módulo. Como $\mathrm{rad}(A)$ é nilpotente, a caracterização anterior nos mostra que $\mathrm{soc}^r(U) = U$ para algum r. O primeiro desses r's é chamado de **comprimento de soco** de U. Temos um resultado análogo à Proposição 1.1.13:

Proposição 1.1.16. A série de socos de um A-módulo U é a cadeia ascendente mais rápida de submódulos de U com quocientes semissimples.

Demonstração: A prova é bem parecida com a demonstração da Proposição 1.1.13. Seja

$$0 = U_0 \subseteq U_1 \subseteq U_2 \subseteq \cdots$$

uma cadeia ascendente com quocientes semissimples. Vamos mostrar por indução que $U_i \subseteq \mathrm{soc}^i(U)$. Se $i = 0$, temos uma igualdade. Suponha agora que $U_i \subseteq \mathrm{soc}^i(U)$ para algum $i \geq 0$. Pela Proposição 1.1.15, $\mathrm{rad}(A)^i U_i = 0$. Agora, como U_{i+1}/U_i é semissimples, temos que $\mathrm{rad}(A)U_{i+1} \subseteq U_i$. Portanto,

$$\mathrm{rad}(A)^{i+1} U_{i+1} \subseteq \mathrm{rad}(A)^i U_i = 0$$

e $U_{i+1} \subseteq \mathrm{soc}^{i+1}(U)$, como preciso. □

Corolário 1.1.17. Se U é um A-módulo, então seu comprimento radical coincide com seu comprimento de soco. Além disso, se r é esse comprimento, então $\mathrm{rad}^i(U) \subseteq \mathrm{soc}^{r-i}(U)$ para todo $0 \leq i \leq r$.

Demonstração: Olhando a série radical do menor termo para o maior termo, temos uma cadeia ascendente de submódulos de U com quocientes semissimples. Pela Proposição 1.1.16, o comprimento de soco é menor ou igual ao comprimento radical. A desigualdade contrária segue de modo análogo a partir da Proposição 1.1.13. A afirmação final segue de qualquer uma das proposições anteriores. □

O comprimento comum apresentado no corolário acima é chamado de **comprimento de Loewy** de U. Segue das Proposições 1.1.13 e 1.1.16 que esse número é o menor comprimento que uma cadeia de 0 a U pode ter se ela possui quocientes semissimples. Uma observação que segue disso é que o comprimento de Loewy é menor ou igual ao comprimento de U no sentido usual, já que uma série de composição possui quocientes simples e, portanto, semissimples.

Exemplo 1.1.18. Vamos calcular a série radical e a série de socos do módulo regular de $A = T_n(k)$. Pelo Exemplo 1.1.11, $\mathrm{rad}(T_n(k))$ é o ideal de $T_n(k)$ formado pelas matrizes com 0 em toda a diagonal principal. Para determinar a série radical, temos que encontrar as potências de $\mathrm{rad}(T_n(k))$. Vamos provar que $\mathrm{rad}(T_n(k))^r$ é o conjunto N_r das matrizes de $T_n(k)$ que têm as r primeiras diagonais nulas, contando a partir da diagonal principal, para $1 \leq r \leq n$. Como mencionamos, $\mathrm{rad}(T_n(k)) = N_1$. Antes de prosseguir, é interessante calcular essas potências com valores pequenos de n, para se entender o que está acontecendo.

Vamos dar uma caracterização de N_r em termos de matrizes elementares. Denotaremos por e_{ij} a matriz elementar cuja entrada (i, j) é 1 e cujas outras são 0. Veja que $T_n(k)$ é o subespaço do espaço das matrizes $n \times n$ gerado pelas matrizes elementares e_{ij} com $i \geq j$. Analogamente, N_r é o subespaço de $T_n(k)$ gerado pelas matrizes elementares e_{ij} com $i - j \geq r$. Para provar que $N_1^r = N_r$, basta mostrar que $N_r N_1 = N_{r+1}$. Das relações

$$e_{ij} e_{st} = \delta_{js} e_{it},$$

sabemos que $e_{ij} \in N_r$ e $e_{st} \in N_1$ implicam em $e_{ij} e_{st} = 0 \in N_{r+1}$, se $j \neq s$, ou, caso contrário, $e_{ij} e_{jt} = e_{it} \in N_{r+1}$, pois

$$i - t = (i - j) + (j - t) \geq r + 1.$$

Isso prova a inclusão $N_r N_1 \subseteq N_{r+1}$. Por outro lado, se $e_{ij} \in N_{r+1}$, então vale

$$e_{ij} = e_{i,j+1}e_{j+1,j} \in N_r N_1,$$

provando a inclusão contrária. Portanto, a série radical de $T_n(k)$ é

$$T_n(k) \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_{n-1} \supseteq N_n = 0.$$

Agora, vejamos que, para $1 \leq r \leq n$, $\operatorname{soc}^r(T_n(k))$ é o subespaço L_r de $T_n(k)$ gerado pelas matrizes e_{ij} com $i \geq n - r + 1$, ou seja, tomamos $T_n(k)$ e zeramos as $n - r$ primeiras linhas. Vamos começar mostrando que essas matrizes elementares estão em $\operatorname{soc}^r(T_n(k))$. Para isso, basta ver que $\operatorname{rad}(T_n(k))^r = N_r$ anula essas matrizes. De fato, se $e_{ij} \in L_r$ e $e_{st} \in N_r$, devemos ter

$$i \geq n - r + 1 > n - r \geq s - r \geq t \implies i \neq t$$

e então $e_{st}e_{ij} = 0$. Como as matrizes elementares em N_r geram N_r, provamos que $e_{ij} \in \operatorname{soc}^r(A)$ sempre que $i \geq n - r + 1$. Com isso, $L_r \subseteq \operatorname{soc}^r(T_n(k))$. Para mostrar a inclusão contrária, tome $X \in \operatorname{soc}^r(T_n(k))$. Queremos mostrar que as $n - r$ primeiras linhas de X são nulas. Dado $1 \leq s \leq n - r$, sabemos que e_{ns} está em N_r. Logo, $e_{ns}X = 0$. Mas $e_{ns}X$ é formada colocando-se a s-ésima linha de X na última linha e zerando o resto, o que implica que a s-ésima linha de X é nula para todo $1 \leq s \leq n - r$, como queríamos. Isso conclui que

$$0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_{n-1} \subseteq L_n = T_n(k)$$

é a série de socos de A. Observe que a série radical e a série de socos não coincidiram, mas têm o mesmo tamanho!

1.2 O Teorema de Wedderburn

Incrivelmente, é possível descrever qualquer álgebra semissimples como o produto direto de álgebras de matrizes sobre certas álgebras de divisão! Esse é o Teorema de Wedderburn, o objetivo desta seção.

Começamos estudando algumas propriedades sobre matrizes:

Lema 1.2.1. Seja D uma álgebra de divisão sobre k e $n \geq 1$ um inteiro. Se $M_n(D)$ denota a álgebra de matrizes $n \times n$ com entradas em D, então:

(1) $M_n(D)$ é uma álgebra simples.

(2) $M_n(D)$ possui um único módulo simples S, a menos de isomorfismo. Além disso, $M_n(D)$ é isomorfo à soma direta de n cópias de S, como $M_n(D)$-módulos, e, em particular, $M_n(D)$ é uma álgebra semissimples.

(3) D é isomorfo a $\operatorname{End}_{M_n(D)}(S)^{\mathrm{op}}$.

Antes de demonstrar o lema, vamos esclarecer algumas notações. Uma **álgebra de divisão** é uma k-álgebra tal que todo elemento não nulo é inversível. Uma **álgebra simples** é aquela cujos únicos ideais bilaterais são os triviais. Por exemplo, é fácil verificar que toda álgebra de divisão é simples. Se U é um A-módulo, então $\operatorname{End}_A(U)$ denota a **álgebra de endomorfismos** de U, ou seja, o k-espaço dos homomorfismos de A-módulos de U em U com produto dado pela composição de funções. Finalmente, se A é uma álgebra sobre k, denotamos por A^{op} a sua **álgebra oposta**[1], que difere de A apenas pela multiplicação dada agora por $a \cdot_{A^{\mathrm{op}}} b = b \cdot_A a$.

[1] É possível evitar o uso da álgebra oposta se trabalharmos com módulos à direita também, que aparecem naturalmente quando consideramos endomorfismos (veja [17]). Entretanto, como faríamos isto apenas nesta seção e mudaríamos a convenção de aplicar funções à esquerda, optamos por usar A^{op}.

Demonstração: Seja I um ideal de $M_n(D)$. Denote por $J \subseteq D$ o conjunto de todos os elementos que aparecem como entrada $(1,1)$ das matrizes em I. Usando que I é ideal de $M_n(D)$, verifica-se que J é ideal de D. Mostremos que $I = M_n(J)$, ou seja, que I é formado pelas matrizes com entradas em J. Denote por e_{ij} a matriz elementar que possui 1 na coordenada (i,j) e 0 nas outras. Se $X = (a_{ij}) \in I$, então

$$e_{1i}Xe_{j1} = a_{ij}e_{11} \in I$$

porque I é ideal. Mas então $a_{ij} \in J$ para todos $1 \leq i,j \leq n$ e $X \in M_n(J)$, provando que $I \subseteq M_n(J)$. Por outro lado, se $Y = (b_{ij}) \in M_n(J)$, para mostrar que $Y \in I$, é suficiente mostrar que $b_{ij}e_{ij} \in I$ para todos $1 \leq i,j \leq n$. Fixados i e j, tome $X = (a_{st}) \in I$ tal que $a_{11} = b_{ij}$. Segue que

$$b_{ij}e_{ij} = a_{11}e_{ij} = e_{i1}Xe_{1j} \in I,$$

como queríamos. Logo, está provada a outra inclusão e temos[1] $I = M_n(J)$. Por fim, como D é uma álgebra de divisão, D é simples e temos $J = 0$ ou $J = D$. Consequentemente, $I = 0$ ou $I = M_n(D)$, demonstrando (1).

Vamos para (2). Seja S o conjunto dos vetores-coluna com n coordenadas em D. Note que $M_n(D)$ age em S por multiplicação à esquerda, de modo que S é um $M_n(D)$-módulo. Por resultados de álgebra linear[2] ou por um cálculo direto, constatamos que qualquer elemento não nulo de S é um gerador, logo S é simples. Além disso, da forma que é definida a multiplicação de matrizes, vemos que o conjunto das matrizes que possuem todas as colunas nulas exceto possivelmente a i-ésima forma um submódulo do módulo regular $M_n(D)$ isomorfo a S. Variando i, é imediato que $M_n(D)$ é a soma direta desses submódulos e, por isso, $M_n(D) \cong S \oplus \cdots \oplus S$ (n vezes) como $M_n(D)$-módulos. Isso prova que $M_n(D)$ é semissimples e que S é o único fator de composição de $M_n(D)$ (desconsiderando multiplicidade), ou seja, S é o único módulo simples sobre $M_n(D)$.

Para concluir que $D \cong \mathrm{End}_{M_n(D)}(S)^{\mathrm{op}}$, basta encontrar um anti-isomorfismo $\rho : D \to \mathrm{End}_{M_n(D)}(S)$, ou seja, um isomorfismo linear entre D e $\mathrm{End}_{M_n(D)}(S)$ que satisfaz $\rho(ab) = \rho(b)\rho(a)$ para $a, b \in D$. Dado $d \in D$, definimos $\rho(d) = \rho_d$ por multiplicação à direita, ou seja, $\rho_d(v) = v \cdot d$ para $v \in S$. Veja que estamos considerando S como um D-módulo à direita, o que pode ser feito do jeito usual dada a construção de S. Da associatividade do produto de matrizes, segue que $\rho_d \in \mathrm{End}_{M_n(D)}(S)$ e tudo está bem definido. Não é difícil verificar que ρ é um anti-homomorfismo e, aplicando ρ_d em qualquer vetor da base canônica de S, podemos ver que ρ é injetor. Terminamos se provarmos que ρ é sobrejetor. Dado $f \in \mathrm{End}_{M_n(D)}(S)$, escreva

$$f\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} = \begin{pmatrix}d\\*\\\vdots\\*\end{pmatrix},$$

com $d \in D$. Então, como f é homomorfismo,

$$f\begin{pmatrix}a_1\\\vdots\\a_n\end{pmatrix} = f\left(\begin{pmatrix}a_1 & 0 & \cdots & 0\\\vdots & \vdots & \vdots & \vdots\\a_n & 0 & \cdots & 0\end{pmatrix}\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}\right) = \begin{pmatrix}a_1 & 0 & \cdots & 0\\\vdots & \vdots & \vdots & \vdots\\a_n & 0 & \cdots & 0\end{pmatrix}\begin{pmatrix}d\\*\\\vdots\\*\end{pmatrix} = \begin{pmatrix}a_1d\\\vdots\\a_nd\end{pmatrix} = \rho_d\begin{pmatrix}a_1\\\vdots\\a_n\end{pmatrix}$$

e $f = \rho_d$, como preciso. □

Lema 1.2.2. Se $A_1, \ldots, A_n$ são k-álgebras semissimples, então o produto direto $A = A_1 \times \cdots \times A_n$ também o é.

[1] Observe que, até aqui, esta prova ainda funciona se D for um anel qualquer.

[2] Sim, funciona sobre álgebras de divisão!

Demonstração: Como A_i é semissimples, podemos escrever $A_i = S_{i1} \oplus \cdots \oplus S_{im_i}$ onde cada S_{ij} é um submódulo simples de A_i. Restringindo escalares para A, é fácil ver que cada S_{ij} continua simples como A-módulo. Dessa forma,

$$_AA = A_1 \oplus \cdots \oplus A_n = \bigoplus_{i,j} S_{ij}$$

e A é semissimples como módulo e, consequentemente, como álgebra. □

Os dois lemas anteriores nos dizem que

$$M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

é uma álgebra semissimples se $D_1, \ldots, D_r$ são álgebras de divisão. Agora veremos que essas são todas as álgebras semissimples. Para isso, começamos com algumas propriedades das álgebras de endomorfismos:

Lema 1.2.3. Há um isomorfismo $\mathrm{End}_A({}_AA) \cong A^{\mathrm{op}}$.

Demonstração: A ideia é parecida com o final da demonstração do Lema 1.2.1. Vamos definir $\rho : A \to \mathrm{End}_A({}_AA)$ levando $a \in A$ na multiplicação à direita por a, ou seja, na função $\rho_a : A \to A$ dada por $\rho_a(x) = xa$. É imediato que ρ_a é homomorfismo de A-módulos, de modo que ρ está bem definida. Além disso, é fácil ver que ρ é um anti-homomorfismo, ou seja, $\rho(ab) = \rho(b)\rho(a)$ para $a, b \in A$. Note que ρ é injetora, já que $\rho_a = \rho_b$ implica em $a = \rho_a(1) = \rho_b(1) = b$. Para terminar, basta verificarmos que ρ é sobrejetora. Seja $\rho \in \mathrm{End}_A({}_AA)$ qualquer. Se $a = \rho(1)$, vale que

$$\rho(x) = \rho(x \cdot 1) = x\rho(1) = xa = \rho_a(x)$$

e, portanto, $\rho = \rho_a$, como preciso. □

Lema 1.2.4 (Schur)**.** Se S é um A-módulo simples, então $\mathrm{End}_A(S)$ é uma álgebra de divisão. Além disso, se k é algebricamente fechado, então $\mathrm{End}_A(S) \cong k$.

Demonstração: Para a primeira parte, é suficiente mostrar que um homomorfismo não nulo $\rho : S \to S$ sempre é um isomorfismo. De fato, se ρ é não nulo, então o núcleo de ρ não é S e a imagem não é 0. Mas a simplicidade de S então implica que $\ker \rho = 0$ e $\mathrm{im}\, \rho = S$, de modo que ρ é isomorfismo.

Agora, suponha que k seja algebricamente fechado. Como S tem dimensão finita, o mesmo vale para $\mathrm{End}_A(S)$. O argumento usual de que não há uma extensão de corpos finita não trivial de k se aplica aqui, mas daremos outro argumento. Sejam $\rho \in \mathrm{End}_A(S)$ e $\lambda \in k$ um autovalor de ρ (que existe porque k é algebricamente fechado). Se $I \in \mathrm{End}_A(S)$ é o operador identidade, então $\rho - \lambda I$ é um endomorfismo de S que não é isomorfismo. Pelo parágrafo anterior, $\rho - \lambda I = 0$ e $\rho = \lambda I$. Com isso, $\mathrm{End}_A(S) = kI$ e o resultado segue. □

O próximo passo é entender como calcular a álgebra de endomorfismos de uma soma direta de módulos. Sejam $U_1, \ldots, U_r$ A-módulos. Defina $M(U_1, \ldots, U_r)$ como sendo o espaço das matrizes cuja entrada (i, j) é um elemento de $\mathrm{Hom}_A(U_j, U_i)$, onde $\mathrm{Hom}_A(U_j, U_i)$ denota o k-espaço dos homomorfismos de A-módulos de U_j em U_i. Veja que o produto usual de matrizes faz sentido, pois, se $X = (\rho_{ij})$ e $Y = (\rho'_{ij})$ são elementos de $M(U_1, \ldots, U_r)$, então podemos compor ρ_{il} com ρ'_{lj} obtendo um homomorfismo de U_j em U_i. Com isso, podemos definir a entrada (i, j) de XY como

$$\sum_{l=1}^{r} \rho_{il}\rho'_{lj} \in \mathrm{Hom}_A(U_j, U_i).$$

Logo, $M(U_1, \ldots, U_r)$ é uma k-álgebra. Introduzimos essa álgebra porque os endomorfismos de $U_1 \oplus \cdots \oplus U_r$ se comportam de modo parecido. Cada endomorfismo pode ser definido componente a componente e a composição se dá como a multiplicação de matrizes acima!

Lema 1.2.5. Há um isomorfismo $\mathrm{End}_A(U_1 \oplus \cdots \oplus U_r) \cong M(U_1, \ldots, U_r)$.

Demonstração: Seja $U = U_1 \oplus \cdots \oplus U_r$ e denote por $\mu_i : U_i \to U$ e $\pi_i : U \to U_i$ a inclusão e a projeção, respectivamente. Dado $\rho \in \mathrm{End}_A(U)$, podemos ver como ρ se comporta da componente U_j até a componente U_i, isto é, podemos considerar $\rho_{ij} = \pi_i \rho \mu_j \in \mathrm{Hom}_A(U_j, U_i)$. Isso nos dá uma transformação linear $f : \mathrm{End}_A(U) \to M(U_1, \ldots, U_r)$ dada por $f(\rho) = (\rho_{ij})$. Se $\rho, \rho' \in \mathrm{End}_A(U)$, então

$$\sum_{l=1}^{r} \rho_{il}\rho'_{lj} = \sum_{l=1}^{r} \pi_i \rho \mu_l \pi_l \rho' \mu_j = \pi_i \rho \left(\sum_{l=1}^{r} \mu_l \pi_l \right) \rho' \mu_j = \pi_i \rho \rho' \mu_j$$

porque $\sum_{l=1}^{r} \mu_l \pi_l$ é a identidade em U. Isso mostra que $f(\rho\rho') = f(\rho)f(\rho')$, ou seja, f é um homomorfismo. Para ver que f é bijeção, basta encontrar uma inversa para f. Não é difícil verificar que a função $g : M(U_1, \ldots, U_r) \to \mathrm{End}_A(U)$ dada por

$$g((\rho_{ij})) = \sum_{i,j=1}^{r} \mu_i \rho_{ij} \pi_j$$

cumpre esse papel. □

Corolário 1.2.6. Se $\mathrm{Hom}_A(U_j, U_i) = 0$ para $i \neq j$, então

$$\mathrm{End}_A(U_1 \oplus \cdots \oplus U_r) \cong \mathrm{End}_A(U_1) \times \cdots \times \mathrm{End}_A(U_r).$$

Demonstração: Nesse caso, $M(U_1, \ldots, U_r)$ é formada por matrizes diagonais e o resultado é consequência imediata do lema anterior. □

Corolário 1.2.7. Se U é um A-módulo e U^n denota a soma direta de n cópias de U, então

$$\mathrm{End}_A(U^n) \cong M_n(\mathrm{End}_A(U)).$$

Demonstração: Consequência imediata do lema anterior. □

Finalmente, falta apenas juntarmos as peças!

Teorema 1.2.8 (Wedderburn[1])**.** Seja A uma álgebra semissimples. Então

$$A \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

para certas álgebras de divisão $D_1, \ldots, D_r$ e inteiros positivos $n_1, \ldots, n_r$. O número r é unicamente determinado, assim como os pares $(n_1, D_1), \ldots, (n_r, D_r)$ (a menos de isomorfismo e de permutação).

Demonstração: Como A é semissimples, podemos escrever

$${}_AA \cong S_1^{n_1} \oplus \cdots \oplus S_r^{n_r},$$

onde $S_1, \ldots, S_r$ é a lista de A-módulos simples não isomorfos dois a dois. A ideia é calcular a álgebra de endomorfismos dos dois módulos acima. Pelo Lema 1.2.3, $\mathrm{End}_A({}_AA) \cong A^{\mathrm{op}}$. Por outro lado, observe que $\mathrm{Hom}_A(S_j^{n_j}, S_i^{n_i}) = 0$ se $i \neq j$ (basta analisar quais fatores de composição a imagem de um homomorfismo pode ter) e, portanto, segue dos Corolários 1.2.6 e 1.2.7 que

$$\mathrm{End}_A(S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}) \cong M_{n_1}(\mathrm{End}_A(S_1)) \times \cdots \times M_{n_r}(\mathrm{End}_A(S_r)).$$

[1] Joseph Wedderburn provou esse resultado como no nosso contexto, para álgebras de dimensão finita. Posteriormente, Emil Artin generalizou o resultado para anéis artinianos quaisquer. Por isso, esse teorema também é chamado de Teorema de Wedderburn-Artin em outros lugares.

Considere $D_i = \mathrm{End}_A(S_i)^{\mathrm{op}}$. Pelo Lema de Schur, cada D_i é uma álgebra de divisão. Juntando o que temos, sabemos de um isomorfismo

$$A^{\mathrm{op}} \cong M_{n_1}(D_1^{\mathrm{op}}) \times \cdots \times M_{n_r}(D_r^{\mathrm{op}}).$$

Tomando a álgebra oposta em ambos os lados, temos o isomorfismo desejado[1].

Vamos provar a unicidade. Suponha que exista outro isomorfismo

$$A \cong M_{n'_1}(D'_1) \times \cdots \times M_{n'_s}(D'_s),$$

onde $D'_1, \ldots, D'_s$ são álgebras de divisão. Como no Lema 1.2.1, seja S'_i o único módulo simples de $M_{n'_i}(D'_i)$. Restringindo escalares, podemos ver cada S'_i como um A-módulo. Note que $S'_i \ncong S'_j$ se $i \neq j$, pois $M_{n'_i}(D'_i)$ anula S'_j mas não S'_i. Pelo item (2) do Lema 1.2.1,

$${}_AA \cong (S'_1)^{n'_1} \oplus \cdots \oplus (S'_s)^{n'_s}.$$

Então, pelo Teorema de Jordan-Hölder, devemos ter $r = s$ e, após uma possível renumeração, $n_i = n'_i$ e $S_i \cong S'_i$. Resta mostrar que $D_i \cong D'_i$. Para isso, note primeiramente que $\mathrm{End}_A(S'_i)$ e $\mathrm{End}_{M_{n'_i}(D'_i)}(S'_i)$ são a mesma álgebra. Logo, pelo item (3) do Lema 1.2.1,

$$D'_i \cong \mathrm{End}_{M_{n'_i}(D'_i)}(S'_i)^{\mathrm{op}} = \mathrm{End}_A(S'_i)^{\mathrm{op}} \cong \mathrm{End}_A(S_i)^{\mathrm{op}} = D_i,$$

como preciso. □

A prova do Teorema de Wedderburn nos diz que o número r é a "quantidade" de módulos simples de A. Além disso, podemos recuperar cada n_i e cada D_i verificando a multiplicidade de cada módulo simples em ${}_AA$ e calculando a sua álgebra de endomorfismos. Quando k é algebricamente fechado, o Lema de Schur nos diz que cada D_i é isomorfo a k e temos a seguinte conclusão:

Corolário 1.2.9. Seja A uma k-álgebra semissimples. Escreva

$${}_AA \cong S_1^{n_1} \oplus \cdots \oplus S_r^{n_r},$$

onde $S_1, \ldots, S_r$ são A-módulos simples dois a dois não isomorfos. Se que k é algebricamente fechado, então $n_i = \dim_k S_i$ e $\dim_k A = n_1^2 + \cdots + n_r^2$.

Demonstração: Na notação do Teorema de Wedderburn, temos que $D_i \cong k$ para todo i, como observado antes do enunciado do corolário. Logo,

$$A \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$$

e vale $\dim_k A = n_1^2 + \cdots + n_r^2$. Como vimos na prova do Teorema de Wedderburn, $M_{n_i}(k)$ é isomorfo a $S_i^{n_i}$ como A-módulos, logo

$$n_i^2 = \dim_k M_{n_i}(k) = \dim_k S_i^{n_i} = n_i \dim_k S_i \implies \dim_k S_i = n_i,$$

concluindo a prova. □

Quando A é semissimples, cada álgebra de matrizes que aparece na decomposição do Teorema de Wedderburn corresponde a um ideal A_i de A. Surpreendentemente, os A_i's estão determinados unicamente, não apenas a menos de isomorfismo! Eles são chamados de **componentes simples**[2] de A. Abaixo, daremos duas caracterizações para esses ideais.

[1] Talvez o mais difícil seja verificar que $M_n(D^{\mathrm{op}}) \cong M_n(D)^{\mathrm{op}}$, mas isso também é tranquilo: basta considerar a função que leva uma matriz em sua transposta.

[2] No Capítulo 4, chamaremos essas componentes de *blocos* e estudaremos o que acontece quando A não é semissimples.

Proposição 1.2.10. Seja A uma k-álgebra semissimples e escreva[1]

$$A = A_1 \oplus \cdots \oplus A_r,$$

onde cada A_i é um ideal de A isomorfo a uma álgebra de matrizes sobre uma álgebra de divisão.

(1) Se $S_1, \ldots, S_r$ representam todos os A-módulos simples, então A_i é, a menos de renumeração, a soma de todos os submódulos de ${}_AA$ isomorfos a S_i.

(2) Todo ideal de A é a soma de alguns dos ideais A_i. Em particular, os A_i's são precisamente os ideais minimais e indecomponíveis de A.

Dizemos que um ideal I de A é **indecomponível** se I não pode ser escrito com a soma direta de dois ideais não nulos.

Demonstração: Imitando a segunda parte da prova do Teorema de Wedderburn, sabemos que cada A_i é a soma direta de alguns submódulos de ${}_AA$ isomorfos a S_i. Então, para concluir (1), basta mostrar que todo submódulo de ${}_AA$ isomorfo a S_i está contido em A_i. Vamos mostrar a contrapositiva. Seja $U \leq {}_AA$ um submódulo simples e suponha que U não está contido em A_i. Então há $j \neq i$ tal que a projeção de U em A_j é não nula. Como U é simples, essa projeção nos dá um isomorfismo de U com um submódulo de A_j. Mas qualquer fator de composição de A_j é isomorfo a S_j e o mesmo vale para qualquer um de seus submódulos. Logo, $U \cong S_j$ e, em particular, $U \ncong S_i$.

Para a segunda parte, seja I um ideal de A. Seja $\mathcal{I} \subseteq \{1, \ldots, r\}$ o conjunto dos índices i tais que S_i é isomorfo a um fator de composição do A-módulo I. Vamos provar que I é igual a $A_{\mathcal{I}} \coloneqq \bigoplus_{i \in \mathcal{I}} A_i$. Comecemos mostrando que $A_i \subseteq I$ para cada $i \in \mathcal{I}$. Como I é um A-módulo semissimples, todo fator de composição aparece como um somando direto. Em particular, existe $S \leq I$ isomorfo a S_i. Se $S' \leq {}_AA$ também é isomorfo a S_i, há um isomorfismo de S em S' que pode ser estendido a um endomorfismo de ${}_AA$, já que S é um somando direto de ${}_AA$. Pelo Lema 1.2.3, esse endomorfismo é a multiplicação à direita por algum elemento de A. Como I é ideal, I é invariante por esse endomorfismo e, consequentemente, S' (que é a imagem de S) está contido em I. Logo, I contém todos os submódulos de ${}_AA$ isomorfos a S_i, ou seja, $A_i \subseteq I$. Com isso, segue que $A_{\mathcal{I}} \subseteq I$. Agora, $A/A_{\mathcal{I}}$ não possui fatores de composição isomorfos a S_i para nenhum $i \in \mathcal{I}$, enquanto um fator de composição de $I/A_{\mathcal{I}}$ (que é um quociente de I) tem que ser isomorfo a algum desses. Mas $I/A_{\mathcal{I}}$ é submódulo de $A/A_{\mathcal{I}}$, então a única possibilidade é $I/A_{\mathcal{I}} = 0$, ou seja, $I = A_{\mathcal{I}}$. □

Observe que a primeira parte da prova de (2) acima pode ser adaptada para dar outra demonstração de (1). Além disso, note que a prova dada para (1) pode ser generalizada para qualquer módulo: se U é um A-módulo semissimples que pode ser escrito como

$$U \cong S_1^{n_1} \oplus \cdots \oplus S_r^{n_r},$$

onde $S_1, \ldots, S_r$ são A-módulos simples dois a dois não isomorfos, então cada componente $S_i^{n_i}$ é unicamente determinada em U como sendo a soma de todos os submódulos de U isomorfos a S_i. Também chamaremos essas componentes de **componentes simples** de U.

1.3 Álgebras de grupo e exemplos

Vamos aplicar os conceitos desenvolvidos até então para estudar o caso que nos interessa neste material! Precisamos de algumas definições.

[1] Como cada A_i é um ideal, segue que $A_i \cdot A_j = 0$ para $i \neq j$. Com isso, a componente da identidade de A na coordenada A_i atua como uma identidade para A_i, que se torna uma álgebra. Também obtemos que A é isomorfa ao produto direto dos A_i's, como aparece no Teorema de Wedderburn.

Seja G um grupo finito. Definimos a **álgebra de grupo** kG como sendo o k-espaço vetorial com base G e multiplicação dada nos elementos da base por multiplicação no grupo. Ou seja, os elementos de kG são combinações k-lineares formais de elementos de G e podemos expressá-los por $\sum_{g\in G} a_g g$ com $a_g \in k$. Além disso, a multiplicação é dada por

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

muito parecido com o que fazemos com polinômios[1]. Como a multiplicação do grupo é associativa, kG é uma álgebra associativa, e a sua identidade é o elemento 1 da base canônica que corresponde à identidade de G. Note que kG tem dimensão finita porque G é finito, então estamos nas condições das seções anteriores.

Notação 1.3.1. Sempre que nos referirmos a um grupo (geralmente denotado por G), estaremos nos referindo a um grupo *finito*. Se um grupo for infinito, deixaremos isso claro.

Definição 1.3.2. Uma **representação** de G sobre k é um kG-módulo.

Se U é uma representação de G sobre k, podemos escrever a ação do módulo como um homomorfismo de álgebras

$$kG \to \mathrm{End}_k(U),$$

onde $\mathrm{End}_k(U)$ denota os endomorfismos de U como espaço vetorial, ou seja, os operadores lineares em U. Repare que a cópia de G em kG é subgrupo do grupo dos inversíveis de kG, logo, ao restringirmos o homomorfismo acima a G, obtemos um homomorfismo de grupos

$$G \to \mathrm{GL}(U),$$

onde $\mathrm{GL}(U) \subseteq \mathrm{End}_k(U)$ é o grupo dos operadores lineares inversíveis em U. Além disso, dado um homomorfismo de grupos como acima, podemos estendê-lo para a álgebra de grupo e obtemos uma representação de G. Essa é, então, uma outra definição para uma representação e, na verdade, é uma das motivações do nosso estudo. Para estudar G, podemos ver como G age em outros objetos. A definição acima captura a ação de G em U por operadores lineares, um caso natural a ser considerado após se estudar ações de grupos em conjuntos. Preferimos adotar a visão de que uma representação é um módulo para aplicar resultados gerais sobre módulos (como os que vimos anteriormente), mas a definição com matrizes inversíveis (isto é, com $\mathrm{GL}(U)$) também é útil para dar exemplos e estudar o problema de outros ângulos, através de, por exemplo, caracteres.

Exemplo 1.3.3. Dado um grupo finito qualquer G, sempre conseguimos construir duas representações especiais. A primeira delas é a **representação trivial** (ou o **módulo trivial**), na qual vemos k como um kG-módulo onde G age trivialmente, ou seja, $g\cdot\lambda = \lambda$ para $g \in G$ e $\lambda \in k$. Veja que essa é uma representação simples (ou irredutível, como geralmente nos referimos no caso de representações). A outra é a **representação regular**, na qual vemos kG como um kG-módulo do jeito usual, ou seja, é o módulo regular ${}_{kG}kG$. Por motivos evidentes, evitaremos utilizar a notação ${}_{kG}kG$ para esse módulo e o denotaremos por kG simplesmente. Ficará claro do contexto quando estaremos vendo kG como módulo ou como álgebra.

Exemplo 1.3.4. Para este exemplo, vamos tomar $k = \mathbb{R}$ e G como sendo o grupo simétrico S_3. Em dimensão 1, temos a representação trivial e também temos a **representação sinal**, cujo espaço subjacente é $\mathbb{R}$ e a ação é dada por $\sigma\cdot\lambda = \mathrm{sgn}(\sigma)\lambda$, com $\sigma \in S_3$ e $\lambda \in \mathbb{R}$. Veja que uma representação de dimensão 1 é determinada por um homomorfismo de G em $k^\times$. Para encontrar representações de dimensão 2, lembre que S_3 é isomorfo a D_3, o grupo diedral de simetrias do

[1] Afinal, a álgebra de polinômios é uma álgebra de *monoide*!

triângulo equilátero no plano. Cada simetria do triângulo vem de uma transformação linear do plano, que pode ser uma rotação ou uma reflexão. Assim, $\mathbb{R}^2$ admite uma estrutura natural de $\mathbb{R}S_3$-módulo. Note que essa representação é irredutível, porque nenhuma reta do plano é invariante sob a rotação de 120°. O interessante é que essas três são todas as representações irredutíveis de S_3 sobre $\mathbb{R}$!

As representações anteriores podem ser definidas sobre corpos quaisquer. Isso é fácil de se fazer no caso das representações de dimensão 1. Para construir a representação de dimensão 2 sobre um corpo qualquer, veja que, no caso real, podemos encontrar uma base do plano de modo que a ação dos elementos (1 2) e (1 2 3) sejam representadas pelas matrizes

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

respectivamente. Para encontrar a base em questão, centralize o triângulo equilátero na origem, enumere seus vértices com 1, 2 e 3 e tome a base como sendo os vértices 1 e 2. As matrizes acima fazem sentido sobre qualquer corpo e podemos utilizá-las para construir a representação desejada, já que (1 2) e (1 2 3) geram S_3. Mas tome cuidado: sobre um corpo de característica 3, essa representação de dimensão 2 não é simples!

Exemplo 1.3.5. Vamos dar alguns exemplos de como construir novas representações a partir de antigas. Assim como funciona para módulos sobre álgebras quaisquer, dadas duas representações U e V, podemos formar a sua soma direta, que também é representação. No caso da álgebra de grupo, também podemos dar uma estrutura de kG-módulo para o produto tensorial[1] $U \otimes V$: dados $g \in G$ e $u \otimes v \in U \otimes V$, definimos

$$g \cdot (u \otimes v) \coloneqq (gu) \otimes (gv).$$

Usando a propriedade universal do produto tensorial, não é difícil ver que isso está bem definido e de fato torna $U \otimes V$ um kG-módulo.

Também podemos tornar $U^* = \mathrm{Hom}_k(U, k)$ um kG-módulo definindo $g \cdot \varphi$ por

$$(g \cdot \varphi)(u) = \varphi(g^{-1}u)$$

para $u \in U$, $g \in G$ e $\varphi \in U^*$. Temos que colocar g^{-1} ao invés de g para que valha $(gh)\cdot\varphi = g\cdot(h\cdot\varphi)$. Generalizando um pouco, dados dois kG-módulos U e V, o espaço das transformações lineares $\mathrm{Hom}_k(U, V)$ tem uma estrutura natural de kG-módulo dada por

$$(g \cdot \varphi)(u) = g\varphi(g^{-1}u),$$

com $u \in U$, $g \in G$ e $\varphi \in \mathrm{Hom}_k(U, V)$. Para ver de onde surge a definição acima, podemos utilizar o isomorfismo canônico entre $\mathrm{Hom}_k(U, V)$ e $U^* \otimes V$ e aplicar as duas construções anteriores.

Exemplo 1.3.6. Tome $k = \mathbb{F}_p$, o corpo de p elementos, e G como sendo o grupo cíclico $C_p = \langle g \rangle$ de ordem p. A matriz

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

tem ordem p, já que estamos em característica p. Com isso, $\mathbb{F}_p^2$ se torna um $\mathbb{F}_pC_p$-módulo cuja ação de g é dada pela matriz acima. É fácil ver que o subespaço U gerado pelo vetor $(1, 0)$ é um submódulo, mas ele não possui complemento! De fato, um complemento conteria algum vetor (a, b) com $b \neq 0$. Então $g \cdot (a, b) = (a + b, b)$ estaria nesse complemento, mas (a, b) e $(a + b, b)$

[1] Sempre que o símbolo $\otimes$ do produto tensorial não estiver acompanhado de um subscrito, o produto em questão é sobre o corpo base k. Quando formos definir o conceito de *indução*, precisaremos tomar o produto tensorial sobre outras álgebras.

seriam linearmente independentes e gerariam todo o espaço, o que não pode ser o caso, pois o complemento conteria U. Portanto, $\mathbb{F}_p^2$ não é semissimples.

O argumento acima mostra que U é o único submódulo não trivial de $\mathbb{F}_p^2$, então a sequência

$$0 \subseteq U \subseteq \mathbb{F}_p^2$$

tem que ser a série radical, a série de socos e a série de composição de $\mathbb{F}_p^2$! Nesse caso, os fatores de composição são isomorfos à representação trivial.

O último exemplo mostra que nem sempre kG é semissimples. Há um critério bem elementar para decidir a semissimplicidade de kG:

Teorema 1.3.7 (Maschke[1])**.** A álgebra kG é semissimples se, e somente se, a característica de k não divide a ordem de G.

Antes de provar o teorema, vamos introduzir alguns conceitos que serão úteis na demonstração. O homomorfismo trivial $G \to \{1\}$ pode ser estendido para as álgebras de grupo, dando origem a um homomorfismo de álgebras $\epsilon : kG \to k$ que leva $\sum_{g\in G} a_g g$ em $\sum_{g\in G} a_g$. Esse homomorfismo é chamado de **função de aumento** de kG. O seu núcleo, denotado por IG, é o **ideal de aumento** de kG. Note que IG consiste dos elementos $\sum_{g\in G} a_g g$ tais que $\sum_{g\in G} a_g = 0$.

Demonstração: Suponha que $\mathrm{char}(k)$ é positiva e divide $|G|$. Para mostrar que kG não é semissimples, basta ver que não é semissimples como kG-módulo. Vejamos que o ideal de aumento IG não tem complemento em kG. Primeiramente, note que a função de aumento se torna um homomorfismo de kG-módulos se considerarmos k com a estrutura trivial de kG-módulo. Pelo Teorema do Isomorfismo, um complemento de IG em kG teria que ser isomorfo à representação trivial. Vejamos que há apenas um único submódulo de kG isomorfo à representação trivial. Se $\sum_{g\in G} a_g g$ é invariante sobre sobre a ação de qualquer $h \in G$, então $a_g = a_{hg}$ para todos $g, h \in G$. Mas então todos os coeficientes a_g são iguais. Portanto, o único submódulo de kG isomorfo à representação trivial é

$$U = \left\{ \lambda \sum_{g\in G} g \mid \lambda \in k \right\}.$$

Como $\mathrm{char}(k) \mid |G|$, a soma dos coeficientes de qualquer elemento de U é 0 e, portanto, $U \subseteq IG$. Mas então U não pode ser complemento de IG em kG, de onde concluímos que IG não possui nenhum complemento.

Para a recíproca, suponha que $\mathrm{char}(k)$ não divida $|G|$, isto é, suponha que $|G|$ seja inversível em k. Mostremos que todos os kG-módulos são semissimples. Seja U um kG-módulo e V um submódulo de U. Queremos mostrar que V é um somando direto de U. Tome $\pi : U \to V$ uma projeção linear, ou seja, uma transformação linear sobrejetora tal que $\pi(v) = v$ para todo $v \in V$. Não é difícil verificar que $U = V \oplus \ker \pi$. A ideia será modificar π para obter uma projeção que também é um homomorfismo de módulos. Com isso, $\ker \pi$ será submódulo de U e, portanto, um complemento para V. Defina $\pi' : U \to V$ por

$$\pi'(u) = \frac{1}{|G|} \sum_{g\in G} g\pi(g^{-1}u)$$

para $u \in U$. Só é possível definir esta função porque estamos supondo que $\mathrm{char}(k) \nmid |G|$. É imediato que π' é linear e veja que a sua imagem de fato está em V porque $\pi(U) = V$ e V é submódulo de U. Além disso, se $v \in V$, então $g^{-1}v \in V$ e temos

$$\pi'(v) = \frac{1}{|G|} \sum_{g\in G} g\pi(g^{-1}v) = \frac{1}{|G|} \sum_{g\in G} g(g^{-1}v) = \frac{1}{|G|} \sum_{g\in G} v = \frac{1}{|G|} \cdot |G|v = v,$$

[1] Apesar de Heinrich Maschke não ter provado nessa generalidade e nessa abordagem, o teorema ainda recebe seu nome em sua homenagem. Na verdade, ele ainda pode ser generalizado para anéis quaisquer: o anel de grupo RG é semissimples se e só se R é semissimples e a ordem de G é inversível em R.

ou seja, π' é a identidade sobre V. Isso também mostra que π' é sobrejetora. Para concluir, basta mostrarmos que π' é homomorfismo de módulos. Se $h \in G$ e $u \in U$, então

$$\begin{aligned}\pi'(hu) = \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}(hu)) &= \frac{1}{|G|}\sum_{g\in G} h(h^{-1}g)\pi((h^{-1}g)^{-1}u) \\ &= h\cdot\frac{1}{|G|}\sum_{x\in G} x\pi(x^{-1}u) \\ &= h\pi'(u),\end{aligned}$$

como preciso. Na penúltima igualdade, usamos que $x = h^{-1}g$ percorre todo o grupo quando variamos $g \in G$. □

Observação 1.3.8. A escolha para a função π' na demonstração anterior não é tão arbitrária assim. A ideia de "tomar uma média" sobre o grupo aparece em vários contextos. Nesse caso, podemos ver como o seguinte: temos um elemento $\pi \in \mathrm{Hom}_k(U,V)$ e queremos levá-lo de um jeito natural a $\mathrm{Hom}_{kG}(U,V)$. Mas note que $\mathrm{Hom}_{kG}(U,V)$ é o subespaço dos pontos fixos de $\mathrm{Hom}_k(U,V)$ pela ação de G definida no Exemplo 1.3.5! De fato, se $\varphi \in \mathrm{Hom}_k(U,V)$, então $g\varphi = \varphi$ para todo $g \in G$ se, e só se,

$$(g\varphi)(u) = \varphi(u) \iff g\varphi(g^{-1}u) = \varphi(u) \iff \varphi(g^{-1}u) = g^{-1}\varphi(u)$$

para todos $u \in U$ e $g \in G$, ou seja, se, e somente se, $\varphi \in \mathrm{Hom}_{kG}(U,V)$. Pelo Exercício A.1.12, podemos tentar aplicar $\frac{1}{|G|}\sum_{g\in G} g$ em π e ver o que acontece. Isso é exatamente o que fazemos na demonstração acima!

Isso explica o motivo de existirem representações como no Exemplo 1.3.6. Esse exemplo ainda nos mostra outra coisa: repare que todos os fatores de composição do módulo em questão são triviais. Isso não é um caso particular! Dessa vez, isso ocorre não só porque a característica p do corpo é positiva, mas também porque o grupo em questão tem p elementos.

Notação 1.3.9. Sempre que não for especificado, p será a característica de k, mesmo quando ela for 0.

Proposição 1.3.10. Se $p > 0$ e G é um p-grupo, então o kG-módulo trivial é o único kG-módulo simples, a menos de isomorfismo.

Se p é um número primo, lembre que um p-grupo é um grupo tal que a ordem de qualquer elemento é uma potência de p. Como estamos lidando apenas com grupos finitos, isso é equivalente, pelo Teorema de Cauchy, a exigir que a ordem do grupo seja uma potência de p.

Demonstração: Seja S um kG-módulo simples. Nossa ideia será encontrar $v \in S$ não nulo fixo pela ação de G. Da simplicidade de S, o submódulo gerado por v será S e, portanto, S será a representação trivial de G. Seja $u \in S$ um elemento não nulo qualquer. Considere T como sendo o subgrupo do grupo aditivo de S gerado pelos elementos gu, com $g \in G$. Note que T é finito (tem no máximo $p^{|G|}$ elementos) e é naturalmente um espaço vetorial sobre $\mathbb{F}_p$. Assim, T é um p-grupo finito sobre o qual G age. Como G é um p-grupo, as órbitas de sua ação em T têm tamanho 1 ou tamanho múltiplo de p. Mas $0 \in T$ é fixo por G. Por isso, como as órbitas particionam T e $|T|$ é divisível por p, deve existir outro $v \in S$, $v \neq 0$, cuja órbita tem tamanho 1. Logo, encontramos $v \in S$ não nulo que é fixo por G, como queríamos. □

Observação 1.3.11. A recíproca da Proposição 1.3.10 é válida e decorre facilmente da Proposição 1.3.14 que demonstraremos daqui a pouco (veja o Exercício A.1.19).

A pergunta natural que surge é: quantas classes de isomorfismo de representações irredutíveis um dado grupo possui? Se k é algebricamente fechado, temos a resposta! Provaremos o seguinte teorema na próxima seção:

Teorema 1.3.12 (Brauer)**.** Se k é algebricamente fechado, então o número de classes de isomorfismo de kG-módulos simples é igual ao número de classes de conjugação p-regulares de G.

Um elemento de G é chamado de **p-regular** se sua ordem não é divisível por p. Uma classe de conjugação de G é dita **p-regular** se os seus elementos são p-regulares. Lembre que todos os elementos numa classe de conjugação têm a mesma ordem, então basta verificar que um elemento da classe é p-regular para ver que tal classe é p-regular. Quando $p = 0$, recuperamos um resultado conhecido de representações de grupos sobre $\mathbb{C}$, que diz que o número de caracteres irredutíveis (isto é, de representações irredutíveis) é igual ao número de classes de conjugação do grupo. Se $p > 0$ e G é p-grupo, recuperamos a Proposição 1.3.10, porque a única classe p-regular de G é a da identidade.

Antes de apresentar mais exemplos, vamos provar mais duas proposições interessantes. Se U é um kG-módulo e $H \leq G$ é um subgrupo, denotamos por U_H o kH-módulo obtido de U restringindo escalares do jeito natural (ou seja, através da inclusão $kH \to kG$). O estudo da restrição (e do seu adjunto, a indução, que veremos depois) é muito importante, pois nos permite passar informações a respeito de representações de G para informações a respeito de representações de H, e vice-versa. O conjunto de ideias e resultados que existem para o caso em que H é subgrupo normal de G chama-se "teoria de Clifford". A próxima proposição é o nosso primeiro encontro com essa teoria:

Proposição 1.3.13 (Clifford[1])**.** Se U é um kG-módulo semissimples e N é um subgrupo normal de G, então U_N é um kN-módulo semissimples.

Demonstração: É imediato que a restrição a um subgrupo respeita somas diretas, logo, podemos assumir que U é simples. Começamos com a seguinte observação: se V é um kN-submódulo de U_N, então o mesmo vale para gV, para todo $g \in G$. De fato, se $n \in N$, vale que $g^{-1}ng \in N$, de modo que $g^{-1}ngV = V$ e

$$n \cdot (gV) = g \cdot (g^{-1}ngV) = gV.$$

Agora, suponha que V é um submódulo *simples* de U_N. Então gV também é simples: se $W \leq gV$ fosse um submódulo não trivial, então $g^{-1}W$ seria um submódulo não trivial de $g^{-1}gV = V$. Por isso, a soma de todos os gV com $g \in G$ é um kN-módulo semissimples. Mas é fácil ver que essa soma é um kG-módulo, logo tem que ser igual a U, provando que U_N é semissimples. □

Vamos aproveitar o Teorema de Clifford para demonstrar um resultado útil.

Proposição 1.3.14. Se $p > 0$, então a interseção dos núcleos das ações de G em cada kG-módulo simples coincide com o maior p-subgrupo normal $O_p(G)$ de G. Em particular, os kG-módulos simples são precisamente os $k[G/O_p(G)]$-módulos simples, vistos como kG-módulos através da projeção canônica $G \to G/O_p(G)$.

Como o produto de dois p-subgrupos normais de G é ainda um p-subgrupo normal, existe o maior p-subgrupo normal $O_p(G)$, como aparece acima. Ele é justamente o produto de todos os p-subgrupos normais de G. Assim, a proposição acima nos dá um modo de encontrar os kG-módulos simples lidando com representações de um grupo possivelmente menor do que G.

Demonstração. Vendo um kG-módulo U como um homomorfismo de G em $\mathrm{GL}(U)$, o núcleo da ação de G em U é o núcleo desse homomorfismo. Observe que ele é formado pelos elementos de G que agem trivialmente em U. Logo, se H é a interseção dos núcleos das ações de G em cada kG-módulo simples, vale

$$H = \{g \in G \mid \text{para todo } S \text{ simples e para todo } s \in S, gs = s\}.$$

[1]Essa é conhecida como a versão fraca do Teorema de Clifford. O Exercício A.1.16 é um passo a passo para provar a versão forte.

Para provar a primeira afirmação do enunciado, devemos verificar que $H = O_p(G)$.

Seja S um kG-módulo simples. Como $O_p(G)$ é normal em G, o Teorema de Clifford diz que $S_{O_p(G)}$ é semissimples. Mas, pela Proposição 1.3.10, o único módulo simples de $O_p(G)$ é o trivial. Isso implica que $O_p(G)$ age trivialmente em S e, como S era qualquer, vale a inclusão $O_p(G) \subseteq H$. Por outro lado, para provar a inclusão $H \subseteq O_p(G)$, basta mostrar que H é um p-subgrupo normal de G. A normalidade é imediata, porque, por construção, H é a interseção de subgrupos normais de G. Vejamos que ele é um p-grupo. Seja $h \in H$. Da definição de radical, vemos que $h-1 \in \mathrm{rad}(kG)$ e, em particular, $h-1$ é nilpotente. Assim, existe $n \geq 0$ suficientemente grande tal que $(h-1)^{p^n} = 0$. Como h e 1 comutam e a característica de k é p, segue que

$$h^{p^n} - 1 = (h-1)^{p^n} = 0$$

e, por isso, a ordem de h é uma potência de p. Como h era qualquer, isso prova que H é p-grupo, como desejado. Concluímos que H é de fato igual a $O_p(G)$.

Sabendo disso, provemos a última afirmação do enunciado. Veremos novamente uma representação de G como um homomorfismo de G em $\mathrm{GL}(S)$ para algum espaço vetorial S. Dada uma representação irredutível $G \to \mathrm{GL}(S)$, $O_p(G)$ está contido no núcleo desse homomorfismo e obtemos uma representação irredutível de $G/O_p(G)$. Reciprocamente, dada uma representação irredutível $G/O_p(G) \to \mathrm{GL}(S)$, podemos compor com a projeção canônica para obter uma representação irredutível de G. Não é difícil ver que essas construções são uma a inversa da outra, de modo que temos a correspondência do enunciado. □

Terminamos a seção estudando as representações irredutíveis de grupos cíclicos e de $\mathrm{SL}_2(p)$. Para ambos os exemplos, suporemos que $p = \mathrm{char}(k) > 0$ e que k é algebricamente fechado.

Exemplo 1.3.15. Seja $G = C_n$ o grupo cíclico de ordem n tal que $n = p^a m$ e m não seja divisível por p. Observe que o polinômio $x^m - 1$ é separável, pois ele e sua derivada mx^{m-1} não possuem fatores comuns (usamos que $m \neq 0$ em k). Portanto, todas as raízes desse polinômio são distintas e, supondo k algebricamente fechado, temos m raízes m-ésimas da unidade em k. Se g é um gerador de C_n e λ é uma dessas raízes m-ésimas da unidade, podemos considerar o espaço unidimensional k e fazer g^i agir por multiplicação por λ^i. Como $\lambda^n = (\lambda^m)^{p^a} = 1$, isso de fato define uma estrutura de kC_n-módulo em k. Como esse módulo tem dimensão 1, ele é simples. Além disso, diferentes escolhas de λ nos dão módulos simples não isomorfos, já que em cada módulo g age de modo diferente.

Vejamos que esses m módulos são todos os kC_n-módulos simples. Dado um kC_n-módulo simples S, tome um autovetor $v \in S$ do operador $g : S \to S$. O subespaço gerado por v é certamente invariante por g e, portanto, por C_n. Da simplicidade de S, v tem que gerar S, logo S tem dimensão 1 e g age por multiplicação por uma raiz n-ésima da unidade, já que $g^n = 1$. Mas em característica p vale $\lambda^n - 1 = (\lambda^m - 1)^{p^a}$, de modo que toda raiz n-ésima da unidade é uma raiz m-ésima. Concluímos que S é isomorfo a um dos módulos simples construídos anteriormente.

Para tirar a conclusão do parágrafo anterior, poderíamos ter usado o Teorema de Brauer. A ordem de um elemento p-regular g^i de C_n tem que dividir m. Usando a fórmula que dá a ordem de g^i, não é difícil ver que devemos ter $p^a \mid i$. Portanto, há exatamente m valores possíveis para i. Como toda classe de conjugação de C_n é unitária, temos m classes p-regulares e o Teorema de Brauer implica que os m módulos que construímos são todos os módulos simples sobre kC_n.

Uma observação feita no exemplo anterior se generaliza para grupos abelianos quaisquer!

Proposição 1.3.16. Se k é algebricamente fechado e G é abeliano, então todo kG-módulo simples é unidimensional.

Demonstração: Seja S um kG-módulo simples. Se $g \in G$ e se $T : S \to S$ é a ação induzida por g, então T é um homomorfismo de módulos porque G é abeliano. Logo, como k é algebricamente fechado, o Lema de Schur nos diz que T é a multiplicação por algum escalar $\lambda \in k$. Com isso, é

fácil ver que todo subespaço de S é também um submódulo. Mas S é simples, então deve valer $\dim_k S = 1$. □

Exemplo 1.3.17. Seja $G = \mathrm{SL}_2(p)$ o grupo das matrizes 2×2 com entradas em $\mathbb{F}_p$ e com determinante 1. Pelo Exercício A.1.21, $\mathrm{SL}_2(p)$ possui p classes de conjugação p-regulares. Logo, supondo k algebricamente fechado, se construirmos p kG-módulos simples distintos, teremos encontrado todos. O argumento que daremos é uma adaptação de ideias sobre pesos em representações de álgebras de Lie.

Seja V_2 o espaço dos vetores-coluna de tamanho 2 com entradas em k. Veja que V_2 é naturalmente uma representação de $\mathrm{SL}_2(p)$, onde a ação é dada pela multiplicação de matrizes (estamos vendo $\mathbb{F}_p \subseteq k$). Fixe

$$x = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{e} \quad y = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Assim, se $g \in \mathrm{SL}_2(p)$ tem entradas

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

então $gx = ax+cy$ e $gy = bx+dy$. A ideia agora é que podemos formar o anel de polinômios $k[x,y]$ e estender essa ação de g em x e y a um automorfismo da álgebra de polinômios. Como x e y são levados em polinômios homogêneos de grau 1, o subespaço V_n de $k[x,y]$ dos polinômios homogêneos de grau $n-1$ é um kG-módulo[1]. Note que a nova definição de V_2 coincide com a antiga e que V_1 é a representação trivial. Além disso, V_n tem como base os monômios $x^{n-1}, x^{n-2}y, \ldots, y^{n-1}$ e, por isso, tem dimensão n. Vamos provar que $V_1, \ldots, V_p$ são simples. Como eles têm dimensões diferentes, eles são dois a dois não isomorfos e, pelo que vimos anteriormente, essas serão todas as representações irredutíveis de $\mathrm{SL}_2(p)$ sobre k.

Já sabemos que V_1 é simples por ter dimensão 1. Agora, tome $1 \leq n < p$ e mostremos que V_{n+1} é simples. Fixaremos dois elementos de $\mathrm{SL}_2(p)$:

$$g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{e} \quad h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Vamos considerar V_{n+1} como representação de $\langle g \rangle$ e de $\langle h \rangle$. Provaremos que x^n é gerador do $k\langle g \rangle$-módulo V_{n+1} e que o subespaço ky^n gerado por y^n é o soco. Trocando x com y e g com h, o mesmo argumento provará que y^n é o gerador do $k\langle h \rangle$-módulo V_{n+1} e que kx^n é o soco. Antes de continuar, vejamos que isso implica que V_{n+1} é simples. Seja W um submódulo não nulo de V_{n+1}. Vendo W como $k\langle g \rangle$-módulo, ele deve conter um $k\langle g \rangle$-módulo simples. Mas o único $k\langle g \rangle$-submódulo simples de V_{n+1} é ky^n. Por isso, $y^n \in W$. Segue que o $k\langle h \rangle$-módulo gerado por y^n está contido em W e, consequentemente, $W = V_{n+1}$, como preciso.

Para provar o que queremos a respeito da estrutura de V_{n+1} como $k\langle g \rangle$-módulo, vamos provar um resultado mais forte que pode ser demonstrado por indução. Para $0 \leq i \leq n$, seja W_{i+1} o subespaço de V_{n+1} de dimensão $i+1$ com base

$$x^i y^{n-i}, x^{i-1}y^{n-i+1}, \ldots, xy^{n-1}, y^n.$$

Defina $W_0 = 0$. Assim temos a cadeia de subespaços

$$V_{n+1} = W_{n+1} \supseteq W_n \supseteq \cdots \supseteq W_1 \supseteq W_0 = 0$$

onde cada quociente tem dimensão 1.

[1] O módulo V_{n+1} é a *n-ésima potência simétrica* de V_2. Também pode ser construído considerando-se o produto tensorial de n cópias de V_2 e quocientado-se pelo subespaço que torna os tensores "simétricos", ou seja, dois tensores puros serão iguais se, a menos de ordenação, possuem as mesmas coordenadas. Para mais detalhes, veja o Exemplo 2.4.9.

Lema 1.3.18. Se $W_0, \ldots, W_{n+1}$ são como definidos acima, então:

(1) W_i é um $k\langle g\rangle$-submódulo de V_{n+1}.

(2) W_i/W_{i-1} é o $k\langle g\rangle$-módulo trivial.

(3) cada elemento de $W_i \setminus W_{i-1}$ gera W_i como $k\langle g\rangle$-módulo.

Demonstração: Vamos provar o resultado por indução em i. Para $i = 0$, é imediato que (1) vale. Como $gy = y$, temos que $gy^n = y^n$ e, por isso, W_1 é um $k\langle g\rangle$-submódulo. É fácil ver que (2) e (3) valem para $i = 1$, já que W_1 tem dimensão 1 e ação de g em W_1 é trivial.

Suponha que o resultado vale para algum $1 \leq i \leq n$ e vamos estudar W_{i+1}. Como $gx = x + y$, vale que

$$gx^i y^{n-i} = (x+y)^i y^{n-i} = x^i y^{n-i} + \binom{i}{1} x^{i-1} y^{n-i+1} + u,$$

onde u é uma combinação linear de $x^{i-2}y^{n-i+2}, \ldots, xy^{n-1}, y^n$ e, portanto, está em W_{i-1}. Como W_{i+1} é gerado por $x^i y^{n-i}$ e W_i e como já sabemos que W_i é $k\langle g\rangle$-módulo, a conta acima mostra que W_{i+1} também é $k\langle g\rangle$-módulo. Mais ainda, a conta também mostra que $gx^i y^{n-i} - x^i y^{n-i} \in W_i$, o que prova que W_{i+1}/W_i é o módulo trivial, já que é gerado pela classe de $x^i y^{n-i}$. Por fim, provemos (3). Como $i \leq n < p$, o binomial que aparece na expressão acima é não nulo em k e então $(g-1)x^i y^{n-i}$ é um elemento de $W_i \setminus W_{i-1}$. Assim, se $v \in W_{i+1} \setminus W_i$, podemos escrever

$$v = \alpha x^i y^{n-i} + w$$

com $\alpha \neq 0$ e $w \in W_i$, logo

$$(g-1)v = \alpha(g-1)x^i y^{n-i} + (g-1)w.$$

Mas $(g-1)w \in W_{i-1}$, porque W_i/W_{i-1} é o $k\langle g\rangle$-módulo trivial, então $(g-1)v \in W_i \setminus W_{i-1}$. Pela hipótese de indução, segue que o $k\langle g\rangle$-módulo gerado por v contém W_i, já que contém um elemento de $W_i \setminus W_{i-1}$, e também contém v, que não está em W_i. Por isso, v tem que gerar W_{i+1} como $k\langle g\rangle$-módulo e a prova está concluída. □

Finalmente, vamos concluir o que está restando. Pelo item (3) do lema anterior, x^n gera $V_{n+1} = W_{n+1}$ como $k\langle g\rangle$-módulo. Agora, note que $g^p = 1$, de modo que $\langle g\rangle$ é um p-grupo. Pela Proposição 1.3.10, o módulo trivial é o único $k\langle g\rangle$-módulo simples, logo, o soco de V_{n+1} como $k\langle g\rangle$-módulo é exatamente o conjunto dos vetores fixos por g. Se $v \in V_{n+1} \setminus W_1$, podemos usar novamente o item (3) do lema para concluir que o submódulo gerado por v não tem dimensão 1 e, consequentemente, $gv \neq v$. Por isso, $W_1 = ky^n$ é o soco, como preciso. Isso termina a prova de que $V_1, \ldots, V_p$ são todos os módulos simples de $\mathrm{SL}_2(p)$.

1.4 Prova do Teorema de Brauer

Nesta seção, vamos provar o Teorema de Brauer (Teorema 1.3.12). Para isso, vamos supor que k é algebricamente fechado. Iremos começar dando a prova para o caso onde a característica p de k é 0. Ela é mais simples e motivará a demonstração do outro caso.

Suponha que $p = 0$. Pelo Teorema de Maschke, kG é semissimples e podemos escrever

$$kG = A_1 \oplus \cdots \oplus A_r,$$

onde $A_1, \ldots, A_r$ são as componentes simples de kG. Como k é algebricamente fechado, sabemos que cada A_i é isomorfo a $M_{n_i}(k)$ para algum $n_i \geq 1$ (note que as entradas das matrizes estão em k). Lembre que o centro[1] de $M_n(k)$ é formado pelas matrizes escalares e, portanto, $\dim_k Z(A_i) = 1$

[1] O **centro** $Z(A)$ de uma álgebra A é a subálgebra formada pelos elementos de A que comutam com todos os outros.

para todo i. Mas o centro de um produto direto de álgebras é o produto direto dos centros, de modo que

$$Z(kG) = Z(A_1) \oplus \cdots \oplus Z(A_r)$$

e $\dim_k Z(kG) = r$. Como r é o número de classes de isomorfismo de módulos simples sobre kG, concluímos a prova se mostrarmos que a dimensão do centro de kG é o número de classes de conjugação de G. Se $\mathcal{C}_1, \ldots, \mathcal{C}_s$ são as classes de conjugação, podemos formar as *somas de classe*

$$\gamma_i \coloneqq \sum_{g \in \mathcal{C}_i} g.$$

Note que $g\gamma_i g^{-1} = \gamma_i$ para todo $g \in G$, já que conjugar uma classe de conjugação apenas permuta os seus elementos. Dessa forma, cada γ_i está em $Z(kG)$. Reciprocamente, se

$$a = \sum_{g \in G} a_g g \in Z(kG),$$

a relação $gag^{-1} = a$ implica que $a_{ghg^{-1}} = a_h$ para todos $g, h \in G$. Mas isso nos diz que a é combinação linear de $\gamma_1, \ldots, \gamma_s$. Como as somas de classe são linearmente independentes, acabamos de provar que uma base de $Z(kG)$ é $\{\gamma_1, \ldots, \gamma_s\}$ e então $r = s$, como queríamos demonstrar.

No caso $p > 0$, poderíamos tentar adaptar a demonstração anterior estudando o centro de $kG/\operatorname{rad}(kG)$. Porém, ao invés de estudar um subespaço desse quociente, será mais fácil entender um quociente desse quociente! Assim, vejamos como podemos "dualizar" o argumento do caso $p = 0$. Para uma álgebra A, denote por $[A, A]$ o **subespaço de comutadores** de A, ou seja, o subespaço gerado pelos elementos $ab - ba$, com $a, b \in A$. Lidaremos com $kG/[kG, kG]$ ao invés de $Z(kG)$. Como no caso do centro, não é difícil ver que

$$[kG, kG] = [A_1, A_1] \oplus \cdots \oplus [A_r, A_r].$$

O seguinte resultado nos diz quem é $[A_i, A_i]$:

Lema 1.4.1. O subespaço de comutadores de $M_n(k)$ é o subespaço das matrizes de traço zero.

Demonstração: Se $X, Y \in M_n(k)$, sabemos que o traço de XY é igual ao traço de YX, o que implica que $[M_n(k), M_n(k)]$ está contido no subespaço V das matrizes de traço zero. Por outro lado, V tem como base o conjunto das matrizes e_{ij} com $i \neq j$ e das matrizes $e_{11} - e_{ii}$ com $i > 1$. Como $e_{ij} = e_{il}e_{lj} - e_{lj}e_{il}$ para $i \neq j$ e $e_{11} - e_{ii} = e_{1i}e_{i1} - e_{i1}e_{1i}$, concluímos que $V \subseteq [M_n(k), M_n(k)]$ e então vale a igualdade. □

Em particular, o lema acima diz que a codimensão de $[A_i, A_i]$ em A_i é 1. Logo, a codimensão de $[kG, kG]$ em kG é r e, neste caso de característica zero, o teorema está provado se mostrarmos que a dimensão de $kG/[kG, kG]$ é o número de classes de conjugação de G. Deixaremos para verificar isso quando estivermos fazendo o caso de característica positiva.

Suponha agora que $p > 0$. Não é difícil ver que o subespaço de comutadores de $kG/\operatorname{rad}(kG)$ é a projeção de $T \coloneqq [kG, kG]$ no quociente. Ou seja, se $S \coloneqq T + \operatorname{rad}(kG)$, então

$$\frac{S}{\operatorname{rad}(kG)} = \left[\frac{kG}{\operatorname{rad}(kG)}, \frac{kG}{\operatorname{rad}(kG)}\right].$$

Como $kG/\operatorname{rad}(kG)$ é semissimples, a codimensão de $S/\operatorname{rad}(kG)$ é o número r de componentes simples de $kG/\operatorname{rad}(kG)$, pelo que vimos anteriormente. Observe que

$$\frac{kG/\operatorname{rad}(kG)}{S/\operatorname{rad}(kG)} \cong \frac{kG}{S}$$

e, portanto, a codimensão de S em kG também é r. Pelo Exercício A.1.8 (que é parecido com a Observação 1.1.10), r é exatamente o número de classes de isomorfismo de kG-módulos simples, então basta provarmos que a dimensão de kG/S é o número de classes de conjugação p-regulares de G.

Sejam $x_1, \ldots, x_s \in G$ representantes das s classes de conjugação p-regulares em G e sejam $x_{s+1}, \ldots, x_t \in G$ representantes das demais classes de conjugação. Mostraremos que o conjunto $\{x_1 + S, \ldots, x_s + S\}$ é uma base de kG/S. Para isso, começamos com a seguinte caracterização de S:

Lema 1.4.2. O subespaço S consiste dos elementos $a \in kG$ tais que $a^{p^i} \in T$ para algum $i \geq 0$.

Demonstração: Seja S_0 o conjunto descrito no enunciado. Vamos primeiro provar que S_0 é de fato um subespaço de kG. Começaremos demonstrando que, se $a, b \in kG$, então

$$(a+b)^p \equiv a^p + b^p \pmod{T}.$$

Cuidado que isso não segue de imediato do "sonho de todo estudante"[1], porque T não é ideal e então não podemos trabalhar diretamente com o produto no quociente kG/T. Expandindo $(a+b)^p$, podemos fazer o grupo cíclico de ordem p agir nos termos por permutações cíclicas. Os termos a^p e b^p são os únicos fixos, enquanto os outros se agrupam em órbitas de p elementos. Se mostrarmos que dois elementos na mesma órbita são congruentes módulo T, então a soma de uma órbita de p elementos será 0 módulo T, já que estamos em característica p. De fato, se $a_1 a_2 \cdots a_p$ é um desses termos e $a_i \cdots a_p a_1 \cdots a_{i-1}$ é uma permutação cíclica, veja que

$$a_1 a_2 \cdots a_p - a_i \cdots a_p a_1 \cdots a_{i-1} = (a_1 \cdots a_{i-1})(a_i \cdots a_p) - (a_i \cdots a_p)(a_1 \cdots a_{i-1}) \in T.$$

Assim, as órbitas de tamanho p se cancelam módulo T e sobram os termos a^p e b^p, provando a congruência desejada.

Outra propriedade de T que precisamos provar é que $T^p \subseteq T$. Por conta da identidade que acabamos de provar, é suficiente mostrar que $(ab-ba)^p \in T$ para $a, b \in kG$. De fato,

$$(ab-ba)^p \equiv (ab)^p - (ba)^p = a(b(ab)^{p-1}) - (b(ab)^{p-1})a \equiv 0 \pmod{T}.$$

Assim, se $a, b \in S_0$, a propriedade $T^p \subseteq T$ nos diz que podemos tomar um mesmo $i \geq 0$ tal que $a^{p^i}, b^{p^i} \in T$. Logo,

$$(\lambda a + \mu b)^{p^i} \equiv \lambda^{p^i} a^{p^i} + \mu^{p^i} b^{p^i} \equiv 0 \pmod{T}$$

e $\lambda a + \mu b \in S_0$ para todos $\lambda, \mu \in k$. Isso prova que S_0 é subespaço de kG.

Finalmente, provemos que $S = S_0$. É imediato da definição que $T \subseteq S_0$ e, como $\operatorname{rad}(kG)$ é nilpotente, $\operatorname{rad}(kG) \subseteq S_0$ também. Como S_0 é subespaço de kG, vale que $S = T + \operatorname{rad}(kG) \subseteq S_0$ e temos uma das inclusões. Para a outra inclusão, seja $a \in S_0$ qualquer. No quociente $kG/\operatorname{rad}(kG)$, fixe uma componente $a_0 + \operatorname{rad}(kG)$ de $a + \operatorname{rad}(kG)$ na decomposição de $kG/\operatorname{rad}(kG)$ como produto direto de álgebras de matrizes. Assim, existe $i \geq 0$ tal que a p^i-ésima potência de $a_0 + \operatorname{rad}(kG)$ está no subespaço de comutadores da álgebra de matrizes correspondente, ou seja, existe i tal que essa potência tem traço zero. Mas, em característica p, o traço da p^i-ésima potência de uma matriz é a p^i-ésima potência do traço, já que o traço é a soma dos autovalores. Isso implica que $a_0 + \operatorname{rad}(kG)$ já tem traço zero. Aplicando esse argumento em todas as componentes de $a + \operatorname{rad}(kG)$, segue que

$$a + \operatorname{rad}(kG) \in \left[\frac{kG}{\operatorname{rad}(kG)}, \frac{kG}{\operatorname{rad}(kG)}\right] = \frac{S}{\operatorname{rad}(kG)}$$

e, consequentemente, $a \in S$. Isso demonstra a inclusão $S_0 \subseteq S$, concluindo o lema. □

[1] É a identidade $(a+b)^p = a^p + b^p$, válida em corpos de característica p ou, mais geralmente, em anéis comutativos de característica p.

Ainda precisaremos de mais um resultado preliminar, desta vez sobre G.

Lema 1.4.3. Cada $g \in G$ pode ser escrito de maneira única como $g = uv$, onde u é p-regular, v tem como ordem uma potência de p e $uv = vu$.

Demonstração: Se a ordem n de g se fatora em $n = \alpha\beta$, onde α é uma potência de p e β não é divisível por p, podemos escrever $1 = \lambda\alpha + \mu\beta$ para certos inteiros λ e μ. Defina $u = g^{\lambda\alpha}$ e $v = g^{\mu\beta}$. É imediato que $g = uv = vu$ e, como $u^\beta = 1$ e $v^\alpha = 1$, sabemos que u é p-regular e a ordem de v é uma potência de p.

Suponha que $g = u_1v_1$ é outra decomposição como no enunciado. Como u_1 e v_1 comutam com g, eles também comutam com u e v, que são potências de g. Assim, $u_1^{-1}u$ é p-regular e v_1v^{-1} tem como ordem uma potência de p. Mas $u_1^{-1}u = v_1v^{-1}$, então esses produtos têm que ser iguais a 1, de modo que $u_1 = u$ e $v_1 = v$, provando a unicidade. □

Estamos prontos para provar que $\{x_1 + S, \ldots, x_s + S\}$ é base de kG/S, o que terminará a demonstração do Teorema de Brauer. Vamos começar mostrando que $x_1 + T, \ldots, x_t + T$ formam uma base de kG/T. Se $x, y \in G$ são conjugados, com $y = gxg^{-1}$, então

$$x - y = x - gxg^{-1} = g^{-1}(gx) - (gx)g^{-1} \in T.$$

Como G gera kG, isso mostra que os $x_i + T$ geram kG/T. Para provar a independência linear, note que T é gerado pelos elementos $gh - hg$ com $g, h \in G$. Mas gh e hg são conjugados: $gh = h^{-1}(hg)h$. Por isso, se

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

a soma dos coeficientes a_g quando g varia somente numa classe de conjugação fixada tem que ser 0. Não é difícil ver que isso na verdade caracteriza T! Dessa forma, se

$$\sum_{i=1}^{t} \alpha_i (x_i + T) = 0$$

em kG/T, então

$$\sum_{i=1}^{t} \alpha_i x_i \in T$$

e, pela propriedade de T que acabamos de verificar, vale $\alpha_i = 0$ para todo i, já que $x_1, \ldots, x_t$ estão em classes de conjugação distintas. Com isso, $\{x_1 + T, \ldots, x_t + T\}$ é de fato base de kG/T.

Voltando para kG/S, note que $x_1 + S, \ldots, x_t + S$ geram kG/S, pois as classes laterais correspondentes em kG/T formam uma base e $T \subseteq S$. Vejamos que podemos descartar os $x_i + S$ com $i > s$. Se $i > s$, escreva $x_i = u_iv_i$ como no Lema 1.4.3. Se p^j é a ordem de v_i, como u_i e v_i comutam, então

$$(x_i - u_i)^{p^j} = u_i^{p^j} v_i^{p^j} - u_i^{p^j} = u_i^{p^j} - u_i^{p^j} = 0 \in T.$$

Pelo Lema 1.4.2, x_i e u_i são congruentes módulo S. Mas, como u_i é p-regular, u_i é conjugado a algum $x_{i'}$ com $i' \leq s$. Assim, $x_i + S = x_{i'} + S$ e podemos descartar $x_i + S$ do conjunto gerador, como queríamos.

Falta mostrar que $x_1 + S, \ldots, x_s + S$ são linearmente independentes. Suponha que

$$\sum_{i=1}^{s} \alpha_i x_i \in S,$$

onde $\alpha_i \in k$. Pelo Lema 1.4.2 e pelo que vimos em sua demonstração,

$$\sum_{i=1}^{s} \alpha_i^{p^j} x_i^{p^j} \equiv \left(\sum_{i=1}^{s} \alpha_i x_i \right)^{p^j} \equiv 0 \pmod{T}$$

para algum $j \geq 0$. Como $x_1, \ldots, x_s$ são p-regulares, podemos supor que j é grande o suficiente de modo que $x_i^{p^j} = x_i$ para todo i. De fato, para cada i, existe j_i tal que p^{j_i} é congruente a 1 módulo a ordem de x_i, logo basta tomar j divisível por $j_1, \ldots, j_s$. Assim, temos que

$$\sum_{i=1}^{s} \alpha_i^{p^j} x_i \in T.$$

Como $x_1, \ldots, x_s$ são linearmente independentes módulo T, segue que $\alpha_i^{p^j} = 0$ e então $\alpha_i = 0$ para todo i. Isso mostra que $x_1 + S, \ldots, x_s + S$ são linearmente independentes, concluindo a prova do Teorema de Brauer.

Capítulo 2

Decompondo representações

Este capítulo é uma coletânea de novas técnicas para o estudo de kG-módulos. Em geral, os resultados de cada seção dão informações sobre certos módulos indecomponíveis e, dessa forma, eles nos ajudam a entender como decompor as representações de um grupo. Apesar de algumas construções não funcionarem para álgebras quaisquer, elas ainda valem em um contexto mais geral do que o de representações de grupos, como o de representações de álgebras de Hopf. Então, por enquanto, a estrutura de G ainda não desempenha um papel muito central na nossa teoria e podemos considerar este capítulo como um capítulo de generalidades.

Ao passarmos do caso semissimples para o caso geral, somos naturalmente levados a estender o conceito de módulo simples ao de módulo indecomponível. Na primeira seção, após vermos alguns critérios de indecomponibilidade, demonstramos o importante Teorema de Krull-Schmidt, um resultado a respeito da unicidade de decomposições em somas diretas de indecomponíveis. Em seguida, damos alguns exemplos concretos, descrevendo, por exemplo, a estrutura das representações indecomponíveis de grupos cíclicos. Também veremos um fato curioso: existem álgebras de grupo que não possuem tipo de representação finito.

A segunda seção se especializa em um tipo particular de módulos: os projetivos. Estudar os módulos projetivos indecomponíveis é o primeiro passo para estudar os módulos indecomponíveis em geral. Eles possuem muitas propriedades boas, como tentamos ilustrar ao longo do capítulo. Nesse ponto, detalhamos como são os projetivos indecomponíveis quando o p-subgrupo de Sylow de G é normal e cíclico, o que nos fornece um caso particular do Teorema 5.1.7, o objetivo final da monografia.

O capítulo se encerra com o tratamento de duas construções importantes: a dualidade e o produto tensorial. Esses conceitos da álgebra linear podem ser enriquecidos para formar representações, como apontamos no Exemplo 1.3.5. Obtemos diversos resultados interessantes utilizando essas novas ferramentas, dentre eles a prova de que todo kG-módulo projetivo é injetivo, e vice-versa, e a descrição de todas as representações projetivas indecomponíveis do grupo $\mathrm{SL}_2(p)$, o que também nos remeterá ao Teorema 5.1.7.

2.1 Módulos indecomponíveis

Quando a álgebra A é semissimples, é suficiente entender os A-módulos simples para estudar todos os A-módulos, já que é relativamente fácil trabalhar com somas diretas. Mas o que acontece no caso não semissimples? Uma ideia é novamente tentar decompor cada módulo como soma direta de módulos menores e entender essas componentes. Decompondo em soma direta até não poder mais, chegamos nos módulos indecomponíveis.

Definição 2.1.1. Um A-módulo não nulo é dito **indecomponível** se não pode ser escrito como a soma direta de dois submódulos não nulos.

Observe que todo módulo simples é indecomponível. A volta vale somente quando exigimos

que o módulo em questão seja semissimples também. Por isso, essa nova definição é interessante para estudar casos mais gerais.

Um conceito útil e importante para o estudos de módulos indecomponíveis é o de idempotente. Um elemento $e \in A$ é chamado de **idempotente** se $e^2 = e$. Dois idempotentes $e, f \in A$ são **ortogonais** se $ef = fe = 0$. Dizemos que um idempotente não nulo $e \in A$ é **primitivo** se e não pode ser escrito como soma de dois idempotentes ortogonais não nulos. A ideia será trabalhar com idempotentes da álgebra de endomorfismos de um módulo U, seguindo a intuição de que tais idempotentes são projeções em submódulos de U.

Proposição 2.1.2. Seja U um A-módulo. Decomposições

$$U = U_1 \oplus \cdots \oplus U_n$$

de U como soma direta de submódulos estão em bijeção com decomposições

$$\mathrm{id}_U = e_1 + \cdots + e_n$$

da identidade $\mathrm{id}_U \in \mathrm{End}_A(U)$ como soma de idempotentes dois a dois ortogonais. Aqui, e_i é obtido de U_i como a composição da projeção $U \to U_i$ e da inclusão $U_i \to U$, enquanto U_i é obtido de e_i como $U_i = e_i(U)$. O somando U_i é indecomponível se e somente se e_i é primitivo.

Demonstração: Começamos com uma decomposição de U como soma direta dos submódulos $U_1, \ldots, U_n$. Definindo e_i como no enunciado, é imediato que id_U é a soma de $e_1, \ldots, e_n$ e que eles são idempotentes dois a dois ortogonais. Vejamos a volta. Se

$$\mathrm{id}_U = e_1 + \cdots + e_n$$

é uma decomposição como no enunciado, defina $U_i = e_i(U)$. Dado $u \in U$, vale que

$$u = \mathrm{id}_U(u) = e_1(u) + \cdots + e_n(u),$$

de modo que U é a soma dos U_i's. Agora, se

$$u_1 + \cdots + u_n = 0,$$

com $u_i \in U_i$, então $e_i(u_i) = u_i$, pois e_i é idempotente, e $e_j(u_i) \in (e_j e_i)(U) = 0$ para $j \neq i$, porque os idempotentes são ortogonais. Logo,

$$u_i = e_i(u_i) = e_i(u_1 + \cdots + u_n) = e_i(0) = 0,$$

provando que a soma $U = U_1 + \cdots + U_n$ é direta. É fácil verificar que as construções anteriores são uma a inversa da outra, estabelecendo a bijeção desejada.

Para a última afirmação da proposição, note que, se $U_i = V_1 \oplus V_2$ com $V_1, V_2 \leq U_i$ não nulos, então

$$U = U_1 \oplus \cdots \oplus U_{i-1} \oplus V_1 \oplus V_2 \oplus U_{i+1} \oplus \cdots \oplus U_n$$

e, seguindo o argumento de antes, e_i será a soma dos idempotentes ortogonais não nulos associados a V_1 e a V_2 na decomposição acima. Reciprocamente, se e_i é a soma de dois idempotentes ortogonais não nulos $f_1, f_2 \in \mathrm{End}_A(U)$, então f_1 e f_2 são ortogonais a cada e_j, com $j \neq i$, pois

$$e_j f_1 = e_j(f_1 + 0) = e_j(f_1^2 + f_2 f_1) = e_j(e_i f_1) = (e_j e_i) f_1 = 0 \cdot f_1 = 0$$

e, analogamente, $f_1 e_j = e_j f_2 = f_2 e_j = 0$. Por isso, obtemos uma decomposição

$$\mathrm{id}_U = e_1 + \cdots + e_{i-1} + f_1 + f_2 + e_{i+1} + \cdots + e_n$$

como no enunciado e, seguindo o argumento anterior, teremos uma decomposição não trivial $U_i = f_1(U) \oplus f_2(U)$. Equivalentemente, acabamos de provar que U_i é indecomponível se e somente se e_i é primitivo, como queríamos. □

Corolário 2.1.3. Um A-módulo U é indecomponível se e somente se os únicos idempotentes de $\mathrm{End}_A(U)$ são 0 e id_U.

Demonstração: Se 0 e id_U são os únicos idempotentes de $\mathrm{End}_A(U)$, então as únicas formas de escrever id_U como soma de dois idempotentes ortogonais são $\mathrm{id}_U = \mathrm{id}_U + 0 = 0 + \mathrm{id}_U$. Pela Proposição 2.1.2, as únicas formas de escrever U como soma direta de submódulos são $U = U \oplus 0 = 0 \oplus U$, ou seja, U é indecomponível. Reciprocamente, suponha que exista um idempotente $e \in \mathrm{End}_A(U)$ diferente de 0 e de id_U. Veja que o "complementar" $f = \mathrm{id}_U - e$ também é um idempotente e e e f são ortogonais. Como $\mathrm{id}_U = e + f$ e tanto e quanto f são não nulos, a Proposição 2.1.2 nos dá uma decomposição não trivial de U como soma direta de submódulos, mostrando que U não é indecomponível nesse caso. □

Há outra definição que se aplica no nosso caso, dando uma nova caracterização para um A-módulo ser indecomponível. Dizemos que A é **local** se A possui um único ideal à esquerda maximal. A nomenclatura vem do caso comutativo, onde um anel comutativo é dito local se possui um único ideal maximal. Antes de ver a relação com a indecomponibilidade, temos algumas caracterizações importantes:

Proposição 2.1.4. Se A é uma k-álgebra de dimensão finita, então são equivalentes:

(1) A é local.

(2) $A/\operatorname{rad}(A)$ é uma álgebra de divisão.

(3) Todo elemento de A é inversível ou nilpotente.

(4) O conjunto dos elementos não inversíveis de A é um ideal bilateral.

Demonstração: Vamos começar mostrando que as afirmações (1), (2) e (4) são equivalentes. Repare como essa parte ainda seria válida se A fosse um anel qualquer. Depois provaremos a equivalência com (3), que depende do fato de A ser uma álgebra de dimensão finita.

(1) $\implies$ (4). Se mostrarmos que todo elemento de $A \setminus \operatorname{rad}(A)$ é inversível, então concluiremos que o conjunto dos elementos não inversíveis de A é $\operatorname{rad}(A)$, que é um ideal bilateral. Como $\operatorname{rad}(A)$ é a interseção dos submódulos maximais de ${}_AA$ e estamos supondo A local, devemos ter que $\operatorname{rad}(A)$ é o único ideal à esquerda maximal de A. Logo, dado $a \in A \setminus \operatorname{rad}(A)$, o ideal à esquerda gerado por a não está contido em nenhum ideal à esquerda maximal, de modo que $Aa = A$ e a é inversível à esquerda. Se $b \in A$ é tal que $ba = 1$, note que $b \notin \operatorname{rad}(A)$, pois $\operatorname{rad}(A)$ é ideal bilateral e não contém 1. Assim, o mesmo argumento mostra que b é inversível à esquerda. Sendo inversível dos dois lados, b é inversível e seu inverso tem que ser a, provando que a também é inversível. Isso demonstra (4).

(4) $\implies$ (2). Seja $a \in A \setminus \operatorname{rad}(A)$. Como $\operatorname{rad}(A)$ é a interseção dos ideais à esquerda maximais de A, existe um ideal à esquerda maximal M de A tal que $a \notin M$. Logo, $M + Aa = A$ e existem $m \in M$ e $b \in A$ tais que $1 = m + ba$. Se ba não fosse inversível, então, como o conjunto dos elementos não inversíveis de A é um ideal e m não é inversível, valeria que 1 não é inversível, uma contradição. Assim, ba é inversível e, em particular, a é inversível à esquerda. Isso mostra que todo elemento não nulo do quociente $A/\operatorname{rad}(A)$ é inversível à esquerda. Um argumento análogo ao do parágrafo anterior nos permite concluir que $A/\operatorname{rad}(A)$ é uma álgebra de divisão.

(2) $\implies$ (1). Seja M um ideal à esquerda maximal de A. Como M contém $\operatorname{rad}(A)$, M corresponde a um ideal à esquerda maximal de $A/\operatorname{rad}(A)$. Mas $A/\operatorname{rad}(A)$ é uma álgebra de divisão e, por isso, possui apenas o ideal nulo como ideal à esquerda maximal. Logo, $M = \operatorname{rad}(A)$. Segue que $\operatorname{rad}(A)$ é o único ideal à esquerda maximal de A e A é local.

(1) $\implies$ (3). Se A é local, então já vimos que vale (4) e, mais do que isso, o conjunto dos elementos não inversíveis de A é $\operatorname{rad}(A)$. Portanto, todo elemento de A é inversível ou então está em $\operatorname{rad}(A)$ e, pelo Teorema 1.1.8, é nilpotente.

(3) $\implies$ (4). Suponha que todo elemento de A seja inversível ou nilpotente. Seja I o conjunto dos elementos não inversíveis de A, ou seja, o conjunto dos elementos nilpotentes. Vamos começar mostrando que I é fechado por multiplicação por qualquer elemento de A. Sejam $n \in I$ e $a \in A$ quaisquer. Se $n = 0$, então $an = na = 0 \in I$. Se $n \neq 0$, seja $r \geq 2$ o menor inteiro tal que $n^r = 0$. Definindo $b = an$, temos que $b \in I$ ou b é inversível. Esse segundo caso não pode ocorrer, porque, se b fosse inversível, então $1 = b^{-1}an$ e

$$n^{r-1} = 1 \cdot n^{r-1} = b^{-1}an^r = b^{-1}a \cdot 0 = 0,$$

contradizendo a definição de r. Analogamente, prova-se que $na \in I$.

Resta mostrar que I é fechado para a soma. Sejam $n, m \in I$ e suponha por absurdo que $n+m$ seja inversível. Logo, existe $a \in A$ inversível com $a(n+m) = 1$. Note que an não é inversível, pois, caso contrário, $n = a^{-1}(an)$ seria inversível, o que não o caso. Assim, an é nilpotente e $am = 1 - an$ é inversível[1]. Mas então $m = a^{-1}(am)$ também é inversível, uma contradição. Portanto, $n + m \in I$ e I também é fechado para a soma. Concluímos que I é um ideal bilateral de A. □

Observação 2.1.5. A caracterização (3) usa fortemente que A é uma álgebra de dimensão finita, porque, para anéis quaisquer, não é verdade que o radical é um ideal nilpotente. Por isso, não conseguimos garantir que um elemento não inversível de um anel local qualquer seja nilpotente. Além disso, veja que a condição (4) é simétrica em relação à direita ou à esquerda, de modo que poderíamos ter definido uma álgebra local como uma álgebra com um único ideal à direita maximal.

Algo semelhante ao Corolário 2.1.3 ocorre com a definição de localidade. Vamos agora provar que um módulo é indecomponível se e só se sua álgebra de endomorfismos é local. Uma das implicações vale para anéis quaisquer, mas a outra decorre do fato de estarmos trabalhando com uma álgebra de dimensão finita.

Lema 2.1.6. Todo idempotente de $A/\operatorname{rad}(A)$ é a projeção de um idempotente de A.

Demonstração: Seja $a \in A$ tal que $a + \operatorname{rad}(A)$ seja idempotente de $A/\operatorname{rad}(A)$. Vamos encontrar um idempotente $e \in A$ congruente a a módulo $\operatorname{rad}(A)$. Se $b = 1 - a$, então $ab = ba = a - a^2 \in \operatorname{rad}(A)$ e, como $\operatorname{rad}(A)$ é nilpotente, existe $r \geq 1$ com $(ab)^r = 0$. Pelo Teorema do Binômio de Newton,

$$1 = (a+b)^{2r} = a^{2r} + c_1a^{2r-1}b + \cdots + c_ra^rb^r + c_{r+1}a^{r-1}b^{r+1} + \cdots + b^{2r},$$

onde os c_i's são os coeficientes binomiais. Defina

$$e = a^{2r} + c_1a^{2r-1}b + \cdots c_ra^rb^r \quad \text{e} \quad f = c_{r+1}a^{r-1}b^{r+1} + \cdots + b^{2r}.$$

Como $a^rb^r = b^ra^r = 0$, segue que $ef = 0$ e $e = e \cdot 1 = e(e+f) = e^2$. Por fim, como $ab \in \operatorname{rad}(A)$, vemos que

$$e \equiv a^{2r} \equiv a \pmod{\operatorname{rad}(A)},$$

onde usamos mais uma vez que $a + \operatorname{rad}(A)$ é idempotente. Dessa forma, e é o idempotente procurado. □

Proposição 2.1.7. Uma k-álgebra A de dimensão finita é local se, e somente se, os seus únicos idempotentes são 0 e 1.

[1] Se $x \in A$ satisfaz $x^r = 0$, então $1 - x$ tem como inverso $1 + x + x^2 + \cdots + x^{r-1}$.

Demonstração: Se existe um idempotente $e \in A$ diferente de 0 e de 1, podemos tomar seu complementar $f = 1-e$, que também é idempotente não trivial e é ortogonal a e. Pela Proposição 2.1.2, a relação $1 = e + f$ nos dá uma decomposição ${}_AA = A_1 \oplus A_2$, onde A_1 e A_2 são submódulos não nulos de ${}_AA$ (utilizamos o Lema 1.2.3 para identificar e e f com idempotentes de $\mathrm{End}_A({}_AA)$). Se B_1 e B_2 são submódulos maximais de A_1 e A_2, respectivamente, então $B_1 \oplus A_2$ e $A_1 \oplus B_2$ são submódulos maximais de ${}_AA$ distintos. Segue que A não é local.

Reciprocamente, suponha que os únicos idempotentes de A sejam 0 e 1. Pelo Lema 2.1.6, todo idempotente de $A/\operatorname{rad}(A)$ é a projeção de 0 ou de 1. Logo, $A/\operatorname{rad}(A)$ também possui apenas os idempotentes triviais. Mas, pelo Teorema de Wedderburn, podemos escrever

$$\frac{A}{\operatorname{rad}(A)} \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r),$$

onde $D_1, \ldots, D_r$ são álgebras de divisão. A única forma de $A/\operatorname{rad}(A)$ ter apenas os idempotentes triviais é se $r = 1$ e $n_1 = 1$. Consequentemente, $A/\operatorname{rad}(A) \cong D_1$ é uma álgebra de divisão e, pelo item (2) da Proposição 2.1.4, A é local. □

Corolário 2.1.8. Um A-módulo U de dimensão finita é indecomponível se e somente se $\mathrm{End}_A(U)$ é local.

Demonstração: Como U tem dimensão finita, o mesmo vale para $\mathrm{End}_A(U)$. Assim, o resultado segue do Corolário 2.1.3 e da Proposição 2.1.7. □

Se U é um A-módulo indecomponível, a Proposição 2.1.4 e o Corolário 2.1.8 nos dão diversas propriedades de $\mathrm{End}_A(U)$. Além disso, olhar para os endomorfismos também nos permitirá decidir se um módulo é indecomponível ou não.

Também queremos entender como um módulo se escreve como soma direta de indecomponíveis. Se U é um A-módulo que não é indecomponível, então podemos escrever $U = U_1 \oplus U_2$ onde U_1 e U_2 são submódulos próprios. Se U_1 ou U_2 não é indecomponível, podemos mais uma vez decompor e, continuando assim, conseguimos escrever U como soma de indecomponíveis. Note que esse processo acaba pois U tem dimensão finita. O problema é que a forma em que "quebramos" cada módulo não é necessariamente única. O próximo teorema nos diz que, incrivelmente, o resultado final é essencialmente sempre o mesmo, independentemente das decomposições que escolhemos!

Teorema 2.1.9 (Krull-Schmidt)**.** Seja U um A-módulo não nulo e sejam

$$U = U_1 \oplus \cdots \oplus U_r = V_1 \oplus \cdots \oplus V_s$$

duas decomposições de U como soma direta de submódulos indecomponíveis. Então $r = s$ e, a menos de reordenação, U_i é isomorfo a V_i para todo $1 \leq i \leq r$.

Demonstração: Provaremos o resultado por indução no mínimo entre r e s. Se esse mínimo é 1, então U é indecomponível e só há um termo em cada decomposição, de onde segue o resultado. Se o mínimo é maior do que 1, vamos mostrar que, após uma reordenação, $U_1 \cong V_1$ e que U é a soma direta de U_1 com $V_2 \oplus \cdots \oplus V_s$. Dessa forma,

$$U_2 \oplus \cdots \oplus U_r \cong \frac{U}{U_1} \cong V_2 \oplus \cdots \oplus V_s$$

e o resultado seguirá da hipótese de indução.

Para todo i, sejam $\pi_i : U \to V_i$ as projeções e $\mu_i : V_i \to U$ as inclusões. Também denote por $\alpha : U \to U_1$ a projeção e por $\beta : U_1 \to U$ a inclusão. Note que

$$\mathrm{id}_{U_1} = \alpha\beta = \alpha \circ \mathrm{id}_U \circ \beta = \alpha \left(\sum_{i=1}^{s} \mu_i \pi_i \right) \beta = \sum_{i=1}^{s} \alpha \mu_i \pi_i \beta.$$

Como U_1 é indecomponível, $\mathrm{End}_A(U_1)$ é local. Usando o item (4) da Proposição 2.1.4, existe um índice $1 \leq i \leq s$ tal que $\alpha\mu_i\pi_i\beta$ é inversível. Reordenando $V_1, \ldots, V_s$, podemos supor que $i = 1$. Se $\varphi = \alpha\mu_1\pi_1\beta$, então $(\varphi^{-1}\alpha\mu_1)(\pi_1\beta) = \mathrm{id}_{U_1}$ e, pelo Exercício A.2.2, a imagem de $\pi_1\beta$ é um somando direto de V_1. Como $\pi_1\beta$ é um homomorfismo não nulo e V_1 é indecomponível, vale que $\pi_1\beta(U_1) = V_1$. Mas $\pi_1\beta$ é injetor e concluímos que $U_1 \cong V_1$.

Agora, como $\pi_1\beta$ é isomorfismo, a restrição de π_1 a U_1 é injetora. Por outro lado, π_1 anula $V_2 \oplus \cdots \oplus V_s$ e então devemos ter $U_1 \cap (V_2 \oplus \cdots \oplus V_s) = 0$. Com isso,

$$\begin{aligned}\dim_k(U_1 \oplus V_2 \oplus \cdots \oplus V_s) &= \dim_k U_1 + \dim_k(V_2 \oplus \cdots \oplus V_s) \\ &= \dim_k V_1 + \dim_k V_2 + \cdots + \dim_k V_s \\ &= \dim_k U\end{aligned}$$

e então $U = U_1 \oplus V_2 \oplus \cdots \oplus V_s$. Como observamos no início, isso conclui a demonstração. □

Corolário 2.1.10. Se U, V e W são A-módulos satisfazendo $U \oplus W \cong V \oplus W$, então $U \cong V$.

Demonstração: Escrevendo U, V e W como soma direta de indecomponíveis, o Teorema de Krull-Schmidt diz que os indecomponíveis que ocorrem em $U \oplus W$ são os mesmos (a menos de isomorfismo) que ocorrem em $V \oplus W$ e têm a mesma multiplicidade. Desconsiderando os indecomponíveis que constituem W, segue que U e V possuem a mesma decomposição como soma de indecomponíveis e, por isso, são isomorfos. □

Exemplo 2.1.11. Seja U um A-módulo não nulo. Suponha que U se escreve como a soma direta de dois submódulos próprios V e W. Pelo Exercício A.1.2, o radical de U é a soma dos radicais de V e W e, por isso, temos

$$\frac{U}{\mathrm{rad}(U)} \cong \frac{V}{\mathrm{rad}(V)} \oplus \frac{W}{\mathrm{rad}(W)}.$$

Assim, $U/\mathrm{rad}(U)$ não é simples. Analogamente, o soco de U também não é simples. Isso nos dá um critério: se $U/\mathrm{rad}(U)$ ou $\mathrm{soc}(U)$ é simples, então U é indecomponível. Por exemplo, suponha que G seja um p-grupo (com $p = \mathrm{char}(k) > 0$). Então kG possui apenas um único módulo simples, que é o trivial. Portanto, o soco de kG são os elementos fixos pela ação de G. Vimos na demonstração do Teorema de Maschke que o único submódulo trivial de kG é o subespaço gerado por $\sum_{g\in G} g$. Consequentemente, $\mathrm{soc}(kG)$ é simples e kG é indecomponível. Note que, pelo Exercício A.1.14, $kG/\mathrm{rad}(kG)$ também é isomorfo ao módulo trivial.

Exemplo 2.1.12. Seja $G = C_n$ o grupo cíclico de ordem n com gerador g. Supondo k algebricamente fechado e de característica $p > 0$, vamos mostrar que C_n possui exatamente n classes de isomorfismo de módulos indecomponíveis. Seja V um kC_n-módulo qualquer. Denote por $T : V \to V$ a ação de g em V. Escrevendo T na forma canônica de Jordan, podemos decompor V como uma soma direta

$$V = V_1 \oplus \cdots \oplus V_r$$

onde cada V_i é um bloco de Jordan para T. Mais especificamente, existe uma base $v_1, \ldots, v_d$ de V_i e um $\lambda \in k$ tal que $(T - \lambda I)(v_j) = v_{j+1}$, se $1 \leq j < d$, e $(T - \lambda I)(v_d) = 0$, onde I denota a identidade em V_i. Como cada V_i é invariante pela ação de g e C_n é gerado por g, vale que cada V_i é um submódulo de V. Além disso, V_i é indecomponível: todo submódulo não nulo de V_i possui um autovetor de T, mas há apenas o autovalor λ e o autoespaço correspondente tem dimensão 1, já que é gerado por v_d. Por isso, todo submódulo não nulo de V_i contém v_d e então a soma de quaisquer dois submódulos não nulos de V_i não pode ser direta.

Acabamos de mostrar que todo indecomponível é um bloco de Jordan de dimensão d e autovalor $\lambda \in k$. Entretanto, nem todo valor de d e λ nos dá um módulo sobre kC_n. Vamos estudar quais funcionam. Seja V um kC_n-módulo que é um bloco de Jordan para a transformação T induzida por g. Escreva $n = p^a m$, onde m não é divisível por p. Como $g^n = 1$, então $T^n = 1$ e o autovalor

λ é uma raiz n-ésima da unidade. Mas a característica de k é p, logo $0 = \lambda^n - 1 = (\lambda^m - 1)^{p^a}$ e λ é uma raiz m-ésima da unidade. Como p não divide m, o polinômio $x^m - 1$ tem exatamente m raízes em k: $\lambda_1 = \lambda, \lambda_2, \ldots, \lambda_m$. Assim,

$$T^m - 1 = (T - \lambda_1 I) \cdots (T - \lambda_m I) = (T - \lambda I)S,$$

onde S é um operador de V que comuta com T e é inversível, pois $\lambda_2, \ldots, \lambda_m$ não são autovalores de T. Logo,

$$0 = T^n - 1 = (T^m - 1)^{p^a} = (T - \lambda I)^{p^a} S^{p^a} \implies (T - \lambda I)^{p^a} = 0.$$

Como $(T - \lambda I)(v_j) = v_{j+1}$ para $1 \leq j < d$ e $(T - \lambda I)(v_d) = 0$, a dimensão d de V tem que satisfazer $d \leq p^a$.

Com isso, vemos que λ e d podem assumir até m e p^a valores, respectivamente, dando a possibilidade de até $p^a m = n$ módulos indecomponíveis. Vejamos que cada um desses valores funciona. Fixe λ uma raiz m-ésima da unidade e d um inteiro positivo com $d \leq p^a$. Seja V um espaço vetorial de dimensão d e T um operador em V de modo que V seja um bloco de Jordan de autovalor λ. Veja que $(T-\lambda I)^d = 0$, logo $(T-\lambda I)^{p^a} = 0$. Multiplicando pelo análogo do operador S definido anteriormente, segue que $(T^m - 1)^{p^a} = 0$, ou seja, $T^n = 1$ e, por isso, podemos definir uma estrutura de kC_n-módulo em V de modo que T corresponda à ação de g. Além disso, valores diferentes de λ e d dão origem a módulos diferentes, porque o bloco de Jordan é completamente determinado por seu autovalor e sua dimensão.

Uma observação interessante é que obtivemos, de outra forma, as representações irredutíveis de C_n. Se $d > 1$, o módulo associado ao bloco de Jordan sempre tem o subespaço gerado por $v_2, \ldots, v_d$ como um submódulo não trivial. Assim, os módulos simples são os blocos de Jordan com $d = 1$, que são exatamente os módulos que encontramos no Exemplo 1.3.15.

Para concluir o exemplo, vamos entender um pouco mais da estrutura dos módulos indecomponíveis calculando a série radical e a série de socos. Seja V o módulo indecomponível de dimensão d e autovalor λ. Em kC_n, temos $(g^m - 1)^{p^a} = g^n - 1 = 0$ e $g^m - 1$ é nilpotente. Como kC_n é uma álgebra comutativa, o ideal gerado por $g^m - 1$ também é nilpotente e, por isso, está contido em $\mathrm{rad}(kC_n)$. Agora, $(g^m - 1)V$ é o subespaço W gerado por $v_2, \ldots, v_d$, pois $(g - \lambda_2) \cdots (g - \lambda_m)V = V$ e $(g - \lambda)V = W$. Logo, W está contido no radical de V e, como tem codimensão 1, devemos ter $W = \mathrm{rad}(V)$. Mas W é o módulo indecomponível de dimensão $d - 1$ e autovalor λ e podemos repetir o argumento. Prosseguindo assim, construímos a série radical de V. Note que cada quociente é o módulo simples associado a λ. Para a série de socos, repare que $\mathrm{soc}(V)$ é a soma dos autoespaços de V (lembre como são os kC_n-módulos simples), logo o soco de V é o subespaço gerado por v_d. Dessa forma, as projeções de $v_1, \ldots, v_{d-1}$ formam uma base de $V/\mathrm{soc}(V)$ e, por isso, esse quociente também é um bloco de Jordan para λ. Assim, o soco de $V/\mathrm{soc}(V)$ é gerado por $v_{d-1} + \mathrm{soc}(V)$ e $\mathrm{soc}^2(V)$ é o subespaço gerado por v_{d-1} e v_d. Continuando assim, vemos que a série de socos de V é exatamente a sua série radical.

O que aconteceu ao final do último exemplo é um caso particular de algo mais geral:

Proposição 2.1.13. Se U é um A-módulo, então as seguintes afirmações são equivalentes:

(1) U possui uma única série de composição.

(2) As camadas radicais de U são simples.

(3) As camadas de soco de U são simples.

Demonstração: Suponha que vale (1) e seja

$$U = U_0 \supseteq U_1 \supseteq \cdots \supseteq U_n = 0$$

a única série de composição de U. Como toda cadeia de submódulos de U pode ser refinada a uma série de composição, U_1 é o único submódulo maximal de U e, por isso, $\operatorname{rad}(U) = U_1$. O mesmo argumento prova que U_2 é o único submódulo maximal de U_1 e temos $\operatorname{rad}^2(U) = \operatorname{rad}(U_1) = U_2$. Continuando assim, provamos que $\operatorname{rad}^i(U) = U_i$ para todo $1 \leq i \leq n$. Logo, a série radical de U é a série de composição acima, cujos quocientes são simples.

Reciprocamente, suponha que as camadas radicais de U sejam simples. Em particular, $U/\operatorname{rad}(U)$ é simples e $\operatorname{rad}(U)$ é maximal em U. Mas então $\operatorname{rad}(U)$ tem que ser o único submódulo maximal de U e toda série de composição de U começa em $U \supseteq \operatorname{rad}(U)$. Da mesma forma, $\operatorname{rad}^2(U)$ é maximal em $\operatorname{rad}(U)$ e concluímos que toda série de composição de $\operatorname{rad}(U)$ começa em $\operatorname{rad}(U) \supseteq \operatorname{rad}^2(U)$. Prosseguindo assim, provamos que a única série de composição de U é a sua série radical.

Estabelecemos a equivalência entre (1) e (2). Um argumento muito parecido funciona para mostrar que (1) e (3) são equivalentes. Nesse caso, começamos utilizando os últimos termos da série de composição ao invés dos primeiros. □

Um A-módulo que satisfaz as afirmações da Proposição 2.1.13 é chamado de **unisseriado**. Note que os únicos submódulos de um módulo unisseriado são aqueles que aparecem em sua única série de composição. Além disso, veja que todo módulo unisseriado é indecomponível. Reciprocamente, no Exemplo 2.1.12, vimos que todo kC_n-módulo indecomponível é unisseriado. Outro exemplo de módulo unisseriado é o $k\langle g\rangle$-módulo V_n do Exemplo 1.3.17 (veja também o Exercício A.1.22).

No Exemplo 2.1.12, vimos um grupo G cujo número de classes de isomorfismo de módulos indecomponíveis é exatamente $|G|$, que, nesse caso, é o número de classes de conjugação de G. Em característica zero, sabemos que todo indecomponível é simples e, por isso, o número de indecomponíveis também é o número de classes de conjugação. Poderíamos conjecturar que isso ocorre em geral. Entretanto, esse não é o caso. Na verdade, pode existir até mesmo um número infinito de indecomponíveis! Esse é o conteúdo do próximo exemplo.

Exemplo 2.1.14. Seja $G = C_p \times C_p$ o produto de dois grupos cíclicos de ordem p com geradores x e y, onde $p = \operatorname{char}(k) > 0$. Vamos construir infinitas representações indecomponíveis de $C_p \times C_p$ sobre k. Fixe um inteiro positivo n e seja V_n um k-espaço vetorial de dimensão $2n$ e base $v_1, \ldots, v_n, w_1, \ldots, w_n$. Definimos transformações lineares $X, Y : V_n \to V_n$ tais que

$$X(v_i) = w_i \text{ e } X(w_i) = 0, \text{ para } 1 \leq i \leq n,$$

e

$$Y(v_i) = w_{i+1}, \text{ para } 1 \leq i \leq n-1, \text{ e } Y(v_n) = Y(w_j) = 0, \text{ para } 1 \leq j \leq n.$$

É fácil ver que $X^2 = Y^2 = 0$, logo, se I denota a identidade de V_n, $(I+X)^p = I + X^p = I$ e, analogamente, $(I+Y)^p = I$. Como X e Y comutam (vale $XY = YX = 0$), o mesmo acontece para $I+X$ e $I+Y$. Por isso, V_n admite uma estrutura de $k[C_p \times C_p]$-módulo com $xv = (I+X)(v)$ e $yv = (I+Y)(v)$, para todo $v \in V_n$.

Vamos provar agora que V_n é indecomponível, de onde concluiremos que $k[C_p \times C_p]$ possui infinitas classes de isomorfismo de módulos indecomponíveis. Pelo Corolário 2.1.8, basta calcular $\operatorname{End}_{kG}(V_n)$ e mostrar que essa álgebra é local. Identificando os operadores lineares em V_n com matrizes $2n \times 2n$ sobre k (através da base $v_1, \ldots, v_n, w_1, \ldots, w_n$), obtemos que $\operatorname{End}_{kG}(V_n)$ é isomorfo ao subespaço de $M_{2n}(k)$ das matrizes que comutam com as matrizes que correspondem às ações de x e y. É imediato da definição que as representações matriciais de $I+X$ e $I+Y$ na base em questão são

$$\tilde{X} = \begin{pmatrix} I & 0 \\ I & I \end{pmatrix} \quad \text{e} \quad \tilde{Y} = \begin{pmatrix} I & 0 \\ N & I \end{pmatrix},$$

respectivamente, onde 0 é a matriz $n \times n$ nula, I é, abusando da notação, a matriz identidade de ordem n e N é a matriz triangular inferior $n \times n$ dada por

$$N = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

com 1's apenas abaixo da diagonal principal e 0's nas outras entradas.

Seja

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

uma matriz $2n \times 2n$ qualquer, onde A, B, C e D são matrizes $n \times n$. Como

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & 0 \\ I & I \end{pmatrix} = \begin{pmatrix} A+B & B \\ C+D & D \end{pmatrix}$$

e

$$\begin{pmatrix} I & 0 \\ I & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ A+C & B+D \end{pmatrix},$$

a condição $M\tilde{X} = \tilde{X}M$ é equivalente a $A = D$ e $B = 0$. Por sua vez, as igualdades

$$\begin{pmatrix} A & 0 \\ C & A \end{pmatrix} \begin{pmatrix} I & 0 \\ N & I \end{pmatrix} = \begin{pmatrix} A & 0 \\ C+AN & A \end{pmatrix}$$

e

$$\begin{pmatrix} I & 0 \\ N & I \end{pmatrix} \begin{pmatrix} A & 0 \\ C & A \end{pmatrix} = \begin{pmatrix} A & 0 \\ NA+C & A \end{pmatrix}$$

implicam que as matrizes que comutam com $\tilde{X}$ e $\tilde{Y}$ são precisamente as matrizes da forma

$$\begin{pmatrix} A & 0 \\ C & A \end{pmatrix}$$

com $AN = NA$. Não é difícil verificar que as matrizes satisfazendo $AN = NA$ são exatamente as matrizes triangulares inferiores com diagonais constantes, ou seja, da forma

$$A = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 & 0 \\ \lambda_2 & \lambda_1 & 0 & \cdots & 0 & 0 \\ \lambda_3 & \lambda_2 & \lambda_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \lambda_{n-1} & \lambda_{n-2} & \lambda_{n-3} & \cdots & \lambda_1 & 0 \\ \lambda_n & \lambda_{n-1} & \lambda_{n-2} & \cdots & \lambda_2 & \lambda_1 \end{pmatrix},$$

com $\lambda_1, \ldots, \lambda_n \in k$.

Como observamos no começo, podemos identificar $\mathrm{End}_{kG}(V_n)$ com o espaço das matrizes da forma descrita anteriormente. Como A é constante na diagonal principal, as matrizes de $\mathrm{End}_{kG}(V_n)$ com diagonal principal nula formam um subespaço de codimensão 1. Mas esse subespaço é a interseção de $\mathrm{End}_{kG}(V_n)$ com $\mathrm{rad}(T_{2n}(k))$ (veja o Exemplo 1.1.11) e, por isso, é um ideal nilpotente e está contido em $\mathrm{rad}(\mathrm{End}_{kG}(V_n))$. Por causa da dimensão, devemos ter então que $\mathrm{rad}(\mathrm{End}_{kG}(V_n))$ é exatamente o subespaço de matrizes de diagonal principal nula. Mas então, novamente pela dimensão, $\mathrm{rad}(\mathrm{End}_{kG}(V_n))$ é ideal à esquerda maximal e $\mathrm{End}_{kG}(V_n)$ tem que ser local, de onde concluímos que V_n é indecomponível.

Observação 2.1.15. É importante ressaltar que os módulos construídos no Exemplo 2.1.14 não representam todas as classes de isomorfismo de módulos indecomponíveis sobre $k[C_p \times C_p]$. Por exemplo, se k é infinito, também conseguimos construir infinitos módulos indecomponíveis dois a dois não isomorfos e todos eles de dimensão 2 (veja o Exercício A.2.3).

Dizemos que uma álgebra A tem **tipo de representação finito** se há apenas um número finito de classes de isomorfismo de A-módulos indecomponíveis. Como acabamos de ver, kG pode não ter tipo de representação finito mesmo para grupos muito simples, como é o caso de $G = C_2 \times C_2$ em característica 2. Porém, ainda sabemos decidir facilmente quando um grupo tem um número finito de representações indecomponíveis! O Teorema 3.2.7 nos diz que basta verificar se um p-subgrupo de Sylow de G é cíclico! Ainda não temos ferramentas para demonstrar esse resultado, então ele ficará para o próximo capítulo.

2.2 Módulos projetivos

Já vimos que pode ser muito complicado descrever todos os módulos indecomponíveis sobre uma álgebra A. Por isso, vamos focar mais no estudo dos somandos indecomponíveis da representação regular ${}_AA$. Nesse contexto, seremos levados a definir módulos projetivos e veremos suas propriedades.

Comecemos com os módulos isomorfos a $A^n = A \oplus \cdots \oplus A$ para algum $n \geq 0$, os chamados **módulos livres**. Esses são os módulos que possuem uma **base**, isto é, um conjunto gerador $\{x_1, \ldots, x_n\}$ (que gera como módulo) que é linearmente independente sobre A, ou seja, se $a_1, \ldots, a_n \in A$, então

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0 \iff a_1 = a_2 = \cdots = a_n = 0.$$

Se U é um A-módulo livre de base $B = \{x_1, \ldots, x_n\}$ e V é um A-módulo qualquer, veja que toda função de B em V se estende unicamente a um homomorfismo de U em V. Reciprocamente, se U possui um subconjunto B com a propriedade descrita anteriormente, então B é base de U e U é livre. As verificações de todas essas afirmações são rotineiras e deixamos a cargo do leitor.

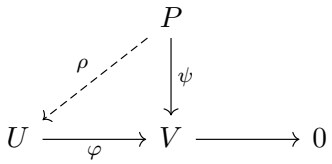
O próximo resultado caracteriza o principal objeto de estudo desta seção.

Proposição 2.2.1. Se P é um A-módulo, então são equivalentes as seguintes afirmações:

(1) P é um somando direto de um módulo livre.

(2) Todo homomorfismo sobrejetor $\varphi : U \to P$ cinde[1].

(3) Se $\varphi : U \to V$ é um homomorfismo sobrejetor e $\psi : P \to V$ é um homomorfismo qualquer, então existe um homomorfismo $\rho : P \to U$ que faz o seguinte diagrama comutar:



Dizemos que um A-módulo P é **projetivo** se satisfaz as afirmações da Proposição 2.2.1. No diagrama apresentado, o homomorfismo nulo está explícito para dar a ideia de que a linha inferior é exata e, por isso, de que φ é sobrejetor. A última caracterização pode ser lembrada como: todo homomorfismo de P em um quociente de U pode ser estendido a um homomorfismo de P em U.

[1] Dizemos que um homomorfismo sobrejetor $\varphi : U \to V$ **cinde** se existe um homomorfismo $\psi : V \to U$ tal que $\varphi\psi = \mathrm{id}_V$. Nesse caso, também dizemos que ψ é um homomorfismo injetor que cinde. Equivalentemente, φ cinde (resp., ψ cinde) quando $\ker\varphi$ (resp., $\operatorname{im}\psi$) é um somando direto de U (veja o Exercício A.2.2).

Demonstração: (1) $\implies$ (3). Suponha que P seja um somando direto de um módulo livre F com base $B = \{x_1, \ldots, x_n\}$. Se $\pi : F \to P$ é a projeção, existem $u_1, \ldots, u_n \in U$ tais que

$$\varphi(u_i) = \psi(\pi(x_i))$$

para todo i, porque φ é sobrejetor. Mas B é base de F, então podemos definir um homomorfismo $\rho' : F \to U$ que leva x_i em u_i. Segue que $\varphi\rho' = \psi\pi$, logo, tomando ρ como a restrição de ρ' a P, concluímos que $\varphi\rho = \psi$. Portanto, encontramos um homomorfismo que faz o diagrama comutar.

(3) $\implies$ (2). Seja $\varphi : U \to P$ um homomorfismo sobrejetor. Tomando $V = P$ e $\psi = \mathrm{id}_P$, a propriedade em (3) nos dá um homomorfismo $\rho : P \to U$ tal que $\varphi\rho = \psi = \mathrm{id}_P$. Isso prova que φ cinde.

(2) $\implies$ (1). Se P é gerado por n elementos (como módulo), então existe um homomorfismo sobrejetor $\varphi : A^n \to P$, já que A^n é livre. Por (2), φ cinde, logo existe um submódulo P' de A^n tal que $A^n = \ker\varphi \oplus P'$. Pelo Teorema do Isomorfismo,

$$P \cong A^n/\ker\varphi \cong P',$$

ou seja, P é (isomorfo a) um somando direto de um módulo livre. □

Repare que os módulos projetivos indecomponíveis são os somandos diretos indecomponíveis do módulo regular ${}_AA$. Isso segue do Teorema de Krull-Schmidt.

Observação 2.2.2. Pela Proposição 2.1.2, um módulo projetivo indecomponível U corresponde a um idempotente primitivo e de $\mathrm{End}_A({}_AA)$. Mas sabemos do Lema 1.2.3 que $\mathrm{End}_A({}_AA) \cong A^{\mathrm{op}}$ e, portanto, podemos supor que e está em A. Se U for um somando direto de ${}_AA$, então a Proposição 2.1.2 juntamente com as identificações nos dão $U = Ae$. Porém, idempotentes primitivos distintos em A podem dar origem a módulos projetivos indecomponíveis isomorfos e, assim, não há uma correspondência biunívoca.

Exemplo 2.2.3. Seja $G = S_3$ e k um corpo algebricamente fechado[1] de característica 2. Vamos decompor kS_3 como soma de (projetivos) indecomponíveis!

Começamos observando que o módulo trivial é a única representação unidimensional de S_3 sobre k. De fato, uma representação unidimensional é determinada por um homomorfismo de grupos $\varphi : S_3 \to k^\times$. Como k tem característica 2, o seu grupo multiplicativo não possui elementos de ordem 2 e então $\varphi((1\ 2)) = 1$. Por outro lado, $(1\ 2\ 3)$ está no subgrupo de comutadores de S_3 e, como $k^\times$ é abeliano, também temos $\varphi((1\ 2\ 3)) = 1$. Como S_3 é gerado pelos dois elementos destacados, φ é o homomorfismo trivial e dá origem ao módulo trivial.

Seja V a representação de dimensão 2 construída no Exemplo 1.3.4. Ela também é simples! De fato, se não fosse, possuiria um submódulo de dimensão 1, que seria trivial pelo que acabamos de ver. Mas é fácil ver que 1 não é autovalor da ação de $(1\ 2\ 3)$ em V. Já veremos que V e o módulo trivial são os únicos módulos simples sobre kS_3.

Seja $\omega \in k$ uma raiz cúbica primitiva da unidade e considere[2] os seguintes elementos de kS_3:

$$\begin{aligned} e_1 &= 1 + (1\ 2\ 3) + (1\ 3\ 2), \\ e_2 &= 1 + \omega(1\ 2\ 3) + \omega^2(1\ 3\ 2), \\ e_3 &= 1 + \omega^2(1\ 2\ 3) + \omega(1\ 3\ 2). \end{aligned}$$

[1] Se tomarmos k como sendo o corpo de 4 elementos, o exemplo continua funcionando. Só precisamos que k tenha raízes cúbicas da unidade.

[2] Por que eu consideraria esses elementos? A ideia é que queremos encontrar idempotentes ortogonais de kS_3. É mais fácil fazer isso para o subgrupo gerado por $(1\ 2\ 3)$, porque ele é abeliano. Note que os coeficientes dos e_i's são os valores dos caracteres irredutíveis de tal subgrupo. Sabe-se que esse exemplo funciona em $\mathbb{C}$, então por que não tentar aqui?

Não é difícil verificar que e_1, e_2 e e_3 são idempotentes dois a dois ortogonais. Como $e_1 + e_2 + e_3 = 3 = 1$, a observação anterior a esse exemplo juntamente com a Proposição 2.1.2 nos dá a decomposição

$$kS_3 = (kS_3)e_1 \oplus (kS_3)e_2 \oplus (kS_3)e_3.$$

Como $(1\ 2)e_i$ não é múltiplo de e_i, vemos que cada um dos somandos acima tem dimensão pelo menos 2. Mas $\dim_k kS_3 = 6$ e então a dimensão de cada somando deve ser exatamente 2. Além disso, $(kS_3)e_i$ é indecomponível, pois, caso contrário, seria a soma de duas representações unidimensionais e então seria trivial, o que não é o caso, já que e_i não é fixo por $(1\ 2)$. Ou seja, conseguimos escrever kS_3 como soma direta de indecomponíveis!

Vamos estudar os projetivos indecomponíveis que apareceram. Já vimos outras vezes que o submódulo dos elementos de kS_3 fixos pela ação de S_3 é gerado por

$$\sum_{g \in S_3} g = e_1 + (1\ 2)e_1 \in (kS_3)e_1.$$

Isso nos diz que $(kS_3)e_1$ não é simples e seu soco é o módulo trivial. Por causa da dimensão, o quociente de $(kS_3)e_1$ pelo soco também é trivial e, pela Proposição 2.1.13, $(kS_3)e_1$ é unisseriado e seu único submódulo não trivial é seu soco. Agora, isso também nos diz que $(kS_3)e_2$ e $(kS_3)e_3$ não possuem submódulos unidimensionais e, portanto, são simples. Ainda vale mais: o isomorfismo linear de $(kS_3)e_2$ em $(kS_3)e_3$ que leva e_2 em $(1\ 2)e_3$ e $(1\ 2)e_2$ em e_3 é um isomorfismo de kS_3-módulos! É necessário realizar algumas contas para constatar isso, mas nada muito complicado. Por fim, não é difícil concluir a partir do que já temos que os fatores de composição de kS_3 são o módulo trivial e $(kS_3)e_2$, cada um aparecendo com multiplicidade 2. Por isso, kS_3 possui apenas dois módulos simples: um de dimensão 1 e outro de dimensão 2. Disso segue que $(kS_3)e_2$ e $(kS_3)e_3$ são isomorfos ao módulo V que construímos anteriormente!

Supor que um módulo indecomponível é projetivo já nos dá muita informação! Isso será exemplificado especialmente pelo próximo resultado.

Teorema 2.2.4. Se P é um A-módulo projetivo indecomponível, então $P/\operatorname{rad}(P)$ é simples. Mais ainda, associar P a $P/\operatorname{rad}(P)$ nos dá uma correspondência biunívoca entre classes de isomorfismo de A-módulos projetivos indecomponíveis e classes de isomorfismo de A-módulos simples.

Demonstração: A nossa estratégia para mostrar que $P/\operatorname{rad}(P)$ é simples será mostrar que $\operatorname{End}_A(P/\operatorname{rad}(P))$ é local. Isso implicará que $P/\operatorname{rad}(P)$ é indecomponível pelo Corolário 2.1.8, mas, como esse módulo também é semissimples, seguirá que $P/\operatorname{rad}(P)$ é simples. Agora, como estamos supondo P indecomponível, já temos que $\operatorname{End}_A(P)$ é local. Usaremos a projetividade de P para provar que $\operatorname{End}_A(P/\operatorname{rad}(P))$ é quociente de $\operatorname{End}_A(P)$. Como quociente de álgebra local também é local (por exemplo, isso segue sem dificuldade da caracterização (3) na Proposição 2.1.4), concluiremos o que queremos e estará provada a primeira parte do teorema.

Vamos encontrar um homomorfismo de álgebras sobrejetor de $\operatorname{End}_A(P)$ em $\operatorname{End}_A(P/\operatorname{rad}(P))$. Temos uma construção bem natural: se $\varphi : P \to P$ é homomorfismo de módulos, então

$$\varphi(\operatorname{rad}(P)) = \varphi(\operatorname{rad}(A)P) = \operatorname{rad}(A)\varphi(P) \subseteq \operatorname{rad}(A)P = \operatorname{rad}(P)$$

e podemos definir $\overline{\varphi} : P/\operatorname{rad}(P) \to P/\operatorname{rad}(P)$ por $\overline{\varphi}(x + \operatorname{rad}(P)) = \varphi(x) + \operatorname{rad}(P)$. É fácil ver que a função que leva φ em $\overline{\varphi}$ é um homomorfismo de álgebras de $\operatorname{End}_A(P)$ em $\operatorname{End}_A(P/\operatorname{rad}(P))$. Resta demonstrar a sobrejetividade. Seja $\psi : P/\operatorname{rad}(P) \to P/\operatorname{rad}(P)$ um homomorfismo qualquer. Denotando por $\pi : P \to P/\operatorname{rad}(P)$ a projeção canônica, temos o seguinte diagrama:

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle \psi\pi} & & \\ P & \xrightarrow{\pi} & \frac{P}{\operatorname{rad}(P)} & \longrightarrow & 0 \end{array}$$

Como P é projetivo, a caracterização (3) da Proposição 2.2.1 nos dá um homomorfismo $\varphi : P \to P$ tal que $\pi\varphi = \psi\pi$. Mas então

$$\psi(x + \operatorname{rad}(P)) = \psi(\pi(x)) = \pi(\varphi(x)) = \varphi(x) + \operatorname{rad}(P) = \overline{\varphi}(x + \operatorname{rad}(P))$$

para todo $x \in P$ e temos $\psi = \overline{\varphi}$, como preciso.

Agora, para provar a correspondência do enunciado, vamos mostrar separadamente a "injetividade" e a "sobrejetividade" da associação que leva P em $P/\operatorname{rad}(P)$. A primeira parte consiste em mostrar que se P e Q são módulos projetivos indecomponíveis tais que $P/\operatorname{rad}(P) \cong Q/\operatorname{rad}(Q)$, então $P \cong Q$. Se $\pi_P : P \to P/\operatorname{rad}(P)$ e $\pi_Q : Q \to Q/\operatorname{rad}(Q)$ são as projeções canônicas e $\psi : P/\operatorname{rad}(P) \to Q/\operatorname{rad}(Q)$ é um isomorfismo, então podemos utilizar um argumento análogo ao usado no parágrafo anterior para encontrar um homomorfismo $\varphi : P \to Q$ tal que $\pi_Q\varphi = \psi\pi_P$. Aqui, utilizamos que P é projetivo. Assim, temos o seguinte diagrama comutativo:

$$\begin{array}{ccc} P & \xrightarrow{\varphi} & Q \\ {\scriptstyle \pi_P}\downarrow & & \downarrow{\scriptstyle \pi_Q} \\ \frac{P}{\operatorname{rad}(P)} & \xrightarrow[\psi]{} & \frac{Q}{\operatorname{rad}(Q)} \end{array}$$

Se $\varphi(P) \subseteq \operatorname{rad}(Q)$, então a imagem de $\pi_Q\varphi$ seria 0, mas $\pi_Q\varphi = \psi\pi_P$ é a composição dos mapas sobrejetores π_P e ψ, uma contradição! Por isso, a imagem de φ não pode estar contida em $\operatorname{rad}(Q)$. Mas $Q/\operatorname{rad}(Q)$ é simples, porque Q é projetivo e indecomponível, então $\operatorname{rad}(Q)$ é maximal em Q e tem que ser o único submódulo maximal de Q. Assim, $\varphi(P) \not\subseteq \operatorname{rad}(Q)$ implica que $\varphi(P) = Q$ e φ é sobrejetor. Como Q é projetivo, o item (2) da Proposição 2.2.1 diz que φ é um homomorfismo sobrejetor que cinde. Logo, $\ker\varphi$ é somando direto de P. Mas P é indecomponível e φ não é nulo, então temos $\ker\varphi = 0$ e φ é injetor. Segue que φ é isomorfismo e $P \cong Q$, como queríamos.

Para acabar, resta mostrar que todo módulo simples é da forma $P/\operatorname{rad}(P)$ para algum módulo projetivo indecomponível P. Seja S um A-módulo simples qualquer. Como ${}_AA$ é livre e S é gerado por qualquer elemento não nulo, existe um homomorfismo sobrejetor $\varphi : {}_AA \to S$. Escrevendo ${}_AA$ como soma direta de indecomponíveis, existe algum $P \leq {}_AA$ projetivo e indecomponível tal que $\varphi(P) \neq 0$. Como S é simples, a restrição de φ a P é sobrejetora. Como $\operatorname{rad}(S) = 0$, $\operatorname{rad}(P)$ está no núcleo de φ e segue que S é imagem homomorfa de $P/\operatorname{rad}(P)$. Mas $P/\operatorname{rad}(P)$ é simples, de onde concluímos que $P/\operatorname{rad}(P) \cong S$. □

Chamaremos o módulo projetivo indecomponível associado a um módulo simples S de **cobertura projetiva** de S. É possível dar um sentido mais geral para o conceito de cobertura projetiva e faremos isso na Seção 5.3. Por enquanto, a definição dada será suficiente. Apenas ressaltaremos uma propriedade de coberturas projetivas que apareceu na demonstração do Teorema 2.2.4.

Lema 2.2.5. Seja U um A-módulo. Se $U/\operatorname{rad}(U)$ é simples, então U é um quociente da cobertura projetiva de $U/\operatorname{rad}(U)$.

Demonstração: Seja P a cobertura projetiva de $U/\operatorname{rad}(U)$. Na prova do Teorema 2.2.4, onde se mostra a "injetividade" da correspondência, troque Q por U. Com isso, obtemos um mapa $\varphi : P \to U$ e a demonstração continua funcionando até o momento onde se prova a sobrejetividade de φ. Pelo Teorema do Isomorfismo, U é um quociente de P. □

Corolário 2.2.6. Sejam $S_1, \ldots, S_r$ todos os A-módulos simples e denote por n_i a multiplicidade de S_i como somando de $A/\operatorname{rad}(A)$. Se P_i é a cobertura projetiva de S_i, então

$${}_AA \cong P_1^{n_1} \oplus \cdots \oplus P_r^{n_r}.$$

Demonstração: Decompondo ${}_AA$ como soma direta de indecomponíveis, sabemos que

$$ {}_AA \cong P_1^{m_1} \oplus \cdots \oplus P_r^{m_r} $$

para certos inteiros positivos $m_1, \ldots, m_r$. Vendo a soma direta acima dentro de A, podemos multiplicar a expressão por $\operatorname{rad}(A)$ para obter

$$ \operatorname{rad}(A) = \operatorname{rad}(P_1)^{m_1} \oplus \cdots \oplus \operatorname{rad}(P_n)^{m_n}. $$

Logo,

$$ \frac{A}{\operatorname{rad}(A)} \cong \left(\frac{P_1}{\operatorname{rad}(P_1)}\right)^{m_1} \oplus \cdots \oplus \left(\frac{P_r}{\operatorname{rad}(P_r)}\right)^{m_r}. $$

Mas sabemos que $P_i/\operatorname{rad}(P_i) \cong S_i$, então devemos ter $m_i = n_i$ para todo $1 \leq i \leq r$, como queríamos. □

Quando k é algebricamente fechado, é fácil descobrir a multiplicidade n_i do corolário acima: ela é exatamente a dimensão de S_i sobre k (veja o Corolário 1.2.9).

A partir de agora, focaremos no caso particular das álgebras de grupo. Veremos alguns resultados e calcularemos alguns exemplos.

Proposição 2.2.7. Se P é um kG-módulo projetivo e H é um subgrupo de G, então a restrição P_H é um kH-módulo projetivo.

Demonstração: Como P é um somando direto de $(kG)^n$ para algum $n \geq 0$, também temos que P_H é um somando direto de $(kG)^n_H$. Logo, é suficiente mostrar que $(kG)_H$ é um kH-módulo livre. Sejam $g_1, \ldots, g_r \in G$ representantes das classes laterais à direita de H em G. Vendo cada Hg_i como um subconjunto de kG, considere kHg_i como sendo o subespaço de kG gerado por Hg_i. Como as classes laterais particionam G, é fácil ver que $kG = kHg_1 \oplus \cdots \oplus kHg_r$. Assim, é suficiente mostrar que kHg_i é invariante sob a ação de H (ou seja, que kHg_i é um kH-submódulo de $(kG)_H$) e que $kHg_i \cong kH$. De fato, é fácil ver que $hHg_i = Hg_i$ para todo $h \in H$, logo kHg_i é invariante sob H. Além disso, o isomorfismo linear $\varphi : kH \to kHg_i$ que leva $h \in H$ em $hg_i \in Hg_i$ é claramente um isomorfismo de kH-módulos. □

Observação 2.2.8. A demonstração anterior pode ser pensada como uma outra forma do Teorema de Lagrange. Para provar esse teorema da teoria de grupos, mostramos que G é uma união de conjuntos disjuntos e de tamanho igual a $|H|$. Dessa vez, mostramos que $(kG)_H$ é uma soma direta de kH-módulos isomorfos a kH. "Linearizamos" as classes laterais e, assim, elas evoluem de meros conjuntos a kH-módulos.

Corolário 2.2.9. Suponha que $p = \operatorname{char}(k) > 0$. Se G possui ordem $p^a m$, onde m não é múltiplo p, então a dimensão de todo kG-módulo projetivo é divisível por p^a.

Demonstração: Seja H um p-subgrupo de Sylow de G. Como vimos no Exemplo 2.1.11, kH é um kH-módulo indecomponível e, por isso, é o único kH-módulo projetivo indecomponível. Assim, todo outro kH-módulo projetivo é soma direta de cópias de kH e é livre. Se P é um kG-módulo projetivo, a Proposição 2.2.7 diz que P_H é kH-módulo projetivo. Consequentemente, $P_H \cong (kH)^n$ para algum $n \geq 0$ e

$$ \dim_k P = \dim_k P_H = \dim_k (kH)^n = n \cdot \dim_k kH = n \cdot p^a, $$

provando o resultado. □

Compare esse corolário com o que encontramos no Exemplo 2.2.3. Já temos mais alguma informação sobre os projetivos indecomponíveis de kG. Inclusive, ela já é suficiente para determinarmos os projetivos indecomponíveis de grupos cíclicos!

Exemplo 2.2.10. Suponha que k seja algebricamente fechado e de característica $p > 0$ e seja $G = C_n$ o grupo cíclico de ordem $n = p^a m$, com m não divisível por p. Vimos no Exemplo 2.1.12 que os módulos indecomponíveis sobre kC_n são exatamente os "blocos de Jordan" cujo autovalor $\lambda \in k$ é uma raiz m-ésima da unidade e cuja dimensão d satisfaz $1 \leq d \leq p^a$. Pelo Corolário 2.2.9, os projetivos indecomponíveis são precisamente os blocos de Jordan de dimensão p^a. No Exemplo 2.1.12, também conseguimos descrever bem a estrutura de cada um dos indecomponíveis e, com isso, é fácil ver que o módulo projetivo indecomponível de autovalor λ é a cobertura projetiva do módulo simples associado a λ. Por fim, como todo kC_n-módulo simples é unidimensional, segue do Corolário 2.2.6 que cada projetivo indecomponível aparece exatamente uma vez numa decomposição de kC_n como soma de indecomponíveis. Com isso, já sabemos basicamente tudo sobre a estrutura do módulo regular kC_n!

Faremos mais um exemplo importante antes de terminar a seção. Assumiremos $p > 0$ a partir de agora. Veremos o que acontece quando o p-subgrupo de Sylow de G é normal e cíclico. Pelo Teorema de Schur-Zassenhaus[1], G é o produto semidireto do p-subgrupo de Sylow e outro subgrupo cuja ordem não é divisível por p. Em certo sentido, isso nos permite isolar a parte de G mais "problemática" e, intuitivamente, esse caso deve ser mais fácil que o caso geral. Precisamos de um resultado preliminar:

Lema 2.2.11. Se N é um p-subgrupo de Sylow normal de G e U é um kG-módulo, então $\operatorname{rad}(U) = \operatorname{rad}(U_N)$. Além disso, se N também é cíclico, então $\operatorname{rad}(U) = (1-x)U$, onde x é um gerador de N.

Demonstração: Como N é normal em G, a conjugação de kN por algum $g \in G$ define um automorfismo de álgebra de kN. Em particular, esse automorfismo leva o radical no radical, ou seja, $g \operatorname{rad}(kN) g^{-1} = \operatorname{rad}(kN)$ para todo $g \in G$. Por isso,

$$g \operatorname{rad}(U_N) = g \operatorname{rad}(kN) U = (g \operatorname{rad}(kN) g^{-1})(gU) = \operatorname{rad}(kN) U = \operatorname{rad}(U_N)$$

para todo $g \in G$, mostrando que $\operatorname{rad}(U_N)$ é um kG-submódulo de U. Vamos mostrar que $U/\operatorname{rad}(U_N)$ é um kG-módulo semissimples, o que mostrará a inclusão $\operatorname{rad}(U) \subseteq \operatorname{rad}(U_N)$. Como $U/\operatorname{rad}(U_N)$ é semissimples como kN-módulo e N é um p-grupo, N age trivialmente nesse quociente. Por isso, $U/\operatorname{rad}(U_N)$ é um $k[G/N]$-módulo naturalmente[2]. Mas p não divide a ordem de G/N, logo, pelo Teorema de Maschke, $U/\operatorname{rad}(U_N)$ é um $k[G/N]$-módulo semissimples e, restringindo escalares a G, vemos que esse quociente é semissimples como kG-módulo também, como queríamos. Para provar a inclusão contrária, note que $U/\operatorname{rad}(U)$ é semissimples como kN-módulo pelo Teorema de Clifford, logo $\operatorname{rad}(U_N) \subseteq \operatorname{rad}(U)$. Disso tudo concluímos a primeira afirmação do enunciado.

Agora suponha que N seja cíclico e gerado por um $x \in N$. Veja que $(1-x)U$ é um kN-submódulo de U_N, já que N é abeliano. Além disso, é imediato que x (e portanto N) age trivialmente em $U/(1-x)U$, logo esse quociente é um kN-módulo semissimples e temos $\operatorname{rad}(U_N) \subseteq (1-x)U$. Por outro lado, $1-x$ anula o único kN-módulo simples, que é o trivial, e deve estar em $\operatorname{rad}(kN)$. Com isso,

$$(1-x)U \subseteq \operatorname{rad}(kN)U = \operatorname{rad}(U_N),$$

concluindo a demonstração[3]. □

Exemplo 2.2.12. Suponha que G possua um p-subgrupo de Sylow N normal, cíclico e de ordem p^a $(a \geq 1)$. Vamos descrever a estrutura de um kG-módulo projetivo indecomponível através do

[1] Esse teorema famoso diz que se N é um subgrupo normal de G tal que sua ordem e a ordem de G/N não possuem fatores em comum, então N possui um complemento em G ou, equivalentemente, G é isomorfo a um produto semidireto de N e G/N.

[2] Para ver isso, é mais fácil lidar com a definição de representação como um homomorfismo de G em $\mathrm{GL}(U/\operatorname{rad}(U_N))$. Nesse caso, N está contido no núcleo desse homomorfismo e podemos passar ao quociente.

[3] Essa segunda afirmação do enunciado também segue sabendo-se que $1-x$ gera $\operatorname{rad}(kN)$ (Exercício A.1.15).

seu módulo simples associado. Seja S um kG-módulo simples de dimensão d e P a sua cobertura projetiva. Vamos começar mostrando que P tem comprimento radical p^a e que cada camada radical tem dimensão d. Pelo Lema 2.2.11, é suficiente mostrar que isso vale para P_N, pois P e P_N possuem a mesma série radical. Como P é projetivo, vimos na demonstração do Corolário 2.2.9 que $P_N \cong (kN)^n$ para algum $n \geq 0$. Como kN é indecomponível (Exemplo 2.1.11), segue do Teorema 2.2.4 que $kN/\operatorname{rad}(kN)$ é um kN-módulo simples e portanto trivial. Logo,

$$\dim_k \frac{P_N}{\operatorname{rad}(P_N)} = \dim_k \frac{(kN)^n}{\operatorname{rad}((kN)^n)} = \dim_k \left(\frac{kN}{\operatorname{rad}(kN)}\right)^n = n \cdot \dim_k \frac{kN}{\operatorname{rad}(kN)} = n.$$

Mas $\operatorname{rad}(P_N) = \operatorname{rad}(P)$, então

$$d = \dim_k S = \dim_k \frac{P}{\operatorname{rad}(P)} = \dim_k \frac{P_N}{\operatorname{rad}(P_N)} = n.$$

Com isso, $P_N \cong (kN)^d$. Agora, como N é cíclico, os Exemplos 2.1.12 e 2.2.10 nos dizem que a dimensão dos termos da série radical de kN cai de 1 em 1. Por isso, a dimensão dos termos da série radical de $P_N \cong (kN)^d$ cai de d em d, ou seja, as camadas radicais de P_N têm dimensão d. Como $\dim_k P_N = \dim_k (kN)^d = p^a d$, o comprimento radical de P_N deve ser p^a.

Nosso próximo objetivo será determinar explicitamente as camadas radicais de P. Já veremos que cada uma delas pode ser obtida de S modificando ligeiramente a ação de G. Para deixar isso mais preciso, devemos começar com o caso do módulo trivial k. Se Q é a cobertura projetiva de k, então $Q/\operatorname{rad}(Q) \cong k$ e, pelo que acabamos de provar, $W := \operatorname{rad}(Q)/\operatorname{rad}^2(Q)$ também tem dimensão 1 (note que $W \neq 0$ porque o comprimento radical de Q é $p^a \geq 2$). Veja que W é submódulo de $M := Q/\operatorname{rad}^2(Q)$ e que $M/W \cong k$. Além disso, M não é semissimples, pois $\operatorname{rad}^2(Q) \subsetneq \operatorname{rad}(Q)$. Voltando ao caso geral, provaremos que as camadas radicais de P são[1]

$$S,\ S \otimes W,\ S \otimes W \otimes W,\ \ldots,\ S \otimes W^{\otimes p^a - 1}.$$

Como W tem dimensão 1, um elemento $g \in G$ age em W por multiplicação por algum escalar $\lambda_g \in k$. Por isso, $S \otimes W^{\otimes i}$ é isomorfo a S como espaço vetorial, mas a ação de g em $S \otimes W^{\otimes i}$ corresponde a aplicar g em S e depois multiplicar pelo escalar λ_g^i. Essa é a alteração na ação de G em S que nos referimos anteriormente.

Comecemos mostrando que $S \otimes W$ é simples. Para isso, defina W' como sendo um k-espaço vetorial de dimensão 1 e faça $g \in G$ agir em W' por multiplicação por λ_g^{-1}. Isso define[2] uma estrutura de kG-módulo em W' e é imediato que $W \otimes W' \cong k$. Portanto[3],

$$(S \otimes W) \otimes W' \cong S \otimes (W \otimes W') \cong S \otimes k \cong S.$$

Assim, se $S \otimes W$ possuísse um submódulo não trivial U, então $U \otimes W'$ seria um submódulo não trivial de $(S \otimes W) \otimes W' \cong S$, o que é impossível porque S é simples. Logo, $S \otimes W$ é de fato simples. Vejamos agora que $S \otimes M$ não é semissimples. Como M não é semissimples, o Lema 2.2.11 diz que $(1-x)M \neq 0$, onde x é um gerador de N. Tome $m \in M$ com $(1-x)m \neq 0$ e $s \in S$ um elemento não nulo qualquer. Como N é um p-subgrupo normal de G, o Teorema de Clifford diz que S_N é semissimples e, por isso, N age trivialmente em S, de modo que

$$(1-x)(s \otimes m) = s \otimes m - xs \otimes xm = s \otimes m - s \otimes xm = s \otimes (1-x)m.$$

[1] Para entender de fato os módulos listados, é importante conhecer explicitamente quem é W. Isso pode ser feito sem conhecer Q (veja o Exercício A.2.9).

[2] A estrutura de kG-módulo de W equivale a um homomorfismo $\varphi : G \to k^\times$, que leva g em λ_g. Compondo com o mapa de inversão em G, continuamos com um homomorfismo (pois $k^\times$ é abeliano), que desta vez dá origem à estrutura desejada de kG-módulo em W'.

[3] Esses isomorfismos e os próximos que aparecerão são isomorfismos de kG-módulos. As justificativas estão na Seção 2.4.

Como s e $(1-x)m$ não são nulos, vale $(1-x)(s\otimes m)\neq 0$. Logo, $\operatorname{rad}(S\otimes M)=(1-x)(S\otimes M)\neq 0$ e $S\otimes M$ não é semissimples, como queríamos. Com isso, conseguimos determinar o radical de $S\otimes M$. De fato, veja que

$$\frac{S\otimes M}{S\otimes W}\cong S\otimes(M/W)\cong S\otimes k\cong S$$

é simples e temos $\operatorname{rad}(S\otimes M)\subseteq S\otimes W$. Mas $S\otimes W$ é simples e $S\otimes M$ não é semissimples, logo tem que valer a igualdade $\operatorname{rad}(S\otimes M)=S\otimes W$.

Como $S\otimes M/\operatorname{rad}(S\otimes M)\cong S$, o Lema 2.2.5 diz que $S\otimes M$ é quociente de P. Portanto,

$$\frac{\operatorname{rad}(S\otimes M)}{\operatorname{rad}^2(S\otimes M)}\cong S\otimes W$$

é quociente da camada radical $\operatorname{rad}(P)/\operatorname{rad}^2(P)$. Como ambos $S\otimes W$ e $\operatorname{rad}(P)/\operatorname{rad}^2(P)$ têm dimensão d, eles são na verdade isomorfos. Já determinamos a segunda camada radical! Estamos quase lá!

Agora, suponha que U seja um kG-módulo com $U/\operatorname{rad}(U)\cong S$. Como antes, U é quociente de P e, por isso, $\operatorname{rad}(U)/\operatorname{rad}^2(U)$ é quociente de $\operatorname{rad}(P)/\operatorname{rad}^2(P)\cong S\otimes W$. Como $S\otimes W$ é simples, então $\operatorname{rad}(U)/\operatorname{rad}^2(U)=0$ ou $\operatorname{rad}(U)/\operatorname{rad}^2(U)\cong S\otimes W$. Essa observação é suficiente para concluir o problema, como veremos a seguir. Já sabemos que $P/\operatorname{rad}(P)\cong S$ e que $\operatorname{rad}(P)/\operatorname{rad}^2(P)\cong S\otimes W$. Mas $S\otimes W$ é simples, logo, nessa última observação, podemos trocar S por $S\otimes W$ e U por $\operatorname{rad}(P)$, de onde segue que $\operatorname{rad}^2(P)/\operatorname{rad}^3(P)=0$ (caso $p^a=2$) ou $\operatorname{rad}^2(P)/\operatorname{rad}^3(P)\cong S\otimes W\otimes W$ (caso contrário). Mas $S\otimes W\otimes W$ é de novo simples e então podemos prosseguir assim. Por isso, as camadas radicais de P são exatamente aquelas que listamos no começo. Durante a demonstração, acabando mostrando que essas camadas radicais são simples e, portanto, P é unisseriado pela Proposição 2.1.13. Em particular, as camadas radicais que encontramos são os fatores de composição de P!

No exemplo anterior, sabendo que $\operatorname{rad}(P)/\operatorname{rad}^2(P)$ era simples para todo projetivo indecomponível P, conseguimos mostrar que todo projetivo indecomponível era unisseriado e encontramos as camadas radicais. Isso funciona num contexto mais geral, como ressaltamos no resultado a seguir retirado do livro [2].

Proposição 2.2.13. Todo A-módulo projetivo indecomponível é unisseriado se, e somente se, $\operatorname{rad}(P)/\operatorname{rad}^2(P)$ é simples ou nulo para todo projetivo indecomponível P.

Demonstração: Uma das implicações é imediata da Proposição 2.1.13. Vamos provar a outra implicação. Suponha que $\operatorname{rad}(P)/\operatorname{rad}^2(P)$ seja simples ou nulo para todo projetivo indecomponível P. Fixando um P desses, basta mostrarmos que $\operatorname{rad}^i(P)/\operatorname{rad}^{i+1}(P)$ é simples ou nulo para todo $i\geq 1$. Provaremos isso por indução em i. Note que o caso $i=1$ é a nossa hipótese. Agora, seja $i\geq 2$ e suponha que $\operatorname{rad}^{i-1}(P)/\operatorname{rad}^i(P)$ seja simples ou nulo. Nesse segundo caso, temos que a série radical de P já terminou em $\operatorname{rad}^{i-1}(P)$ e, por isso, $\operatorname{rad}^i(P)/\operatorname{rad}^{i+1}(P)=0$. No outro caso, temos $\operatorname{rad}^{i-1}(P)/\operatorname{rad}^i(P)$ simples e, pelo Lema 2.2.5, $\operatorname{rad}^{i-1}(P)$ é quociente de um projetivo indecomponível P'. Mas então $\operatorname{rad}^i(P)/\operatorname{rad}^{i+1}(P)$ é um quociente de $\operatorname{rad}(P')/\operatorname{rad}^2(P')$, que é simples ou nulo, de onde concluímos que $\operatorname{rad}^i(P)/\operatorname{rad}^{i+1}(P)$ também é simples ou nulo. □

2.3 A dualidade e suas propriedades

Vimos no Exemplo 1.3.5 que o dual U^* de um kG-módulo U^* é naturalmente um kG-módulo também. Se $\varphi\in U^*$ e $g\in G$, a estrutura de módulo de U^* nos dá

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

para todo $u\in U$. O inverso acima é necessário. Sem ele, U^* seria um kG-módulo *à direita*. Não conseguimos repetir essa construção para uma álgebra A qualquer e, por isso, já temos alguma

distinção entre o caso geral e o caso particular de representações de grupos. Nesta seção, veremos como obter propriedades interessantes, especialmente a respeito dos módulos projetivos, através da dualidade.

Começaremos estudando como algumas propriedades acerca da dualidade de espaços vetoriais se estendem para o caso dos kG-módulos. Se $\rho : U \to V$ é uma transformação entre dois espaços vetoriais, a **transposta** de ρ é a transformação linear $\rho^* : V^* \to U^*$ que leva um funcional $\varphi \in V^*$ ao funcional $\varphi \circ \rho \in U^*$. Temos nossa primeira propriedade importante:

Lema 2.3.1. Se $\rho : U \to V$ é um homomorfismo de kG-módulos, então a transposta $\rho^* : V^* \to U^*$ também o é.

Demonstração: Se $g \in G$ e $\varphi \in V^*$, então

$$(g\rho^*(\varphi))(v) = (\rho^*(\varphi))(g^{-1}v) = \varphi(\rho(g^{-1}v)) = \varphi(g^{-1}\rho(v)) = (g\varphi)(\rho(v)) = (\rho^*(g\varphi))(v)$$

para todo $v \in V$, ou seja, $\rho^*(g\varphi) = g\rho^*(\varphi)$. Isso prova que ρ^* é homomorfismo de kG-módulos. □

Observação 2.3.2. A dualidade define um funtor contravariante da categoria de kG-módulos de dimensão finita nela mesma: levamos um kG-módulo U em seu dual U^* e um homomorfismo $\rho : U \to V$ em sua transposta $\rho^* : V^* \to U^*$. Isso de fato define um funtor contravariante pois a transposta da identidade em U é a identidade em U^* para todo kG-módulo U e vale $(\rho_2 \circ \rho_1)^* = \rho_1^* \circ \rho_2^*$ para quaisquer homomorfismos $\rho_1 : U \to V$ e $\rho_2 : V \to W$. Em particular, a transposta de um isomorfismo é também um isomorfismo. Algo que vale mais geralmente nesse caso é que a transposta de um homomorfismo injetor é um homomorfismo sobrejetor e vice-versa. De fato, se $\rho : U \to V$ é um homomorfismo injetor, então ρ cinde *como transformação linear*, ou seja, existe uma *transformação linear* $\rho' : V \to U$ tal que $\rho' \circ \rho = \mathrm{id}_U$. Aplicando a transposta, segue que $\rho^* \circ (\rho')^* = \mathrm{id}_{U^*}$ e então ρ^* é sobrejetor. Um argumento análogo se aplica para mostrar que a transposta de um homomorfismo sobrejetor é injetora.

Outra propriedade interessante é que o dual de kG-módulos "comuta" com somas diretas e produtos tensoriais.

Lema 2.3.3. Se U e V são kG-módulos, então

$$(U \oplus V)^* \cong U^* \oplus V^* \quad \text{e} \quad (U \otimes V)^* \cong U^* \otimes V^*.$$

Demonstração: Tomando a transposta das inclusões de U e V na soma direta, temos homomorfismos $(U \oplus V)^* \to U^*$ e $(U \oplus V)^* \to V^*$ e, consequentemente, temos um homomorfismo $(U \oplus V)^* \to U^* \oplus V^*$. Não é difícil verificar que esse homomorfismo leva um funcional em $U \oplus V$ ao par consistindo de sua restrição a U e a V, respectivamente. Por isso, esse homomorfismo é injetor e, como a dimensão do domínio é igual à do contradomínio, temos um isomorfismo.

Lembre que temos um isomorfismo de espaços vetoriais $U^* \otimes V^* \to (U \otimes V)^*$ que leva $\varphi \otimes \psi$, onde $\varphi \in U^*$ e $\psi \in V^*$, no funcional de $(U \otimes V)^*$ que manda $u \otimes v$ em $\varphi(u)\psi(v)$ para todos $u \in U$ e $v \in V$. Deixamos a cargo do leitor verificar que esse isomorfismo também é um homomorfismo de kG-módulos. □

Quando U é um espaço vetorial de dimensão finita, lembre que temos um isomorfismo natural canônico $\Phi : U \to U^{**}$. Ele leva um vetor $u \in U$ no funcional $\Phi_u \in U^{**}$ dado por $\Phi_u(\varphi) = \varphi(u)$ para todo $\varphi \in U^*$. Como anteriormente, isso se estende ao caso de kG-módulos.

Lema 2.3.4. Se U é um kG-módulo, então o isomorfismo natural canônico $\Phi : U \to U^{**}$ é um isomorfismo de kG-módulos.

Demonstração: Sejam $g \in G$ e $u \in U$ quaisquer. Dado $\varphi \in U^*$, vale

$$\Phi_{gu}(\varphi) = \varphi(gu) = (g^{-1}\varphi)(u) = \Phi_u(g^{-1}\varphi) = (g\Phi_u)(\varphi).$$

Por isso, $\Phi_{gu} = g\Phi_u$ e Φ é um homomorfismo de kG-módulos. □

Observação 2.3.5. Quando dizemos que o isomorfismo $\Phi : U \to U^{**}$ é "natural", não só queremos dizer que a construção de Φ é natural mas que esse isomorfismo também é natural no sentido categórico. Esse isomorfismo define uma *transformação natural* entre o funtor identidade na categoria dos kG-módulos de dimensão finita e o funtor "bidual", que é obtido aplicando-se a dualidade duas vezes. Ou seja, se $\rho : U \to V$ é um homomorfismo, então o diagrama

$$\begin{array}{ccc} U & \xrightarrow{\rho} & V \\ {\scriptstyle \Phi_U}\downarrow & & \downarrow{\scriptstyle \Phi_V} \\ U^{**} & \xrightarrow[\rho^{**}]{} & V^{**} \end{array}$$

é comutativo, onde Φ_U e Φ_V denotam os isomorfismos canônicos. Um fato importante é que, no diagrama acima, temos $\rho = \Phi_V^{-1} \circ \rho^{**} \circ \Phi_U$. Uma consequência disso é que se $\rho_1 : U \to V$, $\rho_2 : V \to W$ e $\rho_3 : U \to W$ são homomorfismos satisfazendo $\rho_3^* = \rho_1^* \rho_2^*$, então $\rho_3 = \rho_2 \rho_1$. De fato, tomando a transposta, sabemos que $\rho_3^{**} = \rho_2^{**} \rho_1^{**}$. Mas então

$$\rho_3 = \Phi_W^{-1} \rho_3^{**} \Phi_U = \Phi_W^{-1} \rho_2^{**} \rho_1^{**} \Phi_U = (\Phi_W^{-1} \rho_2^{**} \Phi_V)(\Phi_V^{-1} \rho_1^{**} \Phi_U) = \rho_2 \rho_1,$$

como queríamos. Isso só ilustra um exemplo de como o isomorfismo canônico nos permite passar informações do dual de volta para o nosso módulo original.

Para terminar essa parte com as propriedades iniciais, veremos como submódulos de U correspondem a submódulos de U^*. É interessante ver a aplicação de um funcional em um vetor como uma função $\langle \cdot, \cdot \rangle : U^* \times U \to k$ que leva um par (φ, u) em $\varphi(u)$. É fácil ver que $\langle \cdot, \cdot \rangle$ é uma forma bilinear. Isso motiva as seguintes definições[1]: se $V \leq U$ é um submódulo, definimos

$$V^\perp \coloneqq \{\varphi \in U^* \mid \langle \varphi, u \rangle = \varphi(u) = 0 \text{ para todo } u \in V\} \subseteq U^*,$$

e se $W \leq U^*$ é um submódulo, definimos

$$W^\perp \coloneqq \{u \in U \mid \langle \varphi, u \rangle = \varphi(u) = 0 \text{ para todo } \varphi \in W\} \subseteq U.$$

Note que $\langle \cdot, \cdot \rangle$ é invariante pela ação de G, ou seja,

$$\langle g\varphi, gu \rangle = (g\varphi)(gu) = \varphi(g^{-1}(gu)) = \varphi(u) = \langle \varphi, u \rangle$$

para todos $g \in G$, $u \in U$ e $\varphi \in U^*$. Disso decorre que, na definição anterior, $V^\perp$ e $W^\perp$ são submódulos de U^* e U, respectivamente.

Lema 2.3.6. Se $U_1 \subseteq U_2$ são submódulos de um kG-módulo U, então $U_2^\perp \subseteq U_1^\perp$ e

$$\frac{U_1^\perp}{U_2^\perp} \cong \left(\frac{U_2}{U_1}\right)^*$$

como kG-módulos.

Demonstração: A inclusão $U_2^\perp \subseteq U_1^\perp$ segue facilmente das definições desses módulos. Agora, vamos construir um homomorfismo sobrejetor de $U_1^\perp$ em $(U_2/U_1)^*$ cujo núcleo é $U_2^\perp$, de modo que o lema seguirá do Teorema do Isomorfismo.

Se $\varphi \in U_1^\perp$, então, por definição, U_1 está em $\ker \varphi$. Restringindo a U_2 e depois descendo ao quociente, podemos definir $\overline{\varphi} \in (U_2/U_1)^*$ por $\overline{\varphi}(u_2 + U_1) = \varphi(u_2)$ para todo $u_2 \in U_2$. Isso nos dá uma função $\rho : U_1^\perp \to (U_2/U_1)^*$ que leva $\varphi \in U_1^\perp$ em $\overline{\varphi} \in (U_2/U_1)^*$. Note que ρ é linear e que

$$(\overline{g\varphi})(u_2 + U_1) = (g\varphi)(u_2) = \varphi(g^{-1}u_2) = \overline{\varphi}(g^{-1}(u_2 + U_1)) = (g\overline{\varphi})(u_2 + U_1)$$

[1] Chamaremos essas construções de **anuladores** das representações V e W, respectivamente.

para todos $g \in G$, $\varphi \in U_1^\perp$ e $u_2 \in U_2$, provando que $\rho(g\varphi) = g\rho(\varphi)$, ou seja, ρ é homomorfismo de kG-módulos. Veja que $\overline{\varphi} = 0$ se e somente se φ se anula sobre U_2, isto é, se e somente se $\varphi \in U_2^\perp$, o que mostra que $\ker \rho = U_2^\perp$. Resta mostrarmos que ρ é sobrejetor. Se $\psi \in (U_2/U_1)^*$, então $\psi\pi \in U_2^*$, onde $\pi : U_2 \to U_2/U_1$ é a projeção. Se V é um *subespaço* de U tal que $U = U_2 \oplus V$, podemos definir um funcional $\varphi \in U^*$ que é igual a $\psi\pi$ sobre U_2 e que vale 0 sobre V. É fácil ver que $\varphi \in U_1^\perp$ e que $\rho(\varphi) = \psi$, como preciso. □

Observação 2.3.7. Não é difícil verificar que, se $V \leq U$ e $W \leq U^*$, então $\dim_k V^\perp = \dim_k U - \dim_k V$ e $\dim_k W^\perp = \dim_k U - \dim_k W$. Por exemplo, a primeira dessas igualdades segue do Lema 2.3.6 se colocarmos $U_1 = V$ e $U_2 = U$. A outra pode ser provada utilizando o isomorfismo canônico entre U e U^{**} e o mesmo Lema 2.3.6. Uma consequência dessas igualdades é que $(V^\perp)^\perp = V$ e $(W^\perp)^\perp = W$. Isso nos permite reescrever o Lema 2.3.6 de outra forma: se $W_1 \subseteq W_2$ são submódulos de U^*, então $W_2^\perp \subseteq W_1^\perp$ são submódulos de U e temos

$$\frac{W_2}{W_1} \cong \left(\frac{W_1^\perp}{W_2^\perp}\right)^*.$$

Iremos mostrar como a dualidade se comporta com relação aos conceitos discutidos nas seções anteriores.

Proposição 2.3.8. Se U é um kG-módulo, então:

(1) U é simples se e somente se U^* é simples.

(2) U é semissimples se e somente se U^* é semissimples.

(3) U é indecomponível se e somente se U^* é indecomponível.

Demonstração: Para o item (1), se U não é simples, então existe um submódulo $V \leq U$ não nulo e próprio. Pelo Lema 2.3.6, $V^\perp \cong (U/V)^*$ e então $V^\perp$ não é nulo e também não possui a dimensão de U^*, ou seja, $V^\perp$ é um submódulo não nulo e próprio de U^*. Logo, U^* não é simples. Da mesma forma, se U^* não é simples, então $U^{**} \cong U$ também não é.

Para o item (2), basta usar o item (1) e que o dual "comuta" com somas diretas (Lema 2.3.3). O item (3) também segue facilmente do Lema 2.3.3. □

Quando definimos o radical e o soco de um módulo, vimos que eles pareciam conceitos "duais". Não seria estranho esperar então que a dualidade troca o radical pelo soco e vice-versa!

Proposição 2.3.9. Se U é um kG-módulo, então

$$\operatorname{soc}^n(U^*) = \operatorname{rad}^n(U)^\perp \quad \text{e} \quad \operatorname{rad}^n(U^*) = \operatorname{soc}^n(U)^\perp$$

para todo inteiro $n \geq 0$. Consequentemente,

$$\frac{\operatorname{soc}^{n+1}(U^*)}{\operatorname{soc}^n(U^*)} \cong \left(\frac{\operatorname{rad}^n(U)}{\operatorname{rad}^{n+1}(U)}\right)^* \quad \text{e} \quad \frac{\operatorname{rad}^n(U^*)}{\operatorname{rad}^{n+1}(U^*)} \cong \left(\frac{\operatorname{soc}^{n+1}(U)}{\operatorname{soc}^n(U)}\right)^*$$

para todo inteiro $n \geq 0$.

Demonstração: Inicialmente, note que os isomorfismos do enunciado são consequência direta das duas primeiras igualdades e do Lema 2.3.6. Provaremos a primeira igualdade por indução em n. Um argumento análogo demonstrará a segunda igualdade. Para $n = 0$, temos

$$\operatorname{soc}^0(U^*) = 0 = U^\perp = \operatorname{rad}^0(U)^\perp,$$

como preciso. Agora, suponha que $\operatorname{soc}^n(U^*) = \operatorname{rad}^n(U)^\perp$ para algum $n \geq 0$. Vamos mostrar que $\operatorname{soc}^{n+1}(U^*) = \operatorname{rad}^{n+1}(U)^\perp$ através das propriedades do soco e do radical descritas nas Proposições

1.1.14 e 1.1.12, respectivamente. Pelo Lema 2.3.6 e pela hipótese de indução, temos $\operatorname{soc}^n(U^*) = \operatorname{rad}^n(U)^\perp \subseteq \operatorname{rad}^{n+1}(U)^\perp$ e

$$\frac{\operatorname{rad}^{n+1}(U)^\perp}{\operatorname{soc}^n(U^*)} = \frac{\operatorname{rad}^{n+1}(U)^\perp}{\operatorname{rad}^n(U)^\perp} \cong \left(\frac{\operatorname{rad}^n(U)}{\operatorname{rad}^{n+1}(U)}\right)^*.$$

Como $\operatorname{rad}^n(U)/\operatorname{rad}^{n+1}(U)$ é semissimples, o seu dual também é pela Proposição 2.3.8. Por isso, $\operatorname{rad}^{n+1}(U)^\perp/\operatorname{soc}^n(U^*)$ também é semissimples. Mas $\operatorname{soc}^{n+1}(U^*)$ é o maior submódulo W de U^* contendo $\operatorname{soc}^n(U^*)$ tal que o quociente $W/\operatorname{soc}^n(U^*)$ é semissimples. Logo, temos a inclusão $\operatorname{rad}^{n+1}(U)^\perp \subseteq \operatorname{soc}^{n+1}(U^*)$. Para mostrar a inclusão contrária, faremos um argumento parecido: pela observação logo após o Lema 2.3.6, vale que $\operatorname{soc}^{n+1}(U^*)^\perp \subseteq \operatorname{soc}^n(U^*)^\perp = \operatorname{rad}^n(U)$ e

$$\frac{\operatorname{soc}^{n+1}(U^*)}{\operatorname{soc}^n(U^*)} \cong \left(\frac{\operatorname{soc}^n(U^*)^\perp}{\operatorname{soc}^{n+1}(U^*)^\perp}\right)^* = \left(\frac{\operatorname{rad}^n(U)}{\operatorname{soc}^{n+1}(U^*)^\perp}\right)^*.$$

Como $\operatorname{soc}^{n+1}(U^*)/\operatorname{soc}^n(U^*)$ é semissimples, a Proposição 2.3.8 diz que $\operatorname{rad}^n(U)/\operatorname{soc}^{n+1}(U^*)^\perp$ também é. Mas $\operatorname{rad}^{n+1}(U)$ é o menor submódulo V de U contido em $\operatorname{rad}^n(U)$ tal que o quociente $\operatorname{rad}^n(U)/V$ é semissimples. Portanto, temos a inclusão $\operatorname{rad}^{n+1}(U) \subseteq \operatorname{soc}^{n+1}(U^*)^\perp$ e, como consequência, $\operatorname{rad}^{n+1}(U)^\perp \supseteq (\operatorname{soc}^{n+1}(U^*)^\perp)^\perp = \operatorname{soc}^{n+1}(U^*)$. Dessa forma, está provada a igualdade desejada. □

E o que será que acontece com os módulos livres e os módulos projetivos?

Proposição 2.3.10. Se U é um kG-módulo livre, então $U \cong U^*$.

Demonstração: Pelo Lema 2.3.3, é suficiente mostrar que $(kG)^* \cong kG$. A álgebra kG tem uma base canônica dada pelos elementos do grupo. Vamos considerar a base dual a essa base canônica: para cada $g \in G$, defina $\varphi_g \in (kG)^*$ como sendo o funcional que vale 1 em g e 0 nos outros elementos de G. Esses funcionais formam uma base de $(kG)^*$ e temos um isomorfismo linear de kG em $(kG)^*$ que leva cada $g \in G$ em $\varphi_g \in (kG)^*$. Mas acontece que esse isomorfismo linear é na verdade um isomorfismo de kG-módulos! Para verificar isso, é suficiente mostrar que $\varphi_{hg} = h\varphi_g$ para todos $g, h \in G$. De fato, dado $x \in G$, vemos que $\varphi_{hg}(x) = 1$ se e somente se $hg = x$ e, caso contrário, $\varphi_{hg}(x) = 0$. Mas a condição $hg = x$ é equivalente a $g = h^{-1}x$, então segue da definição de φ_g que

$$\varphi_{hg}(x) = \varphi_g(h^{-1}x) = (h\varphi_g)(x)$$

para todo $x \in G$, provando a igualdade desejada. □

Observação 2.3.11. A propriedade que provamos aqui pode ser generalizada. Dizemos que uma álgebra A é uma **álgebra de Frobenius** se se $A^* \cong A$ como A-módulos à esquerda. E qual é a estrutura de A-módulo em A^*? Se $\varphi \in A^*$ e $a \in A$, definimos $(a\varphi)(x) = \varphi(xa)$ para todo $x \in A$. Não é difícil verificar que isso de fato torna A^* em um A-módulo à esquerda. Observe que essa construção não funciona para dar uma estrutura de A-módulo para U^* quando U é um A-módulo qualquer. É uma construção particular para o módulo regular.

Entretanto, a estrutura usual de kG-módulo para $(kG)^*$ não coincide com essa que acabamos de definir, então é preciso ajeitar um pouco a demonstração acima para realmente provar que kG é uma álgebra de Frobenius. Para tanto, a ideia é trocar a inversão que aparece na estrutura usual de $(kG)^*$ e passá-la para o isomorfismo. Mais especificamente, a transformação linear que leva $g \in G$ para $\varphi_{g^{-1}} \in (kG)^*$ é um isomorfismo de kG-módulos de kG em $(kG)^*$ com a estrutura que acabamos de definir.

Algo interessante é que um isomorfismo linear $\psi : A \to A^*$ dá origem a uma forma bilinear não degenerada[1] $(\cdot, \cdot) : A \times A \to k$ através da relação $(a, b) = \psi(b)(a)$ para todos $a, b \in A$.

[1] Lembre que uma forma bilinear é *não degenerada* se $a = 0$ for o único elemento a de A que satisfaz $(a, b) = 0$ para todo $b \in A$. Como A tem dimensão finita, isso é equivalente a exigir que $b = 0$ seja o único elemento b de A satisfazendo $(a, b) = 0$ para todo $a \in A$.

Reciprocamente, através de uma forma bilinear não degenerada, também podemos encontrar um isomorfismo linear de A em A^* do mesmo modo. Com algumas contas, verifica-se que ψ ser um homomorfismo de A-módulos é equivalente à validade da expressão $(ab, c) = (a, bc)$ para todos $a, b, c \in A$. Por isso, A é uma álgebra de Frobenius se e somente se existe uma forma bilinear não degenerada e "associativa" em A. Nesse sentido, o parágrafo anterior nos fornece uma forma bilinear não degenerada e associativa em kG dada por $(g, h) = 1$, se $gh = 1$, e $(g, h) = 0$, caso contrário, para todos $g, h \in G$.

Corolário 2.3.12. Se U é um kG-módulo, então U é projetivo se e somente se U^* é projetivo.

Demonstração: Se U é projetivo, então U é um somando direto de algum módulo livre, logo U^* também é projetivo pelo Lema 2.3.3 e pela Proposição 2.3.10. Por outro lado, se U^* é projetivo, o mesmo argumento mostra que $U^{**} \cong U$ também o é. □

Um fenômeno bem diferente está acontecendo aqui. Por exemplo, repare que na Proposição 2.3.9, a dualidade troca o radical com o soco. Isso era esperado porque a dualidade tem um caráter "contravariante", logo tende a inverter noções que têm alguma ideia de ordem embutida em sua definição. Mas olhe o item (3) da Proposição 2.2.1 que define os módulos projetivos, ele não é nem um pouco simétrico! É, de certo modo, surpreendente que tenhamos o corolário acima. Essa propriedade das álgebras de grupo é valiosa e será explorada.

Vejamos o que deveria ser o verdadeiro dual de um módulo projetivo.

Proposição 2.3.13. Se I é um A-módulo, então são equivalentes as seguintes afirmações:

(1) Todo homomorfismo injetor $\varphi : I \to U$ cinde.

(2) Se $\varphi : V \to U$ é um homomorfismo injetor e $\psi : V \to I$ é um homomorfismo qualquer, então existe um homomorfismo $\rho : U \to I$ que faz o seguinte diagrama comutar:

$$\begin{array}{ccccc} & & I & & \\ & & \uparrow{\scriptstyle \psi} & \nwarrow{\scriptstyle \rho} & \\ 0 & \longrightarrow & V & \xrightarrow[\varphi]{} & U \end{array}$$

Um A-módulo I que satisfaz as condições da Proposição 2.3.13 é chamado de **injetivo**. Note como os itens (1) e (2) dessa proposição são obtidos "invertendo" os itens (2) e (3) da Proposição 2.2.1, respectivamente. No diagrama acima, colocamos o homomorfismo nulo para dar a ideia de que a última linha é exata, ou seja, que φ é injetor. Essa segunda caracterização também pode ser pensada como: todo homomorfismo de um submódulo de U em I pode ser estendido a um homomorfismo de U em I.

Demonstração: (1) $\implies$ (2). Sejam $\varphi : V \to U$ e $\psi : V \to I$ como em (2). Vamos tentar adaptar a prova da implicação (1) $\implies$ (3) da Proposição 2.2.1. Vamos encontrar um módulo com um papel análogo ao módulo livre da demonstração anterior. Suponha que tenhamos um A-módulo M e homomorfismos $i_1 : I \to M$ e $i_2 : U \to M$ fazendo o seguinte diagrama comutar:

$$\begin{array}{ccccc} & & I & \xrightarrow{i_1} & M \\ & & \uparrow{\scriptstyle \psi} & & \uparrow{\scriptstyle i_2} \\ 0 & \longrightarrow & V & \xrightarrow[\varphi]{} & U \end{array}$$

Se i_1 também for injetor, então i_1 cinde por (1) e existe $\pi : M \to I$ tal que $\pi i_1 = \mathrm{id}_I$. Mas então o homomorfismo $\pi i_2 : U \to I$ satisfaz

$$(\pi i_2)\varphi = \pi(i_2\varphi) = \pi(i_1\psi) = (\pi i_1)\psi = \mathrm{id}_I\, \psi = \psi$$

e podemos tomar $\rho = \pi i_2$, concluindo a prova dessa implicação. Logo, basta encontrar o módulo M e os homomorfismos i_1 e i_2 com a propriedades desejadas. Os candidatos naturais seriam a soma direta $I \oplus U$ e as inclusões, mas não necessariamente o diagrama comutará. Então forçaremos essa comutatividade através de um quociente. Defina M como sendo[1] o quociente de $I \oplus U$ pelo submódulo

$$W \coloneqq \{(\psi(v), -\varphi(v)) \in I \oplus U \mid v \in V\}.$$

Tome $i_1 : I \to M$ e $i_2 : U \to M$ como sendo as inclusões seguidas da projeção. Se $v \in V$, temos que

$$i_2(\varphi(v)) = (0, \varphi(v)) + M = (\psi(v), 0) + M = i_1(\psi(v)),$$

de modo que o diagrama desejado comuta. Para concluir, note que se $x \in I$ satisfaz $i_1(x) = 0$, então existe $v \in V$ tal que $(x, 0) = (\psi(v), -\varphi(v))$. Mas então $\varphi(v) = 0$ e, como φ é injetor, temos $v = 0$, implicando que $x = \psi(v) = 0$. Isso mostra que i_1 é injetor, como desejado.

(2) $\implies$ (1). Seja $\varphi : I \to U$ um homomorfismo injetor. Tomando $V = I$ e $\psi = \mathrm{id}_I$, a propriedade em (2) nos dá um homomorfismo $\rho : U \to I$ tal que $\rho\varphi = \psi = \mathrm{id}_I$. Isso prova que φ cinde. □

Sabendo da definição de módulo injetivo, o Corolário 2.3.12 nos dá um importante resultado.

Teorema 2.3.14. Um kG-módulo é projetivo se, e somente se, ele é injetivo.

Demonstração: Seja P um kG-módulo projetivo. Se $\varphi : P \to U$ é um homomorfismo injetor, mostremos que φ cinde. Tomando a transposta, temos um homomorfismo sobrejetor $\varphi^* : U^* \to P^*$. Como P^* é projetivo pelo Corolário 2.3.12, φ^* cinde e existe um homomorfismo $f : P^* \to U^*$ tal que $\varphi^* f = \mathrm{id}_{P^*}$. Pelo Exercício A.2.10, existe um homomorfismo $\psi : U \to P$ tal que $f = \psi^*$. Pela Observação 2.3.5 sobre a "naturalidade do funtor bidual", $\varphi^*\psi^* = \mathrm{id}_{P^*}$ implica que $\psi\varphi = \mathrm{id}_P$, ou seja, φ cinde. Isso prova que P é injetivo.

O argumento anterior essencialmente mostra que se P^* é projetivo, então P é injetivo. Dualizando a prova, é fácil ver que se P^* é injetivo, então P é projetivo. Isso nos permite provar a recíproca. Se P é um kG-módulo injetivo, então $P^{**} = (P^*)^*$ é injetivo e, portanto, P^* é projetivo. Pelo Corolário 2.3.12, P também é projetivo. □

O seguinte corolário é útil quando lidamos com kG-módulos projetivos:

Corolário 2.3.15. Suponha que U seja um kG-módulo com submódulos $U_1 \subseteq U_2 \subseteq U$ tais que $U_2/U_1 = P$ seja projetivo. Então P é um somando direto de U.

Demonstração: Como P é projetivo, a projeção canônica $U_2 \to P$ cinde e P é um somando direto de U_2. Em particular, P é isomorfo a um submódulo de U. Como P também é injetivo, a inclusão $P \to U$ cinde e P é um somando direto de U. □

Temos também outro fato interessante. Se P é um kG-módulo projetivo indecomponível, então P^* também o é pela Proposição 2.3.8 e pelo Corolário 2.3.12. Pelo Teorema 2.2.4, $P^*/\operatorname{rad}(P^*)$ é simples. Mas a Proposição 2.3.9 diz que

$$\frac{P^*}{\operatorname{rad}(P^*)} = \frac{\operatorname{rad}^0(P^*)}{\operatorname{rad}(P^*)} \cong \left(\frac{\operatorname{soc}(P)}{\operatorname{soc}^0(P)}\right)^* \cong \operatorname{soc}(P)^*,$$

ou seja, $\operatorname{soc}(P)^*$ é simples e, consequentemente, $\operatorname{soc}(P)$ também!

Corolário 2.3.16. Se P é um kG-módulo projetivo indecomponível, então $P/\operatorname{rad}(P)$ e $\operatorname{soc}(P)$ são simples.

[1] Se você sabe o que é um *pushout*, o que construímos é exatamente o *pushout* do diagrama formado pelos homomorfismos ψ e φ!

Conseguimos associar dois módulos simples a um projetivo indecomponível. Uma pergunta natural é se esses dois módulos simples são isomorfos. Isso é verdade! A prova disso se baseia em outra propriedade especial da álgebra de grupo. Dizemos que uma k-álgebra A de dimensão finita é uma **álgebra simétrica** se existe uma forma bilinear não degenerada $(\,\cdot\,,\cdot\,) : A \times A \to k$ que é "simétrica" e "associativa", ou seja, para todos $a, b, c \in A$, valem

$$(a, b) = (b, a) \quad \text{e} \quad (ab, c) = (a, bc).$$

Vejamos o porquê de kG ser uma álgebra simétrica. Vamos considerar a forma bilinear que apareceu na Observação 2.3.11, ou seja, defina a forma bilinear $(\,\cdot\,,\cdot\,) : kG \times kG \to kG$ de modo que, dados $g, h \in G$, então (g, h) vale 1, se $gh = 1$, e 0, caso contrário. Nos elementos da base canônica de kG, é fácil ver que valem as propriedades associativa e simétrica, pois o produto em G é associativo e

$$gh = 1 \iff g = h^{-1} \iff hg = 1.$$

Disso segue que a forma bilinear é simétrica e associativa, e não é difícil verificar que ela é não degenerada. Essa forma bilinear nos permite provar o que queremos:

Teorema 2.3.17. Se P é um kG-módulo projetivo indecomponível, então

$$\frac{P}{\operatorname{rad}(P)} \cong \operatorname{soc}(P).$$

Demonstração: Denote por S o módulo simples $P/\operatorname{rad}(P)$. Defina $I \leq kG$ como sendo a soma de todos os submódulos de kG isomorfos a S. Mostremos que I é não nulo. Pela Proposição 2.3.8, S^* é simples e, pelo Teorema 2.2.4, existe um kG-módulo projetivo indecomponível Q tal que $Q/\operatorname{rad}(Q) \cong S^*$. Pela Proposição 2.3.9, temos

$$\operatorname{soc}(Q^*) \cong \left(\frac{Q}{\operatorname{rad}(Q)}\right)^* \cong (S^*)^* \cong S.$$

Mas, pela Proposição 2.3.8 e pelo Corolário 2.3.12, Q^* é projetivo indecomponível, ou seja, Q^* é isomorfo a um somando direto de kG. Como Q^* possui um submódulo isomorfo a S, o mesmo vale para kG, provando que $I \neq 0$. Agora, defina J como sendo o subconjunto de $\operatorname{End}_{kG}(kG)$ dos endomorfismos cuja imagem está contida em I. É fácil verificar que J é um ideal à direita de $\operatorname{End}_{kG}(kG)$. Mais ainda, J é não nulo. De fato, como S é simples, em particular, S é um quociente de kG. Compondo a projeção de kG em S com um homomorfismo injetor de S em kG (que existe porque $I \neq 0$), obtemos um elemento não nulo de J.

Com isso em mãos, vamos demonstrar o teorema. A prova será por contradição. Suponha, por absurdo, que $\operatorname{soc}(P) \ncong S$. Decomponha $kG = U \oplus V$ como a soma direta de submódulos U e V de forma que todos os somandos indecomponíveis de U sejam isomorfos a P e nenhum somando indecomponível de V seja isomorfo a P. Pelo Exercício A.1.2, o soco de U é isomorfo à soma direta de cópias de $\operatorname{soc}(P)$, que é simples pelo Corolário 2.3.16. Mas então, pela nossa suposição, U não pode conter nenhum submódulo isomorfo a S, pois tal submódulo estaria contido em $\operatorname{soc}(U)$, cujos submódulos simples são isomorfos a $\operatorname{soc}(P)$. Assim, a projeção de kG em $kG/V \cong U$ leva qualquer submódulo de kG isomorfo a S em 0, ou seja, devemos ter $I \subseteq V$.

Agora, denote por $\pi : kG \to kG$ a projeção em U com relação à decomposição $kG = U \oplus V$. Como I está contido em $V = \ker \pi$, vemos que $\pi\varphi = 0$ para todo $\varphi \in J$. Por outro lado, vejamos que $\varphi = \varphi\pi$ para todo $\varphi \in J$. Como π é a identidade sobre U e é 0 sobre V, basta mostrarmos que $\varphi(V) = 0$. Como I é a soma de módulos isomorfos a S, então na verdade podemos escrever I como a soma *direta* de módulos isomorfos a S. Dessa forma, qualquer submódulo não nulo de I tem S como fator de composição. Assim, se $\varphi(V) \neq 0$, S seria uma imagem homomorfa de V. Logo, algum somando indecomponível de V também teria S como uma imagem homomorfa. Mas, como V é projetivo, o Teorema 2.2.4 implicaria que tal somando seria isomorfo a P, contradizendo

a definição de V. Por isso, de fato temos $\varphi(V) = 0$ e $\varphi = \varphi\pi$. De tudo isso, concluímos que $\varphi = \varphi - 0 = \varphi\pi - \pi\varphi$, para todo $\varphi \in J$.

Vamos concluir a demonstração. Fixe $\varphi \in J$ não nulo. Se $\alpha \in \mathrm{End}_{kG}(kG)$, então $\varphi\alpha \in J$, pois J é ideal à direita de $\mathrm{End}_{kG}(kG)$. Pelo que vimos anteriormente, vale

$$\varphi\alpha = \varphi\alpha\pi - \pi\varphi\alpha.$$

Pela demonstração do Lema 1.2.3, existem $a, b, c \in kG$ tais que α, φ e π são dados pela multiplicação à direita por a, b e c, respectivamente. Aplicando os homomorfismos da igualdade acima em 1, temos $ab = cab - abc$. Portanto, usando a forma bilinear $(\,\cdot\,,\cdot\,)$ de kG, temos

$$(a, b) = (ab, 1) = (cab, 1) - (abc, 1) = (c, ab) - (ab, c) = 0.$$

Isso vale para todo $\alpha \in \mathrm{End}_{kG}(kG)$, ou seja, para todo $a \in kG$. Como a forma bilinear é não degenerada, devemos ter $b = 0$. Mas então $\varphi = 0$, um absurdo! □

Corolário 2.3.18. Se P é a cobertura projetiva de um kG-módulo simples S, então P^* é a cobertura projetiva de S^*.

Demonstração: Note que S^* é simples pela Proposição 2.3.8, então faz sentido considerar sua cobertura projetiva. Pela proposição que acabamos de usar e pelo Corolário 2.3.12, temos que P^* é projetivo indecomponível. Por fim, pela Proposição 2.3.9, temos

$$\frac{P^*}{\mathrm{rad}(P^*)} \cong \mathrm{soc}(P)^* \cong \left(\frac{P}{\mathrm{rad}(P)}\right)^* \cong S^*,$$

onde o segundo isomorfismo é dado pelo Teorema 2.3.17. □

Concluiremos a seção com alguns exemplos.

Exemplo 2.3.19. Vamos exemplificar esses últimos resultados calculando algum exemplo concreto. Suponha $p > 0$ e tome $G = C_n$ com $n = p^a m$ e m não divisível por p. Suponha também que k seja algebricamente fechado e que $g \in C_n$ seja um gerador. Pelo Exemplo 1.3.15, para cada raiz m-ésima da unidade $\lambda \in k$, temos um kC_n-módulo simples S_λ de dimensão 1 no qual g age por multiplicação por λ. Se $s \in S_\lambda$ é não nulo, então S_λ é gerado como espaço vetorial por s e, tomando a base dual, vemos que o funcional $\varphi : S_\lambda \to k$ que leva s em 1 forma uma base de S_λ^*. Se $g \in G$, note que

$$(g\varphi)(s) = \varphi(g^{-1}s) = \varphi(\lambda^{-1}s) = \lambda^{-1}$$

e, consequentemente, $g\varphi = \lambda^{-1}\varphi$. Portanto, g age em S_λ^* como multiplicação por λ^{-1}, de onde segue que $S_\lambda^* \cong S_{\lambda^{-1}}$!

Pelo Exemplo 2.1.12, o bloco de Jordan $J_d(\lambda)$ de dimensão d e autovalor λ nos dá um kC_n-módulo indecomponível quando $1 \leq d \leq p^a$ e $\lambda \in k$ é raiz m-ésima da unidade. Como $J_d(\lambda)$ tem S_λ como único fator de composição, então é de se esperar que $J_d(\lambda)^* \cong J_d(\lambda^{-1})$. De fato, sabemos que $J_d(\lambda)^*$ também é indecomponível pela Proposição 2.3.8 e, como também tem dimensão d, vale $J_d(\lambda)^* \cong J_d(\mu)$ para alguma raiz m-ésima da unidade $\mu \in k$. Como $J_d(\lambda)$ contém uma cópia de S_λ, pelo Lema 2.3.6 temos

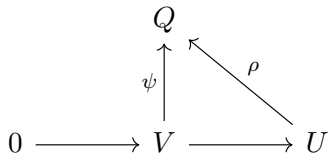
$$\frac{J_d(\lambda)^*}{S_\lambda^\perp} = \frac{0^\perp}{S_\lambda^\perp} \cong S_\lambda^* \cong S_{\lambda^{-1}}.$$

Logo, $J_d(\lambda)^*$ tem $S_{\lambda^{-1}}$ como um fator de composição. Mas os únicos fatores de composição de $J_d(\lambda)^* \cong J_d(\mu)$ são isomorfos a S_μ, então devemos ter $\mu = \lambda^{-1}$, como preciso.

É possível verificar o isomorfismo $J_d(\lambda)^* \cong J_d(\lambda^{-1})$ sem os resultados anteriores, apenas encontrando uma base adequada de $J_d(\lambda)^*$. Porém, o jeito que apresentamos é bem mais prático!

Exemplo 2.3.20. Seja G um grupo finito que possui um p-subgrupo de Sylow normal e cíclico (novamente, estamos supondo $p > 0$). Vimos no Exemplo 2.2.12 que todos os kG-módulos projetivos indecomponíveis são unisseriados. Com o que desenvolvemos nessa seção, podemos demonstrar ainda mais: todos os kG-módulos indecomponíveis são unisseriados! Isso nos diz que todo kG-módulo indecomponível U é determinado pelo quociente $U/\operatorname{rad}(U)$ e pelo seu comprimento. De fato, se U é unisseriado, então, em particular, $U/\operatorname{rad}(U)$ é simples. Pelo Lema 2.2.5, U é um quociente da cobertura projetiva P de $U/\operatorname{rad}(U)$. Mas P é unisseriado, então P tem um único quociente cujo comprimento é o comprimento de U. Como o comprimento de todo kG-módulo projetivo indecomponível é a ordem p^a do p-subgrupo de Sylow de G, até obtemos uma maneira de encontrar os indecomponíveis: dado um módulo simples S e um inteiro d entre 1 e p^a, a cobertura projetiva de S possui um único quociente de comprimento d, que é unisseriado e, portanto, indecomponível. Além disso, todo indecomponível é obtido dessa forma. Em particular, usando o Teorema de Brauer, temos que o número de classes de isomorfismo de kG-módulos indecomponíveis é rp^a, onde r é o número de classes de conjugação p-regulares de G.

Vejamos o porquê de todo indecomponível ser unisseriado. Seja U um kG-módulo indecomponível. Como U é finitamente gerado, existe um inteiro positivo n e um homomorfismo sobrejetor $\varphi : (kG)^n \to U$. Decompondo $(kG)^n$ como soma de projetivos indecomponíveis, vemos que U é a soma das imagens desses somandos através de φ. Logo, o Exercício A.1.4 implica na existência de um indecomponível projetivo P tal que $V \coloneqq \varphi(P)$ tem o mesmo comprimento de Loewy ℓ de U. Como V é quociente do módulo unisseriado P, então V também é unisseriado e, em particular, $\operatorname{soc}(V)$ é simples. Pelo Exercício A.2.16 (o dual do Lema 2.2.5), existe um homomorfismo injetor $\psi : V \to Q$, onde Q é a cobertura projetiva de $\operatorname{soc}(V)$. Mas o Teorema 2.3.14 diz que Q é injetivo, então o item (2) da Proposição 2.3.13 nos dá um homomorfismo $\rho : U \to Q$ fazendo o seguinte diagrama comutar:



Aqui, o homomorfismo injetor de V para U é a inclusão. Como ψ é injetor, $\psi(V)$ tem o mesmo comprimento de Loewy ℓ. Mas $\rho(U)$ contém $\psi(V)$ e é quociente de U, então, novamente pelo Exercício A.1.4, o comprimento de Loewy de $\rho(U)$ também é ℓ. Lembre que Q é projetivo indecomponível, então é unisseriado e possui no máximo um submódulo com comprimento de Loewy ℓ. Por isso, $\rho(U) = \psi(V)$. Como ψ é injetor, podemos restringir seu contradomínio e obter um homomorfismo inverso $\psi' : \psi(V) \to V$. Assim, a composição da inclusão de V em U com $\psi'\rho$ é a identidade em V, de modo que essa inclusão cinde. Consequentemente, V é um somando direto de U. Mas U é indecomponível, logo $U = V$, provando que U é um módulo unisseriado.

Observação 2.3.21. Mais geralmente, dizemos que uma k-álgebra de dimensão finita A é uma **álgebra de Nakayama** se todos os seus módulos projetivos e injetivos indecomponíveis são unisseriados. Como vimos no exemplo anterior, esse é o caso de kG quando o p-subgrupo de Sylow de G é normal e cíclico. Um prova análoga mostra que todo módulo indecomponível sobre uma álgebra de Nakayama é unisseriado.

Exemplo 2.3.22. Vamos terminar com um caso concreto dos Exemplos 2.2.12 e 2.3.20. Fixe k um corpo algebricamente fechado de característica $p = 5$. Seja $G = D_{15}$ o grupo diedral de simetrias de um polígono regular de 15 lados. Lembre que D_{15} possui 30 elementos e pode ser escrito como

$$D_{15} = \langle x, y \mid x^{15} = y^2 = 1, yxy^{-1} = x^{-1} \rangle.$$

Um 5-subgrupo de Sylow N de D_{15} possui 5 elementos e, por isso, é necessariamente cíclico. Além disso, se $\langle x \rangle$ é o subgrupo gerado por x, então todos os elementos de $D_{15} \setminus \langle x \rangle$ têm ordem 2, logo $N \subseteq \langle x \rangle$. Mas $\langle x \rangle$ é abeliano e então possui um único 5-subgrupo de Sylow. Portanto, N é o

único 5-subgrupo de Sylow de G e, consequentemente, é normal. Estamos no caso dos exemplos anteriores!

É fácil ver que x^3 tem ordem 5, então $N = \langle x^3 \rangle$. Como o quociente D_{15}/N tem ordem 6, o Teorema de Schur-Zassenhaus diz que N tem um complemento H em D_{15}, ou seja, um subgrupo H de D_{15} satisfazendo $D_{15} = NH$ e $N \cap H = \{1\}$. Um tal complemento pode ser tomado como o subgrupo gerado por x^5 e y. Geometricamente, formamos um triângulo equilátero a partir de três vértices do polígono regular de 15 lados e consideramos o subgrupo de D_{15} que fixa esse triângulo. Vendo desse modo, é imediato que $H \cong D_3 \cong S_3$. Disso, concluímos que D_{15} é isomorfo a um produto semidireto de C_5 e S_3.

Vamos começar encontrando os kD_{15}-módulos simples. Na notação da Proposição 1.3.14, vale $O_5(D_{15}) = N$, então os kD_{15}-módulos simples coincidem com os módulos simples sobre a álgebra de grupo de $D_{15}/N \cong H \cong S_3$. Assim, basta encontrarmos todos os kS_3-módulos simples. Denote por k, k_{sgn} e U as representações trivial, sinal e a de dimensão 2 descritas no Exemplo 1.3.4. É imediato que k e k_{sgn} são kS_3-módulos simples por serem unidimensionais. Como a característica do corpo é $p = 5$, essas duas representações também são não isomorfas. Como o quociente de S_3 por seu subgrupo de comutadores tem ordem 2, o Exercício A.1.20 nos mostra que essas duas são todas as representações unidimensionais de S_3 sobre k. Agora, mostremos que U é simples. Se isso não acontecesse, U teria um submódulo isomorfo a k ou a k_{sgn}. Em ambos os casos, a transformação induzida por $(1\ 2\ 3) \in S_3$ em U teria algum ponto fixo, o que não é o caso, já que essa transformação é dada pela matriz

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

em alguma base, mas essa matriz não possui 1 como autovalor. Dessa forma, temos três kS_3-módulos simples e eles representam todos os kS_3-módulos simples pelo Teorema de Brauer[1], pois S_3 possui exatamente três classes de conjugação que são todas 5-regulares. Voltando para kD_{15} através da projeção $kD_{15} \to kS_3$, concluímos que k, k_{sgn} e U representam as três únicas classes de isomorfismo de kD_{15}-módulos simples.

Sejam P_k, $P_{k_{\text{sgn}}}$ e P_U as coberturas projetivas dos kD_{15}-módulos k, k_{sgn} e U, respectivamente. Como vimos no Exemplo 2.2.12, todas essas coberturas projetivas são módulos unisseriados e de comprimento $|N| = 5$. Para determinar os fatores de composição, devemos encontrar $W := \operatorname{rad}(P_k)/\operatorname{rad}^2(P_k)$, que é unidimensional por resultados anteriores. Pelo Exercício A.2.9, basta entendermos a ação de H por conjugação em N. Tal ação corresponde a um homomorfismo de H no grupo de automorfismos $\operatorname{Aut}(N)$. Se esse homomorfismo fosse trivial, então a conjugação de N por um elemento de H seria trivial, ou seja, todo elemento de N comutaria com todo elemento de H. Isso não acontece porque, por exemplo, $x^3 \in N$ não comuta com $y \in H$. Então o homomorfismo de H em $\operatorname{Aut}(N)$ não é trivial. Como $H \cong S^3$ e $\operatorname{Aut}(N) \cong \operatorname{Aut}(C_5) \cong C_4$, não é difícil ver que o homomorfismo deve levar todo elemento de ordem 2 de H no único elemento de ordem 2 de $\operatorname{Aut}(N)$ (que é o automorfismo de N que leva um elemento em seu inverso), enquanto os demais elementos de H constituem o núcleo. Ou seja, $hx^3h^{-1} = x^3$, se $h \in H$ não tem ordem 2, e $hx^3h^{-1} = (x^3)^{-1}$, se $h \in H$ tem ordem 2. Segue do Exercício A.2.9 que $W \cong k_{\text{sgn}}$!

Pelo Exemplo 2.2.12, os fatores de composição de P_k são dados por

$$k, W, W \otimes W = W^{\otimes 2}, W^{\otimes 3} \text{ e } W^{\otimes 4}.$$

Mas, sabendo que $W \cong k_{\text{sgn}}$, é fácil ver que $W \otimes W \cong k$. Dessa forma, os fatores de composição de P_k são

$$k, k_{\text{sgn}}, k, k_{\text{sgn}} \text{ e } k,$$

e eles aparecem nessa ordem na única série de composição de P_k. Por um argumento análogo, segue também do Exemplo 2.2.12 que os fatores de composição de $P_{k_{\text{sgn}}}$ são, em ordem,

$$k_{\text{sgn}}, k, k_{\text{sgn}}, k \text{ e } k_{\text{sgn}}.$$

[1] É aqui que usamos que k é algebricamente fechado. Entretanto, k poderia ser um corpo de característica 5 qualquer! A explicação adicional se encontra no Exercício A.2.18.

Por fim, o Exemplo 2.2.12 diz que todos os fatores de composição de P_U têm a mesma dimensão. Como U é um deles e U é o único kD_{15}-módulo simples de dimensão 2, então o único fator de composição de P_U é U, que aparece com multiplicidade 5. Uma informação importante que também sabemos é que[1]

$$kD_{15} \cong P_k \oplus P_{k_{\text{sgn}}} \oplus P_U \oplus P_U$$

pelo Corolário 2.2.6.

Pelo Exemplo 2.3.20, todos os kD_{15}-módulos indecomponíveis são unisseriados e podemos obter seus fatores de composição e a ordem em que aparecem a partir do que acabamos de descobrir sobre os projetivos indecomponíveis. Por exemplo, o indecomponível associado a k_{sgn} de comprimento 3 é quociente de $P_{k_{\text{sgn}}}$ e seus fatores de composição são

$$k_{\text{sgn}}, k \text{ e } k_{\text{sgn}},$$

nessa ordem. Por outro lado, qualquer indecomponível que tenha U como fator de composição não possui k nem k_{sgn} como fator de composição.

Esse é um bom exemplo para se verificar resultados como o Teorema 2.3.17, o Exercício A.2.13 e o Exercício A.2.17.

2.4 O produto tensorial e suas propriedades

Na seção anterior, estudamos mais a fundo algumas das propriedades da dualidade para kG-módulos. Desta vez, exploraremos outra construção importante introduzida no Exemplo 1.3.5: o produto tensorial. Veremos alguns resultados e depois nos concentraremos em encontrar as representações projetivas de $\mathrm{SL}_2(p)$.

Se $\varphi : U \to U'$ e $\psi : V \to V'$ são transformações lineares entre k-espaços vetoriais, podemos definir seu **produto tensorial** como sendo a transformação linear $\varphi \otimes \psi : U \otimes V \to U' \otimes V'$ determinada por

$$(\varphi \otimes \psi)(u \otimes v) = \varphi(u) \otimes \psi(v),$$

para todos $u \in U$ e $v \in V$. Não é difícil usar a propriedade universal do produto tensorial para verificar que a construção acima está bem definida. O primeiro resultado que nos dá alguma compatibilidade entre o produto tensorial e a estrutura de kG-módulo é o seguinte:

Proposição 2.4.1. Se $\varphi : U \to U'$ e $\psi : V \to V'$ são homomorfismos entre kG-módulos, então $\varphi \otimes \psi : U \otimes V \to U' \otimes V'$ também o é.

Demonstração: Se $g \in G$, $u \in U$ e $v \in V$, então

$$\begin{aligned}(\varphi \otimes \psi)(g(u \otimes v)) &= (\varphi \otimes \psi)(gu \otimes gv) \\ &= \varphi(gu) \otimes \psi(gv) \\ &= (g\varphi(u)) \otimes (g\psi(v)) \\ &= g(\varphi(u) \otimes \psi(v)) \\ &= g(\varphi \otimes \psi)(u \otimes v).\end{aligned}$$

Como $\varphi \otimes \psi$ é linear, a proposição segue. □

Corolário 2.4.2. Se U e V são kG-módulos e $U' \leq U$ e $V' \leq V$ são submódulos, então $U' \otimes V'$ é canonicamente isomorfo a um submódulo de $U \otimes V$. Além disso, também temos um isomorfismo

$$\frac{U}{U'} \otimes \frac{V}{V'} \cong \frac{U \otimes V}{U \otimes V' + U' \otimes V}$$

como kG-módulos.

[1] Podemos justificar essa passagem usando que k é algebricamente fechado, pois então sabemos que a multiplicidade de cada simples em $kD_{15}/\operatorname{rad}(kD_{15})$ é a sua dimensão. Porém, não precisamos usar que k é algebricamente fechado: veja o Exercício A.2.18.

Demonstração: Se $i_U : U' \to U$ e $i_V : V' \to V$ são as inclusões, então a Proposição 2.4.1 nos dá um homomorfismo $i_U \otimes i_V$ de $U' \otimes V'$ em $U \otimes V$. Não é difícil verificar que esse homomorfismo é injetor: podemos, por exemplo, tomar uma base de U' e uma de V', construir a base correspondente em $U' \otimes V'$ e então verificar que a imagem dessa base através de $i_U \otimes i_V$ é um conjunto linearmente independente.

Para a segunda parte, considere as projeções $\pi_U : U \to U/U'$ e $\pi_V : V \to V/V'$. A Proposição 2.4.1 nos dá um homomorfismo $\pi_U \otimes \pi_V$ de $U \otimes V$ em $U/U' \otimes V/V'$. Segue facilmente da definição de $\pi_U \otimes \pi_V$ que esse homomorfismo é sobrejetor, porque π_U e π_V o são. Basta verificar então que $\ker(\pi_U \otimes \pi_V) = U \otimes V' + U' \otimes V$. Aplicando $\pi_U \otimes \pi_V$, vemos que $U \otimes V' + U' \otimes V$ está contido no núcleo. Para terminar de provar a igualdade, basta notar que $\ker(\pi_U \otimes \pi_V)$ e $U \otimes V' + U' \otimes V$ têm a mesma dimensão. O cálculo da dimensão de $U \otimes V' + U' \otimes V$ pode ser feito tomando bases de U' e V', completando para bases de U e V e, com isso, mostrando que a interseção de $U \otimes V'$ e $U' \otimes V$ é exatamente a cópia de $U' \otimes V'$ dentro de $U \otimes V$. □

Observação 2.4.3. No resultado anterior, se $U' = 0$, então temos o isomorfismo de kG-módulos

$$U \otimes \frac{V}{V'} \cong \frac{U \otimes V}{U \otimes V'}.$$

Um isomorfismo análogo vale se $V' = 0$.

Proposição 2.4.4. Se U, V e W são kG-módulos, então temos os seguintes isomorfismos de kG-módulos:

(1) $U \otimes V \cong V \otimes U$.

(2) $(U \otimes V) \otimes W \cong U \otimes (V \otimes W)$.

(3) $(U \oplus V) \otimes W \cong (U \otimes W) \oplus (V \otimes W)$.

Demonstração: São propriedades conhecidas do produto tensorial que existem isomorfismos lineares canônicos entre os espaços apresentados. Não é difícil verificar que todos eles preservam a estrutura de kG-módulo. Deixamos essa verificação ao leitor. □

Observação 2.4.5. O item (2) acima implica a associatividade do produto tensorial, mesmo quando temos mais de três fatores. Algo útil é definir um "produto tensorial com mais de dois fatores", isto é, dados espaços vetoriais $V_1, \ldots, V_n$, podemos definir um espaço $V_1 \otimes \cdots \otimes V_n$ e um mapa multilinear $\otimes : V_1 \times \cdots \times V_n \to V_1 \otimes \cdots \otimes V_n$ que satisfaz uma propriedade universal análoga à do produto tensorial, mas desta vez trocamos a bilinearidade pela linearidade nos n fatores. Assim como fizemos no Exemplo 1.3.5, se $V_1, \ldots, V_n$ são kG-módulos, podemos definir uma estrutura de kG-módulo em $V_1 \otimes \cdots \otimes V_n$ fazendo cada $g \in G$ atuar entrada por entrada. Felizmente, esse novo módulo é isomorfo ao módulo que obtemos realizando o produto tensorial dos módulos $V_1, \ldots, V_n$ de dois em dois e em qualquer ordem. Na verdade, já estávamos fazendo essa identificação em seções anteriores!

Outra ponto importante a se observar é que, juntamente com (1), o item (3) implica no seguinte isomorfismo: se $U_1, \ldots, U_n, V_1, \ldots, V_m$ são kG-módulos, então

$$\left(\bigoplus_{i=1}^{n} U_i\right) \otimes \left(\bigoplus_{j=1}^{m} V_j\right) \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} (U_i \otimes V_j),$$

como kG-módulos.

Se U e V são k-espaços vetoriais (de dimensão finita), então temos um isomorfismo canônico

$$U^* \otimes V \cong \mathrm{Hom}_k(U, V).$$

Se $\varphi \in U^*$ e $v \in V$, então o isomorfismo acima leva $\varphi \otimes v$ na transformação linear de U em V que manda $u \in U$ em $\varphi(u)v \in V$. Se U e V também são kG-módulos, vimos no Exemplo 1.3.5 como tornar $\mathrm{Hom}_k(U,V)$ um kG-módulo de modo que o isomorfismo acima também seja um isomorfismo de kG-módulos. Como vimos na Observação 1.3.8, lembre que $\mathrm{Hom}_{kG}(U,V)$ é o subespaço de $\mathrm{Hom}_k(U,V)$ dos vetores fixos pela ação de G!

Proposição 2.4.6. Se U, V e W são kG-módulos, então

$$\mathrm{Hom}_k(U \otimes V, W) \cong \mathrm{Hom}_k(U, V^* \otimes W)$$

como kG-módulos. Em particular,

$$\mathrm{Hom}_{kG}(U \otimes V, W) \cong \mathrm{Hom}_{kG}(U, V^* \otimes W)$$

como espaços vetoriais.

Demonstração: É consequência imediata de alguns resultados que acabamos de ver e do Lema 2.3.3:

$$\begin{aligned}\mathrm{Hom}_k(U \otimes V, W) &\cong (U \otimes V)^* \otimes W \\ &\cong (U^* \otimes V^*) \otimes W \\ &\cong U^* \otimes (V^* \otimes W) \\ &\cong \mathrm{Hom}_k(U, V^* \otimes W).\end{aligned}$$

Como o isomorfismo acima é de kG-módulos, ele induz um isomorfismo de espaços vetoriais entre os subespaços dos elementos fixos pela ação de G. Portanto, também vale a segunda afirmação da proposição. □

Será que o produto tensorial de módulos simples é simples? Se U é um kG-módulo simples de dimensão maior que 1, note que os produtos tensoriais

$$U \otimes U,\ U \otimes U \otimes U,\ U \otimes U \otimes U \otimes U,\ \ldots$$

têm dimensões cada vez maiores. Mas kG possui apenas um número finito de módulos simples, então a sequência acima deixa de conter módulos simples a partir de algum ponto. Por outro lado, se U tiver dimensão 1, então a sequência acima contém apenas módulos de dimensão 1 e então todos eles são simples! Da mesma forma, se V é outro kG-módulo unidimensional, então $U \otimes V$ também tem dimensão 1. Mais ainda, se U tem dimensão 1, conseguimos construir um kG-módulo V unidimensional tal que $U \otimes V \cong k$. Para encontrar tal V, podemos proceder como fizemos no Exemplo 2.2.12. Isto mostra que o conjunto das classes de isomorfismo de kG-módulos unidimensionais é um grupo abeliano com produto dado pelo produto tensorial! Esse é o **grupo dual** de G. Lembrando que representações unidimensionais correspondem a homomorfismos de G em $k^\times$, não é difícil ver que o grupo dual de G é isomorfo ao grupo constituído pelos homomorfismos $G \to k^\times$ cuja operação é a multiplicação de funções ponto a ponto.

Uma observação importante é que o produto tensorial de um kG-módulo simples com um kG-módulo unidimensional é também simples. Isso segue do que acabamos de fazer imitando o argumento dado no Exemplo 2.2.12 para provar que $S \otimes W$ é simples.

E qual a relação do produto tensorial com módulos livres e projetivos?

Proposição 2.4.7. Se U é um kG-módulo qualquer e V é um kG-módulo livre, então $U \otimes V$ também é livre.

Demonstração: Se $V \cong (kG)^n$ para algum $n \geq 0$, então

$$U \otimes V \cong U \otimes (kG)^n \cong (U \otimes kG)^n$$

pela Proposição 2.4.4. Logo, é suficiente mostrar que $U \otimes kG$ é livre.

Observe inicialmente que, se $u \in U$ é não nulo, então $u \otimes 1$ gera um submódulo de $U \otimes kG$ isomorfo a kG. De fato, tal submódulo é o subespaço gerado pelos vetores $g(u \otimes 1) = (gu) \otimes g$ com $g \in G$, que são linearmente independentes, já que as segundas coordenadas desses tensores são linearmente independentes em kG. Assim, é fácil ver que a transformação linear que leva g em $(gu) \otimes g$ é um isomorfismo de kG-módulos entre kG e o submódulo de $U \otimes kG$ gerado por $u \otimes 1$. Agora, se $u_1, \ldots, u_m$ formam uma base de U, podemos definir F_i como sendo o submódulo de $U \otimes kG$ gerado por $u_i \otimes 1$, para $1 \leq i \leq m$. Como vimos, vale $F_i \cong kG$. Como a dimensão de $U \otimes kG$ é $m \cdot |G|$, se mostrarmos que

$$U \otimes kG = F_1 + F_2 + \cdots + F_m,$$

teremos na verdade uma soma direta, concluindo a demonstração. Com efeito, se $u \in U$ e $g \in G$, podemos tomar $\alpha_1, \ldots, \alpha_m \in k$ tais que $g^{-1}u = \alpha_1 u_1 + \cdots + \alpha_m u_m$ e então

$$g(\alpha_1(u_1 \otimes 1) + \cdots + \alpha_m(u_m \otimes 1)) = (g(\alpha_1 u_1 + \cdots + \alpha_m u_m)) \otimes g = u \otimes g.$$

Mas os tensores da forma $u \otimes g$ geram $U \otimes kG$, provando o que precisávamos. □

Corolário 2.4.8. Se U é um kG-módulo qualquer e P é um kG-módulo projetivo, então $U \otimes P$ também é projetivo.

Demonstração: Se P é um somando direto de um módulo livre V, então $U \otimes P$ é um somando direto de $U \otimes V$ pela Proposição 2.4.4. Agora, aplique a Proposição 2.4.7. □

Antes de apresentar o teorema desta seção, vamos mostrar um exemplo que nos ajudará na demonstração.

Exemplo 2.4.9. Vamos generalizar as construções que fizemos no Exemplo 1.3.17. Seja V um kG-módulo de base $\{x_1, \ldots, x_r\} \subseteq V$. Se formarmos a álgebra de polinômios $R = k[x_1, \ldots, x_r]$, onde $x_1, \ldots, x_r$ são vistos como variáveis, podemos tornar R um kG-módulo (de dimensão infinita) da seguinte forma: se $g \in G$, então existem escalares $\alpha_{1j}^g, \cdots, \alpha_{rj}^g \in k$ tais que

$$gx_j = \sum_{i=1}^{r} \alpha_{ij}^g x_i$$

para todo $1 \leq j \leq r$. Assim, vendo a soma acima como um elemento de R, podemos utilizar a propriedade universal da álgebra de polinômios para definir um homomorfismo de k-álgebras $\varphi_g : R \to R$ que leva x_j em gx_j para todos $1 \leq j \leq r$ e $g \in G$. Não é difícil ver que a composta $\varphi_g\varphi_h$ leva cada x_j em $(gh)x_j$ e, portanto, devemos ter $\varphi_g\varphi_h = \varphi_{gh}$ para todos $g, h \in G$. Com isso, observe que $\varphi_g\varphi_{g^{-1}} = \varphi_{g^{-1}}\varphi_g = \varphi_1 = \mathrm{id}_R$, ou seja, φ_g é inversível para todo $g \in G$! Dessa forma, temos um homomorfismo de G no grupo de operadores lineares inversíveis $\mathrm{GL}(R)$ e construímos uma estrutura de kG-módulo em R. Note que, se $f = f(x_1, \ldots, x_r)$ é um polinômio em R, então

$$g \cdot f = \varphi_g(f(x_1, \ldots, x_r)) = f(\varphi_g(x_1), \ldots, \varphi_g(x_r)) = f\left(\sum_{i=1}^{r} \alpha_{i1}^g x_i, \ldots, \sum_{i=1}^{r} \alpha_{ir}^g x_i\right)$$

para todo $g \in G$.

Denote por V_n o subespaço de R formado pelos polinômios homogêneos de grau $n \geq 1$. Como φ_g é homomorfismo de álgebras e leva cada variável x_i em um polinômio homogêneo de grau 1, temos $gV_n \subseteq V_n$ para todos $g \in G$ e $n \geq 1$. Isso mostra que cada V_n é um submódulo de R! Veja que $V_1 \cong V$. Chamamos o kG-módulo V_n de **n-ésima potência simétrica** de V. O objetivo principal deste exemplo é justificar esse nome através do produto tensorial. Para isso, vamos considerar o produto tensorial $V^{\otimes n}$ de n cópias de V. Pela propriedade universal do produto

tensorial, conseguimos encontrar uma transformação linear sobrejetora $\rho : V^{\otimes n} \to V_n$ que leva o tensor $x_{i_1} \otimes \cdots \otimes x_{i_n}$ no polinômio homogêneo $x_{i_1} \cdots x_{i_n}$. Não é complicado ver que

$$g(x_{i_1} \otimes \cdots \otimes x_{i_n}) = (gx_{i_1}) \otimes \cdots \otimes (gx_{i_n})$$

é levado em

$$(gx_{i_1}) \cdots (gx_{i_n}) = g(x_{i_1} \cdots x_{i_n})$$

e, consequentemente, ρ é um homomorfismo de kG-módulos. Agora, seja I o subespaço de $V^{\otimes n}$ gerado pelos elementos da forma

$$(\cdots \otimes v_i \otimes \cdots \otimes v_j \otimes \cdots) - (\cdots \otimes v_j \otimes \cdots \otimes v_i \otimes \cdots),$$

onde todas as coordenadas dos dois tensores puros são as mesmas exceto por duas delas, onde os elementos $v_i, v_j \in V$ estão trocados. Note que I é um submódulo de $V^{\otimes n}$ e está contido no núcleo de ρ, de modo que temos um homomorfismo sobrejetor induzido $\overline{\rho} : V^{\otimes n}/I \to V_n$. Por fim, veja que as projeções dos tensores puros "ordenados"

$$x_1^{\otimes a_1} \otimes x_2^{\otimes a_2} \otimes \cdots \otimes x_r^{\otimes a_r}$$

com $a_1 + \cdots + a_r = n$ geram $V^{\otimes n}/I$ e são levados nos monômios que formam a base canônica de V_n. Concluímos então que $\overline{\rho}$ é um isomorfismo de kG-módulos.

Denotamos $V^{\otimes n}/I$ por $S^n(V)$. Agora é evidente o motivo do nome que demos a esse módulo: a ordem das coordenadas dos tensores puros nesse quociente não importa mais. Estamos, em algum sentido, simetrizando os tensores de $V^{\otimes n}$. Um comentário interessante é que também podemos construir o próprio R através de produtos tensoriais. Não entraremos em detalhes, mas a ideia é colocar um produto no espaço $\bigoplus_{n \geq 0} V^{\otimes n}$ de modo a formar a **álgebra tensorial**. Essa álgebra é isomorfa à álgebra livre sobre $x_1, \ldots, x_r$, cujos elementos são polinômios "não comutativos" nessas variáveis. Simetrizando através de um quociente, construímos a **álgebra simétrica** sobre V, que é isomorfa a R.

Para provar o próximo teorema, usaremos um pouco de teoria de Galois! Vamos enunciar como lemas dois resultados que precisaremos utilizar:

Lema 2.4.10. Sejam K um corpo e G um grupo finito de automorfismos de K. Seja F o subcorpo de K formado pelos elementos fixos por G. Então a extensão $K \supseteq F$ é de Galois e seu grupo de Galois é G.

Lema 2.4.11 (Teorema da Base Normal)**.** Seja $K \supseteq F$ uma extensão de Galois finita e seja G o seu grupo de Galois. Então existe um elemento $\alpha \in K$ tal que as imagens $g(\alpha)$ com $g \in G$ são todas distintas e formam uma base de K sobre F.

As demonstrações podem ser encontradas, por exemplo, em [13]. Esses resultados não estão enunciados desse jeito no livro, mas podem ser encontrados no capítulo sobre teoria de Galois.

Por fim, para enunciar o teorema, precisamos de mais uma definição. Dizemos que um kG-módulo V é **fiel** se cada elemento de G diferente da identidade induz um operador linear em V diferente da identidade. Equivalentemente, V é fiel se o homomorfismo correspondente $G \to \mathrm{GL}(V)$ é injetor.

Teorema 2.4.12. Se V é um kG-módulo fiel e P é um kG-módulo projetivo indecomponível, então P é isomorfo a um somando direto de $V^{\otimes n}$ para algum inteiro não negativo[1] n.

[1] Se $n = 0$, então $V^{\otimes 0}$ denota o kG-módulo trivial.

Demonstração: Seja $\{x_1, \ldots, x_r\}$ uma base de V. Assim como fizemos no Exemplo 2.4.9, podemos formar a álgebra de polinômios $R = k[x_1, \ldots, x_r]$ e dotá-la de uma estrutura de kG-módulo através da ação de G em V. Afirmamos que R possui um submódulo livre W de dimensão finita. Vejamos como isso conclui a prova do teorema. Como no Exemplo 2.4.9, denote por V_n o submódulo de R formado pelos polinômios homogêneos de grau $n \geq 1$. Também denote por V_0 o submódulo trivial de R formado pelos polinômios constantes. Como W tem dimensão finita, os graus de seus elementos são limitados e, portanto, existe um $n_0 \geq 1$ tal que

$$W \subseteq V_0 \oplus V_1 \oplus \cdots \oplus V_{n_0}.$$

Como P é projetivo indecomponível, P é isomorfo a um somando direto de W. Com isso, conseguimos encontrar um homomorfismo injetor de P em $V_0 \oplus \cdots \oplus V_{n_0}$. Mas P é projetivo e, portanto, injetivo, então esse homomorfismo injetor cinde e P é um somando direto de $V_0 \oplus \cdots \oplus V_{n_0}$. Como P é indecomponível, o Teorema de Krull-Schmidt implica na existência de um inteiro $0 \leq m \leq n_0$ tal que P é somando direto de V_m. Se $m = 0$, então $P \cong V_0 \cong V^{\otimes 0}$. Se $m \geq 1$, usamos que $V_m \cong S^m(V)$ para concluir que P é um quociente de $V^{\otimes m}$. Mas P é projetivo, então a projeção $V^{\otimes m} \to P$ cinde e P é um somando direto de $V^{\otimes m}$, como queríamos.

Resta mostrar que W de fato existe. Como R é um domínio de integridade, podemos formar o seu corpo de frações K, que se consiste das funções racionais nas variáveis $x_1, \ldots, x_r$. Podemos estender a ação de G em R para K definindo

$$g \cdot \frac{f_1}{f_2} \coloneqq \frac{g \cdot f_1}{g \cdot f_2}$$

para todos $f_1, f_2 \in R$ ($f_2 \neq 0$) e $g \in G$. Como G age por automorfismos (de álgebra) de R, podemos mostrar que a definição acima independe da escolha do numerador e do denominador que representa a fração. É fácil ver que isso dá uma estrutura de kG-módulo a K e note que a ação de G também é por automorfismos. Como K contém R como submódulo e, por sua vez, como R contém $V \cong V_1$ como submódulo, vemos que K é um kG-módulo fiel, pois V o é. Dessa forma, podemos identificar G com um subgrupo finito do grupo de automorfismos de K. Se F é o subcorpo de K formado pelos elementos fixos por G, o Lema 2.4.10 diz que a extensão $K \supseteq F$ é de Galois com grupo de Galois G. Pelo Lema 2.4.11, existe $\alpha \in K$ tal que os elementos $g\alpha$ com $g \in G$ são distintos e formam uma base de K sobre F. Pela definição de K, existem polinômios $f_1, f_2 \in R$ tais que $\alpha = f_1/f_2$. Observe que o polinômio

$$\prod_{g \in G} g f_2$$

é um elemento de F por ser fixo por G, então

$$f \coloneqq \alpha \cdot \prod_{g \in G} g f_2$$

é um elemento de R tal que os elementos gf com $g \in G$ também formam uma base de K sobre F. Em particular, como F contém k, os elementos gf com $g \in G$ são linearmente independentes sobre k. Segue então que o subespaço W gerado por tais elementos é um submódulo de R isomorfo a kG, concluindo a demonstração. □

Observação 2.4.13. O Teorema 2.4.12 teve sua primeira versão provada por Burnside, mas a demonstração usava caracteres e era válida apenas sobre corpos de característica zero. Posteriormente, em 1962, Robert Steinberg generalizou o resultado para característica qualquer utilizando argumentos com módulos. Porém, essa generalização não lidava com módulos projetivos indecomponíveis, apenas com módulos simples. Brauer também teve uma participação: em característica zero, ele conseguiu limitar o n do enunciado do Teorema 2.4.12 e simplificou a prova de Burnside. O artigo [21] faz um breve resumo sobre esses resultados e fornece mais referências.

Para utilizar o Teorema 2.4.12 na prática, devemos encontrar um kG-módulo fiel pequeno e cujas potências tensoriais possam ser facilmente examinadas. Sempre temos um kG-módulo fiel canônico, que é o próprio kG, mas, nesse caso, o Teorema 2.4.12 não nos dá nada novo. Geralmente, podemos encontrar uma representação fiel menor. Por exemplo, pela Proposição 1.3.14, se $p > 0$ e $O_p(G) = 1$, então o kG-módulo

$$S_1 \oplus S_2 \oplus \cdots \oplus S_n$$

é fiel, onde $S_1, \ldots, S_n$ denotam os kG-módulos simples. Nesse caso, o Teorema 2.4.12 nos diz que basta procurarmos os projetivos indecomponíveis nos produtos tensoriais de módulos simples. Em outros casos, a situação pode ser ainda melhor. Por exemplo, se $p > 0$ e $G = \mathrm{SL}_2(p)$, então o módulo simples V_2 do Exemplo 1.3.17 é fiel! Logo, os projetivos indecomponíveis são somandos diretos das potências $V_2^{\otimes n}$ com $n \geq 0$. Utilizaremos essa ideia para encontrar, no próximo exemplo, os projetivos indecomponíveis de $\mathrm{SL}_2(p)$.

Exemplo 2.4.14. Seja k um corpo algebricamente fechado de característica $p > 0$ e tome $G = \mathrm{SL}_2(p)$. Vamos encontrar todos os kG-módulos projetivos indecomponíveis. No Exemplo 1.3.17, mostramos que os módulos $V_1, \ldots, V_p$ são as representações irredutíveis de G. Um fato muito importante para o que se segue é que V_p é projetivo! Provaremos que V_p é projetivo quando restrito a um p-subgrupo de Sylow de G e, posteriormente (Exemplo 3.2.5), veremos que isso implica a projetividade também como kG-módulo. Esse será o único fato deixado para uma seção futura. Pelo Exercício A.1.21, $|G| = p(p^2 - 1)$ e então um p-subgrupo de Sylow possui ordem p. Mas a matriz

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$$

possui ordem p e gera um dos p-subgrupos de Sylow. Pelo Lema 1.3.18 (e pelo Exercício A.1.22), $(V_p)_{\langle g \rangle}$ é um $k\langle g \rangle$-módulo unisseriado e, portanto, indecomponível. Como $\langle g \rangle$ é cíclico de ordem p e V_p tem dimensão p, o Exemplo 2.2.10 nos dá que $(V_p)_{\langle g \rangle}$ é projetivo, como preciso. Note que nenhum dos outros módulos simples é projetivo, já que todo kG-módulo projetivo tem dimensão divisível por p pelo Corolário 2.2.9.

Sejam $P_1, \ldots, P_p$ as coberturas projetivas de $V_1, \ldots, V_p$, respectivamente. Já sabemos que $P_p \cong V_p$. Vamos descrever a estrutura das outras coberturas e depois provar as nossas afirmações. Primeiramente, se $p = 2$, então P_1 é unisseriado de comprimento 2 e seus fatores de composição são isomorfos a V_1, que aparece com multiplicidade 2. Suponha $p > 2$ agora. Então P_1 é unisseriado de comprimento 3 e seus fatores de composição são

$$V_1, V_{p-2} \text{ e } V_1,$$

que aparecem nessa ordem na única série de composição de P_1. O módulo P_{p-1} também é unisseriado de comprimento 3 e, dessa vez, seus fatores de composição são

$$V_{p-1}, V_2 \text{ e } V_{p-1},$$

nessa ordem. Agora, supondo $p > 3$, se $1 < n < p - 1$, então $\mathrm{soc}(P_n) \subseteq \mathrm{rad}(P_n)$ e

$$\mathrm{rad}(P_n)/\mathrm{soc}(P_n) \cong V_{p+1-n} \oplus V_{p-1-n}$$

(observe que os índices variam de 1 a $p-1$). Nesse último caso, vejamos como fica a estrutura de P_n. Como P_n é a cobertura projetiva de V_n, vale $P_n/\mathrm{rad}(P_n) \cong \mathrm{soc}(P_n) \cong V_n$. Como $\mathrm{rad}(P_n)/\mathrm{soc}(P_n)$ é semissimples, vale $\mathrm{rad}^2(P_n) \subseteq \mathrm{soc}(P_n)$. Mas $\mathrm{soc}(P_n)$ é simples, então $\mathrm{rad}^2(P_n) = \mathrm{soc}(P_n)$ ou $\mathrm{rad}^2(P_n) = 0$. Esse segundo caso não pode ocorrer, pois, se ocorresse, teríamos $\mathrm{rad}(P_n)$ semissimples e $\mathrm{rad}(P_n) \subseteq \mathrm{soc}(P_n)$, o que não é o caso. Portanto, o comprimento de Loewy de P_n é 3. Um argumento análogo mostra que a série de socos de P_n é igual à série radical, e os quocientes sucessivos são

$$V_n, V_{p+1-n} \oplus V_{p-1-n} \text{ e } V_n,$$

nessa ordem. Repare que $\operatorname{rad}(P_n)$ é o único submódulo maximal de P_n e $\operatorname{soc}(P_n)$ é o único submódulo simples de P_n. Com isso, concluímos que P_n possui exatamente 6 submódulos: P_n, $\operatorname{rad}(P_n)$, dois submódulos entre $\operatorname{rad}(P_n)$ e $\operatorname{soc}(P_n)$ (que correspondem a V_{p+1-n} e V_{p-1-n} no quociente $\operatorname{rad}(P_n)/\operatorname{soc}(P_n)$), $\operatorname{soc}(P_n)$ e 0.

Vamos provar que os projetivos indecomponíveis possuem a estrutura descrita. Faremos o caso $p = 2$ separadamente, que é diferente e mais simples. Como k é algebricamente fechado, o Corolário 2.2.6 nos dá

$$kG \cong P_1^{\dim_k V_1} \oplus P_2^{\dim_k V_2} = P_1 \oplus P_2^2 \cong P_1 \oplus V_2 \oplus V_2.$$

Como $\dim_k kG = 2(2^2 - 1) = 6$, temos $\dim_k P_1 = 2$. Veja que $P_1/\operatorname{rad}(P_1) \cong V_1$ tem dimensão 1, então $\operatorname{rad}(P_1)$ também é unidimensional e, portanto, simples. Segue que as camadas radicais de P_1 são simples e P_1 é unisseriado. Seu fatores de composição são $P_1/\operatorname{rad}(P_1) \cong V_1$ e $\operatorname{soc}(P_1) \cong V_1$, provando a estrutura descrita anteriormente. Como vimos no Exercício A.1.21, quando $p = 2$, temos $G \cong S_3$. Compare com o que fizemos no Exemplo 2.2.3!

A partir de agora, suporemos $p > 2$ até o fim. A nossa estratégia será estudar as potências tensoriais de V_2, com base no Teorema 2.4.12, já que V_2 é fiel. Para ajudar a calcular os produtos tensoriais, temos um resultado auxiliar:

Lema 2.4.15. Se $2 \leq n < p$, então $V_2 \otimes V_n \cong V_{n-1} \oplus V_{n+1}$.

Demonstração: Lembre que definimos V_n como sendo o submódulo de $k[x, y]$ dos polinômios homogêneos de grau $n - 1$. Como G age por automorfismos (de álgebra) em $k[x, y]$, o mapa de $V_2 \otimes V_n$ para V_{n+1} dado por multiplicação de polinômios é um homomorfismo. Além disso, como todo monômio de grau n é múltiplo de x ou de y, esse homomorfismo é sobrejetor. Mostremos que o núcleo é isomorfo a V_{n-1}. Como a dimensão do núcleo é

$$\dim_k V_2 \cdot \dim_k V_n - \dim_k V_{n+1} = 2n - (n + 1) = n - 1,$$

é suficiente mostrar que o núcleo contém um submódulo isomorfo a V_{n-1}. Defina uma transformação linear $\varphi : V_{n-1} \to V_2 \otimes V_n$ pondo

$$\varphi(f) = x \otimes yf - y \otimes xf$$

para todo $f \in V_{n-1}$. É imediato verificar que φ está bem definida e que sua imagem está contida no núcleo do homomorfismo anterior. Vejamos que φ é um homomorfismo de kG-módulos. Seja

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

um elemento de G, de modo que temos $ad - bc = 1$. Assim, se $f \in V_{n-1}$, então

$$\begin{aligned} g\varphi(f) &= g(x \otimes yf - y \otimes xf) \\ &= gx \otimes (gy \cdot gf) - gy \otimes (gx \cdot gf) \\ &= (ax + cy) \otimes ((bx + dy) \cdot gf) - (bx + dy) \otimes ((ax + cy) \cdot gf) \\ &= (ad - bc)(x \otimes (y \cdot gf) - y \otimes (x \cdot gf)) \\ &= \varphi(gf), \end{aligned}$$

como preciso. Agora, note que

$$\varphi(x^i y^{n-2-i}) = x \otimes x^i y^{n-1-i} - y \otimes x^{i+1} y^{n-2-i}$$

para todo $0 \leq i \leq n - 2$. Usando as bases canônicas de V_2 e de V_n para construir uma base de $V_2 \otimes V_n$, não é difícil ver que os tensores puros que aparecem acima quando variamos o índice i são todos linearmente independentes. Por consequência, φ manda um base de V_{n-1} em um conjunto

linearmente independente de $V_2 \otimes V_n$, o que prova que φ é injetor. Disso tudo, concluímos que $V_2 \otimes V_n$ possui um submódulo isomorfo a V_{n-1} e cujo quociente é isomorfo a V_{n+1}.

Vamos terminar a prova do lema. Se encontrarmos um submódulo de $V_2 \otimes V_n$ isomorfo a V_{n+1}, então a interseção dele com o submódulo isomorfo a V_{n-1} será trivial, pois eles são módulos simples não isomorfos. Contando as dimensões, seguirá que $V_2 \otimes V_n \cong V_{n-1} \oplus V_{n+1}$, como preciso. Para encontrar V_{n+1} dentro de $V_2 \otimes V_n$, procederemos por indução em n, mas indo de $n = p-1$ a $n = 1$. Se $n = p-1$, vimos que V_p é um quociente de $V_2 \otimes V_{p-1}$. Mas V_p é projetivo, então a projeção de $V_2 \otimes V_{p-1}$ em V_p cinde e V_p é isomorfo a um somando direto de $V_2 \otimes V_{p-1}$, como desejado. Agora, suponha que $2 \leq n < p-1$ e que $V_2 \otimes V_{n+1} \cong V_n \oplus V_{n+2}$. Para mostrar que V_{n+1} é isomorfo a um submódulo de $V_2 \otimes V_n$, basta mostrar que $\mathrm{Hom}_{kG}(V_{n+1}, V_2 \otimes V_n)$ é não nulo. Mas note que $V_2^* \cong V_2$, pois V_2 é o único kG-módulo simples de dimensão 2, então, juntamente com a Proposição 2.4.6, temos:

$$\begin{aligned}\mathrm{Hom}_{kG}(V_{n+1}, V_2 \otimes V_n) &\cong \mathrm{Hom}_{kG}(V_{n+1}, V_2^* \otimes V_n) \\ &\cong \mathrm{Hom}_{kG}(V_{n+1} \otimes V_2, V_n) \\ &\cong \mathrm{Hom}_{kG}(V_n \oplus V_{n+2}, V_n) \neq 0,\end{aligned}$$

concluindo a demonstração. □

Com o Lema 2.4.15, podemos calcular as potências tensoriais de V_2. Por exemplo,

$$V_2^{\otimes 2} = V_2 \otimes V_2 \cong V_1 \oplus V_3$$

e

$$V_2^{\otimes 3} \cong V_2 \otimes (V_1 \oplus V_3) \cong (V_2 \otimes V_1) \oplus (V_2 \otimes V_3) \cong V_2 \oplus V_2 \oplus V_4.$$

Observe que $V_2, V_2^{\otimes 2}, \ldots, V_2^{\otimes p-1}$ são todos semissimples e o primeiro projetivo indecomponível que aparece é V_p em $V_2^{\otimes p-1}$. Se $1 \leq n < p$, não aparecerá nada novo em $V_2 \otimes V_n$, então podemos estudar apenas a sequência

$$V_2 \otimes V_p,\ V_2^{\otimes 2} \otimes V_p,\ V_2^{\otimes 3} \otimes V_p,\ \ldots$$

E já temos algo interessante desde o começo: $V_2 \otimes V_p \cong P_{p-1}$! Vamos provar isso. O primeiro passo é notar que a primeira parte do Lema 2.4.15 pode ser utilizada para mostrar que $V_2 \otimes V_p$ possui um submódulo isomorfo a V_{p-1} e o quociente correspondente é isomorfo a[1] V_{p+1}. Como V_p é projetivo, o Corolário 2.4.8 nos diz que $V_2 \otimes V_p$ também é projetivo. Decompondo

$$V_2 \otimes V_p = Q_1 \oplus \cdots \oplus Q_r$$

como soma de indecomponíveis $Q_1, \ldots, Q_r$, temos que esses indecomponíveis também são projetivos. Tomando o soco, o Exercício A.1.2 nos dá

$$\mathrm{soc}(V_2 \otimes V_p) = \mathrm{soc}(Q_1) \oplus \cdots \oplus \mathrm{soc}(Q_r).$$

Mas $V_{p-1} \subseteq \mathrm{soc}(V_2 \otimes V_p)$ e cada $\mathrm{soc}(Q_i)$ é simples e isomorfo a V_{p-1} somente quando $Q_i \cong P_{p-1}$. Portanto, existe um índice $1 \leq i \leq r$ tal que $Q_i \cong P_{p-1}$ e então P_{p-1} é um somando direto de $V_2 \otimes V_p$. Agora contamos as dimensões: como V_{p-1} não é projetivo (pois p não divide a sua dimensão), P_{p-1} não pode ser semissimples e é diferente de seu soco. Assim, como $P_{p-1}/\mathrm{rad}(P_{p-1}) \cong \mathrm{soc}(P_{p-1}) \cong V_{p-1}$ são simples, devemos ter

$$P_{p-1} \supsetneq \mathrm{rad}(P_{p-1}) \supseteq \mathrm{soc}(P_{p_1}) \supsetneq 0$$

e a dimensão de P_{p-1} é pelo menos $2 \cdot \dim_k V_{p-1} = 2(p-1)$. Como $p > 2$ divide a dimensão de P_{p-1} e $V_2 \otimes V_p$ tem dimensão $2p$, a única possibilidade é $V_2 \otimes V_p \cong P_{p-1}$.

[1] Esse é o submódulo de $k[x,y]$ formado pelos polinômios homogêneos de grau p. Note que ele não é simples!

A partir disso, encontremos a estrutura de P_{p-1}. Sejam $U = \operatorname{rad}(P_{p-1})$ e $V = \operatorname{soc}(P_{p-1})$ e lembre que $U \supseteq V$. Como P_{p-1}/U e V têm dimensão $p-1$, o quociente U/V possui dimensão 2. Como U é o único submódulo maximal de P_{p-1} e V é o único submódulo simples, basta mostrarmos que $U/V \cong V_2$ para concluir que P_{p-1} é unisseriado e que seus fatores de composição são

$$V_{p-1}, V_2 \text{ e } V_{p-1},$$

nessa ordem. Mas vimos que o quociente de $P_{p-1} \cong V_2 \otimes V_p$ pelo seu soco $V \cong V_{p-1}$ é isomorfo a V_{p+1}. Como U é o único submódulo maximal de P_{p-1}, o submódulo de V_{p+1} correspondendo a U/V é o único submódulo maximal de V_{p+1}. Observe que esse submódulo possui dimensão 2, então é suficiente mostrar que V_{p+1} contém um submódulo isomorfo a V_2. Para isso, defina o homomorfismo de k-álgebras $\varphi : k[x,y] \to k[x,y]$ que leva x em x^p e y em y^p. Se $f = f(x,y)$ é um polinômio qualquer, então $\varphi(f) = f(x^p, y^p)$. Note que φ é injetor e leva V_2 (que é gerado por x e y) para dentro de V_{p+1}. Assim, é suficiente mostrar que φ também é um homomorfismo de kG-módulos. Se

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

e $f = f(x,y) \in k[x,y]$, então

$$\varphi(gf) = \varphi(f(gx, gy)) = \varphi(f(ax+cy, bx+dy)) = f(ax^p + cy^p, bx^p + dy^p).$$

Mas $a, b, c, d \in \mathbb{F}_p \subseteq k$ e, se $x \in \mathbb{F}_p$, vale $x^p = x$. Por isso,

$$\begin{aligned} f(ax^p + cy^p, bx^p + dy^p) &= f(a^p x^p + c^p y^p, b^p x^p + d^p y^p) \\ &= f((ax+cy)^p, (bx+dy)^p) \\ &= f((gx)^p, (gy)^p) \\ &= g \cdot f(x^p, y^p) = g\varphi(f), \end{aligned}$$

como preciso.

Estudaremos P_{p-2} através de $V_2 \otimes P_{p-1}$. Como P_{p-1} possui uma série de submódulos cujos quocientes são V_{p-1}, V_2 e V_{p-1}, podemos aplicar a observação feita logo após o Corolário 2.4.2 para obter uma série de submódulos de $V_2 \otimes P_{p-1}$ cujos quocientes são $V_2 \otimes V_{p-1}$, $V_2 \otimes V_2$ e $V_2 \otimes V_{p-1}$, ou seja,

$$V_{p-2} \oplus V_p, V_1 \oplus V_3 \text{ e } V_{p-2} \oplus V_p,$$

pelo Lema 2.4.15. Note também que $V_2 \otimes P_{p-1}$ é projetivo pelo Corolário 2.4.8. Vamos ter que separar em casos agora. Suponha primeiramente que $p = 3$. Assim, $V_2 \otimes P_2$ possui $V_{p-2} = V_1$ como submódulo e, como $V_2 \otimes P_2$ é projetivo, podemos argumentar como anteriormente para mostrar que a cobertura projetiva P_1 de V_1 é somando direto de $V_2 \otimes P_2$. Seja $U \leq V_2 \otimes P_2$ tal que $V_2 \otimes P_2 \cong P_1 \oplus U$. Como P_1 é indecomponível, V_3 não pode ser somando direto de P_1 e, como V_3 é projetivo, também não pode ser fator de composição pelo Corolário 2.3.15. Por isso, V_3 é fator de composição de U com a sua mesma multiplicidade em $V_2 \otimes P_2$, que é 3, logo, aplicando o Corolário 2.3.15 três vezes, segue que $V_3 \oplus V_3 \oplus V_3$ é somando direto de U. Temos então que $P_1 \oplus V_3 \oplus V_3 \oplus V_3$ é um somando direto de $V_2 \otimes P_2$. Como $V_2 \otimes P_2$ tem dimensão 12 e 3 divide a dimensão de P_1, devemos ter $\dim_k P_1 = 3$ e

$$V_2 \otimes P_2 \cong P_1 \oplus V_3 \oplus V_3 \oplus V_3.$$

Mas então V_1 é o único fator de composição de P_1. Como $P_1/\operatorname{rad}(P_1) \cong \operatorname{soc}(P_1) \cong V_1$, a única possibilidade é P_1 unisseriado, como preciso. Com isso, provamos tudo o que precisávamos no caso $p = 3$.

Suporemos $p > 3$ até o final e continuaremos de onde estávamos logo antes do caso $p = 3$. Como $V_2 \otimes P_{p-1}$ é projetivo e possui V_{p-2} como submódulo, podemos argumentar como antes para

mostrar que P_{p-2} é somando direto de $V_2 \otimes P_{p-1}$. Seja $U \leq V_2 \otimes P_{p-1}$ tal que $V_2 \otimes P_{p-1} \cong P_{p-2} \oplus U$. Assim como no caso anterior, podemos utilizar que P_{p-2} é indecomponível e que V_p é projetivo para concluir que V_p é fator de composição de U com a sua mesma multiplicidade em $V_2 \otimes P_{p-1}$, que é 2. Aplicando o Corolário 2.3.15 duas vezes, segue que $V_p \oplus V_p$ é somando direto de U e, consequentemente, $P_{p-2} \oplus V_p \oplus V_p$ é somando direto de $V_2 \otimes P_{p-1}$. Agora veja que P_{p-2} tem dois fatores de composição isomorfos a V_{p-2} e, como sua dimensão é divisível por p, devemos ter $\dim_k P_{p-2} \geq 2p$ (aqui utilizamos $p > 3$). Como $V_2 \otimes P_{p-1}$ tem dimensão $4p$, a única possibilidade é $\dim_k P_{p-2} = 2p$ e

$$V_2 \otimes P_{p-1} \cong P_{p-2} \oplus V_p \oplus V_p.$$

Dessa forma, além dos dois fatores isomorfos a V_{p-2}, P_{p-2} tem V_1 e V_3 como fatores de composição. Tais fatores constituem todos os fatores de composição do quociente $\operatorname{rad}(P_{p-2})/\operatorname{soc}(P_{p-2})$. Resta mostrar que

$$\frac{\operatorname{rad}(P_{p-2})}{\operatorname{soc}(P_{p-2})} \cong V_1 \oplus V_3.$$

Se isso não fosse o caso, esse quociente teria que ser unisseriado. Em particular, tomando o seu dual, os fatores de composição V_1 e V_3 trocariam de ordem e deveríamos obter um novo módulo não isomorfo. Mas, pela Proposição 2.3.9,

$$\left(\frac{\operatorname{rad}(P_{p-2})}{\operatorname{soc}(P_{p-2})}\right)^* \cong \frac{\operatorname{soc}(P_{p-2})^\perp}{\operatorname{rad}(P_{p-2})^\perp} = \frac{\operatorname{rad}(P_{p-2}^*)}{\operatorname{soc}(P_{p-2}^*)}.$$

Como $V_{p-2}^* \cong V_{p-2}$ (porque V_{p-2} é o único módulo simples com sua dimensão), o Corolário 2.3.18 nos dá $P_{p-2}^* \cong P_{p-2}$. Portanto, $\operatorname{rad}(P_{p-2})/\operatorname{soc}(P_{p-2})$ é isomorfo ao seu dual e não pode ser unisseriado, o que conclui a prova da estrutura de P_{p-2}.

Se $2 \leq n \leq p-2$, prosseguiremos por indução em n para mostrar a estrutura de P_n, mas começaremos em $p-2$ e iremos até 2. O caso base foi feito acima. Suponha que $2 < n \leq p-2$ e que P_j tem a estrutura desejada para $n \leq j \leq p-2$ (podemos tomar $j = p-1$ também, já que conhecemos P_{p-1}). Então $V_2 \otimes P_n$ possui uma série de submódulos cujos quocientes são isomorfos a

$$V_2 \otimes V_n,\ V_2 \otimes (V_{p+1-n} \oplus V_{p-1-n}) \ \text{ e } \ V_2 \otimes V_n,$$

que, pelo Lema 2.4.15, são também isomorfos a

$$V_{n-1} \oplus V_{n+1},\ V_{p+2-n} \oplus V_{p-n} \oplus V_{p-n} \oplus V_{p-n-2} \ \text{ e } \ V_{n-1} \oplus V_{n+1},$$

onde o termo V_{p-n-2} deve ser omitido se $n = p-2$. Como P_n é projetivo, o mesmo vale para $V_2 \otimes P_n$. Portanto, como V_{n+1} é submódulo de $V_2 \otimes P_n$, argumentamos como anteriormente para obter que P_{n+1} é um somando direto de $V_2 \otimes P_n$. Seja $U \leq V_2 \otimes P_n$ tal que $V_2 \otimes P_n \cong P_{n+1} \oplus U$. Como V_{n-1} é submódulo simples de $V_2 \otimes P_n$ e P_{n+1} não possui submódulos isomorfos a V_{n-1} (pois $\operatorname{soc}(P_{n+1}) \cong V_{n+1}$), segue que V_{n-1} é submódulo de U. Mas U também é projetivo, por ser somando direto de um módulo projetivo, então o mesmo argumento de antes se aplica para mostrar que P_{n-1} é um somando direto de U. Como sabemos os fatores de composição de $V_2 \otimes P_n$ e de P_{n+1}, vemos que os fatores de composição de U são V_{n-1} com multiplicidade 2, V_{p+2-n} e V_{p-n}. Os dois fatores isomorfos a V_{n-1} aparecem em P_{n-1}, mas, para a dimensão de P_{n-1} ser múltipla de p, os fatores V_{p+2-n} e V_{p-n} devem estar em P_{n-1} também e temos $U \cong P_{n-1}$ (aqui utilizamos que $2 < n \leq p-2$). Logo, $\operatorname{rad}(P_{n-1})/\operatorname{soc}(P_{n-1})$ tem V_{p+2-n} e V_{p-n} como fatores de composição e, assim como fizemos no estudo de P_{p-2}, concluímos que

$$\frac{\operatorname{rad}(P_{n-1})}{\operatorname{soc}(P_{n-1})} \cong V_{p+2-n} \oplus V_{p-n},$$

como queríamos demonstrar.

Finalmente, para acabar, falta apenas estudar P_1, o que faremos através de $V_2 \otimes P_2$. Como na indução realizada anteriormente, esse produto tensorial tem uma série de submódulos cujos quocientes são isomorfos a

$$V_1 \oplus V_3, \ V_p \oplus V_{p-2} \oplus V_{p-2} \oplus V_{p-4} \ \text{ e } \ V_1 \oplus V_3.$$

Como antes, $V_2 \otimes P_2$ é projetivo e tem V_3 como submódulo, então P_3 é um somando direto de $V_2 \otimes P_2$. Se $U \leq V_2 \otimes P_2$ é tal que $V_2 \otimes P_2 \cong P_3 \oplus U$, então U possui V_p como fator de composição, que é projetivo. Pelo Corolário 2.3.15, V_p é um somando direto de U e conseguimos encontrar $U' \leq U$ tal que

$$V_2 \otimes P_2 \cong P_3 \oplus V_p \oplus U'.$$

Por um argumento semelhante ao de antes, como V_1 é submódulo simples de $V_2 \otimes P_2$, então V_1 também tem de ser submódulo de U'. Mas U' é projetivo, então deve conter P_1. Como U' tem dimensão p, vale $U' \cong P_1$. Utilizando a estrutura que conhecemos dos módulos que aparecem na soma direta em destaque acima, vemos que V_1, V_{p-2} e V_1 são os fatores de composição de P_1. Do mesmo modo que argumentamos para P_{p-1}, concluímos que P_1 é unisseriado e seus fatores de composição aparecem na ordem desejada.

Capítulo 3

Módulos e subgrupos

Chegou o momento dos subgrupos de G entrarem em cena! Agora que já possuímos ferramentas suficientes, vamos aprofundar o nosso estudo de representações colocando um pouco mais de teoria de grupos. Aqui aparecerá uma filosofia central na teoria de representações modulares: os subgrupos *locais* de G determinam a estrutura dos kG-módulos. Tentaremos passar essa ideia ao longo deste capítulo.

Para iniciar, introduzimos uma nova ferramenta para construir kG-módulos: a indução. Ela transforma representações de subgrupos de G em representações de G e está associada a uma generalização do conceito de módulo livre. Após definirmos a indução de módulos de dois modos diferentes mas equivalentes, vemos que esta construção é bem natural e satisfaz diversas propriedades, dentre elas, a famosa Reciprocidade de Frobenius. Terminamos a primeira seção com dois teoremas importantes: a Fórmula de Decomposição de Mackey e o Critério de Indecomponibilidade de Green.

Assim como generalizamos o conceito de módulo livre na primeira seção, podemos generalizar o conceito de módulo projetivo. Nesse sentido, definimos a noção de projetividade relativa na segunda seção do capítulo. Ela nos leva rapidamente a teoremas surpreendentes, dentre eles o de que kG possui tipo de representação finito exatamente quando os p-subgrupos de Sylow de G são cíclicos. Em seguida, somos naturalmente levados às definições de vértice e fonte de um kG-módulo indecomponível, cujas propriedades essenciais são demonstradas.

As três últimas seções do capítulo apresentam a Correspondência de Green, que relaciona representações de G com representações de subgrupos locais. Primeiramente, abordamos um caso particular mais intuitivo e damos um exemplo concreto da Correspondência de Green para o grupo $\mathrm{SL}_2(p)$. Com a ideia principal da correspondência em mente, demonstramos o caso geral, que envolve algumas tecnicalidades em seu enunciado. Por fim, concluímos estudando a relação entre a Correspondência de Green e homomorfismos. Como consequência, provamos, dentre outras coisas, o Teorema de Burry-Carlson-Puig, que será necessário para demonstrar o Primeiro Teorema Principal de Brauer no Capítulo 4.

3.1 Indução de módulos

Vamos relembrar uma das caracterizações da definição de módulo livre: um kG-módulo U é livre se existe um subconjunto $B \subseteq U$ tal que toda função de B em um kG-módulo V qualquer se estende a um único homomorfismo de U em V. Sabemos que B é uma base de U como kG-módulo, então B é, em particular, um conjunto linearmente independente sobre k e é base do subespaço X de U gerado por B. Assim, veja que determinar uma função de B em V é o mesmo que determinar uma transformação linear de X em V. Portanto, U possui a seguinte propriedade universal: dada uma transformação linear $T : X \to V$, existe um único homomorfismo de kG-módulos $\varphi_T : U \to V$ tal que a restrição de φ_T a X é T.

Agora, note que um k-espaço vetorial é exatamente um kH-módulo, onde $H = \{1\}$ é o

subgrupo trivial de G! Essa observação nos permite generalizar a definição de módulo livre trocando o subespaço X por um kH-submódulo de U, onde, desta vez, H é um subgrupo qualquer de G.

Definição 3.1.1. Seja H um subgrupo de G. Um kG-módulo U é dito **relativamente H-livre** se existe um kH-submódulo X de U tal que todo homomorfismo de kH-módulos de X em um kG-módulo V qualquer se estende a um único homomorfismo de kG-módulos de U em V.

Na definição anterior, dizemos que U é relativamente H-livre com respeito a X. Se X' for um kH-módulo isomorfo a X, também diremos que U é relativamente H-livre com respeito a X'. Isso nos permite tomar um kH-módulo qualquer e perguntar se U é relativamente H-livre com respeito a tal módulo.

Notação 3.1.2. A partir de agora, H sempre denotará um subgrupo de G.

Como a definição de módulo relativamente livre é dada por uma propriedade universal, temos a seguinte unicidade: se U e V são kG-módulos relativamente H-livres com respeito a kH-submódulos X e Y, respectivamente, e se $X \cong Y$, então $U \cong V$. Mas será que sempre podemos construir um módulo relativamente H-livre com respeito a um kH-módulo qualquer?

Proposição 3.1.3. Se X é um kH-módulo, então existe um kG-módulo relativamente H-livre com respeito a X.

Demonstração: Seja $[G/H] \subseteq G$ um conjunto de representantes das classes laterais à esquerda de H em G e, por simplicidade, suponha que $1 \in [G/H]$. Para cada $s \in [G/H]$, torne o produto cartesiano $\{s\} \times X$ um k-espaço vetorial através da estrutura de X. Defina U como sendo a soma direta dos espaços $\{s\} \times X$ para $s \in [G/H]$. Identificando cada $\{s\} \times X$ como subespaço de U, veja que todo elemento se escreve de modo único na forma

$$\sum_{s \in [G/H]} (s, x_s),$$

onde cada $x_s \in X$. Vamos munir U de uma estrutura de kG-módulo. Se $g \in G$ e $s \in [G/H]$, então gs está em alguma classe lateral de H em G e, portanto, existem únicos $t \in [G/H]$ e $h \in H$ tais que $gs = th$. Com essas notações, defina

$$g \cdot (s, x) \coloneqq (t, hx)$$

para todo $x \in X$. Estendendo por linearidade, cada $g \in G$ define um operador linear em U. Agora, se $g' \in G$ e $g't = uh'$ para certos $u \in [G/H]$ e $h' \in H$, então

$$g' \cdot (g \cdot (s, x)) = g' \cdot (t, hx) = (u, h'hx) = (g'g) \cdot (s, x)$$

para todo $x \in X$, onde usamos que $(g'g)s = g'th = u(h'h)$. Portanto, isso de fato define uma estrutura de kG-módulo em U.

Vejamos que U é relativamente H-livre com respeito a X. Primeiramente, note que o subespaço $\{1\} \times X$ de U é um kH-submódulo naturalmente isomorfo a X. Vamos identificá-los a partir de agora. Se V é um kG-módulo qualquer, seja $\varphi : \{1\} \times X \to V$ um homomorfismo de kH-módulos. Defina uma transformação linear $\tilde{\varphi} : U \to V$ impondo $\tilde{\varphi}((s, x)) = s\varphi(x)$ para todos $s \in [G/H]$ e $x \in X$. Se $g \in G$ e $s \in [G/H]$, defina $t \in [G/H]$ e $h \in H$ como anteriormente e observe que

$$\tilde{\varphi}(g \cdot (s, x)) = \tilde{\varphi}((t, hx)) = t\varphi(hx) = th\varphi(x) = g(s\varphi(x)) = g \cdot \tilde{\varphi}((s, x))$$

para todo $x \in X$. Como $\tilde{\varphi}$ é linear, segue que $\tilde{\varphi}$ é um homomorfismo de kG-módulos. Além disso, $\tilde{\varphi}$ estende φ e é o único homomorfismo com essa propriedade. De fato, se $\psi : U \to V$ é um homomorfismo de kG-módulos que também estende φ, então

$$\psi((s, x)) = \psi(s \cdot (1, x)) = s \cdot \psi((1, x)) = s\varphi(x) = \tilde{\varphi}((s, x))$$

para todos $s \in [G/H]$ e $x \in X$ e, portanto, $\psi = \tilde{\varphi}$. Concluímos que U é relativamente H-livre com respeito a X. □

Observação 3.1.4. Algo importante de se notar é que a construção do módulo U na Proposição 3.1.3 não depende (a menos de isomorfismo) do conjunto de representantes $[G/H]$. Podemos até mesmo trocar o 1 por qualquer elemento $h \in H$. Nesse caso, é preciso verificar que $\{h\} \times X$ continua sendo um kH-submódulo de U isomorfo a X. Para isso, basta ver que $h' \cdot (h, x) = (h, h^{-1}h'hx) \in \{h\} \times X$ para $h' \in H$ e que a função que leva $x \in X$ em $(h, h^{-1}x) \in \{h\} \times X$ é um isomorfismo de kH-módulos.

Daqui em diante, sempre denotaremos por $[G/H]$ um conjunto de representantes das classes laterais à esquerda de H em G.

A construção da Proposição 3.1.3 nos permite dar duas caracterizações muito úteis:

Corolário 3.1.5. Seja U um kG-módulo. Suponha que U possua um subespaço X tal que U seja a soma direta dos subespaços[1] $\{gX \mid g \in G\}$. Se $H = \{g \in G \mid gX = X\}$, então X é um kH-submódulo de U e U é relativamente H-livre com respeito a X.

Demonstração: É imediato que H é um subgrupo de G e que X é um kH-submódulo de U. Para mostrar que U é relativamente H-livre com respeito a X, veremos que U possui a mesma estrutura interna do módulo construído na Proposição 3.1.3. Se $g, g' \in G$ são tais que $gX = g'X$, então note que as classes laterais gH e $g'H$ são iguais, e vice-versa. Dessa forma, pela nossa hipótese,

$$U = \bigoplus_{s \in [G/H]} sX,$$

onde podemos supor $1 \in [G/H]$. Como o operador de U induzido por $s \in [G/H]$ é bijetor, cada elemento de sX se escreve unicamente na forma sx com $x \in X$. Por isso, podemos identificar sX com $\{s\} \times X$. Agora, se $g \in G$ e $s \in [G/H]$, tome $t \in [G/H]$ e $h \in H$ tais que $gs = th$. Então

$$g \cdot (sx) = (gs)x = (th)x = t(hx)$$

para todo $x \in X$. Mas então g age do mesmo modo que age no kG-módulo relativamente H-livre construído anteriormente! Com isso, não é difícil definir um isomorfismo entre U e o módulo da Proposição 3.1.3 que fixa X, de onde segue o resultado. □

Corolário 3.1.6. Se U é um kG-módulo gerado por um kH-submódulo X, então U é relativamente H-livre com respeito a X se, e somente se,

$$\dim_k U = [G : H] \cdot \dim_k X.$$

Demonstração: A construção da Proposição 3.1.3 nos mostra que todo módulo relativamente H-livre com respeito a X tem dimensão $[G : H] \cdot \dim_k X$. Isso mostra uma das implicações. Para a implicação contrária, suponha que a dimensão de U seja como no enunciado e mostremos que U é relativamente H-livre com respeito a X. Por hipótese, U é a soma dos subespaços gX com $g \in G$. Mas X é kH-submódulo, então

$$U = \sum_{s \in [G/H]} sX.$$

A soma acima deve ser direta, já que a dimensão de U é a soma das dimensões de cada parcela. Consequentemente, vemos que $H = \{g \in G \mid gX = X\}$ e podemos aplicar o Corolário 3.1.5 para concluir o que queremos. □

[1] A notação $\{gX \mid g \in G\}$ foi utilizada para indicar o conjunto de todas as possibilidades distintas de gX. Assim, se $gX = hX$ para $g \neq h$, contamos gX apenas uma vez.

Daremos agora uma outra construção para o módulo relativamente livre. Como kH é uma subálgebra de kG, podemos **estender escalares** para tornar todo kH-módulo em um kG-módulo. Isso é usualmente feito a partir do produto tensorial, como veremos a seguir.

Seja V um kH-módulo qualquer. Por multiplicação à direita, kG é naturalmente um kH-módulo *à direita* e, por isso, podemos formar o produto tensorial[1] $kG \otimes_{kH} V$. Lembre que este é um k-espaço vetorial satisfazendo a seguinte propriedade universal: se V' é um k-espaço vetorial qualquer e $B : kG \times V \to V'$ é um mapa bilinear satisfazendo $B(ah, v) = B(a, hv)$ para todos $a \in kG, h \in H$ e $v \in V$, então existe uma única transformação linear $T : kG \otimes_{kH} V \to V'$ que faz o seguinte diagrama comutar:

$$\begin{array}{ccc} kG \otimes_{kH} V & \xrightarrow{T} & V' \\ \uparrow & \nearrow_{B} & \\ kG \times V & & \end{array}$$

O mapa vertical no diagrama acima é o mapa canônico que leva um par (a, v) em $a \otimes v$.

Dado $g \in G$, o mapa $B_g : kG \times V \to kG \otimes_{kH} V$ que leva o par (a, v) no tensor $ga \otimes v$ é bilinear e satisfaz $B_g(ah, v) = B_g(a, hv)$ para todos $a \in kG, h \in H$ e $v \in V$. Pela propriedade universal, temos uma transformação linear $T_g : kG \otimes_{kH} V \to kG \otimes_{kH} V$ que leva $a \otimes v$ em $ga \otimes v$. Isso define uma estrutura de kG-módulo em $kG \otimes_{kH} V$! Denotaremos esse módulo por V^G. Ele é o kG-módulo **induzido** pelo kH-módulo V.

Como era esperado, temos:

Proposição 3.1.7. Se V é um kH-módulo, então o kG-módulo induzido V^G é relativamente H-livre com respeito a V. Mais ainda, temos a decomposição

$$V^G = \bigoplus_{s \in [G/H]} s \otimes V$$

e cada subespaço $s \otimes V$ tem dimensão igual à de V.

Demonstração: Seja U um kG-módulo relativamente H-livre com respeito a V. Defina o mapa bilinear $B : kG \times V \to U$ dado por $B(g, v) = gv$ para todos $g \in G$ e $v \in V$ (estamos identificando V como kH-submódulo de U). É fácil ver que temos $B(ah, v) = B(a, hv)$ para todos $a \in kG$, $h \in H$ e $v \in V$, então a propriedade universal de V^G nos dá uma transformação linear $\varphi : V^G \to U$ tal que $\varphi(g \otimes v) = gv$ para todos $g \in G$ e $v \in V$. Se $g' \in G$, note que

$$\varphi(g'(g \otimes v)) = \varphi(g'g \otimes v) = g'gv = g'\varphi(g \otimes v),$$

provando que φ é um homomorfismo de kG-módulos. Como vimos na Proposição 3.1.3 (e na observação logo após), temos

$$U = \bigoplus_{s \in [G/H]} sV$$

e, com isso, segue que φ é sobrejetor. Mas vale $gh \otimes v = g \otimes hv$ para $g \in G$, $h \in H$ e $v \in V$, de onde segue

$$V^G = \sum_{g \in [G/H]} s \otimes V$$

e então $\dim_k V^G \leq [G : H] \cdot \dim_k V = \dim_k U$. Concluímos que φ é isomorfismo e que a soma acima é direta. Além disso, $\varphi(s \otimes V) = sV$, provando a última parte também. Note que a cópia de V dentro de V^G é $1 \otimes V = h \otimes V$ (para $h \in H$), que é um kH-submódulo de V^G. □

[1] Para mais detalhes a respeito do produto tensorial de módulos sobre anéis quaisquer, consulte, por exemplo, a Seção 3.7 do livro [14].

Exemplo 3.1.8. Como observamos no começo, módulos livres são relativamente H-livres quando $H = \{1\}$ é o subgrupo trivial de G. Por exemplo, note que $kG \cong k^G$, onde k é a representação trivial sobre o subgrupo trivial H. Também podemos verificar isso facilmente através da caracterização com o produto tensorial:

$$k^G = kG \otimes_{kH} k = kG \otimes_k k \cong kG.$$

Esse exemplo se generaliza da seguinte forma: seja Ω um conjunto no qual G age. Veja que

$$k\Omega \coloneqq \bigoplus_{\omega \in \Omega} k\omega$$

possui uma estrutura natural de kG-módulo estendendo a ação de G em Ω. Se a ação de G é transitiva, veja que estão satisfeitas as condições do Corolário 3.1.5 se tomarmos o subespaço $X = k\omega$, para qualquer $\omega \in \Omega$. Nesse caso, se H é o estabilizador de ω, então X é o kH-módulo trivial e temos $k\Omega \cong X^G$. Para obter o exemplo inicial, tome $\Omega = G$ e faça G agir em Ω por translação à esquerda. Mais geralmente, se H é subgrupo qualquer, podemos fazer G agir no conjunto de classes laterais à esquerda $\Omega = G/H$, logo, se k é o kH-módulo trivial, então $k^G \cong k\Omega = k[G/H]$. Quando H é normal em G, este $k[G/H]$ de fato pode ser considerado como a álgebra de grupo de G/H, vista como módulo sobre kG.

Há também outra generalização: note que kH é naturalmente um kH-submódulo de kG e, como $1 \in kH$, ele gera todo o kG. Comparando as dimensões, segue do Corolário 3.1.6 que $(kH)^G \cong kG$. Conhecendo as propriedades do produto tensorial sobre kH, isso é imediato:

$$(kH)^G = kG \otimes_{kH} kH \cong kG,$$

pois $V \otimes_{kH} kH \cong V$ para todo kH-módulo à direita V. Além disso, não é difícil verificar que o isomorfismo acima preserva a estrutura de kG-módulo.

Exemplo 3.1.9. Tome $G = S_3$ e k um corpo algebricamente fechado de característica zero. Se $H = \langle (1\ 2\ 3) \rangle$, considere o kH-módulo unidimensional V tal que

$$(1\ 2\ 3) \cdot v = \lambda v$$

para todo $v \in V$, onde $\lambda \in k$ é uma raiz cúbica primitiva da unidade. Assim, V^G tem dimensão $[S_3 : H] = 2$. Fixe $v \in V$ não nulo e considere a base de V^G dada pelos seguintes elementos:

$$x = (1 + \lambda(1\ 2)) \otimes v \quad \text{e} \quad y = (\lambda + (1\ 2)) \otimes v.$$

É fácil ver que $(1\ 2) \cdot x = y$ e $(1\ 2) \cdot y = x$. Também temos

$$\begin{aligned}(1\ 2\ 3) \cdot x &= (1\ 2\ 3) \otimes v + \lambda(1\ 3) \otimes v \\ &= 1 \otimes (1\ 2\ 3) \cdot v + \lambda(1\ 2) \otimes (1\ 3\ 2) \cdot v \\ &= \lambda \otimes v + \lambda^3(1\ 2) \otimes v \\ &= y\end{aligned}$$

e

$$\begin{aligned}(1\ 2\ 3) \cdot y &= \lambda(1\ 2\ 3) \otimes v + (1\ 3) \otimes v \\ &= \lambda \otimes (1\ 2\ 3) \cdot v + (1\ 2) \otimes (1\ 3\ 2) \cdot v \\ &= \lambda^2 \otimes v + \lambda^2(1\ 2) \otimes v \\ &= (-1 - \lambda)(1 \otimes v + (1\ 2) \otimes v) \\ &= -x - y.\end{aligned}$$

Logo, as ações de (1 2) e (1 2 3) induzem operadores em V^G que, na base $\{x, y\}$, são representados pelas matrizes

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

respectivamente. Consequentemente, V^G é isomorfo ao módulo de dimensão 2 construído no Exemplo 1.3.4!

Agora, listaremos diversas propriedades que a indução satisfaz. Dividiremos os resultados em dois lemas.

Lema 3.1.10. Sejam V, V_1 e V_2 kH-módulos e U um kG-módulo. Então:

(1) $(V_1 \oplus V_2)^G \cong V_1^G \oplus V_2^G$.

(2) Se V é livre (projetivo), então V^G é livre (projetivo).

(3) Se W é um kL-módulo, onde L é um subgrupo de H, então $(W^H)^G \cong W^G$.

(4) $(V^*)^G \cong (V^G)^*$.

(5) $U \otimes V^G \cong (U_H \otimes V)^G$.

Demonstração: Observe que $V_1^G \oplus V_2^G$ possui $V_1 \oplus V_2$ como kH-submódulo e, como V_1 e V_2 geram V_1^G e V_2^G, respectivamente, então $V_1 \oplus V_2$ gera $V_1^G \oplus V_2^G$. Comparando as dimensões, o Corolário 3.1.6 prova (1). Com isso, para provar (2), basta mostrar que V^G é livre se V o for. Mas se V é livre, então V é relativamente 1-livre com relação a um subespaço X, logo $V^G \cong (X^H)^G$. Se provarmos (3), então teremos que $V^G \cong X^G$, portanto, V^G será relativamente 1-livre, ou seja, livre[1].

Vamos demonstrar (3). Observe que

$$\dim_k (W^H)^G = [G : H] \cdot \dim_k W^H = [G : H][H : L] \cdot \dim_k W = [G : L] \cdot \dim_k W.$$

Pelo Corolário 3.1.6, basta provar que $(W^H)^G$ é gerado por um kL-módulo isomorfo a W. Identificando W dentro de W^H e W^H dentro de $(W^H)^G$, note que

$$(W^H)^G = \sum_{g \in G} gW^H = \sum_{g \in G} \sum_{h \in H} ghW = \sum_{g \in G} gW,$$

como preciso.

Vejamos que (4) é verdade. Note que

$$\widetilde{V} = \bigoplus_{\substack{s \in [G/H] \\ s \notin H}} s \otimes V$$

é um kH-submódulo de V^G. Dessa forma, $\widetilde{V}^\perp$ é um kH-submódulo de $(V^G)^*$. Pelo Lema 2.3.6, temos

$$\widetilde{V}^\perp \cong \left(\frac{V^G}{\widetilde{V}} \right)^* \cong (1 \otimes V)^* \cong V^*.$$

Como $\dim_k V^G = \dim_k (V^G)^*$ e $\dim_k V = \dim_k \widetilde{V}^\perp$, novamente pelo Corolário 3.1.6 é suficiente mostrar que $(V^G)^*$ é gerado como kG-módulo por $\widetilde{V}^\perp$. Se $s, t \in [G/H]$, $v \in V$ e $\varphi \in \widetilde{V}^\perp$, então

$$(t\varphi)(s \otimes v) = \varphi(t^{-1}s \otimes v)$$

[1] Outra forma de ver que V^G é livre é dada no segundo parágrafo do Exemplo 3.1.8.

é igual a 0 se $t \neq s$. Com isso, não é difícil ver que $t\widetilde{V}^{\perp}$ consiste dos funcionais lineares que se anulam em $s \otimes V$ para $s \neq t$. Como V^G é a soma direta dos subespaços $s \otimes V$ para $s \in [G/H]$, temos então que

$$(V^G)^* = \sum_{t \in [G/H]} t\widetilde{V}^{\perp},$$

como preciso.

Finalmente, provemos (5). Ressaltamos que os produtos tensoriais do enunciado são sobre k e a estrutura de módulo é dada como no Exemplo 1.3.5. Identificado V como um kH-submódulo de V^G, vemos que $U \otimes V^G$ possui $U_H \otimes V$ como um kH-submódulo. Além disso,

$$\dim_k(U \otimes V^G) = \dim_k U \cdot \dim_k V^G = [G : H] \cdot \dim_k U \cdot \dim_k V = [G : H] \cdot \dim_k(U_H \otimes V).$$

Pelo Corolário 3.1.6, falta mostrar que $U_H \otimes V$ gera $U \otimes V^G$. Como V gera V^G, todo elemento de V^G se escreve como soma de elementos da forma gv com $g \in G$ e $v \in V$. Consequentemente, todo elemento de $U \otimes V^G$ é soma de tensores da forma $u \otimes gv$ com $u \in U$, $v \in V$ e $g \in G$. Mas

$$u \otimes gv = g \cdot (g^{-1}u \otimes v) \in g(U_H \otimes V),$$

de onde concluímos o que queríamos. □

Lema 3.1.11. Sejam V, V_1, V_2 e V_3 kH-módulos e U um kG-módulo. Então:

(1) (Reciprocidade de Frobenius) Temos isomorfismos lineares

$$\mathrm{Hom}_{kG}(V^G, U) \cong \mathrm{Hom}_{kH}(V, U_H) \quad \text{e} \quad \mathrm{Hom}_{kG}(U, V^G) \cong \mathrm{Hom}_{kH}(U_H, V).$$

(2) Se $\alpha \in \mathrm{Hom}_{kH}(V_1, V_2)$, então existe um único $\alpha^G \in \mathrm{Hom}_{kG}(V_1^G, V_2^G)$ que estende α. Além disso, vale $(\mathrm{id}_V)^G = \mathrm{id}_{V^G}$ e, se $\alpha \in \mathrm{Hom}_{kH}(V_1, V_2)$ e $\beta \in \mathrm{Hom}_{kH}(V_2, V_3)$, então $(\beta\alpha)^G = \beta^G\alpha^G$.

(3) Se a sequência

$$0 \longrightarrow V_1 \xrightarrow{\alpha} V_2 \xrightarrow{\beta} V_3 \longrightarrow 0$$

é exata, então o mesmo vale para

$$0 \longrightarrow V_1^G \xrightarrow{\alpha^G} V_2^G \xrightarrow{\beta^G} V_3^G \longrightarrow 0$$

e uma cinde se, e só se, a outra cinde.

No item (3), dizemos que a primeira sequência exata cinde se β cinde. Pelo Exercício A.2.2, isso ocorre quando $\ker\beta$ é somando direto de V_2. Mas $\ker\beta = \mathrm{im}\,\alpha$, então β cinde se e somente se $\mathrm{im}\,\alpha$ é somando direto de V_2, ou seja, se e somente se α cinde.

Demonstração: O primeiro isomorfismo em (1) é uma consequência imediata da propriedade universal de módulos relativamente H-livres. De fato, se $\varphi : V \to U_H$ é um homomorfismo de kH-módulos, sabemos por essa propriedade universal que existe um único homomorfismo de kG-módulos $\psi : V^G \to U$ que estende φ. Não é difícil ver que a função de $\mathrm{Hom}_{kH}(V, U_H)$ em $\mathrm{Hom}_{kG}(V^G, U)$ que leva φ em ψ é linear e injetora. Mas ela também é sobrejetora, já que todo homomorfismo em $\mathrm{Hom}_{kG}(V^G, U)$ é a extensão de sua restrição a V.

Podemos usar esse primeiro isomorfismo para encontrar o segundo isomorfismo em (1). Pela Proposição 2.4.6 (ou então pelo Exercício A.2.10), temos

$$\mathrm{Hom}_{kG}(U, V^G) \cong \mathrm{Hom}_{kG}((V^G)^*, U^*).$$

Aplicando o item (4) do Lema 3.1.10 e o isomorfismo que mostramos no parágrafo anterior,

$$\mathrm{Hom}_{kG}((V^G)^*, U^*) \cong \mathrm{Hom}_{kG}((V^*)^G, U^*) \cong \mathrm{Hom}_{kH}(V^*, (U^*)_H) = \mathrm{Hom}_{kH}(V^*, (U_H)^*).$$

Usando mais uma vez a Proposição 2.4.6, concluímos que $\mathrm{Hom}_{kG}(U, V^G)$ e $\mathrm{Hom}_{kH}(U_H, V)$ são isomorfos, como preciso. Se quiser um isomorfismo explícito, veja o Exercício A.3.1.

A primeira parte do item (2) também é imediata da propriedade universal de módulos relativamente H-livres. Se $\alpha \in \mathrm{Hom}_{kH}(V_1, V_2)$, podemos identificar V_2 com o kH-submódulo $1 \otimes V_2$ de V_2^G e então α é um homomorfismo de kH-módulos de V_1 em V_2^G. Logo, existe um único $\alpha^G \in \mathrm{Hom}_{kG}(V_1^G, V_2^G)$ que estende α. Sendo homomorfismo de kG-módulos, note que α^G é dado por:

$$\alpha^G\left(\sum_{s\in[G/H]} s \otimes v_s\right) = \sum_{s\in[G/H]} \alpha^G(s(1\otimes v_s)) = \sum_{s\in[G/H]} s\alpha^G(1\otimes v_s) = \sum_{s\in[G/H]} s \otimes \alpha(v_s),$$

onde os v_s's são elementos de V_1. Usando essa definição explícita, é fácil ver que vale a segunda parte do item (2), que também segue da unicidade da extensão α^G de α.

Vamos para o último item. Uma observação inicial a ser feita é que, pela Proposição 3.1.7, todo elemento de V^G se escreve na forma

$$\sum_{s\in[G/H]} s \otimes v_s,$$

onde, para cada $s \in [G/H]$, v_s é um elemento de V unicamente determinado. Se a primeira sequência em (3) é exata, segue facilmente dessa observação e do parágrafo anterior que α^G é injetor e que β^G é sobrejetor. Também segue que

$$\mathrm{im}\,\alpha^G = \sum_{s\in[G/H]} s \otimes \mathrm{im}\,\alpha = \sum_{s\in[G/H]} s \otimes \ker\beta = \ker\beta^G.$$

Logo, a segunda sequência em (3) também é exata.

Agora, suponha que a primeira sequência exata em (3) cinda. Então β cinde e existe um homomorfismo $\gamma : V_3 \to V_2$ tal que $\beta\gamma = \mathrm{id}_{V_3}$. Pelo item (2), vale $\beta^G\gamma^G = \mathrm{id}_{V_3^G}$, ou seja, β^G cinde e, portanto, a segunda sequência exata também cinde. Vejamos a recíproca. Suponha que a segunda sequência cinda, isto é, suponha que exista $\psi \in \mathrm{Hom}_{kG}(V_3^G, V_2^G)$ tal que $\beta^G\psi$ seja a identidade de V_3^G. Seja $\pi : V_2^G \to V_2$ o homomorfismo[1] de kH-módulos que leva $1 \otimes v_2$ em v_2 e $s \otimes v_2$ em 0, se $v_2 \in V_2$, $s \in G$, $s \notin H$. Defina $\gamma : V_3 \to V_2$ por

$$\gamma(v_3) = \pi(\psi(1 \otimes v_3))$$

para todo $v_3 \in V_3$. Note que γ é homomorfismo de kH-módulos. Para concluir, mostremos que $\beta\gamma$ é a identidade em V_3. Se $v_3 \in V_3$, então podemos escrever

$$\psi(1 \otimes v_3) = \sum_{s\in[G/H]} s \otimes u_s$$

para certos $u_s \in V_2$ e podemos supor que $1 \in [G/H]$. Assim,

$$1 \otimes v_3 = \beta^G(\psi(1 \otimes v_3)) = \sum_{s\in[G/H]} s \otimes \beta(u_s)$$

[1]Note que π é a projeção com relação à decomposição $V_2^G = V_2 \oplus \widetilde{V}_2$, onde este último módulo é como definido na demonstração do item (4) do Lema 3.1.10.

e devemos ter $\beta(u_1) = v_3$. Mas

$$\gamma(v_3) = \pi(\psi(1 \otimes v_3)) = \pi\left(\sum_{s\in[G/H]} s \otimes u_s\right) = u_1,$$

então $\beta(\gamma(v_3)) = \beta(u_1) = v_3$, como preciso. □

Observação 3.1.12. Os itens (2) e (3) nos dizem que a indução define um funtor exato da categoria dos kH-módulos para a categoria dos kG-módulos. Por outro lado, é fácil ver que a restrição de kG para kH induz um funtor exato no outro sentido. A Reciprocidade de Frobenius nos diz que esses funtores são **adjuntos**! Na verdade, ainda é preciso verificar que podemos tomar os isomorfismos em (1) com uma certa condição de "naturalidade": veja o Exercício A.3.2.

O próximo resultado nos explicará como se comporta uma indução seguida de uma restrição. Precisaremos de dois conceitos antes de enunciá-lo.

Sejam H e L dois subgrupos de G. Dado $g \in G$, podemos formar a **classe lateral dupla**

$$LgH \coloneqq \{lgh \mid l \in L \text{ e } h \in H\}.$$

Assim como se prova no caso das classes laterais usuais, mostra-se que G é a união disjunta das diferentes classes laterais duplas. Usaremos a notação $[L\backslash G/H]$ para denotar um subconjunto de G de representantes dessas classes laterais duplas.

Agora, seja H um subgrupo de G e V um kH-módulo. Se $g \in G$, defina uma representação ${}^gV$ para gHg^{-1} da seguinte forma: ${}^gV$ é igual a V, como k-espaços vetoriais, mas definimos a ação de um $ghg^{-1} \in gHg^{-1}$ em $v \in {}^gV$ por

$$ghg^{-1} \cdot v \coloneqq hv,$$

onde usamos a estrutura do kH-módulo V no membro à direita. Vendo representações como homomorfismos de um grupo em $\mathrm{GL}(V)$, vemos que ${}^gV$ é obtida compondo o mapa de conjugação $gHg^{-1} \to H$ com o mapa $H \to \mathrm{GL}(V)$ que define a representação V. Diremos que ${}^gV$ é a representação obtida de V por **conjugação por** g. É importante ressaltar que já encontramos esse conceito antes, ele só não estava definido. De fato, sabemos que

$$V^G = \bigoplus_{s\in[G/H]} s \otimes V$$

pela Proposição 3.1.7, e o subespaço destacado $s\otimes V$ é um $k[sHs^{-1}]$-módulo naturalmente isomorfo a ${}^sV$: note que

$$shs^{-1} \cdot (s \otimes v) = sh \otimes v = s \otimes hv$$

para todos $h \in H$ e $v \in V$, então o isomorfismo linear de $s \otimes V$ em ${}^sV$ que leva $s \otimes v$ em v é um isomorfismo de $k[sHs^{-1}]$-módulos.

Teorema 3.1.13 (Fórmula de Decomposição de Mackey)**.** Sejam H e L subgrupos de G. Se V é um kH-módulo, então

$$(V^G)_L \cong \bigoplus_{g\in[L\backslash G/H]} (({}^gV)_{L\cap gHg^{-1}})^L.$$

Demonstração: Pela Proposição 3.1.7, temos a decomposição

$$V^G = \bigoplus_{s\in[G/H]} s \otimes V.$$

Dado $g \in [L\backslash G/H]$, vejamos que

$$W_g \coloneqq \bigoplus_{\substack{s\in[G/H]\\ s\in LgH}} s\otimes V$$

é kL-submódulo de $(V^G)_L$. Se $s \in [G/H]$ é tal que $s \in LgH$ e $l \in L$, então existem $t \in [G/H]$ e $h \in H$ tais que $ls = th$. Mas então $t = lsh^{-1} \in LgH$ e temos

$$l \cdot (s \otimes V) = t \otimes hV = t \otimes V \subseteq W_g,$$

mostrando que W_g é kL-módulo, como preciso.

Como as classes laterais duplas particionam G, vemos que

$$(V^G)_L = \bigoplus_{g\in[L\backslash G/H]} W_g$$

e, para concluir, bastar mostrarmos que

$$W_g \cong ({}^gV)_{L\cap gHg^{-1}})^L$$

para todo $g \in G$. Para isso, usaremos o Corolário 3.1.5. Note que $g \otimes V$ está contido em W_g, pois existem $s \in [G/H]$ e $h \in H$ tais que $g = sh$, então $s \in LgH$ e $g \otimes V = s \otimes V$ como espaços. Além disso, se $t \in [G/H]$ satisfaz $t \in LgH$, então existem $l \in L$ e $h \in H$ tais que $t = lgh$ e vale

$$t \otimes V = l \cdot (g \otimes V).$$

Assim, estão satisfeitas as hipóteses do Corolário 3.1.5! Logo, $g \otimes V$ é um kL'-módulo e $W_g \cong (g \otimes V)^L$, onde

$$L' = \{l \in L \mid l \cdot (g \otimes V) = g \otimes V\} = \{l \in L \mid g^{-1}lg \in H\} = L \cap gHg^{-1}.$$

Mas, quando definimos a conjugação de representações, vimos que $g\otimes V$ também é um $k[gHg^{-1}]$-módulo naturalmente isomorfo a ${}^gV$, então vemos que a restrição de $g \otimes V$ a L' é isomorfa a $({}^gV)_{L'}$, concluindo a demonstração. □

Exemplo 3.1.14. Sejam N um subgrupo normal de G e V um kN-módulo. Como sabemos, vale

$$V^G = \bigoplus_{g\in[G/N]} g \otimes V.$$

Mas $g\otimes V$ é uma representação sobre $gNg^{-1} = N$ isomorfa a ${}^gV$! Ou seja, a soma acima descreve V^G como soma de kN-módulos, logo

$$(V^G)_N \cong \bigoplus_{g\in[G/N]} {}^gV.$$

Isso está de acordo com a Fórmula de Decomposição de Mackey. A única parte menos aparente é que $[N\backslash G/N]$ também é um conjunto de representantes das classes laterais à esquerda de N em G. Isso segue do fato de que toda classe lateral dupla é uma classe lateral à esquerda, pois

$$NgN = g(g^{-1}Ng)N = gN$$

para todo $g \in G$, onde usamos que $g^{-1}Ng = N$, já que N é subgrupo normal.

Terminaremos a seção com mais um teorema:

Teorema 3.1.15 (Critério de Indecomponibilidade de Green)**.** Seja k um corpo algebricamente fechado de característica $p > 0$. Se N é um subgrupo normal de G com G/N p-grupo e V é um kN-módulo indecomponível, então V^G também é indecomponível.

Demonstração: É um resultado conhecido de teoria dos grupos que todo p-grupo finito $\tilde{G}$ é *solúvel*, logo existe uma cadeia de subgrupos

$$0 = \tilde{G}_0 \subseteq \tilde{G}_1 \subseteq \cdots \subseteq \tilde{G}_{r-1} \subseteq \tilde{G}_r = \tilde{G}$$

onde $\tilde{G}_{i-1}$ é normal em $\tilde{G}_i$ e o quociente $\tilde{G}_i/\tilde{G}_{i-1}$ é cíclico de ordem p, para todo índice $1 \leq i \leq r$. Aplicando essa propriedade a G/N, encontramos uma cadeia de subgrupos

$$N = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{r-1} \subseteq G_r = G$$

com G_{i-1} normal em G_i e de índice p, para todo $1 \leq i \leq r$. Agora, suponha que tenhamos provado o teorema quando o grupo quociente do enunciado possui ordem p. Consequentemente, V^{G_1} é indecomponível. Mas, aplicando o teorema de novo, segue que $(V^{G_1})^{G_2}$ também é indecomponível, e podemos prosseguir assim. Pelo item (3) do Lema 3.1.10, concluímos que V^G é indecomponível.

Assim, podemos supor que $[G : N] = p$. Como G/N é cíclico, podemos encontrar $g \in G$ tal que as potências $1, g, g^2, \ldots, g^{p-1}$ representem todas as classes laterais à esquerda de N em G. Como vimos no Exemplo 3.1.14,

$$(V^G)_N \cong \bigoplus_{i=0}^{p-1} {}^{g^i}V.$$

Pelo item (b) do Exercício A.3.4, cada ${}^{g^i}V$ é indecomponível, então essa é a decomposição de $(V^G)_N$ como soma de indecomponíveis. Agora, suponha que dois desses módulos sejam isomorfos, ou seja, que

$${}^{g^i}V \cong {}^{g^j}V$$

para $0 \leq i < j \leq p-1$. Com isso,

$$V = {}^{g^{-i}}({}^{g^i}V) \cong {}^{g^{-i}}({}^{g^j}V) = {}^{g^{j-i}}V$$

e, como $g^{j-i}N$ gera G/N, podemos iterar o isomorfismo acima para concluir, junto com o item (c) do Exercício A.3.4, que $V, {}^{g}V, \ldots, {}^{g^{p-1}}V$ são todos isomorfos. Por isso, ou todos os p somandos de $(V^G)_N$ são isomorfos ou todos eles são dois a dois não isomorfos. Trataremos os dois casos separadamente.

Suponha que os somandos de $(V^G)_N$ não sejam isomorfos. Seja W um somando direto não nulo de V^G. Pelo item (c) do Exercício A.3.4, $W \cong {}^{g}W$ e então $W_N \cong ({}^{g}W)_N = {}^{g}(W_N)$ como kN-módulos, onde, nessa última igualdade, usamos que N é normal. Como W_N é somando direto de $(V^G)_N$, o Teorema de Krull-Schmidt diz que W_N possui um somando direto isomorfo a ${}^{g^i}V$ para algum $0 \leq i \leq p-1$. Consequentemente, $W_N \cong {}^{g}(W_N)$ tem um somando direto isomorfo a ${}^{g}({}^{g^i}V) = {}^{g^{i+1}}V$. Prosseguindo assim, usamos o Teorema de Krull-Schmidt de novo para concluir que, numa decomposição de W_N como soma direta de indecomponíveis, temos somandos isomorfos a cada um dos módulos $V, {}^{g}V, \ldots, {}^{g^{p-1}}V$. Mas esses módulos são dois a dois não isomorfos, logo todos eles aparecem na decomposição em soma direta e

$$\dim_k W = \dim_k W_N \geq p \cdot \dim_k V = \dim_k V^G.$$

Segue que $W = V^G$ e então V^G é indecomponível, como queríamos.

Vamos estudar o caso onde todos os módulos ${}^{g^i}V$ são isomorfos. Desta vez, nossa estratégia será mostrar que $\mathrm{End}_{kG}(V^G)$ é local para poder aplicar o Corolário 2.1.8. Seja T o operador linear induzido em V^G por g. Assim, $\mathrm{End}_{kG}(V^G)$ consiste dos operadores lineares em V^G que comutam com T e com a ação de N, ou seja, $\mathrm{End}_{kG}(V^G)$ consiste dos elementos de $\mathrm{End}_{kN}((V^G)_N)$ que comutam com T. Vejamos que a conjugação por T deixa $\mathrm{End}_{kN}((V^G)_N)$ invariante. De fato, se S é um kN-endomorfismo de $(V^G)_N$, então

$$(TST^{-1})(nu) = gS(g^{-1}nu) = gS((g^{-1}ng)g^{-1}u) = g(g^{-1}ng)S(g^{-1}u) = n(TST^{-1})(u)$$

para todos $n \in N$ e $u \in V^G$, logo $TST^{-1} \in \mathrm{End}_{kN}((V^G)_N)$. Consequentemente, a conjugação por T induz um automorfismo de $\mathrm{End}_{kN}((V^G)_N)$. Note que $\mathrm{End}_{kG}(V^G)$ consiste dos pontos fixos desse automorfismo.

Como $(V^G)_N$ é a soma direta de p cópias de V, o Corolário 1.2.7 nos dá

$$\mathrm{End}_{kN}((V^G)_N) \cong M_p(\mathrm{End}_{kN}(V)).$$

Para $1 \leq i \leq p$, seja E_i o endomorfismo de $(V^G)_N$ que é a identidade em ${}^{g^{i-1}}V$ e é 0 nos outros somandos. Através do isomorfismo acima, E_i é levado na matriz elementar $e_{ii} \in M_p(\mathrm{End}_{kN}(V))$ que vale zero em todas as entradas exceto na entrada (i,i), onde é a identidade de V. Como $T({}^{g^i}V) = {}^{g^{i+1}}V$ (lembre que ${}^{g^i}V$ corresponde ao subespaço $g^i \otimes V$ de V^G), não é difícil ver que $TE_iT^{-1} = E_{i+1}$ (onde E_{p+1} denota E_1). Portanto, o automorfismo α de $M_p(\mathrm{End}_{kN}(V))$ que corresponde ao automorfismo induzido por T em $\mathrm{End}_{kN}((V^G)_N)$ permuta as matrizes $e_{11}, e_{22}, \ldots, e_{pp}$ ciclicamente. Com essas identificações, devemos mostrar que os pontos fixos de α formam uma álgebra local.

Faremos uma redução agora. Denote $E = \mathrm{End}_{kN}(V)$. Como $\mathrm{rad}(E)$ é um ideal nilpotente de E, é fácil verificar que $M_p(\mathrm{rad}(E))$ é um ideal nilpotente de $M_p(E)$. Dessa forma, $M_p(\mathrm{rad}(E))$ está contido no radical de $M_p(E)$. Mas V é indecomponível, então E é local e $E/\mathrm{rad}(E)$ é álgebra de divisão. Como k é algebricamente fechado, vale $E/\mathrm{rad}(E) \cong k$ e então $M_p(E)/M_p(\mathrm{rad}(E)) \cong M_p(k)$ é uma álgebra simples. Por isso, $M_p(\mathrm{rad}(E))$ é ideal maximal de $M_p(E)$ e devemos ter[1]

$$M_p(\mathrm{rad}(E)) = \mathrm{rad}(M_p(E)).$$

Portanto, como α é automorfismo de álgebra, α deve manter o radical $M_p(\mathrm{rad}(E))$ invariante, o que induz um automorfismo β no quociente $M_p(k)$. Vejamos que é suficiente mostrar que a álgebra dos pontos fixos de β é local. Denote por A a álgebra dos pontos fixos de α e por B a álgebra dos pontos fixos de β. Suponha que B seja local e mostremos que A é local. Se

$$\overline{A} := \frac{A + M_p(\mathrm{rad}(E))}{M_p(\mathrm{rad}(E))},$$

não é difícil ver que β fixa todo elemento de $\overline{A}$ e então $\overline{A}$ é subálgebra de B. Começaremos mostrando que $\overline{A}$ é local. Como $\mathrm{rad}(B)$ é ideal nilpotente de B, vale que $\overline{A} \cap \mathrm{rad}(B)$ é ideal nilpotente de $\overline{A}$ e está contido em $\mathrm{rad}(\overline{A})$. Passando a inclusão de $\overline{A}$ em B ao quociente, obtemos um homomorfismo de álgebras injetor

$$\frac{\overline{A}}{\overline{A} \cap \mathrm{rad}(B)} \longrightarrow \frac{B}{\mathrm{rad}(B)}.$$

Como B é local e k é algebricamente fechado, temos $B/\mathrm{rad}(B) \cong k$, então o quociente de $\overline{A}$ por $\overline{A} \cap \mathrm{rad}(B)$ é isomorfo a 0 ou a k, por questões de dimensão. Como $1 \notin \mathrm{rad}(B)$, o ideal $\overline{A} \cap \mathrm{rad}(B)$ não pode ser igual a $\overline{A}$, então esse quociente é isomorfo a k. Por conta da dimensão, segue que $\overline{A} \cap \mathrm{rad}(B)$ é ideal maximal de $\overline{A}$ que está contido em $\mathrm{rad}(\overline{A})$ e, portanto, $\overline{A} \cap \mathrm{rad}(B) = \mathrm{rad}(\overline{A})$. Obtemos então que $\overline{A}/\mathrm{rad}(\overline{A}) \cong k$ é uma álgebra de divisão e $\overline{A}$ é local. Com isso, vamos concluir que A é local. Pelo Segundo Teorema do Isomorfismo,

$$\frac{A}{A \cap M_p(\mathrm{rad}(E))} \cong \frac{A + M_p(\mathrm{rad}(E))}{M_p(\mathrm{rad}(E))} = \overline{A}.$$

Usando a definição de localidade, vale que o ideal $A \cap M_p(\mathrm{rad}(E))$ está contido num único ideal à esquerda maximal de A. Como $M_p(\mathrm{rad}(E))$ é nilpotente, então o mesmo vale para $A \cap M_p(\mathrm{rad}(E))$ e esse ideal está contido em $\mathrm{rad}(A)$. Mas então $A \cap M_p(\mathrm{rad}(E))$ está contido em todos os ideais

[1] É possível provar algo mais geral: se R é um anel, então $\mathrm{rad}(M_n(R)) = M_n(\mathrm{rad}(R))$. Veja a página 57 de [17].

à esquerda maximais de A. Concluímos que A possui um único ideal à esquerda maximal e A é local, como preciso.

Para finalmente acabar a demonstração, precisamos provar que B é de fato local. Como β é automorfismo de $M_p(k)$, o Teorema de Skolem-Noether (Exercício A.1.7) diz que β é interno, ou seja, existe uma matriz $M \in M_p(k)$ inversível tal que

$$\beta(X) = MXM^{-1}$$

para todo $X \in M_p(k)$. Como α permuta as matrizes elementares $e_{11}, \ldots, e_{pp}$ ciclicamente, então, passando ao quociente, β permuta as matrizes elementares correspondentes $\overline{e}_{11}, \ldots, \overline{e}_{pp}$ ciclicamente. Com isso, não é difícil ver que M é da forma[1]

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & \lambda_p \\ \lambda_1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_{p-1} & 0 \end{pmatrix}$$

para certos escalares $\lambda_1, \lambda_2, \ldots, \lambda_p \in k$ não nulos. Se $\mu \in k$ é tal que $\mu^p = \lambda_1 \cdots \lambda_p$, então a forma canônica de Jordan de M é um único bloco

$$J = \begin{pmatrix} \mu & 0 & 0 & \cdots & 0 & 0 \\ 1 & \mu & 0 & \cdots & 0 & 0 \\ 0 & 1 & \mu & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \mu & 0 \\ 0 & 0 & 0 & \cdots & 1 & \mu \end{pmatrix}.$$

Sabemos que B é a subálgebra de $M_p(k)$ formada pelas matrizes que comutam com M, então B é isomorfa à subálgebra formada pelas matrizes que comutam com J, pois M e J são semelhantes. Se $I \in M_p(k)$ denota a matriz identidade, então μI está no centro de $M_p(k)$ e, por isso, as matrizes que comutam com J são exatamente aquelas que comutam com $J - \mu I$. Mas vimos ao final do Exemplo 2.1.14 que uma matriz desse tipo é da forma

$$\begin{pmatrix} \alpha_1 & 0 & 0 & \cdots & 0 & 0 \\ \alpha_2 & \alpha_1 & 0 & \cdots & 0 & 0 \\ \alpha_3 & \alpha_2 & \alpha_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{p-1} & \alpha_{p-2} & \alpha_{p-3} & \cdots & \alpha_1 & 0 \\ \alpha_p & \alpha_{p-1} & \alpha_{p-2} & \cdots & \alpha_2 & \alpha_1 \end{pmatrix}$$

e, com um argumento análogo ao dado nesse exemplo, concluímos que a álgebra formada por essas matrizes é local. □

Suponha que o subgrupo N no enunciado do teorema anterior não seja normal em G, mas suponha que exista uma cadeia de subgrupos

$$N = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{r-1} \subseteq G_r = G$$

de modo que G_{i-1} seja normal em G_i e que o quociente G_i/G_{i-1} seja um p-grupo, para todo $1 \leq i \leq r$. Aplicando o Critério de Indecomponibilidade de Green diversas vezes e usando a

[1] Para não estender ainda mais a demonstração, este cálculo e as próximas afirmações estão compilados no Exercício A.3.5.

transitividade da indução (item (3) do Lema 3.1.10), segue que V^G é um kG-módulo indecomponível para todo kN-módulo V indecomponível. Sempre existe essa cadeia de subgrupos de N a G quando G é um p-grupo (veja, por exemplo, o Primeiro Teorema de Sylow em [12]), logo, temos o seguinte corolário:

Corolário 3.1.16. Sejam k um corpo algebricamente fechado de característica $p > 0$ e G um p-grupo. Se H é um subgrupo qualquer de G e V é um kH-módulo indecomponível, então V^G também é indecomponível.

3.2 Projetividade relativa, vértices e fontes

Na seção anterior, vimos como generalizar a definição de módulo livre utilizando os subgrupos de G. Com a mesma ideia, podemos generalizar a definição de módulo projetivo.

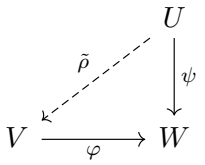
Proposição 3.2.1. Se U é um kG-módulo e H é um subgrupo de G, então as seguintes afirmações são equivalentes:

(1) U é um somando direto de um módulo relativamente H-livre.

(2) U é um somando direto de $(U_H)^G$.

(3) Se $\varphi : V \to U$ é um homomorfismo sobrejetor de kG-módulos cuja restrição φ_H cinde como homomorfismo de kH-módulos, então φ cinde.

(4) Sejam $\varphi : V \to W$ e $\psi : U \to W$ homomorfismos de kG-módulos. Se existe um homomorfismo de kH-módulos $\tilde{\rho} : U_H \to V_H$ que faz o seguinte diagrama comutar



então existe um homomorfismo de kG-módulos $\rho : U \to V$ que também faz o diagrama anterior comutar.

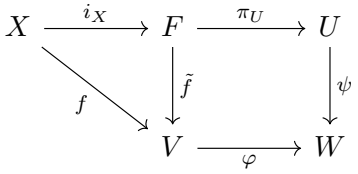
Dizemos que um kG-módulo U é **relativamente H-projetivo** se satisfaz as afirmações da Proposição 3.2.1. Quando $H = \{1\}$ é o subgrupo trivial de G, recuperamos a definição de módulo projetivo, pois um módulo relativamente 1-livre é o mesmo que um módulo livre. Veja que a condição (2) da Proposição 2.2.1 é equivalente à condição (3) da Proposição 3.2.1 quando $H = \{1\}$, pois toda transformação linear sobrejetora cinde. A condição (4) apresentada acima é a análoga da condição (3) da Proposição 2.2.1, mas note que, dessa vez, não exigimos a sobrejetividade de φ. Isso ocorre pois, quando $H = \{1\}$ e φ é sobrejetora, conseguimos achar uma transformação linear $\tilde{\rho}$ de U em V fazendo o diagrama comutar. Com isso, poderíamos ter substituído a hipótese da sobrejetividade pela hipótese mais fraca de que existe a transformação linear que torna o diagrama comutativo.

Demonstração: Iremos adaptar a demonstração da Proposição 2.2.1, mas, desta vez, temos que tomar cuidado, pois não podemos usar bases.

(1) $\implies$ (4). Suponha que U seja um somando direto de algum módulo F relativamente H-livre com respeito a algum kH-submódulo X. Sejam φ, ψ e $\tilde{\rho}$ como descritos no item (4) e vamos mostrar a existência do homomorfismo de kG-módulos $\rho : U \to V$. Denote por $i_X : X \to F$ e $i_U : U \to F$ as inclusões e por $\pi_U : F \to U$ uma projeção de F em U de acordo com alguma decomposição de F como soma direta de U e outro submódulo. Assim, a composta

$$f = \tilde{\rho} \circ \pi_U \circ i_X$$

é um homomorfismo de kH-módulos de X em V. Pela propriedade universal de módulos relativamente H-livres, existe um homomorfismo $\tilde{f} : F \to V$ que estende f, ou seja, $\tilde{f} i_X = f$. Assim, temos um diagrama:



Vamos mostrar que esse diagrama é comutativo. Como o "triângulo" à esquerda já é comutativo, temos que mostrar que $\varphi\tilde{f} = \psi\pi_U$. Mas vale

$$(\varphi\tilde{f})i_X = \varphi(\tilde{f}i_X) = \varphi f = \varphi(\tilde{\rho}\pi_U i_X) = (\varphi\tilde{\rho})(\pi_U i_X) = \psi(\pi_U i_X) = (\psi\pi_U)i_X,$$

então $\varphi\tilde{f}$ e $\psi\pi_U$ estendem um mesmo homomorfismo de kH-módulos de X em W, logo, eles são iguais pela propriedade universal de F. Finalmente, podemos definir o homomorfismo de kG-módulos ρ como sendo a composta

$$\rho = \tilde{f} \circ i_U.$$

Lembrando que $\pi_U i_U = \mathrm{id}_U$, temos

$$\varphi\rho = \varphi(\tilde{f}i_U) = (\varphi\tilde{f})i_U = (\psi\pi_U)i_U = \psi(\pi_U i_U) = \psi\,\mathrm{id}_U = \psi,$$

como preciso.

(4) $\implies$ (3). Seja $\varphi : V \to U$ um homomorfismo sobrejetor que cinde como homomorfismo de kH-módulos. Logo, existe $\tilde{\rho} : U_H \to V_H$ tal que $\varphi\tilde{\rho} = \mathrm{id}_U$. Assim, tomando $W = U$ e $\psi = \mathrm{id}_U$, a propriedade (4) nos dá um homomorfismo de kG-módulos $\rho : U \to V$ tal que $\varphi\rho = \psi = \mathrm{id}_U$. Isso prova que φ também cinde como homomorfismo de kG-módulos.

(3) $\implies$ (2). Como $(U_H)^G$ é relativamente H-livre com respeito a U_H, a identidade de U_H em U se estende a um homomorfismo sobrejetor $\varphi : (U_H)^G \to U$. Assim, denotando por $i_{U_H} : U_H \to (U_H)^G$ a inclusão canônica, vale $\varphi i_{U_H} = \mathrm{id}_U$. Mas i_{U_H} é homomorfismo de kH-módulos, logo, isso mostra que a restrição φ_H é um homomorfismo de kH-módulos que cinde. Por (3), segue que φ cinde como homomorfismo de kG-módulos e concluímos que U é um somando direto de $(U_H)^G$.

(2) $\implies$ (1). É imediato, porque $(U_H)^G$ é relativamente H-livre. □

Observação 3.2.2. A partir de agora, os p-subgrupos de G serão mais proeminentes. Mas eles só fazem sentido se $p > 0$. Por isso, faremos uma convenção: de agora em diante, a característica p de k **sempre será positiva**, a menos que explicitamente especifiquemos o contrário.

Quando relativizamos a noção de projetividade, ganhamos uma boa propriedade: todo kG-módulo é relativamente projetivo com respeito a um subgrupo especial!

Teorema 3.2.3. Se H é um subgrupo de G contendo um p-subgrupo de Sylow de G, então todo kG-módulo é relativamente H-projetivo.

Apesar de não parecer, essa é uma generalização do Teorema de Maschke. De fato, quando p não divide a ordem de G, podemos considerar que os p-subgrupos de Sylow de G são triviais, então podemos aplicar o teorema acima com $H = \{1\}$. Segue que todo kG-módulo é relativamente 1-projetivo, ou seja, é projetivo. Pelo Exercício A.2.4, kG é uma álgebra semissimples.

Demonstração: Seja U um kG-módulo qualquer. Para verificar que U é relativamente H-projetivo, vamos usar a caracterização (3) da Proposição 3.2.1. Seja $\varphi : V \to U$ um homomorfismo sobrejetor de kG-módulos que cinde como um homomorfismo de kH-módulos. Assim, o núcleo

W de φ é um somando direto de V se considerado como kH-módulo, ou seja, existe um kH-submódulo W' de V tal que $V = W \oplus W'$. Para mostrar que φ cinde, temos que verificar que W é um somando direto de V como kG-módulo. Para isso, adaptaremos a prova de uma das implicações do Teorema de Maschke.

Tome $\pi : V \to W$ como sendo a projeção com relação à decomposição $V = W \oplus W'$. Como W e W' são kH-submódulos de V, π é homomorfismo de kH-módulos. Se $[G/H]$ é um conjunto de representantes das classes laterais à esquerda de H em G, então defina $\pi' : V \to W$ por

$$\pi'(v) = \frac{1}{[G:H]} \sum_{s \in [G/H]} s\pi(s^{-1}v)$$

para $v \in V$. Como H contém um p-subgrupo de Sylow de G, então $[G : H]$ não é divisível por p e podemos definir a função acima. Além disso, a imagem de π' de fato está em W, pois a imagem de π é W e W é kG-submódulo de V. Como fizemos na prova do Teorema de Maschke, podemos verificar que π' é linear e que é a identidade se restrita a W, logo, é uma projeção linear em W. Se mostrarmos que π' é homomorfismo de kG-módulos, então π' será um homomorfismo de kG-módulos que cinde (a inversa à direita de π' é a inclusão de W em V) e seguirá que W é somando direto de V como kG-módulo, como precisamos. Se $g \in G$ e $s, t \in [G/H]$, então note que

$$g^{-1}sH = g^{-1}tH \iff sH = tH \iff s = t.$$

Portanto, variando $s \in [G/H]$, $g^{-1}s$ percorre todas as classes laterais de H em G. Para cada $s \in [G/H]$, tome $t_s \in [G/H]$ e $h_s \in H$ tais que $g^{-1}s = t_s h_s$. Pelo que vimos, vale

$$[G/H] = \{t_s \mid s \in [G/H]\}.$$

Consequentemente, se $v \in V$, então

$$\begin{aligned}
\pi'(gv) = \frac{1}{[G:H]} \sum_{s \in [G/H]} s\pi(s^{-1}gv) &= \frac{1}{[G:H]} \sum_{s \in [G/H]} g(g^{-1}s)\pi((g^{-1}s)^{-1}v) \\
&= g \cdot \frac{1}{[G:H]} \sum_{s \in [G/H]} t_s h_s \pi((t_s h_s)^{-1}v) \\
&= g \cdot \frac{1}{[G:H]} \sum_{s \in [G/H]} t_s h_s h_s^{-1} \pi(t_s^{-1}v) \\
&= g \cdot \frac{1}{[G:H]} \sum_{s \in [G/H]} s\pi(s^{-1}v) \\
&= g\pi'(v),
\end{aligned}$$

como queríamos. Na quarta igualdade, usamos que π é homomorfismo de kH-módulos e, na quinta igualdade, utilizamos que t_s percorre todo o conjunto de representantes $[G/H]$ quando variamos $s \in [G/H]$. □

Corolário 3.2.4. Seja H um subgrupo de G contendo um p-subgrupo de Sylow de G. Se U é um kG-módulo com U_H projetivo, então U é projetivo.

Demonstração: Pelo Teorema 3.2.3, U é relativamente H-projetivo e, pela caracterização (2) da Proposição 3.2.1, U é um somando direto de $(U_H)^G$. Como U_H é projetivo, o item (2) do Lema 3.1.10 nos dá que $(U_H)^G$ é projetivo e então o mesmo vale para U. □

Exemplo 3.2.5. Seja $G = \mathrm{SL}_2(p)$. Vimos no Exemplo 2.4.14 que o módulo simples V_p é projetivo quando visto como representação de um p-subgrupo de Sylow de G. Pelo Corolário 3.2.4, V_p é um kG-módulo projetivo! Isso prova a afirmação pendente nesse exemplo anterior.

O Teorema 3.2.3 também nos permite descobrir quando kG tem tipo de representação finito!

Lema 3.2.6. Seja P um p-subgrupo de Sylow de G. Então kG tem tipo de representação finito se, e somente se, kP tem tipo de representação finito.

Demonstração: Primeiramente, suponha que kG tenha tipo de representação finito. Note que um kP-módulo V é sempre um somando direto de $(V^G)_P$. Já encontramos um complemento de V em $(V^G)_P$, por exemplo, na demonstração do item (4) do Lema 3.1.10. Assim, existe um kG-módulo U tal que V é um somando direto de U_P. Se V é indecomponível, então podemos decompor U como soma direta de indecomponíveis e, pelo Teorema de Krull-Schmidt, V é somando direto da restrição de algum desses somandos. Isto é, se V é indecomponível, existe um kG-módulo indecomponível U' tal que V é somando direto de U'_P. Mas há apenas um número finito de classes de isomorfismo de kG-módulos indecomponíveis e a restrição de cada um desses módulos possui um número finito de somandos diretos. Logo, há apenas um número finito de possibilidades para a classe de isomorfismo do kP-módulo indecomponível V. Isso mostra que kP tem tipo de representação finito.

Reciprocamente, suponha que kP tenha tipo de representação finito. Pelo Teorema 3.2.3, todo kG-módulo U é relativamente P-projetivo. Assim, existe um kP-módulo V tal que U é somando direto de V^G. Se U é indecomponível, então, como a indução respeita somas diretas, podemos fazer como antes e supor que V é indecomponível. Como há apenas um número finito de classes de isomorfismo de kP-módulos indecomponíveis, procedemos como no parágrafo anterior para concluir que kG também tem tipo de representação finito. □

Teorema 3.2.7 (D. G. Higman)**.** Seja k um corpo de característica $p > 0$. Então kG tem tipo de representação finito se, e somente se, os p-subgrupos de Sylow de G são cíclicos.

Demonstração: Pelo Lema 3.2.6, podemos supor que G seja um p-grupo. Temos que mostrar que G tem tipo de representação finito se, e só se, G é cíclico. Se G for cíclico, vimos no Exemplo 2.1.12 que kG possui exatamente $|G|$ classes de isomorfismo de módulos indecomponíveis, logo, kG tem tipo de representação finito. É muito importante ressaltar que, no nosso caso, não é preciso supor que k é algebricamente fechado, porque a ordem de G é uma potência de p. De fato, com a notação do início do Exemplo 2.1.12, veja que a ordem do gerador g é uma potência de p, então a transformação linear induzida $T : V \to V$ possui apenas 1 como autovalor, já que 1 é a única raiz p-ésima de 1 em k. Com isso, a forma canônica de Jordan de T possui entradas em k e conseguimos decompor V como a soma de blocos de Jordan sem estender escalares a um corpo algebricamente fechado. O restante do argumento dado no exemplo funciona igualmente no nosso contexto.

Agora, suponha que G não seja cíclico. Por conta de algumas propriedades de p-grupos (Exercício A.3.7), $C_p \times C_p$ é um quociente de G. Restringindo escalares através do mapa quociente $kG \to k[C_p \times C_p]$, podemos tornar todo $k[C_p \times C_p]$-módulo em um kG-módulo. Como estamos restringindo escalares através de um mapa sobrejetor, a restrição preserva submódulos, de onde concluímos que todo $k[C_p \times C_p]$-módulo indecomponível se restringe a um kG-módulo indecomponível. Mas, como mostramos no Exemplo 2.1.14, $k[C_p \times C_p]$ não tem tipo de representação finito, então o mesmo vale para kG. □

Observação 3.2.8. Esse teorema nos dá mais uma ideia de como a estrutura do p-subgrupo de Sylow influencia as representações de G. Sentimos um pouco disso também no Exemplo 2.2.12, onde estudamos os projetivos indecomponíveis quando o p-subgrupo de Sylow é normal e cíclico. E até o Teorema de Maschke reflete algo nesse sentido: kG é semissimples se e só se os p-subgrupos de Sylow de G são triviais. No Capítulo 4, quando especializarmos da álgebra de grupo para os seus blocos, será o *grupo de defeito* que terá um papel análogo ao de p-subgrupo de Sylow, controlando como são as representações do bloco.

Agora, vamos explorar melhor sobre quais subgrupos um determinado módulo indecomponível é relativamente projetivo. Prepararemos o terreno para enunciar a Correspondência de Green nas próximas seções.

Notação 3.2.9. Sejam U e V kG-módulos. Quando U for (isomorfo a) um somando direto de V, escreveremos $U \mid V$. Como utilizaremos decomposições em somas diretas com mais frequência, essa abreviação será muito útil.

Definição 3.2.10. Seja U um kG-módulo indecomponível.

(1) Dizemos que um subgrupo Q de G é um **vértice** de U se Q é minimal com relação à propriedade de U ser relativamente Q-projetivo.

(2) Fixado um vértice Q de U, dizemos que um kQ-módulo indecomponível S é uma **fonte** de U (com relação a Q) se $U \mid S^G$.

Essa definição é uma forma de medir o quão longe U está de ser projetivo. Veja que, se U é projetivo, então ele é relativamente 1-projetivo e $Q = \{1\}$ é o único vértice de U. Reciprocamente, se o subgrupo trivial é um vértice de U, então U é relativamente 1-projetivo, ou seja, é projetivo.

Como U é relativamente G-projetivo, então certamente existe um vértice de U. Se Q é um deles, então U é relativamente Q-projetivo e existe um kQ-módulo T tal que $U \mid T^G$. Decompondo T como soma de indecomponíveis e induzindo a G, segue do Teorema de Krull-Schmidt que $U \mid S^G$ para algum submódulo indecomponível S de T, pois U é indecomponível. Assim, U também possui alguma fonte. Mas será que há apenas um vértice ou apenas uma fonte?

Lema 3.2.11. Se V é um kH-módulo e $g \in G$, então $({}^gV)^G \cong V^G$.

Demonstração: Como sabemos, podemos decompor

$$V^G = \bigoplus_{s \in [G/H]} s \otimes V,$$

onde $[G/H]$ é um conjunto de representantes das classes laterais à esquerda de H em G. Podemos tomar $[G/H]$ de modo que $g \in [G/H]$. Assim, $g \otimes V$ aparece na soma acima e é imediato que $g \otimes V$ gera V^G como kG-submódulo. Além disso, se $g' \in G$, então

$$g' \cdot (g \otimes V) = g \otimes V \iff g^{-1}g'g \in H \iff g' \in gHg^{-1}.$$

Como $g \otimes V$ é um $k[gHg^{-1}]$-módulo isomorfo a ${}^gV$, segue do Corolário 3.1.5 que $V^G \cong ({}^gV)^G$, como queríamos. □

Isso nos diz que a indução não "percebe" a conjugação. Se U é um kG-módulo indecomponível relativamente Q-projetivo, então U também será relativamente gQg^{-1}-projetivo para todo $g \in G$. Com isso, não é difícil ver que um conjugado de um vértice de U é também um vértice. Agora, fixado um vértice Q de U, seja S um kQ-módulo indecomponível que é fonte de U. Se

$$N_G(Q) \coloneqq \{g \in G \mid gQg^{-1} = Q\}$$

é o **normalizador** de Q em G, então ${}^gS$ sempre é um kQ-módulo indecomponível para todo $g \in N_G(Q)$ e ainda temos $U \mid ({}^gS)^G$ pelo lema anterior, já que $U \mid S^G$. Ou seja, ${}^gS$ também é fonte de U para todo $g \in N_G(Q)$.

O próximo teorema diz que encontramos todos os vértices e todas as fontes de U no parágrafo anterior!

Teorema 3.2.12. Sejam U um kG-módulo indecomponível e $Q \leq G$ um vértice de U. Valem as seguintes afirmações:

(1) Se $H \leq G$, então U é relativamente H-projetivo se, e somente se, H contém um conjugado de Q.

(2) Os vértices de U são exatamente os conjugados de Q. Além disso, Q é um p-grupo.

(3) Uma fonte de U (com relação a Q) é única a menos de conjugação por um elemento de $N_G(Q)$. Ademais, toda fonte de U é um somando direto de U_Q e possui Q como vértice.

Demonstração: Seja $H \leq G$ e suponha que H contenha gQg^{-1} para algum $g \in G$. Como observamos antes de enunciar o teorema, U é relativamente projetivo com relação a gQg^{-1} e então $U \mid (U_{gQg^{-1}})^G$. Pela transitividade da indução,

$$((U_{gQg^{-1}})^H)^G \cong (U_{gQg^{-1}})^G$$

e então U é somando direto de um módulo relativamente H-livre. Portanto, U é relativamente H-projetivo.

Como U é relativamente Q-projetivo, temos $U \mid (U_Q)^G$. Como U é indecomponível, podemos encontrar um somando indecomponível S de U_Q tal que $U \mid S^G$. Agora, vamos provar a implicação restante em (1). Suponha que U seja relativamente H-projetivo e seja V um kH-módulo tal que $U \mid V^G$. Usando novamente a indecomponibilidade de U, podemos tomar V indecomponível também. Como $S \mid U_Q$ e $U_Q \mid (V^G)_Q$, segue que S é um somando direto de $(V^G)_Q$. Pela Fórmula de Decomposição de Mackey,

$$(V^G)_Q \cong \bigoplus_{g \in [Q\backslash G/H]} ({}^gV)_{Q \cap gHg^{-1}})^Q$$

e então, como S é indecomponível, existe $g \in [Q\backslash G/H]$ com

$$S \mid ({}^gV)_{Q \cap gHg^{-1}})^Q.$$

Induzindo a G, obtemos que

$$S^G \mid (({}^gV)_{Q \cap gHg^{-1}})^Q)^G \cong ({}^gV)_{Q \cap gHg^{-1}})^G$$

e, como $U \mid S^G$, temos que U é um somando direto do módulo mais à direita na expressão acima. Logo, U é relativamente projetivo com relação a $Q \cap gHg^{-1}$. Da minimalidade de Q, é preciso valer $Q = Q \cap gHg^{-1}$ e, consequentemente, $g^{-1}Qg \subseteq H$, provando que H contém um conjugado de Q.

Vejamos o porquê de (2) ser verdade. Já sabemos que todo conjugado de Q é um vértice de U. Reciprocamente, seja Q' um vértice qualquer de U. Como U é relativamente Q'-projetivo, o item (1) implica que Q' contém um conjugado de Q. Da minimalidade de Q', deve valer a igualdade, mostrando que Q' é um conjugado de Q. Agora, vamos mostrar que Q é um p-grupo. Se $P \leq Q$ é um p-subgrupo de Sylow, então o Teorema 3.2.3 nos dá que S é relativamente P-projetivo, ou seja, existe um kP-módulo T tal que $S \mid T^Q$. Mas então U é somando direto de S^G e $S^G \mid (T^Q)^G \cong T^G$, mostrando que U também é relativamente P-projetivo. Da minimalidade de Q, temos que $Q = P$ e Q é um p-grupo.

Vamos concluir demonstrando (3). Seja S a fonte de U construída anteriormente. Como notamos antes de começar a provar o teorema, ${}^gS$ também é fonte de U para todo $g \in N_G(Q)$. Mostremos a recíproca. Seja V um kQ-módulo indecomponível tal que $U \mid V^G$. Imitando a demonstração do item (1), encontramos $g \in G$ tal que

$$S \mid ({}^gV)_{Q \cap gQg^{-1}})^Q$$

e obtemos que

$$U \mid ({}^gV)_{Q \cap gQg^{-1}})^G.$$

Da minimalidade de Q, vale $Q = Q \cap gQg^{-1}$. Portanto, $Q = gQg^{-1}$ e $g \in N_G(Q)$. Também temos $S \mid ((^gV)_Q)^Q = {}^gV$ e, como V é indecomponível, devemos ter $S \cong {}^gV$ e então $V \cong {}^{g^{-1}}S$, como queríamos. Para a última afirmação, como S é somando direto de U_Q, todo conjugado ${}^gS$ com $g \in N_G(Q)$ é somando direto de ${}^g(U_Q)$, que é isomorfo a U_Q pelo Exercício A.3.4. Ou seja, toda fonte de U é somando direto de U_Q. Além disso, se $Q' \leq Q$ é um vértice de S, então S é relativamente Q'-projetivo e, como $U \mid S^G$, segue da transitividade da indução que U também é relativamente Q'-projetivo. Mas $Q' \leq Q$ e Q é vértice de U, então vale $Q' = Q$, ou seja, Q é um vértice de S. □

Observação 3.2.13. Como acabamos de demonstrar, qualquer vértice de um módulo indecomponível é um p-subgrupo de G. Essa é a primeira aparição importante de um p-subgrupo que não é necessariamente de Sylow. Veja que também estamos lidando com normalizadores de p-subgrupos. Chamaremos esses p-subgrupos e seus normalizadores de **subgrupos locais** de G. Eles serão cada vez mais recorrentes.

Exemplo 3.2.14. Denote por k o kG-módulo trivial. Vamos mostrar que os vértices de k são os p-subgrupos de Sylow de G. Dessa forma, k está o mais longe possível de ser projetivo! Encontrar as fontes de k é mais fácil: como uma fonte de k em relação a um vértice Q é um somando direto do módulo unidimensional k_Q, concluímos que k_Q é a única fonte de k.

Fixe P um p-subgrupo de Sylow qualquer de G e Q um vértice de k. Como k é relativamente Q-projetivo, então $k \mid (k_Q)^G$ e

$$k_P \mid ((k_Q)^G)_P \cong \bigoplus_{g \in [P\backslash G/Q]} (({}^g(k_Q))_{P \cap gQg^{-1}})^P.$$

Mas ${}^g(k_Q) \cong k_{gQg^{-1}}$ e, como k_P é indecomponível, existe $g \in [P\backslash G/Q]$ tal que

$$k_P \mid (k_{P \cap gQg^{-1}})^P.$$

Seja $R = P \cap gQg^{-1}$. Vamos mostrar que $(k_R)^P$ é indecomponível. Com isso, devemos ter um isomorfismo $k_P \cong (k_R)^P$ e, comparando dimensões, segue $R = P$. Assim, $P \subseteq gQg^{-1}$. Como ambos são p-grupos e P é um Sylow, deve valer a igualdade[1] $P = gQg^{-1}$, mostrando que P é um vértice de k.

Provemos o que nos resta. Mostraremos que o soco de $(k_R)^P$ é unidimensional e então $(k_R)^P$ será indecomponível pelo Exemplo 2.1.11. Como P é um p-grupo, então k_P é o único kP-módulo simples e segue que a dimensão de $\operatorname{soc}((k_R)^P)$ é a multiplicidade de k_P nesse soco. Pelo Exercício A.1.11, essa multiplicidade é

$$\dim_k \operatorname{Hom}_{kP}(k_P, (k_R)^P) = \dim_k \operatorname{Hom}_{kR}(k_R, k_R) = 1,$$

onde usamos a Reciprocidade de Frobenius. Isso demonstra o que queríamos.

Observação 3.2.15. O exemplo anterior mostra a recíproca do Teorema 3.2.3! Se H é um subgrupo de G e todo kG-módulo é relativamente H-projetivo, então, em particular, o módulo trivial é relativamente H-projetivo. Mas então H deve conter um vértice do módulo trivial, que é um p-subgrupo de Sylow de G.

Observação 3.2.16. Acabamos de verificar que os p-subgrupos de Sylow de G aparecem como vértices de um kG-módulo indecomponível. Vale algo mais geral: todo p-subgrupo de G é vértice de um kG-módulo indecomponível! Veja o Exercício A.3.11.

Ao final do exemplo anterior, acabamos provando um resultado interessante que destacaremos para o futuro:

[1] Isso dá uma outra prova de que os p-subgrupos de Sylow de G são conjugados!

Corolário 3.2.17. Se G é um p-grupo e k denota o kG-módulo trivial, então $(k_H)^G$ é indecomponível para todo subgrupo H de G.

Terminaremos a seção com algumas propriedades úteis sobre vértices.

Lema 3.2.18. Se U é um kG-módulo indecomponível com vértice Q e H é um subgrupo de G contendo Q, então, para cada escolha de duas das afirmações a seguir, existe um kH-módulo indecomponível V que as satisfaz:

(1) $V \mid U_H$.

(2) $U \mid V^G$.

(3) Q é um vértice de V.

Demonstração: Temos três pares de afirmações a considerar:

(1) e (2). Como H contém Q, U é relativamente H-projetivo, logo, $U \mid (U_H)^G$. Decompondo U_H como soma de indecomponíveis, encontramos um kH-módulo indecomponível V tal que $V \mid U_H$ e $U \mid V^G$. Aqui utilizamos o Teorema de Krull-Schmidt, pois U é indecomponível. Assim, V satisfaz as duas afirmações escolhidas.

(1) e (3). Seja S uma fonte de U com relação a Q. Pelo Teorema 3.2.12, $S \mid U_Q = (U_H)_Q$. Decompondo U_H como soma de indecomponíveis e usando que S é kQ-módulo indecomponível, encontramos um kH-módulo indecomponível V tal que $V \mid U_H$ e $S \mid V_Q$. Provaremos que Q é um vértice de V, como preciso. Se R é um vértice de V, então existe um kR-módulo W tal que $V \mid W^H$. Como $S \mid V_Q$, então $S \mid (W^H)_Q$. Usando a Fórmula de Decomposição de Mackey e que S é indecomponível, encontramos $h \in H$ tal que

$$S \mid ({}^hW)_{Q \cap hRh^{-1}})^Q.$$

Mas Q é vértice de S pelo Teorema 3.2.12, logo, $Q = Q \cap hRh^{-1}$ e temos $Q \subseteq hRh^{-1}$. Por outro lado, usando que $V \mid U_H$ e que $U \mid S^G$, segue que $V \mid (S^G)_H$. Novamente pela Fórmula de Decomposição de Mackey e pela indecomponibilidade de V, encontramos $g \in G$ tal que

$$V \mid ({}^gS)_{H \cap gQg^{-1}})^H.$$

Então V é relativamente $(H \cap gQg^{-1})$-projetivo e $H \cap gQg^{-1}$ contém um conjugado de R. Essa última continência nos dá que a ordem de R é menor ou igual à ordem de Q. Mas valia $Q \subseteq hRh^{-1}$, então concluímos que vale a igualdade $Q = hRh^{-1}$ e, como Q é conjugado de R em H, vemos que Q é vértice de V.

(2) e (3). Seja S uma fonte de U com relação a Q. Então $U \mid S^G \cong (S^H)^G$. Decompondo S^H como soma de indecomponíveis e usando a indecomponibilidade de U, encontramos um kH-módulo indecomponível V tal que $V \mid S^H$ e $U \mid V^G$. Resta mostrarmos que Q é um vértice de V. Primeiramente, V é relativamente Q-projetivo, pois $V \mid S^H$. Agora, se R é um vértice de V contido em Q, então existe um kR-módulo W tal que $V \mid W^H$ e temos $U \mid (W^H)^G \cong W^G$. Isso diz que U é relativamente R-projetivo, então devemos ter $R = Q$, pois Q é vértice de U. Ou seja, mostramos que Q é um vértice de V. □

Observação 3.2.19. Quando tivermos a Correspondência de Green em mãos, será possível provar que existe um kH-módulo indecomponível V satisfazendo as três condições do lema acima simultaneamente, desde que exijamos que $H \supseteq N_G(Q)$.

Lema 3.2.20. Se Q é um subgrupo de G contido em H e se V é um kH-módulo relativamente Q-projetivo, então

$$(V^G)_H \cong V \oplus W,$$

onde todo somando indecomponível de W é relativamente projetivo com relação a um subgrupo da forma $H \cap gQg^{-1}$ para $g \in G$ e $g \notin H$.

Demonstração: Como V é um módulo relativamente Q-projetivo, existe um kQ-módulo U tal que $V \mid U^H$. Seja T um kH-módulo tal que $U^H \cong V \oplus T$. Então $U^G \cong V^G \oplus T^G$ e vale

$$(U^G)_H \cong V \oplus W \oplus T \oplus X,$$

onde $(V^G)_H \cong V \oplus W$ e $(T^G)_H \cong T \oplus X$ para certos kH-módulos W e X. Aqui, para ver que $V \mid (V^G)_H$ e $T \mid (T^G)_H$, lembre que a cópia de um módulo dentro de seu módulo induzido é um somando direto. Por outro lado, escolhendo um conjunto de representantes $[H\backslash G/Q]$ contendo 1, a Fórmula de Decomposição de Mackey nos dá

$$(U^G)_H \cong \bigoplus_{g \in [H\backslash G/Q]} ({}^gU)_{H \cap gQg^{-1}})^H \cong U^H \oplus Y,$$

onde o somando correspondente ao elemento $1 \in [H\backslash G/Q]$ é U^H, enquanto Y é a soma direta dos outros termos. Como apenas a classe lateral dupla da identidade contém H, concluímos que todo somando indecomponível de Y é relativamente projetivo com relação a um subgrupo da forma $H \cap gQg^{-1}$, onde $g \notin H$. Aplicando o Teorema de Krull-Schmidt nas duas decomposições obtidas, segue que $Y \cong W \oplus X$ e W possui a propriedade desejada. □

Lema 3.2.21. Seja H um subgrupo qualquer de G. Se U é um kG-módulo indecomponível com vértice Q e fonte trivial, então U_H possui um somando indecomponível com um vértice contendo $Q \cap H$.

Demonstração: Denote por k o kG-módulo trivial. Como U tem fonte trivial, temos $k_Q \mid U_Q$ pelo item (3) do Teorema 3.2.12. Restringindo a $Q \cap H$, temos $k_{Q\cap H} \mid U_{Q\cap H}$. Decompondo U_H como soma de indecomponíveis, encontramos um kH-módulo indecomponível V tal que $V \mid U_H$ e $k_{Q\cap H} \mid V_{Q\cap H}$. Seja R um vértice de V. Para concluir o lema, vamos mostrar que um conjugado de R contém $Q \cap H$. Como V é relativamente R-projetivo, podemos aplicar a Fórmula de Decomposição de Mackey para obter que todo somando indecomponível de $V_{Q\cap H}$ é relativamente projetivo com relação a $(Q \cap H) \cap hRh^{-1}$ para algum $h \in H$. Em particular, como $k_{Q\cap H} \mid V_{Q\cap H}$, existe $h \in H$ tal que $k_{Q\cap H}$ é relativamente projetivo com relação a $Q \cap H \cap hRh^{-1}$. Mas, como $Q \cap H$ é p-grupo, vimos no Exemplo 3.2.14 que $Q \cap H$ é vértice de $k_{Q\cap H}$, então devemos ter $Q \cap H \cap hRh^{-1} = Q \cap H$ e $Q \cap H \subseteq hRh^{-1}$, como preciso. □

Lema 3.2.22. Suponha que k seja algebricamente fechado. Seja U um kG-módulo tal que U_N é indecomponível, onde N é um subgrupo normal de G. Se Q é um vértice de U, então QN/N é um p-subgrupo de Sylow de G/N.

Demonstração: Seja P um p-subgrupo de Sylow de G que contém Q, de modo que PN/N é um p-subgrupo de Sylow[1] de G/N que contém QN/N. Como $U_N = (U_{QN})_N = (U_{PN})_N$ é indecomponível, então U_{QN} e U_{PN} são ambos indecomponíveis. Pelo Lema 3.2.18, existe um somando indecomponível de U_{PN} que possui Q como vértice. Da indecomponibilidade de U_{PN}, esse somando é o próprio U_{PN} e, como $Q \subseteq QN$, em particular vale que U_{PN} é relativamente QN-projetivo e temos $U_{PN} \mid (U_{QN})^{PN}$. Se mostrarmos que $(U_{QN})^{PN}$ é indecomponível, deveremos ter um isomorfismo $U_{PN} \cong (U_{QN})^{PN}$ e, comparando as dimensões, temos $QN = PN$. Dessa forma, $QN/N = PN/N$ é p-subgrupo de Sylow de G/N, como desejado.

Provemos o que falta. Como PN/N é p-grupo, conseguimos encontrar uma cadeia de subgrupos de QN/N a PN/N onde cada termo é normal no seguinte e, claramente, cada quociente é um p-grupo. Pelo Teorema da Correspondência, obtemos uma cadeia com a mesma propriedade indo de QN a PN. Mas U_{QN} é indecomponível e k é algebricamente fechado, então podemos aplicar o Critério de Indecomponibilidade de Green repetidas vezes para concluir que $(U_{QN})^{PN}$ é indecomponível, como queríamos. □

[1] Para ver que isto é um p-subgrupo de Sylow, lembre que a ordem de PN/N é igual a $|P|$ dividido por $|P \cap N|$. Se p^a e p^b são as maiores potências de p que dividem $|G|$ e $|N|$, então não é difícil ver que a maior potência de p que divide $|PN/N|$ é p^{a-b}.

3.3 A Correspondência de Green: considerações iniciais

Uma das principais ideias da teoria de representações modulares de grupos finitos é a de que os subgrupos locais de G determinam as representações de G. Lembre que estes subgrupos locais são dados pelos p-subgrupos de G e seus normalizadores. Na seção anterior, tais subgrupos começaram a aparecer quando estudamos os vértices dos kG-módulos indecomponíveis. A Correspondência de Green, que estudaremos agora, mostra ainda mais a importância de entender a "estrutura local" de G.

Para motivar e tornar as ideias mais acessíveis, consideraremos apenas um caso particular nesta seção. Fixe P um p-subgrupo de Sylow de G. Assumiremos ao longo desta seção que P é um subgrupo de **interseção trivial**, isto é, se $g \in G$, então $P \cap gPg^{-1}$ é igual a P ou a $\{1\}$. Denotando o normalizador de P em G por $L = N_G(P)$, então $P \cap gPg^{-1} = \{1\}$ sempre que $g \notin L$.

O caso da Correspondência de Green que abordaremos agora é dado pelo seguinte teorema:

Teorema 3.3.1. Sejam P um p-subgrupo de Sylow de G e $L = N_G(P)$. Se P é de interseção trivial, então as seguintes afirmações são verdadeiras:

(1) Seja U um kG-módulo indecomponível e não projetivo. Se decompormos U_L como soma de indecomponíveis, então existe um único somando indecomponível $f(U)$ que não é projetivo. Assim, podemos escrever
$$U_L \cong f(U) \oplus X$$
para algum kL-módulo projetivo X.

(2) Seja V um kL-módulo indecomponível e não projetivo. Se decompormos V^G como soma de indecomponíveis, então existe um único somando indecomponível $g(V)$ que não é projetivo. Assim, podemos escrever
$$V^G \cong g(V) \oplus Y$$
para algum kG-módulo projetivo Y.

(3) Temos isomorfismos $g(f(U)) \cong U$ e $f(g(V)) \cong V$. Isso estabelece uma correspondência biunívoca entre as classes de isomorfismo de kG-módulos indecomponíveis não projetivos e as classes de isomorfismo de kL-módulos indecomponíveis não projetivos.

Anteriormente, estudamos muito mais as propriedades dos projetivos indecomponíveis. Observe que agora estamos obtendo informações sobre módulos indecomponíveis que não são projetivos, complementando o nosso estudo a respeito dos kG-módulos.

Demonstração: Vamos começar com o item (2). Seja V um kL-módulo indecomponível e não projetivo. Pela Fórmula de Decomposição de Mackey, temos
$$(V^G)_L \cong \bigoplus_{g \in [L\backslash G/L]} ({}^gV)_{L \cap gLg^{-1}})^L,$$
onde supomos que $1 \in [L\backslash G/L]$. Logo, na decomposição acima, temos o somando V correspondente a $g = 1$, enquanto os outros somandos são induzidos de subgrupos da forma $L \cap gLg^{-1}$ para $g \notin L$. Como P e gPg^{-1} são normais em L e gLg^{-1}, respectivamente, eles são os únicos p-subgrupos de Sylow de tais grupos. Como um p-subgrupo de um grupo sempre está contido em um p-subgrupo de Sylow, segue disso que $P \cap gPg^{-1}$ é o p-subgrupo de Sylow de $L \cap gLg^{-1}$. Mas P é de interseção trivial, então, se $g \notin L$, obtemos que a ordem de $L \cap gLg^{-1}$ não é divisível por p. Pelo Teorema de Maschke, todo módulo sobre $L \cap gLg^{-1}$ é semissimples e, portanto, projetivo (veja o Exercício A.2.4). Como a indução preserva a projetividade, concluímos que os somandos na decomposição acima correspondentes a $g \notin L$ são todos projetivos. Dessa forma, $(V^G)_L$ possui um único somando indecomponível não projetivo, que é isomorfo a V.

Agora, expresse $V^G \cong U_1 \oplus \cdots \oplus U_n$, onde cada U_i é indecomponível. Como L contém um p-subgrupo de Sylow de G, a Proposição 2.2.7 e o Corolário 3.2.4 nos dizem que U_i é projetivo se, e somente se, $(U_i)_L$ é projetivo. Mas $(V^G)_L$ possui um único somando indecomponível que não é projetivo, então existe um único $1 \leq i \leq n$ tal que $g(V) := U_i$ não é projetivo e tal que U_j é projetivo para $j \neq i$. Agrupando esses somandos projetivos, conseguimos escrever $V^G \cong g(V) \oplus Y$, onde Y é um kG-módulo projetivo. Além disso, como $g(V)_L$ não pode ser projetivo e é somando direto de $(V^G)_L$, vale $g(V)_L \cong V \oplus X$ para algum kL-módulo projetivo X. Quando demonstrarmos (1), repare que essa última afirmação implica em $f(g(V)) \cong V$.

Vamos para o item (1). Seja U um kG-módulo indecomponível e não projetivo. Como L contém um p-subgrupo de Sylow de G, o Teorema 3.2.3 nos dá que todo kG-módulo é relativamente L-projetivo. Em particular, existe um kL-módulo V tal que $U \mid V^G$. Como U é indecomponível, podemos tomar V indecomponível também. Mas U não é projetivo, então o mesmo vale para V^G e, consequentemente, V não pode ser projetivo. Pelo argumento do parágrafo anterior, $(V^G)_L$ tem um único somando indecomponível não projetivo, que é isomorfo a V, então podemos concluir como antes que $U_L \cong V \oplus X$ para algum kL-módulo projetivo X. Assim, podemos definir $f(U) := V$ para satisfazer as condições do item (1). Além disso, como $U \mid V^G$ e V^G possui um único somando indecomponível não projetivo, também temos $V^G \cong U \oplus Y$ para algum kG-módulo projetivo Y, de onde concluímos que $g(f(U)) \cong U$. Com isso, o item (3) também está provado. □

Nas condições acima, se tivermos $f(U) \cong V$ (ou, equivalentemente, $U \cong g(V)$), diremos que V é o **correspondente de Green** de U, e vice-versa. Por simplicidade, também diremos que V é o correspondente de U ou que V corresponde a U.

Exemplo 3.3.2. Pelo Teorema 3.2.7, os grupos para os quais existe uma chance maior de se classificar todas as representações indecomponíveis são aqueles que possuem um p-subgrupo de Sylow P cíclico. Quando P é cíclico de ordem p, então P é de interseção trivial e podemos aplicar o caso particular da Correspondência de Green descrito no Teorema 3.3.1. Assim, para começar a entender os kG-módulos indecomponíveis não projetivos, podemos estudar os módulos indecomponíveis do normalizador L de P em G. Mas veja que P é cíclico e normal em L, então podemos aplicar a descrição que obtivemos nos Exemplos 2.2.12 e 2.3.20! Por exemplo, com o que temos, já conseguimos descobrir o número exato de kG-módulos indecomponíveis. Se s_L denota o número de classes de isomorfismo de kL-módulos simples, sabemos que existem s_L classes de isomorfismo de kL-módulos projetivos indecomponíveis, e cada um desses é unisseriado e de comprimento $|P| = p$. Os indecomponíveis não projetivos sobre L são exatamente os quocientes não triviais dos projetivos indecomponíveis, logo, o número de classes de isomorfismo de kL-módulos indecomponíveis não projetivos é $(p-1)s_L$. Pelo Teorema 3.3.1, esse também é o número de classes de isomorfismo de kG-módulos indecomponíveis não projetivos. Como o número de kG-módulos indecomponíveis projetivos é o número s_G de kG-módulos simples, concluímos que existem exatamente

$$(p-1)s_L + s_G$$

classes de isomorfismo de kG-módulos indecomponíveis. Quando k é algebricamente fechado, os números s_L e s_G são facilmente calculados através do Teorema de Brauer, desde que conheçamos as classes de conjugação de L e de G.

É possível extrair muitas outras informações. Por exemplo, conhecendo as dimensões dos kL-módulos simples, conseguimos limitar as dimensões dos kG-módulos indecomponíveis não projetivos. E também já sabemos onde encontrar tais módulos: basta induzirmos os indecomponíveis sobre L para G. Em breve, mostraremos como aplicar essas ideias para estudar o grupo $G = \mathrm{SL}_2(p)$.

Vejamos algumas propriedades que decorrem do Teorema 3.3.1.

Corolário 3.3.3. Suponha que G possua um p-subgrupo de Sylow P de interseção trivial e denote $L = N_G(P)$. Sejam U_1 e U_2 kG-módulos indecomponíveis não projetivos e V_1 e V_2 os respectivos kL-módulos correspondentes. Então existe uma sequência exata

$$0 \longrightarrow U_1 \longrightarrow U \longrightarrow U_2 \longrightarrow 0$$

que não cinde se, e somente se, existe uma sequência exata

$$0 \longrightarrow V_1 \longrightarrow V \longrightarrow V_2 \longrightarrow 0$$

que não cinde.

Demonstração: Suponha que

$$0 \longrightarrow V_1 \longrightarrow V \longrightarrow V_2 \longrightarrow 0$$

seja uma sequência exata que não cinde. Induzindo a G, o Lema 3.1.11 nos dá uma sequência exata

$$0 \longrightarrow V_1^G \longrightarrow V^G \longrightarrow V_2^G \longrightarrow 0$$

que também não cinde. Pelo Teorema 3.3.1, existem kG-módulos projetivos R_1 e R_2 tais que

$$V_1^G \cong U_1 \oplus R_1 \quad \text{e} \quad V_2^G \cong U_2 \oplus R_2.$$

Por simplicidade, identificaremos U_1 e R_1 como submódulos de V_1^G, valendo a igualdade $V_1^G = U_1 \oplus R$. Também suporemos que $V_1^G \subseteq V^G$, já que o mapa $V_1^G \to V^G$ na sequência acima é injetivo. Pela exatidão da sequência, temos

$$\frac{V^G}{V_1^G} \cong V_2^G \cong R_2 \oplus U_2.$$

Logo, existe um submódulo W de V^G que contém V_1^G e satisfaz $V^G/W \cong R_2$ e $W/V_1^G \cong U_2$. Mas

$$\frac{W/R_1}{V_1^G/R_1} \cong \frac{W}{V_1^G} \cong U_2$$

e, como $V_1^G/R_1 \cong U_1$, temos uma sequência exata

$$0 \longrightarrow U_1 \longrightarrow W/R_1 \longrightarrow U_2 \longrightarrow 0.$$

Mostremos que essa sequência não cinde. Para isso, suporemos que esse não é o caso e mostraremos que V_1^G é um somando direto de V^G, o que será uma contradição, pois a sequência

$$0 \longrightarrow V_1^G \longrightarrow V^G \longrightarrow V_2^G \longrightarrow 0$$

não cinde. Nossa suposição nos dá que V_1^G/R_1 é um somando direto de W/R_1, então existe um submódulo X de W tal que $W = X + V_1^G$ e $X \cap V_1^G = R_1$. Como R_1 é projetivo, ele também é injetivo pelo Teorema 2.3.14, então a inclusão $R_1 \to X$ cinde e R_1 é somando direto de X. Seja Y um submódulo de X tal que $X = Y \oplus R_1$. Afirmamos que W é a soma direta de Y e V_1^G. De fato, como $R_1 \subseteq V_1^G$ e $Y \subseteq X$, vale

$$Y + V_1^G = Y + R_1 + V_1^G = X + V_1^G = W$$

e

$$Y \cap V_1^G = Y \cap X \cap V_1^G = Y \cap R_1 = 0,$$

como preciso. Estamos quase lá. Veja que o núcleo da projeção

$$\frac{V^G}{Y} \to \frac{V^G/Y}{W/Y}$$

é W/Y. Mas

$$\frac{V^G/Y}{W/Y} \cong \frac{V^G}{W} \cong R_2$$

é projetivo, então a projeção anterior cinde e W/Y é somando direto de V^G/Y. Consequentemente, existe um submódulo Z de V^G tal que $V^G = Z + W$ e $Z \cap W = Y$. Finalmente, como $Y \subseteq Z$ e $V_1^G \subseteq W$, temos

$$Z + V_1^G = Z + Y + V_1^G = Z + W = V^G$$

e

$$Z \cap V_1^G = Z \cap W \cap V_1^G = Y \cap V_1^G = 0,$$

provando que $V^G = Z \oplus V_1^G$. Concluímos que V_1^G é somando direto de V^G, como queríamos.

Com tudo isso, demonstramos uma das implicações. Reciprocamente, suponha que

$$0 \longrightarrow U_1 \longrightarrow U \longrightarrow U_2 \longrightarrow 0$$

seja uma sequência exata que não cinde. Restringindo, obtemos uma sequência exata

$$0 \longrightarrow (U_1)_L \longrightarrow U_L \longrightarrow (U_2)_L \longrightarrow 0.$$

Afirmamos que essa sequência não cinde também. De fato, como L contém um p-subgrupo de Sylow de G, então U_2 é relativamente L-projetivo pelo Teorema 3.2.3. Como o mapa $U \to U_2$ da primeira sequência não cinde, a caracterização (3) da Proposição 3.2.1 diz que o mapa $U_L \to (U_2)_L$ da segunda sequência também não cinde. Agora, pelo Teorema 3.3.1, existem kL-módulos projetivos Q_1 e Q_2 tais que

$$(U_1)_L \cong V_1 \oplus Q_1 \quad \text{e} \quad (U_2)_L \cong V_2 \oplus Q_2.$$

Repare que essas são essencialmente as mesmas condições do caso anterior! Então podemos imitar a demonstração de antes para encontrar um kL-módulo V e uma sequência exata

$$0 \longrightarrow V_1 \longrightarrow V \longrightarrow V_2 \longrightarrow 0$$

que não cinde, terminando a demonstração do corolário. □

O próximo resultado será usado em capítulos futuros. Precisamos de uma nova definição. Se U_1 e U_2 são kG-módulos, definimos $\overline{\mathrm{Hom}}_{kG}(U_1, U_2)$ como o quociente do espaço vetorial $\mathrm{Hom}_{kG}(U_1, U_2)$ pelo subespaço formado por todos os homomorfismos de U_1 em U_2 que se fatoram através de um kG-módulo projetivo, isto é, aqueles homomorfismos que são a composição de um homomorfismo de U_1 em um projetivo com um homomorfismo para U_2. Vejamos que isso é de fato um subespaço. É imediato que o homomorfismo nulo se fatora através de qualquer projetivo. Agora, se f_1 e f_2 se fatoram através de projetivos P_1 e P_2, mostremos que $f_1 + f_2$ se fatora através de $P_1 \oplus P_2$, que é projetivo. Sejam $\varphi_i : U_1 \to P_i$ e $\psi_i : P_i \to U_2$ homomorfismos tais que $f_i = \psi_i\varphi_i$, para $i = 1, 2$. Defina $\varphi : U_1 \to P_1 \oplus P_2$ por

$$\varphi(u_1) \coloneqq (\varphi_1(u_1), \varphi_2(u_1))$$

para todo $u_1 \in U_1$, e $\psi : P_1 \oplus P_2 \to U_2$ por

$$\psi(p_1, p_2) = \psi_1(p_1) + \psi_2(p_2)$$

para todos $p_1 \in P_1$ e $p_2 \in P_2$. É fácil verificar que φ e ψ são homomorfismos de kG-módulos. Além disso,

$$(\psi\varphi)(u_1) = \psi(\varphi_1(u_1), \varphi_2(u_1)) = (\psi_1\varphi_1)(u_1) + (\psi_2\varphi_2)(u_1) = f_1(u_1) + f_2(u_1) = (f_1 + f_2)(u_1)$$

para todo $u_1 \in U_1$, ou seja, $f_1 + f_2 = \psi\varphi$, como preciso. Por fim, se $\lambda \in k$, não é difícil ver que $\lambda f_1 = (\lambda\psi_1)\varphi_1$, então λf_1 também se fatora através do projetivo P_1.

Corolário 3.3.4. Suponha que G possua um p-subgrupo de Sylow P de interseção trivial e denote $L = N_G(P)$. Se U_1 e U_2 são kG-módulos indecomponíveis não projetivos e V_1 e V_2 são os kL-módulos correspondentes, então

$$\overline{\mathrm{Hom}}_{kG}(U_1, U_2) \cong \overline{\mathrm{Hom}}_{kL}(V_1, V_2).$$

Demonstração: Pelo Teorema 3.3.1, existem um kL-módulo projetivo X e um kG-módulo projetivo Y tais que

$$(U_2)_L \cong V_2 \oplus X \quad \text{e} \quad V_1^G \cong U_1 \oplus Y.$$

Pelo Exercício A.3.15, temos

$$\overline{\mathrm{Hom}}_{kG}(V_1^G, U_2) \cong \overline{\mathrm{Hom}}_{kG}(U_1 \oplus Y, U_2) \cong \overline{\mathrm{Hom}}_{kG}(U_1, U_2)$$

e

$$\overline{\mathrm{Hom}}_{kL}(V_1, (U_2)_L) \cong \overline{\mathrm{Hom}}_{kL}(V_1, V_2 \oplus X) \cong \overline{\mathrm{Hom}}_{kL}(V_1, V_2),$$

onde usamos que X e Y são projetivos. Logo, é suficiente mostrar que

$$\overline{\mathrm{Hom}}_{kG}(V_1^G, U_2) \cong \overline{\mathrm{Hom}}_{kL}(V_1, (U_2)_L).$$

Pela Reciprocidade de Frobenius, vale

$$\mathrm{Hom}_{kG}(V_1^G, U_2) \cong \mathrm{Hom}_{kL}(V_1, (U_2)_L),$$

então basta provar que um homomorfismo $V_1^G \to U_2$ se fatora através de um projetivo se e só se a sua imagem pelo isomorfismo acima possui a mesma propriedade.

Por simplicidade, denote V_1 por V e U_2 por U. Seja $i_V : V \to V^G$ a inclusão canônica. Assim, se $\varphi \in \mathrm{Hom}_{kG}(V^G, U)$, vimos na demonstração do Lema 3.1.11 que o isomorfismo em questão leva φ em $\varphi i_V \in \mathrm{Hom}_{kL}(V, U_L)$. Se φ se fatora através de um kG-módulo projetivo R, então, compondo com i_V, é imediato que φi_V se fatora através de R_L, que é um kL-módulo projetivo pela Proposição 2.2.7. Reciprocamente, suponha que φi_V se fatore através de um kL-módulo projetivo Q. Logo, existem homomorfismos de kL-módulos $\alpha : V \to Q$ e $\beta : Q \to U$ de modo que o seguinte diagrama comuta:

$$\begin{array}{ccc} V^G & \xrightarrow{\ \varphi\ } & U \\ {\scriptstyle i_V}\uparrow & & \uparrow{\scriptstyle \beta} \\ V & \xrightarrow[\ \alpha\ ]{} & Q \end{array}$$

Seja $\alpha^G : V^G \to Q^G$ a extensão de $\alpha : V \to Q$ e, pela propriedade universal de Q^G, tome $\tilde{\beta} : Q^G \to U$ como sendo o único homomorfismo de kG-módulos tal que $\tilde{\beta} i_Q = \beta$, onde $i_Q : Q \to Q^G$ é a inclusão canônica. Assim, $\tilde{\beta}\alpha^G : V^G \to U$ é um homomorfismo de kG-módulos satisfazendo

$$(\tilde{\beta}\alpha^G) i_V = \tilde{\beta}(\alpha^G i_V) = \tilde{\beta}(i_Q \alpha) = (\tilde{\beta} i_Q)\alpha = \beta\alpha = \varphi i_V.$$

Mas então $\tilde{\beta}\alpha^G$ e φ estendem o mesmo homomorfismo de V em U. Pela unicidade na propriedade universal de V^G, vemos que $\tilde{\beta}\alpha^G = \varphi$ e φ se fatora através de Q^G, que é projetivo pelo item (2) do Lema 3.1.10. Isso conclui a demonstração do resultado. □

Exemplo 3.3.5. Seja k um corpo de característica $p > 2$ e seja $G = \mathrm{SL}_2(p)$. Por enquanto, não precisaremos supor que k é algebricamente fechado. Vamos aplicar o Teorema 3.3.1 para obter de um modo diferente alguns dos resultados do Exemplo 2.4.14. Sabemos que um dos p-subgrupos de Sylow de $\mathrm{SL}_2(p)$ é o subgrupo P formado pelas matrizes

$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$$

com $\lambda \in \mathbb{F}_p$. Como $|P| = p$, certamente P é de interseção trivial e podemos aplicar o que vimos nesta seção. Precisamos encontrar o normalizador L de P em $\mathrm{SL}_2(p)$. Dada uma matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(p),$$

veja que sua inversa é

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

logo, utilizando a relação $ad - bc = 1$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 + bd\lambda & -b^2\lambda \\ d^2\lambda & 1 - bd\lambda \end{pmatrix}$$

para todo $\lambda \in \mathbb{F}_p$. Para a matriz inicial estar em L, devemos ter $b = 0$. Como o determinante da matriz é 1, também concluímos que $ad = 1$, valendo $a \neq 0$ e $d = a^{-1}$. Portanto, L é formado pelas matrizes

$$\alpha = \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}$$

com $a, c \in \mathbb{F}_p$ e $a \neq 0$. Observe que a função que leva uma matriz α como acima em a é um homomorfismo de grupos sobrejetor de L em $\mathbb{F}_p^\times$ cujo núcleo é P. Portanto, L/P é cíclico de ordem $p - 1$. Observe que k possui uma raiz $(p-1)$-ésima primitiva da unidade, pois $\mathbb{F}_p$ possui. Dessa forma, conseguimos construir os $p - 1$ $k[L/P]$-módulos simples do Exemplo 1.3.15. Mas a dimensão de $k[L/P]$ é $p - 1$, então esses são todos módulos simples para essa álgebra, já que cada módulo simples aparece como fator de composição. Restringindo através do homomorfismo sobrejetor $kL \to k[L/P]$, obtemos $p-1$ módulos simples sobre kL. Esses são todos os kL-módulos simples pois P é um p-subgrupo de Sylow normal em L (veja a Proposição 1.3.14).

Vamos construir os kL-módulos simples explicitamente. Se $j \in \mathbb{Z}$, defina S_j como sendo o kL-módulo de dimensão 1 no qual a matriz α acima atua por multiplicação por a^j. Como a função que associa tal matriz a a^j é um homomorfismo de L em $\mathbb{F}_p^\times$, isso de fato define um kL-módulo. Como $\mathbb{F}_p$ possui uma raiz $(p-1)$-ésima primitiva da unidade, não é difícil ver que $S_{j_1} \cong S_{j_2}$ se, e somente se, $j_1 \equiv j_2 \pmod{p-1}$. Com isso, construímos $p-1$ kL-módulos simples e, portanto, eles representam todas as classes de isomorfismo. Uma observação que precisaremos em breve é que $S_{j_1} \otimes S_{j_2}$ é unidimensional e α atua por multiplicação por $a^{j_1} \cdot a^{j_2} = a^{j_1+j_2}$, então $S_{j_1} \otimes S_{j_2} \cong S_{j_1+j_2}$.

Relembre que no Exemplo 1.3.17 nós construímos os kG-módulos simples $V_1, \ldots, V_p$. Vamos entender as suas restrições a L. Começaremos com $(V_2)_L$. Tal módulo possui $\{x, y\}$ como base e vale

$$\alpha \cdot x = ax + cy \quad \text{e} \quad \alpha \cdot y = a^{-1}y.$$

Isso mostra que o subespaço gerado por y é um submódulo de $(V_2)_L$ isomorfo a S_{-1} e, formando o quociente, temos um módulo isomorfo a S_1. Procedendo como no Exemplo 1.3.6, vemos que $(V_2)_L$ possui apenas um submódulo próprio, então $(V_2)_L$ é unisseriado e seus fatores de composição são S_1 e S_{-1}, nessa ordem (começando pelo quociente de $(V_2)_L$ pelo seu radical).

Isso nos permite entender todos os kL-módulos indecomponíveis! Para isso, lembre que P é p-subgrupo normal e cíclico de L. Assim, pelos Exemplos 2.2.12 e 2.3.20, todo kL-módulo indecomponível é unisseriado e existe um kL-módulo simples W tal que, se S_j é um fator de composição de um indecomponível, o "próximo" fator de composição é $S_j \otimes W$. Agora, pelo que vimos da estrutura de $(V_2)_L$, deve valer $S_1 \otimes W \cong S_{-1}$. Consequentemente, $W \cong S_{-2}$. Portanto, se U é um kL-módulo indecomponível com $U/\operatorname{rad}(U) \cong S_j$, então os seus fatores de composição em sua única série de composição são

$$S_j, S_{j-2}, S_{j-4}, \ldots,$$

nessa ordem, e a quantidade deles é exatamente a dimensão de U, que é no máximo $|P| = p$.

Vejamos qual é a estrutura de $(V_i)_L$, para $1 \leq i \leq p$. No Exemplo 1.3.17, provamos que o soco de $(V_i)_P$ é o subespaço gerado por y^{i-1}. Como P é normal em L, o Teorema de Clifford implica que o soco de $(V_i)_L$ está contido no soco de $(V_i)_P$ e, por questões de dimensão, esse soco também é gerado, como subespaço, por y^{i-1}. Mas

$$\alpha \cdot y^{i-1} = (\alpha \cdot y)^{i-1} = (a^{-1}y)^{i-1} = a^{-i+1}y,$$

então $\operatorname{soc}((V_i)_L) \cong S_{-i+1}$. Como o soco é simples, $(V_i)_L$ é indecomponível. Assim, $(V_i)_L$ é unisseriado e seus fatores de composição são

$$S_{i-1}, S_{i-3}, S_{i-5}, \ldots, S_{-i+1}.$$

Note que temos i módulos acima, pois a dimensão de $(V_i)_L$ é i. Dessa forma, $(V_i)_L$ é o kL-módulo indecomponível de dimensão i e quociente radical S_{i-1}.

Agora, podemos começar a descrever os kG-módulos. O primeiro passo é observar que, para $1 \leq i < p$, V_i não pode ser projetivo, pois sua dimensão não é divisível por p. Como $(V_i)_L$ é indecomponível, segue do Teorema 3.3.1 que $(V_i)_L$ é o correspondente de Green de V_i. Isso nos permitirá usar o Corolário 3.3.3 para entender um pouco da estrutura dos kG-módulos projetivos indecomponíveis.

Lema 3.3.6. Para todo $1 \leq i < p-1$, existe uma sequência exata

$$0 \longrightarrow V_{p-i-1} \longrightarrow V \longrightarrow V_i \longrightarrow 0$$

que não cinde.

Demonstração: Pela observação logo antes do lema e pelo Corolário 3.3.3, basta encontrar uma sequência exata

$$0 \longrightarrow (V_{p-i-1})_L \longrightarrow U \longrightarrow (V_i)_L \longrightarrow 0$$

que não cinde. Tome U como sendo o kL-módulo indecomponível de dimensão $p-1$ com $U/\operatorname{rad}(U) \cong S_{i-1}$. Então $U/\operatorname{rad}^i(U)$ tem dimensão i e quociente radical isomorfo a S_{i-1}. Logo, $U/\operatorname{rad}^i(U) \cong (V_i)_L$. Por outro lado, veja que o quociente radical de $\operatorname{rad}^i(U)$ é o fator de composição de U que está logo após o soco de $U/\operatorname{rad}^i(U)$, que é isomorfo a S_{-i+1}. Por isso, o quociente radical de $\operatorname{rad}^i(U)$ é isomorfo a

$$S_{-i-1} \cong S_{(p-i-1)-1}$$

e, como $\dim_k \operatorname{rad}^i(U) = p-i-1$, vale $\operatorname{rad}^i(U) \cong (V_{p-i-1})_L$. Com isso, temos uma sequência exata

$$0 \longrightarrow (V_{p-i-1})_L \longrightarrow U \longrightarrow (V_i)_L \longrightarrow 0$$

e ela não cinde porque U é indecomponível. □

Lema 3.3.7. Para todo $1 < i \leq p-1$, existe uma sequência exata

$$0 \longrightarrow V_{p-i+1} \longrightarrow V \longrightarrow V_i \longrightarrow 0$$

que não cinde.

Demonstração: Procederemos como no lema anterior. Seja $U = Q_{i-1} \oplus S_{-i+1}$, onde Q_{i-1} é a cobertura projetiva de S_{i-1}. Assim, Q_{i-1} é o indecomponível de dimensão p e quociente radical isomorfo a S_{i-1}. Defina $W = \mathrm{rad}^{i-1}(Q_{i-1}) \subseteq Q_{i-1}$, que possui dimensão $p-i+1$. Como

$$(i-1) - 2(i-1) = -i+1,$$

vale que

$$\frac{W}{\mathrm{rad}(W)} \cong S_{-i+1} \cong S_{(p-i+1)-1}.$$

Portanto, $W \cong (V_{p-i+1})_L$. Agora, seja $\varphi : W \to S_{-i+1}$ um homomorfismo sobrejetor. Se definirmos $\psi : W \to U$ por

$$\psi(w) = (w, \varphi(w))$$

para todo $w \in W$, é fácil ver que ψ é um homomorfismo injetor. Seja Z a imagem de ψ, que é isomorfa a $W \cong (V_{p-i+1})_L$. Se mostrarmos que $U/Z \cong (V_i)_L$, então teremos uma sequência exata

$$0 \longrightarrow (V_{p-i+1})_L \longrightarrow U \longrightarrow (V_i)_L \longrightarrow 0.$$

Como $U \cong Q_{i-1} \oplus S_{-i+1}$, seguirá do Teorema de Krull-Schmidt que essa sequência não cinde. Pelo Corolário 3.3.3, teremos provado o lema.

Como Z e U possuem dimensão $p-i+1$ e $p+1$, respectivamente, então U/Z tem dimensão i. Logo, para concluir que $U/Z \cong (V_i)_L$, é suficiente mostrar que o seu quociente radical é isomorfo a S_{i-1}. Pelo Exercício A.1.3, temos

$$\mathrm{rad}(U/Z) \cong \frac{\mathrm{rad}(U) + Z}{Z},$$

então precisamos mostrar que

$$\frac{U}{\mathrm{rad}(U) + Z} \cong S_{i-1}.$$

Como

$$\frac{U}{\mathrm{rad}(Q_{i-1}) \oplus S_{-i+1}} \cong \frac{Q_{i-1}}{\mathrm{rad}(Q_{i-1})} \oplus \frac{S_{-i+1}}{S_{-i+1}} \cong S_{i-1},$$

temos a inclusão $\mathrm{rad}(U) \subseteq \mathrm{rad}(Q_{i-1}) \oplus S_{-i+1}$. Mas $Z \subseteq W \oplus S_{-i+1} \subseteq \mathrm{rad}(Q_{i-1}) \oplus S_{-i+1}$, então vale $\mathrm{rad}(U) + Z \subseteq \mathrm{rad}(Q_{i-1}) \oplus S_{-i+1}$. Assim, para concluir a demonstração, basta mostrar que $\mathrm{rad}(Q_{i-1}) \oplus S_{-i+1} \subseteq \mathrm{rad}(U) + Z$. Certamente, $\mathrm{rad}(Q_{i-1}) \subseteq \mathrm{rad}(U) \subseteq \mathrm{rad}(U) + Z$. Por outro lado, se $s \in S_{-i+1}$, escolha $w \in W$ tal que $\varphi(w) = s$. Então,

$$(0, s) = (w, s) - (w, 0) = \psi(w) - (w, 0) \in Z + W \subseteq Z + \mathrm{rad}(Q_{i-1}) \subseteq Z + \mathrm{rad}(U)$$

e vale $S_{-i+1} \subseteq \mathrm{rad}(U) + Z$. Concluímos que $\mathrm{rad}(Q_{i-1}) \oplus S_{-i+1} \subseteq \mathrm{rad}(U) + Z$, como preciso. □

Estamos prontos para analisar a estrutura dos kG-módulos projetivos indecomponíveis. Sejam $P_1, \ldots, P_p$ as coberturas projetivas dos módulos simples $V_1, \ldots, V_p$. Como estamos supondo $p > 2$, o Lema 3.3.6 (para $i = 1$) garante a existência de um kG-módulo unisseriado cujos fatores de composição são V_1 e V_{p-2}, nessa ordem. Pelo Lema 2.2.5, tal módulo é quociente de P_1. Portanto, existe um submódulo $W_1 \subseteq P_1$ contido em[1] $\mathrm{rad}(P_1)$ satisfazendo $\mathrm{rad}(P_1)/W_1 \cong V_{p-2}$. Como

[1] Lembre que $\mathrm{rad}(P_1)$ é o único submódulo maximal de P_1, pois $P_1/\mathrm{rad}(P_1) \cong V_1$ é simples.

$\operatorname{soc}(P_1) \cong V_1$ é o único submódulo simples de P_1, temos[1] $\operatorname{soc}(P_1) \subseteq W_1$. Contando esses fatores de composição, vemos que a dimensão de P_1 é pelo menos

$$1 + (p-2) + 1 = p.$$

Além disso, a dimensão de P_1 é exatamente p se e só se $\operatorname{soc}(P_1) = W_1$ ou, equivalentemente, $\operatorname{rad}(P_1)/\operatorname{soc}(P_1) \cong V_{p-2}$. Com um argumento análogo, o Lema 3.3.7 (para $i = p-1$) nos dá $\dim_k P_{p-1} \geq 2p$, valendo a igualdade se, e somente se, $\operatorname{rad}(P_{p-1})/\operatorname{soc}(P_{p-1}) \cong V_2$. Assim, veja que, se P_1 e P_{p-1} possuem dimensões p e $2p$, respectivamente, esses módulos possuem a estrutura descrita no Exemplo 2.4.14.

Agora, suponha $1 < i < p-1$. Aplicando os Lemas 3.3.6 e 3.3.7, encontramos submódulos W_- e W_+ de $\operatorname{rad}(P_i)$ tais que $\operatorname{rad}(P_i)/W_- \cong V_{p-i-1}$ e $\operatorname{rad}(P_i)/W_+ \cong V_{p-i+1}$. Como W_- e W_+ são maximais em $\operatorname{rad}(P_i)$ (pois os quocientes são simples), então temos $\operatorname{rad}(P_i) = W_- + W_+$. Por isso, se definirmos $W = W_- \cap W_+$, vale

$$\frac{\operatorname{rad}(P_i)}{W} = \frac{W_-}{W} \oplus \frac{W_+}{W}.$$

Além disso, aplicando o Segundo Teorema do Isomorfismo, temos

$$\frac{W_-}{W} = \frac{W_-}{W_- \cap W_+} \cong \frac{W_- + W_+}{W_+} = \frac{\operatorname{rad}(P_i)}{W_+} \cong V_{p-i+1}$$

e, analogamente, $W_+/W \cong V_{p-i-1}$. Note que $W \neq 0$, pois, caso contrário, a dimensão de P_i seria $i + (p-i+1) + (p-i-1) = 2p - i$, que não é divisível por p. Logo, W contém $\operatorname{soc}(P_i) \cong V_i$. Somando a dimensão dos fatores de composição já encontrados, temos

$$\dim_k P_i \geq i + (p-i+1) + (p-i-1) + i = 2p$$

e vale a igualdade se e só se $W = \operatorname{soc}(P_i)$ ou, equivalentemente,

$$\frac{\operatorname{rad}(P_i)}{\operatorname{soc}(P_i)} \cong V_{p-i+1} \oplus V_{p-i-1}.$$

Novamente, quando P_i tem dimensão $2p$, temos a estrutura descrita no Exemplo 2.4.14.

Para o argumento final, precisaremos supor k algebricamente fechado. Com essa hipótese, segue do Corolário 2.2.6 que, numa decomposição de kG como soma de indecomponíveis, cada P_i aparece $\dim_k V_i$ vezes. Por isso,

$$\begin{aligned} p(p^2-1) = |G| &= \dim_k kG \\ &\geq \sum_{i=1}^{p} (\dim_k V_i) \cdot (\dim_k P_i) \\ &\geq 1 \cdot p + (2 + 3 + \cdots + (p-2)) \cdot 2p + (p-1) \cdot 2p + p \cdot p \\ &= p^3 - p = p(p^2-1). \end{aligned}$$

Mas então todas as desigualdades que encontramos são igualdades! Logo, os projetivos indecomponíveis $P_1, \ldots, P_p$ possuem a estrutura descrita no Exemplo 2.4.14. O argumento que fizemos é muito diferente do anterior. Por exemplo, nem precisamos usar que V_p é projetivo. E isso segue da conta acima: estimamos $\dim_k P_p \geq p$ pois P_p é projetivo e então sua dimensão é divisível por p. Como obtemos a igualdade $\dim_k P_p = p = \dim_k V_p$, devemos ter $P_p \cong V_p$, como preciso. Note também que não precisávamos saber que $V_1, \ldots, V_p$ eram todos os kG-módulos simples. Na

[1] Veja que não podemos ter $W_1 = 0$, pois a dimensão de P_1 seria apenas $p-1$, que não é divisível por p, contradizendo o Corolário 2.2.9.

verdade, também provamos isso quando mostramos que a primeira desigualdade acima é uma igualdade!

Também temos algumas informações sobre os kG-módulos indecomponíveis não projetivos. Pelo Exemplo 3.3.2, o número de kG-módulos indecomponíveis é

$$(p-1)\cdot(p-1)+p = p^2-p+1.$$

Não faremos isso, mas sabemos onde procurar por esses indecomponíveis: basta induzir o kL-módulos indecomponíveis!

3.4 A Correspondência de Green: o caso geral

Nosso objetivo será generalizar o Teorema 3.3.1. Esse caso particular da Correspondência de Green lidava com módulos indecomponíveis que não eram projetivos. Agora poderemos ser mais específicos utilizando a noção de vértice que introduzimos anteriormente, pois ela é uma espécie de medida do quanto um módulo "deixa de ser" projetivo. A ideia será a seguinte: fixado um p-subgrupo Q de G e um subgrupo $L \leq G$ contendo $N_G(Q)$, teremos uma bijeção entre as classes de isomorfismo de kG-módulos indecomponíveis de vértice Q e as classes de isomorfismo de kL-módulos indecomponíveis com o mesmo vértice. Além disso, essa correspondência também será determinada por indução e por restrição: se U é um kG-módulo indecomponível de vértice Q que corresponde ao kL-módulo V, então

$$U_L \cong V \oplus Y \quad \text{e} \quad V^G \cong U \oplus X,$$

onde nenhum somando indecomponível de X e de Y possui vértice Q.

Teremos mais informações a respeito dos somandos indecomponíveis de X e Y, mas, para isso, precisamos introduzir duas famílias de subgrupos de G. A partir de agora, fixe Q um p-subgrupo de G e L um subgrupo contendo $N_G(Q)$.

Definição 3.4.1. Fixadas as escolhas de Q e L, definimos

$$\mathfrak{X} = \{Q \cap gQg^{-1} \mid g \in G, g \notin L\}$$

e

$$\mathfrak{Y} = \{L \cap gQg^{-1} \mid g \in G, g \notin L\}.$$

Devemos pensar em $\mathfrak{X}$ e $\mathfrak{Y}$ como sendo as famílias de "subgrupos pequenos" com relação a Q. Por exemplo, se $g \notin L$, então $g \notin N_G(Q)$ e $Q \cap gQg^{-1} \subsetneq Q$. Portanto, $Q \notin \mathfrak{X}$ e, da mesma forma, $Q \notin \mathfrak{Y}$ (apesar de que $\mathfrak{Y}$ pode conter um conjugado de Q). Assim, exigir que L contenha $N_G(Q)$ garante que Q seja um "subgrupo grande". Isso fará mais sentido quando começarmos a demonstrar a Correspondência de Green.

Definição 3.4.2. Se $\mathscr{H}$ é uma família de subgrupos de G, dizemos que um kG-módulo U é **relativamente $\mathscr{H}$-projetivo** se cada somando indecomponível de U é relativamente projetivo com relação a algum subgrupo em $\mathscr{H}$. Note que somandos diferentes de U podem ser relativamente projetivos com relação a subgrupos diferentes de $\mathscr{H}$.

Estamos prontos para enunciar a Correspondência de Green:

Teorema 3.4.3 (Correspondência de Green)**.** Com as notações acima, as seguintes afirmações são verdadeiras:

(1) Seja U um kG-módulo indecomponível e com vértice Q. Se decompormos U_L como soma de indecomponíveis, então existe um único somando indecomponível $f(U)$ que possui vértice Q. Além disso, se escrevermos

$$U_L \cong f(U) \oplus Y,$$

então Y é um kL-módulo relativamente $\mathfrak{Y}$-projetivo.

(2) Seja V um kL-módulo indecomponível e com vértice Q. Se decompormos V^G como soma de indecomponíveis, então existe um único somando indecomponível $g(V)$ que possui vértice Q. Além disso, se escrevermos
$$V^G \cong g(V) \oplus X,$$
então X é um kG-módulo relativamente $\mathfrak{X}$-projetivo.

(3) Temos isomorfismos $g(f(U)) \cong U$ e $f(g(V)) \cong V$. Isso estabelece uma correspondência biunívoca entre as classes de isomorfismo de kG-módulos indecomponíveis com vértice Q e as classes de isomorfismo de kL-módulos indecomponíveis com esse mesmo vértice.

A princípio, essa correspondência não parece generalizar de imediato o Teorema 3.3.1 por um motivo: quando um módulo não é projetivo, sabemos que seu vértice pode ser qualquer p-subgrupo de G diferente do trivial. Mas a correspondência acima lida apenas com um vértice de cada vez. Antes de dar uma demonstração do teorema acima, vejamos como usá-lo para estender ligeiramente a correspondência e obter de fato uma generalização do Teorema 3.3.1.

Notação 3.4.4. Se H e R são subgrupos de G, escreveremos $R \subseteq_G H$ para denotar que algum conjugado de R está contido em H. Se $\mathscr{H}$ é uma família de subgrupos de G, então denotaremos $R \subseteq_G \mathscr{H}$ se $R \subseteq_G H$ para algum $H \in \mathscr{H}$.

Temos uma nova família importante de subgrupos de G.

Definição 3.4.5. Definimos
$$\mathfrak{Z} = \{R \subseteq Q \mid R \not\subseteq_G \mathfrak{X}\}.$$

Os elementos de $\mathfrak{Z}$ são os "subgrupos grandes" de Q. Observe que todo elemento de $\mathfrak{X}$ é um subgrupo próprio de Q, então $Q \in \mathfrak{Z}$.

Corolário 3.4.6. Existe uma bijeção entre as classes de isomorfismo de kG-módulos indecomponíveis com vértice em $\mathfrak{Z}$ e as classes de isomorfismo de kL-módulos indecomponíveis com vértice em $\mathfrak{Z}$. Se U e V são módulos sobre kG e sobre kL, respectivamente, que se correspondem, então U e V possuem o mesmo vértice e
$$U_L \cong V \oplus Y \quad \text{e} \quad V^G \cong U \oplus X,$$
onde Y é um kL-módulo relativamente $\mathfrak{Y}$-projetivo e X é um kG-módulo relativamente $\mathfrak{X}$-projetivo.

Demonstração: Fixe $R \in \mathfrak{Z}$. Mostremos que $N_G(R) \subseteq L$. Se $g \in N_G(R)$, então $R = gRg^{-1}$ e
$$R \subseteq Q \implies R = gRg^{-1} \subseteq gQg^{-1}.$$
Logo, $R \subseteq Q \cap gQg^{-1}$. Se $g \notin L$, então valeria $Q \cap gQg^{-1} \in \mathfrak{X}$ e $R \subseteq_G \mathfrak{X}$, uma contradição, pois, por hipótese, $R \in \mathfrak{Z}$. Consequentemente, devemos ter $g \in L$, provando a inclusão desejada.

Agora que temos $N_G(R) \subseteq L$, podemos utilizar a Correspondência de Green para obter uma bijeção entre as classes de isomorfismo de kG-módulos indecomponíveis com vértice R e as classes de isomorfismo de kL-módulos com o mesmo vértice. Defina as novas famílias
$$\mathfrak{X}_R = \{R \cap gRg^{-1} \mid g \in G, g \notin L\}$$
e
$$\mathfrak{Y}_R = \{L \cap gRg^{-1} \mid g \in G, g \notin L\}.$$
Sejam U um kG-módulo e V um kL-módulo, ambos com vértice R. Se U e V se correspondem, então a Correspondência de Green diz que
$$U_L \cong V \oplus Y \quad \text{e} \quad V^G \cong U \oplus X,$$

onde Y é um kL-módulo relativamente $\mathfrak{Y}_R$-projetivo e X é um kG-módulo relativamente $\mathfrak{X}_R$-projetivo. Mas $R \subseteq Q$, então todo elemento de $\mathfrak{X}_R$ está contido em um elemento de $\mathfrak{X}$ e, da mesma forma, todo elemento de $\mathfrak{Y}_R$ está contido em um elemento de $\mathfrak{Y}$. Logo, Y é relativamente $\mathfrak{Y}$-projetivo e X é relativamente $\mathfrak{X}$-projetivo.

O resultado está provado se "colarmos" as bijeções que obtivemos para cada $R \in \mathfrak{Z}$. Um último detalhe a ser considerado é que um kG-módulo ou um kL-módulo pode possuir mais de um vértice em $\mathfrak{Z}$. Pelo Teorema 3.2.12, vértices estão bem definidos a menos de conjugados, mas dois subgrupos de $\mathfrak{Z}$ poderiam ser conjugados sobre G mas não sobre L, o que poderia potencialmente atrapalhar a "colagem" das bijeções. Mostremos que isso não acontece. Sejam $R, R' \in \mathfrak{Z}$ tais que $R' = gRg^{-1}$ para algum $g \in G$. Vamos verificar que $g \in L$. Como $R, R' \subseteq Q$, então

$$R' = R' \cap gRg^{-1} \subseteq Q \cap gQg^{-1}.$$

Se $g \notin L$, então teríamos $Q \cap gQg^{-1} \in \mathfrak{X}$, contradizendo que $R' \in \mathfrak{Z}$. Por isso, $g \in L$, como queríamos. □

Observação 3.4.7. Apesar de estender a correspondência, o enunciado do Corolário 3.4.6 dá uma informação mais fraca a respeito dos módulos X e Y ao se limitar às famílias $\mathfrak{X}$ e $\mathfrak{Y}$. Poderíamos fazer como na demonstração e trabalhar com $\mathfrak{X}_R$ e $\mathfrak{Y}_R$ para todo $R \in \mathfrak{Z}$, mas seriam muitas famílias em consideração. Por isso, optamos por enunciar a Correspondência de Green como no Teorema 3.4.3.

Exemplo 3.4.8. O Corolário 3.4.6 generaliza o Teorema 3.3.1! Vejamos o porquê. Suponha neste exemplo que Q seja um p-subgrupo de Sylow de G de interseção trivial e que $L = N_G(Q)$. Assim, se $g \notin L$, temos $gQg^{-1} \neq Q$ e, como Q é de interseção trivial, concluímos que $Q \cap gQg^{-1} = \{1\}$. Por isso, $\mathfrak{X}$ consiste apenas do grupo trivial $\{1\}$. Mostremos que $\mathfrak{Y}$ também só contém o grupo trivial. Note primeiramente que, como Q é p-subgrupo de Sylow de G e é normal em L, Q é o único p-subgrupo de Sylow de L. Logo, se $g \in G$, como $L \cap gQg^{-1}$ é p-subgrupo de L, temos $L \cap gQg^{-1} \subseteq Q$. Então

$$Q \cap gQg^{-1} = (Q \cap L) \cap gQg^{-1} = Q \cap (L \cap gQg^{-1}) = L \cap gQg^{-1}.$$

Se $g \notin L$, então, pela igualdade acima, $L \cap gQg^{-1} = \{1\}$. Dessa forma, $\mathfrak{Y} = \{\{1\}\}$, como queríamos.

Com isso, os módulos relativamente $\mathfrak{X}$-projetivos e os relativamente $\mathfrak{Y}$-projetivos são na verdade os módulos projetivos! Além disso,

$$\mathfrak{Z} = \{R \subseteq Q \mid R \neq \{1\}\}.$$

Assim, um módulo possui vértice em $\mathfrak{Z}$ se e só se não é projetivo. Concluímos que o Teorema 3.3.1 é um caso particular do Corolário 3.4.6.

Vamos demonstrar a Correspondência de Green. Para isso, provaremos alguns lemas que, juntos, implicarão o Teorema 3.4.3.

Lema 3.4.9. Se R é um subgrupo de Q, então as seguintes afirmações são equivalentes:

(1) $R \subseteq_G \mathfrak{X}$.

(2) $R \subseteq_L \mathfrak{X}$.

(3) $R \subseteq_L \mathfrak{Y}$.

Demonstração: (1) $\implies$ (2). Suponha que exista $x \in G$ tal que $xRx^{-1} \subseteq Q \cap gQg^{-1}$ para algum $g \in G$, $g \notin L$. Se $x \in L$, então certamente $R \subseteq_L \mathfrak{X}$. Caso contrário, se $x \notin L$ temos

$$xRx^{-1} \subseteq Q \implies R \subseteq x^{-1}Qx$$

e, como $R \subseteq Q$ por hipótese, temos $R \subseteq Q \cap x^{-1}Qx \in \mathfrak{X}$, mostrando que $R \subseteq_L \mathfrak{X}$.

(2) $\implies$ (3). Suponha que exista $x \in L$ tal que $xRx^{-1} \subseteq Q \cap gQg^{-1}$ para algum $g \in G, g \notin L$. Como $Q \subseteq L$, então facilmente vemos que $xRx^{-1} \subseteq L \cap gQg^{-1}$ e $R \subseteq_L \mathfrak{Y}$.

(3) $\implies$ (1). Suponha que exista $x \in L$ tal que $xRx^{-1} \subseteq L \cap gQg^{-1}$ para algum $g \in G, g \notin L$. Portanto, $R \subseteq L \cap (x^{-1}g)Q(x^{-1}g)^{-1}$ e, como $R \subseteq Q$, vale

$$R \subseteq Q \cap (x^{-1}g)Q(x^{-1}g)^{-1}.$$

Como $x \in L$ e $g \notin L$, temos $x^{-1}g \notin L$ e, consequentemente, a interseção em destaque acima está em $\mathfrak{X}$ e vale (1). □

Esse resultado nos ajuda a justificar o fato de pensarmos que os subgrupos de $\mathfrak{X}$ e $\mathfrak{Y}$ são "pequenos", enquanto os de $\mathfrak{Z}$ são "grandes"! Vejamos como. Suponha que V seja um kL-módulo indecomponível e de vértice Q. Suponha também que exista uma decomposição

$$V^G = U \oplus X,$$

onde U é um kG-módulo indecomponível de vértice Q e X é um kG-módulo relativamente $\mathfrak{X}$-projetivo. Então um vértice R de um somando indecomponível de X satisfaz $R \subseteq_G \mathfrak{X}$ pelo Teorema 3.2.12. Em particular, $R \neq Q$ e R é um vértice "pequeno". Isso nos dá a unicidade do item (2) do Teorema 3.4.3, desde que encontremos a decomposição acima.

Por outro lado, suponha que U seja um kG-módulo indecomponível e de vértice Q. Assuma que tenhamos uma decomposição

$$U_L = V \oplus Y,$$

onde V é um kL-módulo indecomponível de vértice Q e Y é um kL-módulo relativamente $\mathfrak{Y}$-projetivo. Mostremos que nenhum somando de Y pode ter vértice Q. Se esse fosse o caso, então o Teorema 3.2.12 nos daria $Q \subseteq_L \mathfrak{Y}$ e, pelo Lema 3.4.9, $Q \subseteq_G \mathfrak{X}$, o que é um absurdo, já que todo subgrupo em $\mathfrak{X}$ é um subgrupo próprio de Q. Com isso, também teremos a unicidade do item (1) do Teorema 3.4.3 quando encontrarmos uma decomposição como acima.

Pelos argumentos que acabamos de dar, $\mathfrak{Z}$ consiste dos subgrupos de Q que não podem ser vértices de kG-módulos indecomponíveis relativamente $\mathfrak{X}$-projetivos e nem de kL-módulos indecomponíveis relativamente $\mathfrak{Y}$-projetivos. Portanto, pensamos que eles são "grandes". Isso mostra que a correspondência dada no Corolário 3.4.6 é determinada pela indução e pela restrição, já que, com as notações desse resultado, se U possui vértice $R \in \mathfrak{Z}$, então V se caracteriza como o único somando indecomponível com vértice R de U_L, enquanto U é o único somando indecomponível com vértice R de V^G.

Lema 3.4.10. Se U é um kG-módulo relativamente $\mathfrak{X}$-projetivo, então U_L é relativamente $\mathfrak{Y}$-projetivo. Por outro lado, se V é um kL-módulo relativamente Q-projetivo e relativamente $\mathfrak{Y}$-projetivo, então V^G é relativamente $\mathfrak{X}$-projetivo.

Demonstração: Seja W um somando indecomponível de U. Por hipótese, U é relativamente $\mathfrak{X}$-projetivo, então W é relativamente projetivo com relação a algum subgrupo da forma $Q \cap gQg^{-1}$, onde $g \notin L$. Pela Fórmula de Decomposição de Mackey, W_L é relativamente projetivo com relação à coleção de subgrupos da forma

$$L \cap x(Q \cap gQg^{-1})x^{-1} = L \cap xQx^{-1} \cap (xg)Q(xg)^{-1},$$

com $x \in G$. Se $x \notin L$, então $L \cap xQx^{-1} \in \mathfrak{Y}$, enquanto se $x \in L$, temos $xg \notin L$ (pois $g \notin L$) e vale $L \cap (xg)Q(xg)^{-1} \in \mathfrak{Y}$. Em qualquer caso, o subgrupo em destaque acima está contido em um elemento de $\mathfrak{Y}$ e W_L é relativamente $\mathfrak{Y}$-projetivo. Como U_L é a soma direta dos módulos W_L quando W percorre os somandos indecomponíveis de U, concluímos que U_L também é relativamente $\mathfrak{Y}$-projetivo.

Agora, denotemos por W um somando indecomponível de V. Como V é relativamente Q-projetivo, o mesmo vale para W. Logo, podemos encontrar um vértice R de W contido em Q. Como W é relativamente $\mathfrak{Y}$-projetivo, o Teorema 3.2.12 nos dá $R \subseteq_L \mathfrak{Y}$ e, pelo Lema 3.4.9, $R \subseteq_G \mathfrak{X}$. Pela transitividade da indução, W^G também é relativamente R-projetivo, então concluímos de $R \subseteq_G \mathfrak{X}$ que W^G é relativamente $\mathfrak{X}$-projetivo. Como V^G é a soma direta dos módulos W^G quando W percorre os somandos indecomponíveis de V, concluímos que V^G também é relativamente $\mathfrak{X}$-projetivo. □

Os próximos dois resultados estabelecerão as duas direções da correspondência. Utilizaremos os Lemas 3.2.18 e 3.2.20. Note que o primeiro desses lemas lembra muito a Correspondência de Green: temos os módulos indecomponíveis U e V que possuem os mesmos vértices e satisfazem pelo menos uma das condições $U \mid V^G$ e $V \mid U_H$. Por sua vez, é o segundo lema que definitivamente introduzirá a família $\mathfrak{Y}$ na correspondência!

Lema 3.4.11. Se U é um kG-módulo indecomponível e com vértice Q, então

$$U_L \cong V \oplus Y,$$

onde V é um kL-módulo indecomponível com vértice Q, $U \mid V^G$ e Y é um kL-módulo relativamente $\mathfrak{Y}$-projetivo.

Demonstração: Pelo Lema 3.2.18, existe um kL-módulo indecomponível V com vértice Q tal que $U \mid V^G$. Como V é relativamente Q-projetivo, o Lema 3.2.20 diz que

$$(V^G)_L \cong V \oplus Y_1,$$

onde Y_1 é um kL-módulo relativamente $\mathfrak{Y}$-projetivo. Como observamos logo após o Lema 3.4.9, V é o único somando indecomponível de $(V^G)_L$ que possui vértice Q, já que Y_1 é relativamente $\mathfrak{Y}$-projetivo. Novamente pelo Lema 3.2.18, U_L possui um somando indecomponível de vértice Q, então, como $U_L \mid (V^G)_L$, devemos ter $U_L \cong V \oplus Y$, onde Y é um somando direto de Y_1 e, portanto, também é relativamente $\mathfrak{Y}$-projetivo. □

Lema 3.4.12. Se V é um kL-módulo indecomponível e com vértice Q, então

$$V^G \cong U \oplus X,$$

onde U é um kG-módulo indecomponível com vértice Q, $V \mid U_L$ e X é um kG-módulo relativamente $\mathfrak{X}$-projetivo.

Demonstração: Seja

$$V^G = U_1 \oplus \cdots \oplus U_n$$

uma decomposição de V^G como soma direta de indecomponíveis. Como V é relativamente Q-projetivo, o Lema 3.2.20 nos dá uma decomposição

$$(V^G)_L \cong V \oplus Y,$$

onde Y é um kL-módulo relativamente $\mathfrak{Y}$-projetivo. Mas veja que $(V^G)_L$ é a soma direta de $(U_1)_L, \ldots, (U_n)_L$, então podemos renumerar os índices de modo que $(U_1)_L \cong V \oplus Y_1$ e $(U_i)_L \cong Y_i$ para $1 < i \leq n$, onde $Y_1, \ldots, Y_n$ são somandos diretos de Y. Vamos mostrar que U_1 possui vértice Q e que U_i é relativamente $\mathfrak{X}$-projetivo para $1 < i \leq n$. Com isso, a demonstração termina se tomarmos $U = U_1$ e $X = U_2 \oplus \cdots \oplus U_n$.

Comecemos mostrando que $U = U_1$ possui vértice Q. Como V é relativamente Q-projetivo, o mesmo vale para V^G e, como $U \mid V^G$, podemos encontrar um vértice R de U contido em Q. Pelo Lema 3.2.18, U_L possui um somando indecomponível W de vértice R. Como $U_L \cong V \oplus Y_1$, temos $W \cong V$ ou temos W isomorfo a um somando direto de Y_1. Suponha, por absurdo, que esse segundo

caso aconteça. Então W é relativamente $\mathfrak{Y}$-projetivo e, pelo Teorema 3.2.12, $R \subseteq_L \mathfrak{Y}$. Pelo Lema 3.4.9, $R \subseteq_G \mathfrak{X}$ e U é relativamente $\mathfrak{X}$-projetivo. Agora, pelo Lema 3.4.10, U_L é relativamente $\mathfrak{Y}$-projetivo, o que é um absurdo, pois V é um somando direto de U_L de vértice Q e, por isso, V não pode ser relativamente $\mathfrak{Y}$-projetivo pelo que observamos logo após o Lema 3.4.9. Concluímos que $W \cong V$ e, como Q é vértice de V, devemos ter $R = Q$, como queríamos.

Seja $1 < i \leq n$. A demonstração de que U_i é relativamente $\mathfrak{X}$-projetivo é parecida com o que fizemos no parágrafo anterior. Como V é relativamente Q-projetivo e $U_i \mid V^G$, podemos encontrar um vértice R de U_i contido em Q. Pelo Lema 3.2.18, $(U_i)_L \cong Y_i$ possui um somando indecomponível de vértice R. Como Y_i é relativamente $\mathfrak{Y}$-projetivo, o Teorema 3.2.12 nos dá $R \subseteq_L \mathfrak{Y}$ e, pelo Lema 3.4.9, $R \subseteq_G \mathfrak{X}$. Assim, U_i é relativamente $\mathfrak{X}$-projetivo, concluindo a demonstração. □

Estamos prontos para terminar a prova do Teorema 3.4.3! Seja U um kG-módulo indecomponível e com vértice Q. Pelo Lema 3.4.11, podemos escrever

$$U_L \cong f(U) \oplus Y,$$

onde $f(U)$ é um kL-módulo indecomponível de vértice Q satisfazendo $U \mid f(U)^G$ e Y é um kL-módulo relativamente $\mathfrak{Y}$-projetivo. Como observamos após o Lema 3.4.9, $f(U)$ é o único somando indecomponível de U_L com vértice Q, porque Y é relativamente $\mathfrak{Y}$-projetivo. Com isso, está provado o item (1) do Teorema 3.4.3. Para o próximo item, seja V um kL-módulo indecomponível e com vértice Q. Pelo Lema 3.4.12, podemos escrever

$$V^G \cong g(V) \oplus X,$$

onde $g(V)$ é um kG-módulo indecomponível de vértice Q satisfazendo $V \mid g(V)_L$ e X é um kG-módulo relativamente $\mathfrak{X}$-projetivo. Novamente pela observação após o Lema 3.4.9, $g(V)$ é o único somando indecomponível de V^G com vértice Q, pois X é relativamente $\mathfrak{X}$-projetivo. Dessa forma, também está demonstrado o item (2) da correspondência. Por fim, aplicando esse item (2) do Teorema 3.4.3 ao kL-módulo $f(U)$, vemos que $f(U)^G$ possui um único somando indecomponível $g(f(U))$ que possui vértice Q. Mas U possui vértice Q e $U \mid f(U)^G$, então vale

$$g(f(U)) \cong U.$$

Analogamente, segue do item (1) do Teorema 3.4.3 e de $V \mid g(V)_L$ que

$$f(g(V)) \cong V.$$

A Correspondência de Green está, finalmente, completamente provada!

3.5 A Correspondência de Green: mapas

Veremos nesta seção como o estudo dos homomorfismos pode nos dar novas informações sobre a Correspondência de Green. Manteremos as notações da seção anterior: Q é um p-subgrupo de G, L é um subgrupo de G que contém $N_G(Q)$ e $\mathfrak{X}$ e $\mathfrak{Y}$ são as famílias de subgrupos que aparecem na Definição 3.4.1.

O Corolário 3.3.4 lidava com homomorfismos que se fatoravam através de projetivos. Aqui, iremos generalizar trocando o módulo projetivo por um módulo relativamente projetivo. Será conveniente introduzir mais uma notação.

Notação 3.5.1. Seja $\mathscr{H}$ uma família de subgrupos de G. Se M e N são kG-módulos, denotamos o espaço de todos os homomorfismos de M em N que se fatoram através de um módulo relativamente $\mathscr{H}$-projetivo por

$$\mathrm{Hom}_{kG,\mathscr{H}}(M, N),$$

e cada um desses homomorfismos será chamado de $\mathscr{H}$**-projetivo**. O quociente do espaço de homomorfismos $\mathrm{Hom}_{kG}(M,N)$ pelo subespaço $\mathrm{Hom}_{kG,\mathscr{H}}(M,N)$ é denotado por

$$\overline{\mathrm{Hom}}^{\mathscr{H}}_{kG}(M,N).$$

Por simplicidade, quando $\mathscr{H}$ possuir um único subgrupo H, trocaremos $\mathscr{H}$ por H nas notações anteriores.

Como soma direta de módulos relativamente $\mathscr{H}$-projetivos também é um módulo relativamente $\mathscr{H}$-projetivo, o argumento dado logo antes do Corolário 3.3.4 pode ser facilmente adaptado para provar que $\mathrm{Hom}_{kG,\mathscr{H}}(M,N)$ de fato é um subespaço de $\mathrm{Hom}_{kG}(M,N)$. Lembre que um módulo relativamente 1-projetivo é o mesmo que um módulo projetivo, logo, quando $\mathscr{H}$ contém apenas do grupo trivial $\{1\}$, vemos que $\mathrm{Hom}_{kG,\mathscr{H}}(M,N)$ é o subespaço dos homomorfismos que se fatoram através de um módulo projetivo e

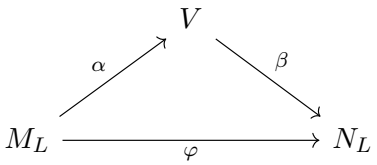
$$\overline{\mathrm{Hom}}^{\{1\}}_{kG}(M,N) = \overline{\mathrm{Hom}}_{kG}(M,N).$$

Lema 3.5.2. Se M e N são kG-módulos, então

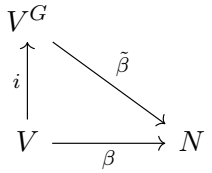
$$\mathrm{Hom}_{kL,Q}(M,N) \subseteq \mathrm{Hom}_{kL,\mathfrak{Y}}(M,N) + \mathrm{Hom}_{kG,Q}(M,N) \subseteq \mathrm{Hom}_{kL}(M,N).$$

A última inclusão apenas serve para lembrar que a soma de subespaços em questão está sendo feita dentro de $\mathrm{Hom}_{kL}(M,N)$. Esse resultado nos diz que todo homomorfismo de kL-módulos Q-projetivo de M em N pode ser "aproximado" por um homomorfismo de kG-módulos Q-projetivo com um "erro" em $\mathrm{Hom}_{kL,\mathfrak{Y}}(M,N)$.

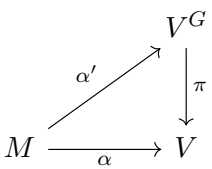
Demonstração: Seja $\varphi \in \mathrm{Hom}_{kL,Q}(M,N)$ qualquer. Assim, existem um kL-módulo V relativamente Q-projetivo e homomorfismos de kL-módulos $\alpha : M_L \to V$ e $\beta : V \to N_L$ fazendo o seguinte diagrama comutar:



Se $i : V \to V^G$ é a inclusão canônica que leva $v \in V$ em $1 \otimes v \in V^G$, então a propriedade universal dos módulos relativamente L-projetivos garante a existência de um homomorfismo de kG-módulos $\tilde{\beta} : V^G \to N$ comutando o seguinte diagrama:



Agora, como descrito no Exercício A.3.1, seja $\pi : V^G \to V$ a projeção canônica que leva $1 \otimes v$ em v e $s \otimes v$ em 0, se $s \notin L$. Por esse mesmo exercício, temos um homomorfismo de kG-módulos $\alpha' : M \to V^G$ que torna o seguinte diagrama comutativo:



Juntando essas três informações, concluímos que

$$\varphi = \beta\alpha = \tilde{\beta}i\pi\alpha' = \tilde{\beta}\alpha' + (\tilde{\beta}i\pi\alpha' - \tilde{\beta}\alpha') = \tilde{\beta}\alpha' + \tilde{\beta}(i\pi - \mathrm{id}_{V^G})\alpha'.$$

Note que $\tilde{\beta}\alpha'$ é um homomorfismo de kG-módulos de M em N que se fatora por V^G, que é relativamente Q-projetivo pois V o é. Logo, $\tilde{\beta}\alpha' \in \mathrm{Hom}_{kG,Q}(M,N)$. Para terminar, basta provarmos que

$$\tilde{\beta}(i\pi - \mathrm{id}_{V^G})\alpha' \in \mathrm{Hom}_{kL,\mathfrak{Y}}(M,N),$$

sendo suficiente mostrar que $i\pi - \mathrm{id}_{V^G}$ se fatora através de um kL-módulo relativamente $\mathfrak{Y}$-projetivo. Definindo

$$Y \coloneqq \bigoplus_{\substack{s\in[G/L]\\ s\notin L}} s\otimes V,$$

vemos que Y é um kL-submódulo de $(V^G)_L$ e temos a decomposição $(V^G)_L = V \oplus Y$, onde identificamos V com a imagem da inclusão i. Observe que $i\pi$ é a projeção de V^G em V, então a imagem de $i\pi - \mathrm{id}_{V^G}$ está contida em Y e esse homomorfismo se fatora por Y. Mas, pelo Lema 3.2.20, $(V^G)_L \cong V \oplus W$ onde W é um kL-módulo relativamente $\mathfrak{Y}$-projetivo. Pelo Teorema de Krull-Schmidt, concluímos que $Y \cong W$ e então Y é relativamente $\mathfrak{Y}$-projetivo, terminando a demonstração. □

O lema anterior tem uma aplicação interessante. Seja U um kG-módulo indecomponível com vértice Q e seja V o seu correspondente de Green. Suponha que M seja um kG-módulo indecomponível com vértice Q satisfazendo $V \mid M_L$. Pela Correspondência de Green, M_L tem apenas um único somando indecomponível de vértice Q, que é o seu kL-módulo correspondente, então concluímos que M corresponde a V e, portanto, $M \cong U$. Surpreendentemente, veremos a seguir que a hipótese de que M possuía vértice Q era desnecessária!

Teorema 3.5.3 (Burry-Carlson-Puig)**.** Sejam U um kG-módulo indecomponível com vértice Q e V o kL-módulo correspondente.

(1) Se M é um kG-módulo indecomponível e $V \mid M_L$, então $M \cong U$.

(2) Se M é um kG-módulo qualquer, então $U \mid M$ se, e somente se, $V \mid M_L$.

Esse teorema deve ser visto como um refinamento de parte da Correspondência de Green. A princípio, um kG-módulo indecomponível M não precisa estar sendo considerado na correspondência, pois não temos informações sobre o seu vértice. Porém, se soubermos que a restrição de M a L possui um somando indecomponível de vértice Q, então M também possui vértice Q e a correspondência se aplica a M.

Demonstração: Inicialmente, vejamos que o item (1) implica o item (2). Se M é um kG-módulo qualquer e $U \mid M$, então $U_L \mid M_L$ e, como $V \mid U_L$ pela Correspondência de Green, temos $V \mid M_L$. Reciprocamente, se $V \mid M_L$, existe um somando indecomponível M' de M tal que $V \mid M'_L$, pois V é indecomponível. Pelo item (1), $M' \cong U$ e então $U \mid M$, como preciso.

Demonstremos o item (2). Seja M um kG-módulo indecomponível com $V \mid M_L$. Como observamos imediatamente antes de enunciar o resultado, é suficiente mostrar que M possui vértice Q para concluir que $M \cong U$. Faremos mais uma redução: é suficiente mostrar que M é relativamente Q-projetivo. Com essa hipótese, M possui um vértice R contido em Q. Como $V \mid M_L$ e M é somando direto de um módulo relativamente R-livre, a Fórmula de Decomposição de Mackey diz que V é relativamente projetivo com relação a $L \cap gRg^{-1}$ para algum $g \in G$. Mas Q é vértice de V, então um conjugado de Q está contido em $L \cap gRg^{-1}$ e temos

$$|Q| \leq \left|L \cap gRg^{-1}\right| \leq \left|gRg^{-1}\right| = |R|.$$

Como $R \subseteq Q$, devemos ter $R = Q$ e então Q é um vértice de M.

Mostrar que M é relativamente Q-projetivo é equivalente a mostrar que a identidade id_M é um homomorfismo Q-projetivo. De fato, como id_M se fatora por M, se M é relativamente Q-projetivo, então id_M é Q-projetivo. Reciprocamente, se id_M se fatora através de um módulo relativamente Q-projetivo W, então existem homomorfismos $\lambda : M \to W$ e $\mu : W \to M$ tais que $\mathrm{id}_M = \mu\lambda$. Mas então μ é um homomorfismo sobrejetor que cinde, de onde concluímos que M é somando direto de W e então M é relativamente Q-projetivo, como queríamos. Assim, devemos provar que $\mathrm{id}_M \in \mathrm{Hom}_{kG,Q}(M, M)$.

Como $V \mid M_L$, existe um kL-módulo V' tal que $M_L \cong V \oplus V'$. Seja $\pi : M \to M$ a projeção de M em V com núcleo V'. Note que π se fatora através da imagem V, que é um módulo relativamente Q-projetivo, então $\pi \in \mathrm{Hom}_{kL,Q}(M, M)$ e, pelo Lema 3.5.2, existem

$$\alpha \in \mathrm{Hom}_{kG,Q}(M, M) \quad \text{e} \quad \beta \in \mathrm{Hom}_{kL,\mathfrak{Y}}(M, M)$$

tais que $\pi = \alpha + \beta$. Agora, suponha, por absurdo, que $\mathrm{id}_M \notin \mathrm{Hom}_{kG,Q}(M, M)$. Não é difícil mostrar que $\mathrm{Hom}_{kG,Q}(M, M)$ é um ideal de $\mathrm{End}_{kG}(M)$ e, pela nossa suposição, esse ideal é próprio. Mas $\mathrm{End}_{kG}(M)$ é uma álgebra local por conta da indecomponibilidade de M (Corolário 2.1.8), então todo elemento de $\mathrm{Hom}_{kG,Q}(M, M)$ é nilpotente pela Proposição 2.1.4. Em particular, temos $\alpha^n = 0$ para algum inteiro $n \geq 1$. Desenvolvendo o binômio

$$\pi = \pi^n = (\alpha + \beta)^n,$$

segue que π é a soma de $\alpha^n = 0$ com termos envolvendo β. Como β é $\mathfrak{Y}$-projetivo, concluímos que π também o é. Por outro lado, a identidade id_V é a composição de uma inclusão de V em M, π e um homomorfismo de M em V, de onde concluímos que id_V também é $\mathfrak{Y}$-projetivo. Pelo mesmo argumento do parágrafo anterior, segue que V é relativamente $\mathfrak{Y}$-projetivo e então temos $Q \subseteq_L \mathfrak{Y}$. Pelo Lema 3.4.9, $Q \subseteq_G \mathfrak{X}$, uma contradição. Por isso, $\mathrm{id}_M \in \mathrm{Hom}_{kG,Q}(M, M)$ e a demonstração está concluída. □

Iremos enunciar o outro grande resultado desta seção. Utilizaremos a família $\mathfrak{Z}$ que aparece na Definição 3.4.5.

Teorema 3.5.4. Sejam U um kG-módulo indecomponível com vértice em $\mathfrak{Z}$ e V o kL-módulo correspondente. Se M é um kG-módulo qualquer, então

$$\overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(M, U) \cong \overline{\mathrm{Hom}}^{\mathfrak{X}}_{kL}(M_L, V) \cong \overline{\mathrm{Hom}}^{\mathfrak{Y}}_{kL}(M_L, V).$$

A prova deste teorema necessita de dois lemas que agora demonstraremos.

Lema 3.5.5. Sejam H um subgrupo de G, V um kH-módulo e U um kG-módulo. Se $\varphi : V^G \to U$ é um homomorfismo de kG-módulos, então φ se fatora por $(U_H)^G$.

Demonstração: Seja $i : V \to V^G$ a inclusão canônica que leva $v \in V$ em $1 \otimes v \in V^G$ e seja $\pi : V^G \to V$ a projeção canônica que leva $1 \otimes v$ em v e $s \otimes v$ em 0, se $s \notin H$. Defina $\psi = \varphi i \pi$, que é um homomorfismo de kH-módulos de $(V^G)_H$ em U_H. Pelo Exercício A.3.1, temos um homomorfismo de kG-módulos $\psi' : V^G \to (U_H)^G$ dado por

$$\psi'(x) = \sum_{s \in [G/H]} s \otimes \psi(s^{-1}x)$$

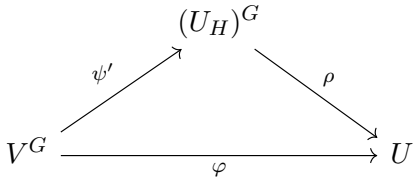
para todo $x \in V^G$. Agora, seja $\rho : (U_H)^G \to U$ o homomorfismo de kG-módulos que estende a identidade em U. Se

$$\sum_{t \in [G/H]} t \otimes u_t \in (U_H)^G,$$

então

$$\rho\left(\sum_{t\in[G/H]} t\otimes u_t\right) = \sum_{t\in[G/H]} t\cdot\rho(1\otimes u_t) = \sum_{t\in[G/H]} tu_t.$$

Para concluir o lema, vamos mostrar que o seguinte diagrama comuta:



Dado

$$\sum_{t\in[G/H]} t\otimes v_t \in V^G,$$

vale

$$\begin{aligned}\rho\psi'\left(\sum_{t\in[G/H]} t\otimes v_t\right) &= \rho\left(\sum_{s\in[G/H]} s\otimes\psi\left(s^{-1}\sum_{t\in[G/H]} t\otimes v_t\right)\right)\\ &= \sum_{s\in[G/H]} s\cdot(\varphi i\pi)\left(\sum_{t\in[G/H]} s^{-1}t\otimes v_t\right)\\ &= \sum_{s\in[G/H]} s\varphi(1\otimes v_s)\\ &= \varphi\left(\sum_{s\in[G/H]} s\otimes v_s\right),\end{aligned}$$

como queríamos. □

Lema 3.5.6. Sejam U, V e W kG-módulos e sejam $\mathscr{H}$ e $\mathscr{K}$ famílias de subgrupos de G. Se $\alpha : U \to V$ é um homomorfismo $\mathscr{H}$-projetivo e se $\beta : V \to W$ é um homomorfismo $\mathscr{K}$-projetivo, então $\beta\alpha : U \to W$ é um homomorfismo $\mathscr{L}$-projetivo, onde

$$\mathscr{L} = \{H \cap gKg^{-1} \mid H \in \mathscr{H}, K \in \mathscr{K}, g \in G\}.$$

Demonstração: Como $\alpha : U \to V$ é $\mathscr{H}$-projetivo, existem um kG-módulo relativamente $\mathscr{H}$-projetivo M e mapas $\lambda : U \to M$ e $\mu : M \to V$ tais que $\alpha = \mu\lambda$. Decompondo

$$M = M_1 \oplus \cdots \oplus M_r,$$

onde $M_1, \ldots, M_r$ são kG-módulos indecomponíveis, a definição de módulo relativamente $\mathscr{H}$-projetivo nos diz que cada M_j é relativamente H_j-projetivo para algum $H_j \in \mathscr{H}$. Para cada $1 \leq j \leq r$, sejam $i_j : M_j \to M$ e $\pi_j : M \to M_j$ a inclusão e a projeção canônicas, respectivamente, e defina $\alpha_j : U \to V$ por $\alpha_j = \mu i_j \pi_j \lambda$. Note que α_j se fatora por M_j e, como M_j é somando direto de um módulo relativamente H_j-livre, α_j também se fatora por esse módulo relativamente H_j-livre. Agora, observe que

$$\alpha = \mu\lambda = \mu \circ \mathrm{id}_M \circ \lambda = \mu\left(\sum_{j=1}^{r} i_j\pi_j\right)\lambda = \sum_{j=1}^{r}\alpha_j.$$

Com um argumento análogo, podemos escrever

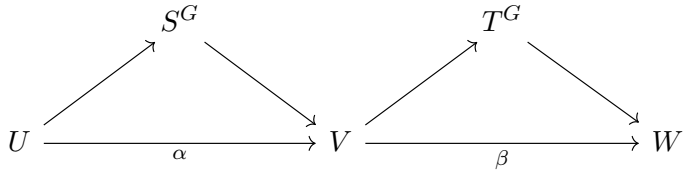
$$\beta = \sum_{j=1}^{s} \beta_j,$$

onde cada $\beta_j : V \to W$ é um homomorfismo de kG-módulos que se fatora através de um módulo relativamente K_j-livre para algum $K_j \in \mathscr{K}$. Assim, temos

$$\beta\alpha = \sum_{j_1=1}^{r} \sum_{j_2=1}^{s} \beta_{j_2}\alpha_{j_1}.$$

Como $\mathrm{Hom}_{kG,\mathscr{L}}(U,W)$ é um subespaço de $\mathrm{Hom}_{kG}(U,W)$, é suficiente mostrar que cada parcela na soma acima está em $\mathrm{Hom}_{kG,\mathscr{L}}(U,W)$ para concluir que $\beta\alpha$ é $\mathscr{L}$-projetivo.

Pelo parágrafo anterior, podemos assumir que α se fatora através de um módulo H-livre e que β se fatora através de um módulo K-livre, onde $H \in \mathscr{H}$ e $K \in \mathscr{K}$. Logo, temos um diagrama comutativo



onde S é um kH-módulo e T é um kK-módulo. Seja $\varphi : S^G \to T^G$ o homomorfismo dado pela composição dos mapas $S^G \to V$ e $V \to T^G$ do diagrama acima. Para mostrar que $\beta\alpha \in \mathrm{Hom}_{kG,\mathscr{L}}(U,W)$, basta provar que φ se fatora através de um módulo relativamente $\mathscr{L}$-projetivo. Mas o Lema 3.5.5 diz que φ se fatora por $((T^G)_H)^G$. Pela Fórmula de Decomposição de Mackey, $(T^G)_H$ é relativamente $\mathscr{L}$-projetivo e, pela transitividade da indução (item (3) do Lema 3.1.10), o mesmo vale para $((T^G)_H)^G$, concluindo a demonstração. □

Agora conseguimos demonstrar o Teorema 3.5.4!

Demonstração: Vamos começar mostrando que

$$\overline{\mathrm{Hom}}^{\mathfrak{X}}_{kL}(M_L, V) \cong \overline{\mathrm{Hom}}^{\mathfrak{Y}}_{kL}(M_L, V)$$

e, para isso, vamos provar que

$$\mathrm{Hom}_{kL,\mathfrak{X}}(M_L, V) = \mathrm{Hom}_{kL,\mathfrak{Y}}(M_L, V).$$

Como todo elemento de $\mathfrak{X}$ está contido num elemento de $\mathfrak{Y}$, todo kL-módulo relativamente $\mathfrak{X}$-projetivo também é relativamente $\mathfrak{Y}$-projetivo, de onde obtemos a inclusão

$$\mathrm{Hom}_{kL,\mathfrak{X}}(M_L, V) \subseteq \mathrm{Hom}_{kL,\mathfrak{Y}}(M_L, V).$$

Para mostrar a outra inclusão, seja $\varphi \in \mathrm{Hom}_{kL,\mathfrak{Y}}(M_L, V)$. Como V é relativamente Q-projetivo (pois possui um vértice em $\mathfrak{Z}$, que é uma família de subgrupos de Q), a identidade id_V é um homomorfismo Q-projetivo. Mas $\varphi = \mathrm{id}_V \circ \varphi$, então, pelo Lema 3.5.6, φ é projetivo com relação à família dos subgrupos da forma $H \cap xQx^{-1}$ para $H \in \mathfrak{Y}$ e $x \in L$. Note que $H \cap xQx^{-1}$ é conjugado em L a $x^{-1}Hx \cap Q$, então φ também é projetivo com relação à família

$$\begin{aligned}
\{Q \cap xHx^{-1} \mid H \in \mathfrak{Y}, x \in L\} &= \{Q \cap xLx^{-1} \cap xgQg^{-1}x^{-1} \mid x \in L, g \in G, g \notin L\} \\
&= \{Q \cap L \cap (xg)Q(xg)^{-1} \mid x \in L, g \in G, g \notin L\} \\
&= \{Q \cap gQg^{-1} \mid g \in G, g \notin L\} \\
&= \mathfrak{X},
\end{aligned}$$

ou seja, $\varphi \in \mathrm{Hom}_{kL,\mathfrak{X}}(M_L, V)$ e provamos a outra inclusão que queríamos demonstrar. Utilizamos a definição de $\mathfrak{Y}$ na primeira igualdade acima, depois usamos que $x \in L$ na segunda e, para a terceira, notamos que $Q \subseteq L$ e que sempre temos $xg \notin L$ e, consequentemente, podemos supor $x = 1$ na definição do conjunto.

Agora, vamos para a segunda metade da demonstração. Provaremos que

$$\overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(M, U) \cong \overline{\mathrm{Hom}}^{\mathfrak{Y}}_{kL}(M_L, V).$$

Pelo Corolário 3.4.6, $V^G \cong U \oplus X$ para algum kG-módulo relativamente $\mathfrak{X}$-projetivo X. Usando um resultado análogo ao Exercício A.3.15, vemos que

$$\overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(M, V^G) \cong \overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(M, U) \oplus \overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(M, X) \cong \overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(M, U).$$

Logo, basta mostrarmos que

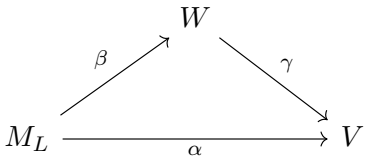
$$\overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(M, V^G) \cong \overline{\mathrm{Hom}}^{\mathfrak{Y}}_{kL}(M_L, V).$$

A Reciprocidade de Frobenius nos dá um isomorfismo

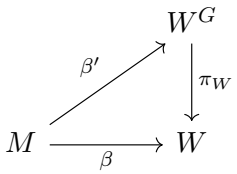
$$\mathrm{Hom}_{kG}(M, V^G) \cong \mathrm{Hom}_{kL}(M_L, V),$$

logo, utilizando a descrição explícita desse isomorfismo dada pelo Exercício A.3.1, provaremos que homomorfismos de kG-módulos $\mathfrak{X}$-projetivos correspondem a homomorfismos de kL-módulos $\mathfrak{Y}$-projetivos, o que concluirá a demonstração.

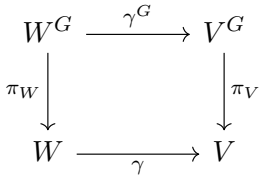
Primeiramente, seja $\alpha \in \mathrm{Hom}_{kL,\mathfrak{Y}}(M_L, V)$. Pela primeira parte da demonstração, $\alpha \in \mathrm{Hom}_{kL,\mathfrak{X}}(M_L, V)$. Logo, existem um kL-módulo relativamente $\mathfrak{X}$-projetivo W e homomorfismos $\beta : M_L \to W$ e $\gamma : W \to V$ que comutam o seguinte diagrama:



Vamos mostrar que o homomorfismo $\alpha' : M \to V^G$ que corresponde a α se fatora por W^G, que é relativamente $\mathfrak{X}$-projetivo, já que W o é. Denote por $\pi_V : V^G \to V$ e $\pi_W : W^G \to W$ as projeções descritas no item (c) do Exercício A.3.1. Por esse exercício, se $\beta' : M \to W^G$ é o homomorfismo que corresponde a β, então temos o diagrama comutativo:



Note também que temos mais um diagrama comutativo:



De fato, se

$$\sum_{s \in [G/L]} s \otimes w_s \in W^G,$$

então

$$\pi_V \gamma^G \left(\sum_{s \in [G/L]} s \otimes w_s \right) = \pi_V \left(\sum_{s \in [G/L]} s \otimes \gamma(w_s) \right) = \gamma(w_1)$$

e

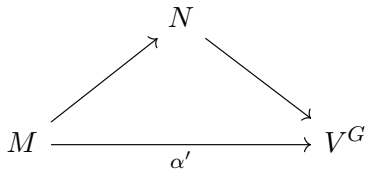
$$\gamma \pi_W \left(\sum_{s \in [G/L]} s \otimes w_s \right) = \gamma(w_1),$$

de onde segue que $\pi_V \gamma^G = \gamma \pi_W$. Juntando esses três diagramas comutativos, concluímos que

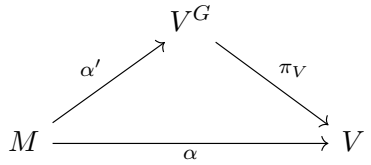
$$\pi_V(\gamma^G \beta') = (\pi_V \gamma^G)\beta' = (\gamma \pi_W)\beta' = \gamma(\pi_W \beta') = \gamma\beta = \alpha.$$

Pelo Exercício A.3.1, o isomorfismo entre $\mathrm{Hom}_{kG}(M, V^G)$ e $\mathrm{Hom}_{kL}(M_L, V)$ leva o homomorfismo $\gamma^G \beta'$ em $\pi_V(\gamma^G \beta') = \alpha$, de onde obtemos que $\alpha' = \gamma^G \beta'$. Dessa forma, α' se fatora através de W^G e $\alpha' \in \mathrm{Hom}_{kG,\mathfrak{X}}(M, V^G)$, como preciso.

Para terminar, suponha agora que $\alpha \in \mathrm{Hom}_{kL}(M_L, V)$ e que o correspondente α' esteja em $\mathrm{Hom}_{kG,\mathfrak{X}}(M, V^G)$. Mostremos que $\alpha \in \mathrm{Hom}_{kL,\mathfrak{Y}}(M_L, V)$. Seja N um kG-módulo relativamente $\mathfrak{X}$-projetivo de modo que tenhamos um diagrama comutativo:



Pelo item (c) do Exercício A.3.1, temos outro diagrama comutativo:



Juntando os dois diagramas, segue que α se fatora por N_L. Mas N_L é relativamente $\mathfrak{Y}$-projetivo pelo Lema 3.4.10, então $\alpha \in \mathrm{Hom}_{kL,\mathfrak{Y}}(M_L, V)$, como queríamos. Assim, a demonstração do teorema está concluída. □

Corolário 3.5.7. Se U_1 e U_2 são kG-módulos indecomponíveis com vértices em $\mathfrak{Z}$ e se V_1 e V_2 são os kL-módulos correspondentes, então

$$\overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(U_1, U_2) \cong \overline{\mathrm{Hom}}^{\mathfrak{X}}_{kL}(V_1, V_2) \cong \overline{\mathrm{Hom}}^{\mathfrak{Y}}_{kL}(V_1, V_2).$$

Esse corolário é uma generalização do Corolário 3.3.4. De fato, como vimos no Exemplo 3.4.8, as hipóteses do Corolário 3.3.4 nos dão que $\mathfrak{X}$ e $\mathfrak{Y}$ contêm apenas o subgrupo $\{1\}$ e que os módulos indecomponíveis com vértice em $\mathfrak{Z}$ são exatamente os não projetivos.

Demonstração: Pelo Corolário 3.4.6, sabemos que $(U_1)_L \cong V_1 \oplus Y$, onde Y é um kL-módulo relativamente $\mathfrak{Y}$-projetivo. Pelo Teorema 3.5.4 e por um resultado análogo ao Exercício A.3.15, vale

$$\overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(U_1, U_2) \cong \overline{\mathrm{Hom}}^{\mathfrak{X}}_{kL}(V_1 \oplus Y, V_2) \cong \overline{\mathrm{Hom}}^{\mathfrak{X}}_{kL}(V_1, V_2) \oplus \overline{\mathrm{Hom}}^{\mathfrak{X}}_{kL}(Y, V_2).$$

e

$$\overline{\mathrm{Hom}}^{\mathfrak{X}}_{kG}(U_1, U_2) \cong \overline{\mathrm{Hom}}^{\mathfrak{Y}}_{kL}(V_1 \oplus Y, V_2) \cong \overline{\mathrm{Hom}}^{\mathfrak{Y}}_{kL}(V_1, V_2) \oplus \overline{\mathrm{Hom}}^{\mathfrak{Y}}_{kL}(Y, V_2).$$

Mas V_2 é relativamente Q-projetivo, então, assim como fizemos na primeira parte da demonstração do Teorema 3.5.4, segue que

$$\mathrm{Hom}_{kL,\mathfrak{X}}(Y, V_2) = \mathrm{Hom}_{kL,\mathfrak{Y}}(Y, V_2).$$

Como Y é relativamente $\mathfrak{Y}$-projetivo, temos

$$\mathrm{Hom}_{kL,\mathfrak{Y}}(Y, V_2) = \mathrm{Hom}_{kL}(Y, V_2)$$

e então

$$\overline{\mathrm{Hom}}^{\mathfrak{X}}_{kL}(Y, V_2) = \overline{\mathrm{Hom}}^{\mathfrak{Y}}_{kL}(Y, V_2) = 0,$$

terminando a demonstração do corolário. □

Observação 3.5.8. Note que o resultado anterior não exige que U_1 e U_2 tenham o mesmo vértice. É por conta dessa flexibilidade que utilizamos a família $\mathfrak{Z}$ ao invés de apenas considerar módulos indecomponíveis com vértice Q.

Capítulo 4

Teoria dos blocos

Agora, trataremos de um dos aspectos mais relevantes da teoria de representações modulares: a teoria dos blocos.

A definição de bloco pode ser dada para álgebras quaisquer, então é nessa generalidade que começamos o capítulo. Ela é natural e pode ser pensada como uma generalização da decomposição dada pelo Teorema de Wedderburn para álgebras semissimples. Após abordar esses conceitos, a primeira seção também apresenta como a decomposição de uma álgebra em blocos se reflete em uma decomposição dos módulos da álgebra. Apresentamos alguns critérios para decidir quando duas representações simples pertencem ao mesmo bloco e, ao final, também damos uma motivação para o nome "bloco" introduzindo a matriz de Cartan.

Voltando ao caso das representações de G, observamos como tornar um bloco de kG em um $k[G \times G]$-módulo indecomponível. Com isso, podemos atacar os blocos de álgebras de grupo usando a teoria de vértices e fontes desenvolvida anteriormente! Somos prontamente levados a definir o grupo de defeito de um bloco. Assim como um vértice mede o quão longe um módulo indecomponível está de ser projetivo, o grupo de defeito também captura uma certa noção de complexidade do bloco. Provamos algumas propriedades que apontam nessa direção.

A terceira seção contém os mais importantes resultados do capítulo: os três Teoremas Principais de Brauer. Eles giram em torno da Correspondência de Brauer, que nos permite relacionar blocos de G com blocos de um subgrupo H e é muito similar à Correspondência de Green. Esses três teoremas nos dão propriedades fortes dessa correspondência quando H contém o normalizador de um grupo de defeito de um bloco de kG. A partir deles, obtemos novos resultados sobre os próprios grupos de defeito e conseguimos, por exemplo, caracterizar os blocos de defeito zero. Para ilustrar esses resultados, aplicamos a Correspondência de Brauer no caso concreto do grupo $\mathrm{SL}_2(p)$.

O capítulo se encerra com duas seções mais técnicas. A primeira delas estuda melhor a teoria de Clifford para blocos, ou seja, a relação dos blocos de G com os blocos de um subgrupo normal. Duas consequências desse estudo são um refinamento do Primeiro Teorema Principal de Brauer e uma prova da versão forte do Terceiro Teorema. A partir dessa última demonstração, somos motivados a definir o conceito de subpar e concluímos mostrando como os subpares de G se comportam de modo muito semelhante aos p-subgrupos de G.

4.1 Definições e propriedades iniciais

Voltaremos a trabalhar no contexto mais geral de álgebras associativas e de dimensão finita. Suponha que decomponhamos uma álgebra A como uma soma direta

$$A = A_1 \oplus \cdots \oplus A_r,$$

onde $A_1, \ldots, A_r$ são ideais bilaterais. Note que cada A_i é uma álgebra. De fato, o único ponto problemático seria encontrar uma identidade para A_i. Como cada um dos somandos acima é um

ideal, não é difícil ver que $A_i \cdot A_j = 0$ para índices $i \neq j$. Portanto, decompondo

$$1 = e_1 + \cdots + e_r,$$

onde $e_i \in A_i$ para todo $1 \leq i \leq r$, é fácil ver que

$$e_i \cdot a_i = 1 \cdot a_i = a_i$$

e

$$a_i \cdot e_i = a_i \cdot 1 = a_i$$

para todos $a_i \in A_i$ e $1 \leq i \leq r$. Ou seja, a identidade de A_i é o elemento e_i! Além disso, A é isomorfo ao produto direto das álgebras $A_1, \ldots, A_r$. Veja também que $e_1, \ldots, e_r$ são idempotentes dois a dois ortogonais e, como e_i comuta com todos os elementos de A_i e com todos os elementos de A_j para $j \neq i$ (pois $e_i A_j = A_j e_i = 0$), esses idempotentes também estão no centro de A.

Definição 4.1.1. Um elemento $e \in A$ é um **idempotente central** se e é um idempotente do centro $Z(A)$. Dizemos que um idempotente não nulo $e \in A$ é **central primitivo** se e é um idempotente primitivo de $Z(A)$, ou seja, se e é central e não pode ser escrito como soma de dois idempotentes centrais ortogonais não nulos.

Observação 4.1.2. Um idempotente central primitivo $e \in A$ não é necessariamente um idempotente primitivo de A. De fato, apenas sabemos que e não se escreve como soma de dois idempotentes *centrais* ortogonais não nulos, mas pode acontecer de e se escrever como soma de dois idempotentes ortogonais não nulos (e tais idempotentes não podem ser ambos centrais).

Definição 4.1.3. Uma álgebra (não nula) A é dita **indecomponível** se A não pode ser escrita como a soma direta de dois ideais bilaterais não nulos.

Temos um resultado análogo à Proposição 2.1.2:

Proposição 4.1.4. Seja A um k-álgebra de dimensão finita. Decomposições

$$A = A_1 \oplus \cdots \oplus A_r$$

de A como soma direta de ideais bilaterais estão em bijeção com decomposições

$$1 = e_1 + \cdots + e_r$$

da identidade como soma de idempotentes centrais dois a dois ortogonais. Aqui, e_i é dado pela identidade de A_i, enquanto A_i é obtido de e_i como $A_i = Ae_i$. O somando A_i é uma álgebra indecomponível se, e somente se, e_i é um idempotente central primitivo.

Demonstração: A prova é análoga à demonstração da Proposição 2.1.2, mas devemos identificar A^{op} com $\mathrm{End}_A({}_A A)$ como feito no Lema 1.2.3. Para um maior esclarecimento, daremos os detalhes.

Começamos com uma decomposição de A como soma direta de ideais $A_1, \ldots, A_r$. Como vimos no começo desta seção, cada A_i é uma álgebra com uma identidade e_i, e vale

$$1 = e_1 + \cdots + e_r.$$

Isso estabelece uma direção da bijeção. Para a outra direção, decomponha

$$1 = e_1 + \cdots + e_r,$$

onde $e_1, \ldots, e_r$ são idempotentes centrais dois a dois ortogonais. Para cada $1 \leq i \leq r$, defina $A_i = Ae_i$ e note que A_i é ideal bilateral de A justamente por e_i ser central. Vejamos que A é a soma direta de $A_1, \ldots, A_r$. Se $a \in A$, então

$$a = a \cdot 1 = a \cdot (e_1 + \cdots + e_r) = ae_1 + \cdots + ae_r$$

e $a \in A_1 + \cdots + A_r$, provando que A é a soma de $A_1, \ldots, A_r$. Por outro lado, se vale

$$a_1 + \cdots + a_r = 0,$$

onde cada $a_i \in A_i$, temos que $a_i e_i = a_i$ (pois $e_i^2 = e_i$) e $a_i e_j = 0$ se $j \neq i$ (pois $e_i e_j = 0$). Logo, multiplicando a igualdade acima por e_i, obtemos que $a_i = 0$, para todo $1 \leq i \leq r$. Isso prova que a soma $A_1 + \cdots + A_r$ é direta, como queríamos. Por fim, é fácil verificar que as construções anteriores são uma a inversa da outra, estabelecendo a bijeção desejada.

Para a segunda parte do enunciado, podemos aplicar a primeira parte para a álgebra A_i. Pela bijeção entre as decomposições, sabemos que A_i é uma álgebra indecomponível se, e somente se, a sua identidade não se escreve como soma de idempotentes centrais ortogonais não nulos. Ou seja, A_i é uma álgebra indecomponível se, e somente se, e_i é um idempotente central primitivo de A_i. Assim, basta verificar que, se e_i é um idempotente central primitivo de A_i, então e_i é um idempotente central primitivo de A (a outra implicação é imediata). Vamos mostrar a contrapositiva dessa afirmação. Suponha que $e_i = e + f$, onde $e, f \in A$ são idempotentes centrais ortogonais não nulos. Multiplicando essa expressão por e_i, obtemos $e_i = ee_i + fe_i$. Veja que

$$ee_i = e(e + f) = e^2 + ef = e$$

e, analogamente, $fe_i = f$. Isso mostra que $e \in A_i$ e $f \in A_i$, pois $A_i = Ae_i$. Por isso, conseguimos escrever e_i como soma de idempotentes centrais ortogonais não nulos de A_i, como preciso. □

Exemplo 4.1.5. Se A é uma álgebra semissimples, o Teorema de Wedderburn nos permite escrever A como uma soma direta de ideais isomorfos a álgebras de matrizes sobre álgebras de divisão. Como esses ideais são álgebras simples, certamente são indecomponíveis como álgebras. Pela Proposição 4.1.4, vemos que a identidade de uma álgebra de matrizes é um idempotente central primitivo. Isso nos dá um exemplo de um idempotente central primitivo que não é um idempotente primitivo! De fato, se considerarmos a álgebra de matrizes $M_2(k)$, então a identidade é a soma das matrizes

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

que são idempotentes ortogonais não nulos de $M_2(k)$ que não são centrais. Da mesma forma, temos um resultado análogo para $M_n(D)$ com $n \geq 2$ e D uma álgebra de divisão.

Quando A é semissimples, vimos na Proposição 1.2.10 que há uma unicidade muito forte para uma decomposição de A como soma de ideais indecomponíveis. No caso geral, essa unicidade também vale!

Teorema 4.1.6. Se A é uma k-álgebra de dimensão finita, então existe uma decomposição

$$A = A_1 \oplus \cdots \oplus A_r,$$

onde cada A_i é um ideal bilateral indecomponível (como álgebra). O inteiro positivo r e os ideais $A_1, \ldots, A_r$ estão unicamente determinados (a menos de permutação). Além disso, todo ideal de A que também é um somando direto se escreve como a soma de alguns dos ideais A_i's.

Demonstração: A existência da decomposição é imediata, porque A possui dimensão finita. Vamos mostrar a unicidade. Decomponha A de duas formas:

$$A = A_1 \oplus \cdots \oplus A_r = B_1 \oplus \cdots \oplus B_s,$$

onde $A_1, \ldots, A_r, B_1, \ldots, B_s$ são ideais indecomponíveis de A. Se e_i é a identidade de A_i, então a primeira decomposição nos permite escrever

$$1 = e_1 + \cdots + e_r$$

e a Proposição 4.1.4 diz que $e_1, \ldots, e_r$ são idempotentes centrais primitivos e dois a dois ortogonais. Se $b \in B_1$, podemos escrever

$$b = a_1 + \cdots + a_r,$$

onde $a_i \in A_i$ para todo $1 \leq i \leq r$. Multiplicando a expressão acima por e_i, temos

$$be_i = a_1e_i + \cdots + a_re_i = a_i$$

e, como B_1 é ideal, segue que $a_i \in B_1$. Por isso,

$$B_1 = (B_1 \cap A_1) \oplus \cdots \oplus (B_1 \cap A_r).$$

Como cada $B_1 \cap A_i$ é um ideal de B_1, que é indecomponível, encontramos um único $1 \leq i_0 \leq r$ tal que $B_1 = B_1 \cap A_{i_0}$, ou seja, $B_1 \subseteq A_{i_0}$, e tal que $B_1 \cap A_i = 0$ para $i \neq i_0$. Trocando o papel dos A_i's e dos B_j's, encontramos um único $1 \leq j_0 \leq s$ tal que $A_{i_0} \subseteq B_{j_0}$ e $A_{i_0} \cap B_j = 0$ para $j \neq j_0$. Como $A_{i_0} \cap B_1 = B_1 \neq 0$, concluímos que $j_0 = 1$ e então $A_{i_0} = B_1$. Trocando B_1 por um B_j qualquer, o mesmo argumento prova que cada B_j é igual a um único A_i. Analogamente, cada A_i também é igual a um único B_j. Portanto, $r = s$ e, a menos de permutação, os ideais $A_1, \ldots, A_r$ são os ideais $B_1, \ldots, B_s$.

Por fim, para mostrar a última afirmação do enunciado, vamos lidar diretamente com idempotentes centrais. Como no parágrafo anterior, denote por e_i a identidade de A_i para $1 \leq i \leq r$. Pela Proposição 4.1.4, basta mostrar que todo idempotente central de A é a soma de alguns dos e_i's. Se $e \in A$ é um idempotente central, então podemos escrever

$$e_i = ee_i + (e_i - ee_i) = ee_i + (1 - e)e_i.$$

Veja que ee_i e $(1 - e)e_i$ são idempotentes centrais e ortogonais. Da primitividade de e_i, temos $ee_i = e_i$ ou $ee_i = 0$. Portanto, como

$$e = e \cdot 1 = ee_1 + \cdots + ee_r,$$

vemos que e é a soma de alguns dos e_i's. □

O Teorema 4.1.6 motiva a seguinte definição:

Definição 4.1.7. Seja A uma k-álgebra de dimensão finita e seja

$$A = A_1 \oplus \cdots \oplus A_r$$

a única decomposição de A como soma direta de ideais indecomponíveis. Os ideais $A_1, \ldots, A_r$ são chamados de **blocos** da álgebra A.

Observação 4.1.8. Juntando a Proposição 4.1.4 e o Teorema 4.1.6, concluímos que as unidades $e_1, \ldots, e_r$ dos blocos $A_1, \ldots, A_r$ são os únicos idempotentes centrais primitivos de A. Devido à importância desses idempotentes, algumas referências definem cada e_i como sendo um bloco de A.

Notação 4.1.9. Ao longo desta seção, sempre denotaremos os blocos de A por $A_1, \ldots, A_r$ e os idempotentes associados por $e_1, \ldots, e_r$.

Exemplo 4.1.10. Vamos ilustrar esses últimos conceitos encontrando a decomposição em blocos da subálgebra A de $T_3(k)$ (veja o Exemplo 1.1.11) constituída pelas matrizes da forma

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ d & 0 & c \end{pmatrix}$$

com $a, b, c, d \in k$. Não é difícil verificar que o centro $Z(A)$ é formado pelas matrizes com $a = c$ e $d = 0$. Sabendo disso, concluímos que há apenas dois idempotentes centrais não triviais:

$$e_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad e_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Eles são os idempotentes centrais primitivos de A. Se $A_1 \coloneqq Ae_1$ e $A_2 \coloneqq Ae_2$, então A_1 e A_2 são os blocos de A. Observe que A_1 é dado pelas matrizes da forma anterior com $b = 0$, enquanto A_2 é dado pelas matrizes com $a = c = d = 0$. Isso e mais algumas contas nos permitem concluir que $A_1 \cong T_2(k)$ e $A_2 \cong k$, logo $A \cong A_1 \times A_2 \cong T_2(k) \times k$ e conseguimos decompor A como o produto de álgebras indecomponíveis conhecidas.

Como o nosso objetivo é estudar representações, vamos relacionar A-módulos com módulos sobre os blocos de A. Fixe $1 \leq i \leq r$. Se U é um A_i-módulo, podemos ver U como um A-módulo restringindo escalares através da projeção $A \to A_i$. Nesse caso, temos $A_iU = U$ e $A_jU = 0$ para $j \neq i$. Note que todo A-módulo satisfazendo essas condições vem de um A_i-módulo.

Definição 4.1.11. Um A-módulo U **pertence ao bloco** A_i se[1] $A_iU = U$ e $A_jU = 0$ para $j \neq i$.

Observação 4.1.12. Há uma correspondência natural entre A-módulos pertencentes ao bloco A_i e A_i-módulos, como apontamos acima. Ela preserva diversas propriedades, como a simplicidade e a indecomponibilidade. Essas afirmações não são difíceis de se verificar, mas suas demonstrações podem ser encontradas na solução do Exercício A.4.3.

Temos um critério simples para decidir se U pertence ao bloco A_i utilizando os idempotentes associados:

Lema 4.1.13. Um A-módulo U pertence ao bloco A_i se, e somente se, e_i age trivialmente em U e $e_jU = 0$ para $j \neq i$.

Demonstração: ($\implies$) Se U pertence a A_i, então $A_jU = 0$ e, portanto, $e_jU = 0$ para $j \neq i$. Além disso, se $u \in U = A_iU$, existem $a_1, \ldots, a_n \in A_i$ e $u_1, \ldots, u_n \in U$ tais que

$$u = a_1u_1 + \cdots + a_nu_n.$$

Como e_i é a identidade de A_i, temos

$$e_iu = (e_ia_1)u_1 + \cdots + (e_ia_n)u_n = a_1u_1 + \cdots + a_nu_n = u.$$

Concluímos que e_i age trivialmente em U.

($\impliedby$) Reciprocamente, suponha que e_i aja trivialmente em U e que $e_jU = 0$ se $j \neq i$. Então temos $e_iU = U$ e, portanto, $A_iU = U$. Além disso,

$$A_jU = (Ae_j)U = A(e_jU) = A \cdot 0 = 0$$

se $j \neq i$. Concluímos que U pertence ao bloco A_i. □

A propriedade de um módulo pertencer a um bloco se comporta bem com submódulos, quocientes, somas diretas e extensões:

Lema 4.1.14. Se

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

é uma sequência exata de A-módulos, então V pertence ao bloco A_i se, e somente se, U e W pertencem ao bloco A_i.

[1] Basta pedir uma das condições: veja o Exercício A.4.1. Optamos por escrever assim para ressaltar as duas condições.

Demonstração: ($\Longrightarrow$) Suponha que V pertença ao bloco A_i. Então e_i age trivialmente em V e $e_jV = 0$ se $j \neq i$. Como U é isomorfo a um submódulo de V e W é um quociente de V, então é imediato que e_i também age trivialmente em U e W e que e_j anula U e W para $j \neq i$. Logo, U e W pertencem ao bloco A_i.

($\Longleftarrow$) Reciprocamente, suponha que U e W pertençam a A_i. Por simplicidade, podemos assumir que $U \leq V$ e $W = V/U$. Assim, se $j \neq i$, temos

$$e_jW = 0 \implies e_j \cdot \frac{V}{U} = 0 \implies e_jV \subseteq U$$

e então

$$e_jV = e_j^2V \subseteq e_jU = 0.$$

Por outro lado, como e_i age trivialmente em U e W, temos $(1-e_i)U = 0$ e $(1-e_i)W = 0$. Mas $1-e_i$ é um idempotente, então podemos repetir o argumento acima para concluir que $(1 - e_i)V = 0$, ou seja, e_i age trivialmente em V. Dessa forma, V pertence ao bloco A_i. □

Lembre que, se A é uma álgebra semissimples, podemos estudar um A-módulo U através de suas componentes simples, como vimos logo após a Proposição 1.2.10. Nesse caso, cada componente simples pertence a um bloco de A. Algo análogo pode ser feito para uma álgebra qualquer, como veremos a seguir. Portanto, o estudo de A-módulos pode ser reduzido ao estudo dos módulos sobre os blocos de A.

Proposição 4.1.15. Se U é um A-módulo, então U possui uma única decomposição

$$U = U_1 \oplus \cdots \oplus U_r$$

onde U_i pertence ao bloco A_i para todo $1 \leq i \leq r$.

Demonstração: Defina $U_i \coloneqq A_iU$. Então U_i é um submódulo de U que pertence a A_i, pois

$$A_iU_i = A_i(A_iU) = A_i^2U = A_iU = U_i$$

e, se $j \neq i$,

$$A_jU_i = A_j(A_iU) = (A_jA_i)U = 0.$$

Aqui usamos que

$$A_i^2 = Ae_iAe_i = Ae_i^2 = Ae_i = A_i$$

e que

$$A_jA_i = Ae_jAe_i = Ae_je_i = 0$$

para $j \neq i$. Assim,

$$U = AU = (A_1 + \cdots + A_r)U = A_1U + \cdots + A_rU = U_1 + \cdots + U_r.$$

Além disso, a soma acima é direta. De fato, se $u_1 + \cdots + u_r = 0$, onde $u_i \in U_i$, então podemos multiplicar essa expressão por e_i para obter $u_i = 0$ para cada $1 \leq i \leq r$.

Para mostrar a unicidade da decomposição, suponha que tenhamos outra decomposição

$$U = V_1 \oplus \cdots \oplus V_r,$$

onde cada V_i pertence ao bloco A_i. Dessa forma,

$$V_i = A_iV_i \subseteq A_iU = U_i.$$

Mas U é a soma direta dos V_i's, então a inclusão $V_i \subseteq U_i$ tem de ser necessariamente uma igualdade. □

Uma consequência imediata, mas muito importante, é a seguinte:

Corolário 4.1.16. Se U é um A-módulo indecomponível, então U pertence a um único bloco de A.

Dessa forma, podemos particionar as classes de isomorfismo de A-módulos indecomponíveis agrupando aqueles que pertencem ao mesmo bloco. O mesmo pode ser feito para os módulos simples, já que eles também são indecomponíveis.

Isso nos permite entender melhor os blocos se tivermos algumas informações sobre os A-módulos. Por exemplo, suponha que consigamos escrever

$$_AA = P_1 \oplus \cdots \oplus P_s,$$

onde $P_1, \ldots, P_s$ são módulos (projetivos) indecomponíveis. Seja B um bloco de A e suponha que $P_1, \ldots, P_j$, $j \leq s$, pertençam a B, enquanto $P_{j+1}, \ldots, P_s$ não pertençam. Assim, se $1 \leq i \leq j$, vale $BP_i = P_i$ e, se $j < i \leq s$, temos $BP_i = 0$. Portanto,

$$B = BA = BP_1 \oplus \cdots \oplus BP_s = P_1 \oplus \cdots \oplus P_j$$

e conseguimos encontrar quem é B! Veja que era preciso saber quais dos P_i's pertenciam a um mesmo bloco.

Pelo Lema 4.1.14, um A-módulo U pertence a um bloco A_i se e somente se todos os seus fatores de composição pertencem a esse bloco. Por isso, para determinar um bloco através dos módulos que pertencem a ele, devemos descobrir quando dois módulos *simples* pertencem a um mesmo bloco. O próximo resultado nos dá dois critérios bem interessantes:

Teorema 4.1.17. Se S e T são A-módulos simples, então as seguintes afirmações são equivalentes:

(1) S e T pertencem ao mesmo bloco.

(2) Existe uma sequência de A-módulos simples

$$S = S_1, S_2, \ldots, S_n = T$$

de modo que, para todo $1 \leq i < n$, S_i e S_{i+1} são fatores de composição de um mesmo A-módulo projetivo indecomponível.

(3) Existe uma sequência de A-módulos simples

$$S = S_1, S_2, \ldots, S_n = T$$

de modo que, para todo $1 \leq i < n$, S_i e S_{i+1} são isomorfos ou então existe uma extensão de um deles pelo outro que não cinde.

Durante a demonstração, veremos que uma das implicações é mais complicada que as outras. Será útil um resultado auxiliar:

Lema 4.1.18. Sejam $\mathscr{C}_1$ e $\mathscr{C}_2$ dois conjuntos de A-módulos simples que particionam o conjunto das classes de isomorfismo de módulos simples e tais que, para todos $S \in \mathscr{C}_1$ e $T \in \mathscr{C}_2$, toda extensão de S por T ou de T por S cinde. Então todo A-módulo U pode ser escrito como $U = U_1 \oplus U_2$, onde todo fator de composição de U_1 está representado em $\mathscr{C}_1$ e todo fator de composição de U_2 está representado em $\mathscr{C}_2$. Além disso, U_1 e U_2 são determinados unicamente como os maiores submódulos de U cujos fatores de composição estão todos em $\mathscr{C}_1$ e em $\mathscr{C}_2$, respectivamente.

Demonstração: Vamos encontrar uma série de composição

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = U$$

de modo que, para algum $0 \leq i \leq n$, todos os fatores de composição de V_i estejam em $\mathscr{C}_1$ e todos os fatores de composição de U/V_i estejam em $\mathscr{C}_2$. Começamos com uma série de composição arbitrária, como acima. Se existe $0 < j < n$ tal que V_j/V_{j-1} está em $\mathscr{C}_2$ e V_{j+1}/V_j está em $\mathscr{C}_1$, então a sequência exata

$$0 \longrightarrow V_j/V_{j-1} \longrightarrow V_{j+1}/V_{j-1} \longrightarrow V_{j+1}/V_j \longrightarrow 0$$

cinde por conta da hipótese sobre $\mathscr{C}_1$ e $\mathscr{C}_2$. Ou seja, V_{j+1}/V_{j-1} é a soma direta de V_j/V_{j-1} com V_{j+1}/V_j e conseguimos encontrar uma série de composição de V_{j+1}/V_{j-1} cujo primeiro termo é V_{j+1}/V_j. Dessa forma, conseguimos encontrar um submódulo $V' \leq U$ com

$$V_{j-1} \subseteq V' \subseteq V_{j+1}$$

e

$$\frac{V'}{V_{j-1}} \cong \frac{V_{j+1}}{V_j} \quad \text{e} \quad \frac{V_{j+1}}{V'} \cong \frac{V_j}{V_{j-1}}.$$

Repetindo essa construção quantas vezes for necessário, conseguimos encontrar uma série de composição de U onde todos os fatores de composição de U que estão em $\mathscr{C}_1$ aparecem "à esquerda" de todos os fatores que estão em $\mathscr{C}_2$. Nessa nova série, o índice i para o qual ocorre a transição de $\mathscr{C}_1$ para $\mathscr{C}_2$ nos fornece o módulo V_i que desejávamos. Definimos $U_1 \coloneqq V_i$. Trocando os papéis de $\mathscr{C}_1$ e $\mathscr{C}_2$, o mesmo argumento constrói um submódulo $U_2 \leq U$ tal que todos os fatores de composição de U_2 estão em $\mathscr{C}_2$ e todos os fatores de composição de U/U_2 estão em $\mathscr{C}_1$. Como U_1 e U_2 não possuem fatores de composição em comum, vale $U_1 \cap U_2 = 0$ e então a soma $U_1 + U_2$ é direta. Mas, pela construção, $U_1 \oplus U_2$ tem o mesmo comprimento de U, então $U = U_1 \oplus U_2$, como queríamos.

Para a unicidade, suponha que $U_1' \leq U$ possua todos os seus fatores de composição em $\mathscr{C}_1$. Assim, o mesmo vale para $U_1 + U_1'$. Mas U_1 contém todos os fatores de composição de U que estão em $\mathscr{C}_1$. Por isso, U_1 e $U_1 + U_1'$ possuem o mesmo comprimento e vale $U_1 = U_1 + U_1'$, ou seja, $U_1' \subseteq U_1$. A unicidade de U_2 é provada da mesma forma. □

Agora conseguimos demonstrar o Teorema 4.1.17.

Demonstração: Uma observação inicial importante é que os itens (1), (2) e (3) definem relações de equivalência no conjunto das classes de isomorfismo de A-módulos simples. Assim, devemos mostrar que as três relações são, na verdade, a mesma.

(3) $\implies$ (2). Sejam S e T módulos simples e suponha que exista uma sequência exata

$$0 \longrightarrow S \longrightarrow U \longrightarrow T \longrightarrow 0$$

que não cinde. Assim, U é um A-módulo de comprimento 2 e não pode ser semissimples, já que, caso contrário, a sequência cindiria. Dessa forma, U é unisseriado e devemos ter $\operatorname{rad}(U) \cong S$ e $U/\operatorname{rad}(U) \cong T$. Pelo Lema 2.2.5, U é quociente da cobertura projetiva de T. Como S e T são fatores de composição de U, então eles também são fatores de composição dessa cobertura projetiva. Isso mostra que, se dois módulos simples estão relacionados pela relação em (3), então eles também estão relacionados pela relação em (2).

(2) $\implies$ (1). Sejam S e T módulos simples e suponha que eles sejam fatores de composição de um mesmo módulo projetivo indecomponível P. Pelo Corolário 4.1.16, P pertence a algum bloco e, pelo Lema 4.1.14, todos os seus fatores de composição, incluindo S e T, pertencem a este mesmo bloco. Portanto, se dois módulos simples estão relacionados pela relação em (2), então eles também estão relacionados pela relação em (1).

(1) $\implies$ (3). Sejam S e T módulos simples que pertencem a um mesmo bloco. Escolha um conjunto de representantes das classes de isomorfismo de módulos simples e o particione como $\mathscr{C}_1 \cup \mathscr{C}_2$, onde $\mathscr{C}_1$ consiste dos módulos relacionados com S pela relação em (3) e $\mathscr{C}_2$ consiste dos módulos restantes. Pela definição da relação em (3), $\mathscr{C}_1$ e $\mathscr{C}_2$ satisfazem as hipóteses do Lema 4.1.18, então existe uma decomposição do módulo regular ${}_AA = A_1 \oplus A_2$ onde todo fator de composição de A_1 está em $\mathscr{C}_1$ e todo fator de composição de A_2 está em $\mathscr{C}_2$. Esses submódulos A_1 e A_2 são ideais à esquerda de A. É menos evidente, mas eles também são ideais à direita: se $x \in A$, então a multiplicação à direita por x é um homomorfismo de módulos de ${}_AA$ em ${}_AA$ e leva A_i em A_ix, para $i = 1, 2$. Então A_ix é quociente de A_i e todos os fatores de composição de A_ix estão em $\mathscr{C}_i$ e, pela unicidade do Lema 4.1.18, vale $A_ix \subseteq A_i$ para $i = 1, 2$, provando que A_1 e A_2 são ideais à direita também. Dessa forma, escrevendo A_1 e A_2 como soma de ideais indecomponíveis, encontramos a decomposição de A como soma direta de seus blocos. Como S apenas é fator de composição de A_1, o bloco que contém S e T está contido em A_1 e concluímos que T é isomorfo a algum representante em $\mathscr{C}_1$. Por isso, S e T estão relacionados pela relação em (3). □

Exemplo 4.1.19. Seja k um corpo algebricamente fechado de característica $p = 5$ e considere o grupo diedral $G = D_{15}$. Vimos no Exemplo 2.3.22 que existem três classes de isomorfismo de kD_{15}-módulos simples, representados pelos módulos k, k_{sgn} e U. Se P_k, P_{sgn} e P_U são as respectivas coberturas projetivas, esse exemplo mostra que P_k e P_{sgn} ambos têm k e k_{sgn} como fatores de composição, enquanto P_U apenas possui U como fator de composição. Segue do item (2) do Teorema 4.1.17 que kD_{15} possui exatamente[1] dois blocos: um "contendo" k e k_{sgn} e outro "contendo" U. Pela observação feita logo antes do enunciado do Teorema 4.1.17 e pela estrutura de kD_{15} encontrada no Exemplo 2.3.22, sabemos que um dos blocos é isomorfo como kD_{15}-módulo a $P_k \oplus P_{k_{\text{sgn}}}$, enquanto o outro é isomorfo a $P_U \oplus P_U$.

Exemplo 4.1.20. Seja k um corpo algebricamente fechado de característica $p > 0$ e tome $G = \mathrm{SL}_2(p)$. Com a notação do Exemplo 1.3.17, lembre que $V_1, \ldots, V_p$ são todos os kG-módulos simples. Vamos descobrir quais estão nos mesmos blocos. Começamos com o caso $p = 2$. Pelo Exemplo 2.4.14, a cobertura projetiva P_1 de V_1 apenas possui V_1 como fator de composição, enquanto $P_2 \cong V_2$. Pelo item (2) do Teorema 4.1.17, kG possui exatamente dois blocos: um "contendo" V_1 e outro "contendo" V_2.

Agora, suponha $p > 2$. Vamos mostrar que kG possui três blocos e que a partição induzida nos módulos simples é

$$\{V_1, V_3, \ldots, V_{p-2}\} \cup \{V_2, V_4, \ldots, V_{p-1}\} \cup \{V_p\}.$$

Como V_p é projetivo, vimos no Exemplo 2.4.14 que o único projetivo indecomponível contendo V_p como fator de composição é o próprio V_p. Por isso, pelo Teorema 4.1.17, V_p é o único módulo simples pertencente ao seu bloco. Para encontrar os outros blocos, o ponto fundamental é observar que, pela análise feita no Exemplo 2.4.14, as dimensões dos fatores de composição de um projetivo indecomponível possuem sempre a mesma paridade. Portanto, se $1 \leq i \leq j < p$ e V_i e V_j pertencem ao mesmo bloco, então os índices i e j possuem a mesma paridade. Isso nos dá pelo menos dois blocos a mais, um para cada paridade. Para concluir o que queremos, devemos provar a recíproca: se i e j possem a mesma paridade, então V_i e V_j pertencem ao mesmo bloco.

Quando $p = 3$, isso é imediato, pois V_1 apenas aparece na sua cobertura projetiva e V_2 também só aparece na sua cobertura projetiva. Assim, suporemos $p \geq 5$. Basta mostrar que, se $1 \leq n \leq p-3$, então V_n e V_{n+2} pertencem ao mesmo bloco. De fato, se $1 \leq n \leq p-3$, temos $2 \leq p-1-n \leq p-2$, então o Exemplo 2.4.14 diz que a cobertura projetiva de V_{p-1-n} contém

$$V_{p-1-(p-1-n)} = V_n \quad \text{e} \quad V_{p+1-(p-1-n)} = V_{n+2}$$

[1] Lembre que, para cada bloco, existe um módulo simples que pertence a ele!

como fatores de composição. Logo, pelo item (2) do Teorema 4.1.17, V_n e V_{n+2} pertencem ao mesmo bloco, como desejado.

Terminaremos a seção dando uma justificativa para a escolha da palavra "bloco". Iremos introduzir uma nova definição. Se S e T são A-módulos simples e P_T é a cobertura projetiva de T, denotaremos por c_{ST} a multiplicidade de S como fator de composição de P_T. Esses números são chamados de **invariantes de Cartan** de A e formam a matriz $C = (c_{ST})$, cujas linhas e colunas são indexadas pelas classes de isomorfismo de A-módulos simples. Esta é a **matriz de Cartan** de A. Ela codifica parte da estrutura dos módulos projetivos indecomponíveis.

Já poderíamos ter introduzido a matriz de Cartan no Capítulo 2. Na verdade, alguns dos exercícios desse capítulo já davam propriedades dessa matriz! Se P_S e P_T denotam a cobertura projetiva dos módulos simples S e T, o Exercício A.2.8 mostra que

$$c_{ST} = \frac{\dim_k \operatorname{Hom}_A(P_S, P_T)}{\dim_k \operatorname{End}_A(S)}.$$

Por sua vez, o Exercício A.2.13 mostra que, se $A = kG$ e k é algebricamente fechado, então a matriz de Cartan de kG é simétrica!

Exemplo 4.1.21. Se k é um corpo algebricamente fechado de característica $p = 5$ e se $G = D_{15}$ é o grupo diedral, o Exemplo 2.3.22 mostra que a matriz de Cartan de kD_{15} é

$$\begin{pmatrix} 3 & 2 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix},$$

onde as linhas e as colunas estão indexadas por k, k_{sgn} e U, nesta ordem.

Exemplo 4.1.22. Se k é um corpo algebricamente fechado de característica $p = 7$ e se $G = \mathrm{SL}_2(7)$, então o Exemplo 2.4.14 mostra que a matriz de Cartan de kG é

$$\begin{pmatrix} 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

onde as linhas e as colunas estão indexadas por $V_1, V_3, V_5, V_2, V_4, V_6$ e V_7, nesta ordem.

Nos dois exemplos anteriores, repare que foi possível escrever a matriz de Cartan na forma diagonal por blocos. Para isso, tivemos que indexar as linhas e as colunas agrupando os módulos simples que pertenciam a um mesmo bloco de kG. Mais ainda, cada bloco de kG corresponde a um bloco na matriz de Cartan! Isso vale em geral:

Proposição 4.1.23. Seja A uma k-álgebra de dimensão finita. Se listarmos os A-módulos simples agrupando aqueles que pertencem a um mesmo bloco de A, então a matriz de Cartan de A é diagonal por blocos com um bloco para cada bloco de A. A menos de permutação dos módulos simples dentro de um bloco e de permutação dos blocos entre si, esta é a única decomposição da matriz de Cartan numa forma diagonal por blocos com o número máximo de blocos.

Demonstração: Para a primeira afirmação, basta mostrar que, se S e T são módulos simples que não pertencem ao mesmo bloco de A, então S não é fator de composição da cobertura projetiva P_T de T e temos $c_{ST} = 0$. De fato, como T é fator de composição de P_T, isso é imediato do item (2) do Teorema 4.1.17.

Agora, mostremos a unicidade descrita na segunda afirmação. Decomponha a matriz de Cartan de A em alguma forma diagonal por blocos e denote a matriz obtida por C. Se S e T são módulos simples pertencentes ao mesmo bloco de A, vamos provar que as linhas de C associadas a S e a T devem necessariamente passar por um mesmo bloco da decomposição de C na forma diagonal por blocos. Denote por P_S e por P_T as coberturas projetivas de S e T, respectivamente. Pelo item (2) do Teorema 4.1.17 (ou, mais especificamente, por um refinamento dado pelo Exercício A.4.4), é suficiente mostrar o que queremos quando $\mathrm{Hom}_A(P_S, P_T) \neq 0$. Pelo Exercício A.2.8, $c_{ST} \neq 0$ e então a linha associada a S se encontra com a coluna associada a T num mesmo bloco B da matriz C. Por outro lado, como $c_{TT} \neq 0$, a linha associada a T também se encontra com a coluna associada a T num mesmo bloco B' de C. Mas cada coluna passa por exatamente um bloco, então temos $B = B'$ e concluímos que as linhas associadas a S e T passam pelo mesmo bloco, como queríamos. Isso mostra que o número de blocos na decomposição de C é no máximo o número de blocos de A. Além disso, isso também prova que, se o número de blocos de C é igual ao número de blocos de A, então a decomposição de C é a decomposição obtida na primeira afirmação (a menos das permutações descritas no enunciado). □

4.2 Grupos de defeito

Estudaremos com mais detalhes a teoria dos blocos para a álgebra de grupo kG. O objetivo desta seção é associar a cada bloco um p-subgrupo de G, chamado de *grupo de defeito*. Ele é uma medida da complexidade do bloco. Para defini-lo, utilizaremos alguns resultados do capítulo anterior.

O primeiro passo é observar que podemos enxergar os blocos de kG como submódulos indecomponíveis! Mas cuidado que eles não são indecomponíveis como kG-módulos. Teremos que introduzir uma nova estrutura de módulo. Se $g_1, g_2 \in G$ e $a \in kG$, definimos

$$(g_1, g_2) \cdot a \coloneqq g_1 a g_2^{-1}.$$

Não é difícil verificar que isso dá uma estrutura de $k[G\times G]$-módulo a kG. Além disso, os $k[G\times G]$-submódulos de kG são os subespaços invariantes pela ação de G pelos dois lados, ou seja, são os ideais de kG. Por isso, cada bloco é um $k[G\times G]$-submódulo indecomponível e a decomposição de kG em blocos é a única decomposição de kG como soma de $k[G\times G]$-submódulos indecomponíveis. Note que, como $k[G \times G]$-módulos, os blocos são dois a dois não isomorfos. De fato, através da identificação $G \cong G \times \{1\}$ e da inclusão $G \times \{1\} \subseteq G \times G$, podemos ver um idempotente e associado a um bloco como um elemento de $k[G \times G]$. Nesse caso, e age trivialmente no bloco correspondente mas anula os outros.

Com essa nova estrutura, podemos nos perguntar quais são os vértices de cada bloco. Para isso, será importante considerar o homomorfismo $\delta : G \to G \times G$ dado por $\delta(g) = (g, g)$ para todo $g \in G$.

Proposição 4.2.1. Se B é um bloco de kG, então, visto como $k[G \times G]$-módulo, B possui um vértice da forma $\delta(D)$, onde D é um p-subgrupo de G. O subgrupo D é único a menos de conjugação.

Demonstração: Mostraremos que B é relativamente $\delta(G)$-projetivo. Assim, $\delta(G)$ conterá um vértice de B. Mas todo vértice é um p-subgrupo, então ele será da forma $\delta(D)$ para algum p-subgrupo D de G, como preciso.

Como B é somando direto de kG, basta verificar que kG é relativamente $\delta(G)$-livre como um $k[G \times G]$-módulo. Para mostrar isso, utilizaremos o Corolário 3.1.5. Considere o subespaço X de kG gerado pelo elemento 1. É imediato que kG é a soma direta dos subespaços $(g_1, g_2)X$ com $(g_1, g_2) \in G \times G$, pois a cópia de G em kG é uma base. Note também que, se $g_1, g_2 \in G$, então

$$(g_1, g_2)X = X \iff (g_1, g_2) \cdot 1 \in X \iff g_1 g_2^{-1} \in X \iff g_1 g_2^{-1} = 1 \iff g_1 = g_2,$$

de modo que $\delta(G) = \{(g_1, g_2) \in G \times G \mid (g_1, g_2)X = X\}$. Pelo Corolário 3.1.5, kG é relativamente $\delta(G)$-livre (com respeito a X), como queríamos.

Já garantimos a existência de D. Vamos terminar verificando a unicidade. Suponha que D' seja um conjugado de D em G. Se $g \in G$ é tal que $D' = gDg^{-1}$, então é imediato que $\delta(D') = (g, g)\delta(D)(g, g)^{-1}$ e, portanto, $\delta(D')$ é um vértice de B. Reciprocamente, seja D' um subgrupo de G de modo que $\delta(D')$ seja um vértice de B. Assim, $\delta(D')$ é conjugado a $\delta(D)$ em $G \times G$ e existem $g_1, g_2 \in G$ com $\delta(D') = (g_1, g_2)\delta(D)(g_1, g_2)^{-1}$. Olhando para a primeira coordenada, vemos que $g_1 D g_1^{-1} \subseteq D'$. Mas D e D' possuem a mesma ordem, então concluímos que $D' = g_1 D g_1^{-1}$, ou seja, D' é um conjugado de D. □

Com a notação acima, os p-subgrupos D de G tais que $\delta(D)$ é um vértice de B são chamados de **grupos de defeito** do bloco B. Eles formam uma classe de conjugação de p-subgrupos de G. Dizemos que B possui **defeito** d se a ordem de D é p^d.

Vimos anteriormente que a ideia por trás da definição de vértice é medir o quão longe um módulo está de ser projetivo. O grupo de defeito pode ser pensado de forma semelhante: ele mede o quão longe o bloco B está de ser uma álgebra semissimples. Para justificar essa afirmação, precisamos de um resultado:

Teorema 4.2.2. Se B é um bloco de kG e D é um grupo de defeito de B, então todo kG-módulo indecomponível pertencente a B possui um vértice contido em D.

Demonstração: Veja que podemos tornar B um kG-módulo através da conjugação: se $g \in G$ e $x \in B$, então definimos $g \cdot x = gxg^{-1}$. Se U é um kG-módulo qualquer, vamos utilizar essa nova estrutura em B para encontrar homomorfismos entre U e $B \otimes U$. Como $B \subseteq kG$, podemos definir uma transformação linear $\varphi : B \otimes U \to U$ que leva $x \otimes u$ em xu, para $x \in B$ e $u \in U$. Veja que φ está bem definida pois a função $(x, u) \mapsto xu$ é bilinear. Se $g \in G$, $x \in B$ e $u \in U$, note que

$$\varphi(g \cdot (x \otimes u)) = \varphi((gxg^{-1}) \otimes gu) = (gxg^{-1})(gu) = g(xu) = g \cdot \varphi(x \otimes u),$$

logo, φ é um homomorfismo de kG-módulos. Agora, se e é o idempotente associado ao bloco B, defina a transformação linear $\psi : U \to B \otimes U$ dada por $\psi(u) = e \otimes u$ para $u \in U$. Como e está no centro de kG, isto é um homomorfismo de kG-módulos:

$$\psi(gu) = e \otimes gu = (geg^{-1}) \otimes gu = g \cdot (e \otimes u) = g \cdot \varphi(u)$$

para todos $u \in U$ e $g \in G$. Se U pertence ao bloco B, então e age trivialmente em U e temos

$$\varphi(\psi(u)) = \varphi(e \otimes u) = eu = u$$

para todo $u \in U$. Logo, ψ é um homomorfismo injetor que cinde e então U é um somando direto de $B \otimes U$. Dessa forma, se U é um módulo indecomponível pertencente ao bloco B, então basta provar que $B \otimes U$ é relativamente D-projetivo para mostrar que U possui um vértice contido em D. Finalmente, pelo Exercício A.3.8 (que segue do item (5) do Lema 3.1.10), é suficiente demonstrar que B é relativamente D-projetivo.

Como $G \cong \delta(G)$ através de δ, podemos ver B como um $k[\delta(G)]$-módulo onde $(g, g) \cdot x = gxg^{-1}$ para todo $g \in G$ e $x \in B$. Com essa identificação, mostrar que o kG-módulo B é relativamente D-projetivo é equivalente a mostrar que o $k[\delta(G)]$-módulo B é relativamente $\delta(D)$-projetivo, já que δ leva D em $\delta(D)$. Mas essa estrutura de $k[\delta(G)]$-módulo em B é exatamente a restrição da sua estrutura de $k[G \times G]$-módulo. Como D é um grupo de defeito de B, então o $k[G \times G]$-módulo B é relativamente $\delta(D)$-projetivo e, assim, pela Fórmula de Decomposição de Mackey, a restrição a $k[\delta(G)]$ é relativamente projetiva com relação à coleção de subgrupos da forma

$$\delta(G) \cap (g_1, g_2)\delta(D)(g_1, g_2)^{-1}$$

com $g_1, g_2 \in G$. Como a indução não "percebe" a conjugação (Lema 3.2.11), para mostrar que o $k[\delta(G)]$-módulo B é relativamente $\delta(D)$-projetivo, é suficiente provar que um subgrupo da forma

acima é conjugado em $\delta(G)$ a um subgrupo de $\delta(D)$. De fato, dados $d \in D$ e $g_1, g_2 \in G$, se $(g_1, g_2)\delta(d)(g_1, g_2)^{-1} \in \delta(G)$, então $g_1 d g_1^{-1} = g_2 d g_2^{-1}$ e temos

$$(g_1, g_2)\delta(d)(g_1, g_2)^{-1} = (g_1 d g_1^{-1}, g_2 d g_2^{-1}) = (g_1 d g_1^{-1}, g_1 d g_1^{-1}) = \delta(g_1)\delta(d)\delta(g_1)^{-1}.$$

Portanto, $\delta(G) \cap (g_1, g_2)\delta(D)(g_1, g_2)^{-1}$ está contido em $\delta(g_1)\delta(D)\delta(g_1)^{-1}$, que é conjugado a $\delta(D)$ em $\delta(G)$. □

Corolário 4.2.3. Se um bloco B de kG possui defeito zero, então B é uma álgebra semissimples (e, portanto, simples).

Demonstração: Como B possui defeito zero, seu único grupo de defeito é o grupo trivial. Se U é um kG-módulo indecomponível que pertence a B, então o Teorema 4.2.2 implica que U é relativamente 1-projetivo, ou seja, é projetivo. Quando vemos U como um B-módulo, U continua sendo projetivo (veja o Exercício A.4.3). Como todo B-módulo indecomponível vem de um kG-módulo indecomponível pertencente a B, segue que todo B-módulo indecomponível é projetivo e, consequentemente, qualquer B-módulo é projetivo. Pelo Exercício A.2.4, B é uma álgebra semissimples. Por fim, como B é uma álgebra indecomponível, segue do Teorema de Wedderburn que B é isomorfo a uma álgebra de matrizes sobre uma álgebra de divisão, que é simples. □

Observação 4.2.4. Para de fato poder dizer que o grupo de defeito mede o quão longe o bloco está de ser uma álgebra semissimples, o ideal seria ter também a recíproca do corolário acima. Ela de fato vale e a sua demonstração se encontra na próxima seção (Corolário 4.3.7).

Exemplo 4.2.5. O **bloco principal** de kG é o bloco ao qual pertence o kG-módulo trivial. Em geral, ele é considerado o bloco mais importante de kG. Como os vértices do módulo trivial são os p-subgrupos de Sylow de G (Exemplo 3.2.14), concluímos do Teorema 4.2.2 que os grupos de defeito do bloco principal também são os p-subgrupos de Sylow. Assim, o bloco principal possui defeito máximo!

Exemplo 4.2.6. Tome k algebricamente fechado de característica $p > 0$ e $G = \mathrm{SL}_2(p)$. Se $p > 2$, vimos nos Exemplo 4.1.20 que kG possui três blocos: o principal, um "contendo" o módulo simples V_2 de dimensão 2 e outro "contendo" o único módulo simples projetivo. Sabemos que os grupos de defeito do bloco principal são os p-subgrupos de Sylow de G. Como V_2 não é projetivo, seu vértice não é trivial e, pelo Teorema 4.2.2, o defeito do seu bloco é positivo. Como os p-subgrupos de Sylow têm ordem p, eles também são os grupos de defeito do bloco associado a V_2. Por fim, segue do Corolário 4.3.7 (que provaremos na próxima seção) que o defeito do bloco associado ao módulo simples projetivo é zero.

Pelo Exercício A.3.11, todo p-subgrupo de G é um vértice de algum kG-módulo indecomponível. Porém, não é verdade que todo p-subgrupo de G é um grupo de defeito de algum bloco de kG. Por exemplo, se G é um p-grupo, então o único kG-módulo simples é o trivial e, portanto, kG possui apenas o bloco principal e seu grupo de defeito é G. Como veremos agora, um grupo de defeito possui algumas propriedades especiais. Precisaremos relembrar uma definição de teoria dos grupos: se D é um subgrupo de G, então o subgrupo

$$C_G(D) \coloneqq \{g \in G \mid gd = dg \text{ para todo } d \in D\}$$

é o **centralizador** de D em G.

Teorema 4.2.7. Seja D um grupo de defeito de um bloco B de kG. Se P é um p-subgrupo de Sylow de G que contém D, então $D = P \cap cPc^{-1}$ para algum $c \in C_G(D)$.

Para provar este teorema, é necessário entender como se comporta a restrição do $k[G \times G]$-módulo kG a $P \times P$. Portanto, iremos demonstrar primeiramente um lema, que também nos ajudará no futuro.

Lema 4.2.8. Sejam H um subgrupo de G e $t \in G$.

(1) O $k[H \times H]$-submódulo $kHtH$ de kG é induzido do módulo trivial do subgrupo

$$(1,t)^{-1}\delta(H \cap tHt^{-1})(1,t).$$

(2) Se H é um p-subgrupo de G, então $kHtH$ é um $k[H \times H]$-módulo indecomponível e possui

$$(1,t)^{-1}\delta(H \cap tHt^{-1})(1,t)$$

como vértice.

(3) Se Q é um p-subgrupo de H, se $C_G(Q) \subseteq H$ e se $t \notin H$, então nenhum somando indecomponível de $kHtH$ possui um vértice contendo $\delta(Q)$.

Aqui, $kHtH$ denota o subespaço de kG gerado pelos elementos da classe lateral dupla HtH. É fácil ver que esse espaço é invariante pela ação de $H \times H$ e, portanto, $kHtH$ é de fato um $k[H \times H]$-submódulo de kG.

Demonstração: Para provar (1), utilizaremos o Corolário 3.1.5. Seja X o subespaço de $kHtH$ gerado pelo elemento t. É imediato que $kHtH$ é a soma direta dos subespaços $(h_1, h_2)X$ com $(h_1, h_2) \in H \times H$. Vamos encontrar qual é o estabilizador de X. Veja que $(h_1, h_2)X = X$ se e somente se $h_1 t h_2^{-1} \in X$. Mas o único elemento de G em X é t, então (h_1, h_2) fixa X exatamente quando (h_1, h_2) fixa t. Se $h_1 t h_2^{-1} = t$, então $h_2 = t^{-1}h_1 t$, e vice-versa. Assim, o estabilizador de X é formado pelos elementos da forma $(h, t^{-1}ht)$ com $h \in H$ e $t^{-1}ht \in H$, ou seja, com $h \in H \cap tHt^{-1}$. Mas veja que

$$(h, t^{-1}ht) = (1,t)^{-1}(h,h)(1,t),$$

então o estabilizador em questão é o subgrupo

$$(1,t)^{-1}\delta(H \cap tHt^{-1})(1,t).$$

Por isso, X é um módulo para o subgrupo em destaque acima e, pelo que observamos, é o módulo trivial. Pelo Corolário 3.1.5, $kHtH \cong X^{H \times H}$, como queríamos.

Agora, suponha que H seja um p-subgrupo de G. Como $kHtH$ é induzido do módulo trivial do subgrupo $Q = (1,t)^{-1}\delta(H \cap tHt^{-1})(1,t)$, o Corolário 3.2.17 mostra que $kHtH$ é indecomponível. Mas sabemos do Exemplo 3.2.14 que o vértice do kQ-módulo trivial é Q, então o item (a) do Exercício A.3.11 mostra que o vértice de $kHtH$ também é Q. Isso prova o item (2).

Provaremos o item (3) por absurdo. Suponha que $kHtH$ possua um somando indecomponível com um vértice R contendo $\delta(Q)$. Pelo item (1), $kHtH$ é relativamente projetivo com relação ao subgrupo $(1,t)^{-1}\delta(H \cap tHt^{-1})(1,t)$, então algum conjugado de R em $H \times H$ está contido nesse subgrupo. Em particular, existem $h_1, h_2 \in H$ tais que

$$(h_1, h_2)\delta(Q)(h_1, h_2)^{-1} \subseteq (1,t)^{-1}\delta(G)(1,t),$$

ou seja,

$$(1,t)(h_1, h_2)\delta(Q)(h_1, h_2)^{-1}(1,t)^{-1} \subseteq \delta(G).$$

Logo, se $x \in Q$, então

$$h_1 x h_1^{-1} = t h_2 x h_2^{-1} t^{-1} \implies x(h_1^{-1}th_2) = (h_1^{-1}th_2)x.$$

Segue que $h_1^{-1}th_2 \in C_G(Q)$. Mas $C_G(Q) \subseteq H$ e $h_1, h_2 \in H$, então $t \in H$, contradizendo uma das hipóteses. □

Com isso, podemos provar o Teorema 4.2.7.

Demonstração: Vendo B como um $k[G \times G]$-módulo, sabemos que $\delta(D)$ é um vértice de B. Como $\delta(D) \subseteq P \times P$, o Lema 3.2.18 garante a existência de um somando indecomponível de $B_{P\times P}$ que possui $\delta(D)$ como vértice. Por outro lado, B é somando direto do $k[G \times G]$-módulo kG. Mas

$$(kG)_{P\times P} = \bigoplus_{t\in[P\backslash G/P]} kPtP,$$

pois as classes laterais duplas particionam G, que forma uma base de kG. Como P é um p-subgrupo de G, o Lema 4.2.8 diz que cada somando $kPtP$ acima é indecomponível e possui $(1,t)^{-1}\delta(P \cap tPt^{-1})(1,t)$ como vértice. Disso tudo concluímos que existe $t \in G$ tal que $\delta(D)$ é conjugado em $P \times P$ a $(1,t)^{-1}\delta(P \cap tPt^{-1})(1,t)$. Logo, existem $r, s \in P$ tais que

$$\delta(D) = (r,s)(1,t)^{-1}\delta(P \cap tPt^{-1})(1,t)(r,s)^{-1}.$$

Isso implica que

$$|D| = |\delta(D)| = \left|\delta(P \cap tPt^{-1})\right| = \left|P \cap tPt^{-1}\right|$$

e que

$$(1,t)(r,s)^{-1}\delta(D)(r,s)(1,t)^{-1} \subseteq \delta(G).$$

Dessa última inclusão, obtemos que, para todo $d \in D$,

$$r^{-1}dr = ts^{-1}dst^{-1} \implies d(rts^{-1}) = (rts^{-1})d,$$

ou seja, $rts^{-1} \in C_G(D)$. Se $c \coloneqq rts^{-1}$, mostremos que $D = P \cap cPc^{-1}$. Como $D \subseteq P$ e $c \in C_G(D) \subseteq N_G(D)$, temos $D = cDc^{-1} \subseteq cPc^{-1}$ e então $D \subseteq P \cap cPc^{-1}$. Resta mostrar que esses dois subgrupos possuem o mesmo tamanho. De fato, utilizando que $r, s \in P$, obtemos

$$\begin{aligned}
\left|P \cap cPc^{-1}\right| &= \left|P \cap rts^{-1}Pst^{-1}r^{-1}\right| \\
&= \left|P \cap rtPt^{-1}r^{-1}\right| \\
&= \left|r^{-1}Pr \cap tPt^{-1}\right| \\
&= \left|P \cap tPt^{-1}\right| \\
&= |D|,
\end{aligned}$$

como preciso. □

Corolário 4.2.9. Se D é um grupo de defeito de um bloco de kG, então

$$D \supseteq O_p(G) \quad \text{e} \quad D = O_p(N_G(D)).$$

No enunciado acima, $O_p(G)$ denota o maior p-subgrupo normal de G, como definimos na Proposição 1.3.14.

Demonstração: Seja P um p-subgrupo de Sylow de G que contém D. Pelo Teorema 4.2.7, existe $c \in C_G(D)$ com $D = P \cap cPc^{-1}$. Como $O_p(G)$ é um p-subgrupo de G, ele está contido em algum p-subgrupo de Sylow de G. Mas $O_p(G)$ é normal em G e todos os p-subgrupos de Sylow são conjugados. Em particular[1], $O_p(G) \subseteq P$ e $O_p(G) \subseteq cPc^{-1}$, ou seja, $O_p(G) \subseteq D$.

Agora, seja Q um p-subgrupo de Sylow de $N_G(D)$ contendo D e, dessa vez, tome P como sendo um p-subgrupo de Sylow de G contendo Q. Seja $c \in C_G(D)$ como antes. Como D é p-subgrupo normal em $N_G(D)$, vale $D \subseteq O_p(N_G(D))$. Agora, como $c \in C_G(D) \subseteq N_G(D)$, temos $D = cDc^{-1} \subseteq cQc^{-1}$ e então

$$D \subseteq Q \cap cQc^{-1} \subseteq P \cap cPc^{-1} = D.$$

Logo, $D = Q \cap cQc^{-1}$ é a interseção de dois p-subgrupos de Sylow de $N_G(D)$. Imitando o argumento do parágrafo anterior, segue que $O_p(N_G(D)) \subseteq D$. Concluímos então que $D = O_p(N_G(D))$. □

[1] Na verdade, $O_p(G)$ é a interseção dos p-subgrupos de Sylow de G! De fato, isso mostra que $O_p(G)$ está contido nessa interseção. Por outro lado, essa interseção é um p-subgrupo normal de G, já que é a interseção de uma classe de conjugação de subgrupos de G.

4.3 A Correspondência de Brauer

Quando estudamos a Correspondência de Green, ficou evidente a importância dos subgrupos locais de G para a teoria de representações de G. Conseguimos obter certas informações através das representações desses subgrupos. O que veremos nesta seção é parecido, mas desta vez lidaremos com blocos ao invés de kG-módulos, introduzindo a Correspondência de Brauer! É importante mencionar que Brauer descobriu essa correspondência antes do estudo de vértices e fontes iniciado por Green. Inclusive, os métodos de Brauer eram diferentes dos que utilizaremos aqui, até mesmo a sua definição de grupo de defeito era outra! Consulte [7] e [22] para conhecer um pouco dessa outra abordagem.

Seja H um subgrupo de G. Relacionaremos os blocos de kH com os blocos de kG de uma maneira bem simples. Se b é um bloco de kH e B é um bloco de kG, então dizemos que B **corresponde a** b se b é um somando direto de $B_{H\times H}$ (onde estamos vendo b como $k[H\times H]$-módulo e B como $k[G\times G]$-módulo) e se B é o único bloco de kG com essa propriedade. Nessas condições, escreveremos $B = b^G$, mas cuidado que isso não é indução! A notação apenas passa a ideia de que estamos "subindo" de H para G. Quando o bloco b possui um correspondente em kG, dizemos que b^G **está definido**. Assim, temos um mapa que parte de algum subconjunto dos blocos de kH e chega no conjunto dos blocos de kG.

O próximo resultado agrupa algumas propriedades básicas dessa correspondência. O item de mais importância é o último, porque nos dá uma condição para garantir que b^G está definido.

Lema 4.3.1. Seja b um bloco de kH, onde $H \leq G$, e seja D um grupo de defeito de b.

(1) Se b^G está definido, então D está contido em algum grupo de defeito de b^G.

(2) Suponha que H esteja contido em um subgrupo K de G. Se os blocos b^K e b^G estão definidos, então $(b^K)^G$ também está definido e vale $(b^K)^G = b^G$.

(3) Se $C_G(D) \subseteq H$, então b^G está definido.

Demonstração: Para (1), seja E um grupo de defeito de $B := b^G$. Como os conjugados de um grupo de defeito ainda são grupos de defeito, basta mostrar que D é conjugado a um subgrupo de E. Vendo B como $k[G\times G]$-módulo, sabemos que B é relativamente $\delta(E)$-projetivo, então segue da Fórmula de Decomposição de Mackey que $B_{H\times H}$ é relativamente projetivo com relação à família de subgrupos da forma

$$(H\times H)\cap (g_1,g_2)\delta(E)(g_1,g_2)^{-1}$$

com $g_1, g_2 \in G$. Como $b \mid B_{H\times H}$ e b é um $k[H\times H]$-módulo indecomponível, obtemos que b é relativamente projetivo com relação a algum subgrupo da forma acima e, como $\delta(D)$ é um vértice de b, concluímos que algum conjugado de $\delta(D)$ em $G\times G$ está contido em $\delta(E)$. Disso segue que algum conjugado de D em G está contido em E, como preciso.

Antes de trabalhar com (2), provemos (3). Suponha que $C_G(D) \subseteq H$. Vamos mostrar que b aparece como somando direto de $(kG)_{H\times H}$ apenas uma vez, onde estamos vendo kG como um $k[G\times G]$-módulo. Isso mostrará que existe exatamente um bloco B de kG com $b \mid B_{H\times H}$, como queremos. Como as classes laterais duplas de H em G particionam G, temos a decomposição

$$(kG)_{H\times H} = \bigoplus_{t\in[H\backslash G/H]} kHtH.$$

Note que kH é um dos somandos que aparece acima. Como os blocos de kH são dois a dois não isomorfos como $k[H\times H]$-módulos, sabemos que b aparece exatamente uma vez como somando direto de kH. Assim, devemos provar que b não é somando direto de $kHtH$ se $t \notin H$. Como b possui $\delta(D)$ como vértice, isso segue do item (3) do Lema 4.2.8.

Por fim, vamos para a propriedade (2). Se b^K está definido, então temos $b \mid (b^K)_{H\times H}$. Logo, se B é um bloco de kG satisfazendo $b^K \mid B_{K\times K}$, segue que $b \mid B_{H\times H}$. Mas, como b^G está definido, b é somando direto apenas da restrição a $H \times H$ do bloco b^G de kG. Por isso, concluímos que $B = b^G$. Ou seja, se existir um bloco B de kG satisfazendo $b^K \mid B_{K\times K}$, então $B = b^G$, mostrando que $(b^K)^G$ está definido e $(b^K)^G = b^G$. A existência de B pode ser garantida como no parágrafo anterior, utilizando-se que kK é um somando direto de $(kG)_{K\times K}$. □

Observação 4.3.2. O argumento dado na demonstração do item (3) nos mostra que, se b é um bloco de kH, então existe um bloco B de kG tal que $b \mid B_{H\times H}$, mas precisamos de mais hipóteses para garantir a unicidade de B. De qualquer forma, essa é uma informação útil e foi usada, por exemplo, na demonstração do item (2).

Observe também que podemos generalizar ligeiramente o item (2): se C é um bloco de kK com $b \mid C_{K\times K}$ e se b^G está definido, então C^G está definido e vale $C^G = b^G$. O ponto interessante de deixar o enunciado como ele está é que fica destacada a "transitividade" da correspondência que estamos estudando.

A Correspondência de Brauer é exatamente essa correspondência entre b e b^G mas num caso particular e bem comportado. Ela pode ser motivada pela seguinte pergunta: como é a Correspondência de Green para blocos? Se B é um bloco de kG, então B é um $k[G \times G]$-módulo indecomponível e de vértice $\delta(D)$, onde D é um grupo de defeito. Note que o normalizador de $\delta(D)$ em $G \times G$ está contido em $N_G(D) \times N_G(D)$, já que cada coordenada desse normalizador precisa normalizar D. Nesse sentido, podemos aplicar a Correspondência de Green e encontrar o $k[N_G(D) \times N_G(D)]$-módulo correspondente.

Teorema 4.3.3 (Primeiro Teorema Principal de Brauer)**.** Seja D um p-subgrupo de G e seja H um subgrupo de G contendo $N_G(D)$. Então existe uma correspondência biunívoca entre os blocos de kH com grupo de defeito D e os blocos de kG com esse mesmo grupo de defeito. A correspondência leva um bloco b de kH no bloco b^G de kG.

Demonstração: Como $C_G(D) \subseteq N_G(D) \subseteq H$, então o item (3) do Lema 4.3.1 nos diz que b^G está definido para todo bloco b de kH com grupo de defeito D. Logo, a função indicada no enunciado faz sentido. Agora, como comentamos antes de enunciar o teorema, o normalizador de $\delta(D)$ em $G\times G$ está contido em $N_G(D)\times N_G(D) \subseteq H \times H$ e podemos aplicar a Correspondência de Green para o vértice $\delta(D)$. Mostraremos que a função do enunciado é uma restrição da correspondência entre $k[G \times G]$-módulos e $k[H \times H]$-módulos indecomponíveis de vértice $\delta(D)$.

Seja b um bloco de kH com grupo de defeito D e denote $B = b^G$. Como $b \mid B_{H\times H}$, segue do Teorema de Burry-Carlson-Puig que B também possui vértice $\delta(D)$ e B é o correspondente de Green de b. Dessa forma, B é um bloco de kG com grupo de defeito D. Além disso, a função $b \mapsto b^G$, definida sobre o conjunto de blocos de kH com grupo de defeito D, é uma restrição da Correspondência de Green e, em particular, é injetora.

Resta mostrar que a correspondência em questão é sobrejetora. Seja B um bloco de kG com grupo de defeito D. Pelo Lema 3.2.18, existe um somando indecomponível de $B_{H\times H}$ de vértice $\delta(D)$. Agora, sabemos que $B \mid kG$, então $B_{H\times H} \mid (kG)_{H\times H}$. Mas

$$(kG)_{H\times H} = \bigoplus_{t\in[H\backslash G/H]} kHtH$$

e, se $t \notin H$, então $kHtH$ não pode conter um somando indecomponível de vértice $\delta(D)$ pelo Lema 4.2.8. Logo, o somando indecomponível de $B_{H\times H}$ com vértice $\delta(D)$ é um somando de kH, isto é, um bloco de kH! Assim, encontramos um bloco b de kH com grupo de defeito D satisfazendo $b \mid B_{H\times H}$ e temos $B = b^G$. Isso termina a prova do teorema. □

A correspondência acima é a **Correspondência de Brauer**. Nesse contexto, dizemos que b e b^G são um o **correspondente de Brauer** do outro.

E o que acontece com os módulos pertencentes aos blocos de kG quando passamos pela correspondência? Quando estamos em condições de aplicar a Correspondência de Green, o Segundo Teorema Principal de Brauer nos diz que essas duas correspondências são compatíveis! Ressaltamos que a versão do teorema a seguir é devida ao matemático Hirosi Nagao e possui um enunciado bem diferente da versão original provada por Brauer.

Teorema 4.3.4 (Segundo Teorema Principal de Brauer)**.** Seja U um kG-módulo indecomponível pertencente ao bloco B de kG. Dado $H \leq G$, seja V um kH-módulo indecomponível pertencente ao bloco b de kH e com um vértice Q satisfazendo $C_G(Q) \subseteq H$. Se $V \mid U_H$, então b^G está definido e $b^G = B$.

Demonstração: Pelo Teorema 4.2.2, existe um grupo de defeito D de b que contém o vértice Q de V. Dessa forma, $C_G(D) \subseteq C_G(Q) \subseteq H$ e, pelo Lema 4.3.1, b^G está definido. Para mostrar que $b^G = B$, argumentaremos por contradição. Assim, suponha por absurdo que $b^G \neq B$.

Denote por e a identidade do bloco b. Decomponha $kG = kH \oplus M$, onde M é a soma dos espaços $kHtH$ para $t \notin H$. Multiplicando por e, obtemos uma decomposição em soma direta de subespaços:

$$ekG = ekH \oplus eM = b \oplus eM.$$

Como kG, kH e M são $k[H \times H]$-módulos e e comuta com todos os elementos de kH, a expressão acima é uma decomposição de ekG como soma direta de $k[H \times H]$-submódulos. Agora, temos $B \mid kG$ como $k[G \times G]$-módulos e, com o mesmo argumento, temos

$$eB \mid ekG = b \oplus eM$$

como $k[H \times H]$-módulos. Mas b é um $k[H \times H]$-módulo indecomponível e estamos supondo que b não é um somando direto de $B_{H\times H}$. Dessa forma, como $eB \mid B_{H\times H}$ (veja a Proposição 4.1.15), então b não pode ser somando direto de eB e segue que $eB \mid eM$. Por sua vez, temos $eM \mid M$ e então obtemos $eB \mid M$. Pelo Lema 4.2.8, concluímos que nenhum somando indecomponível do $k[H \times H]$-módulo eB possui um vértice contendo $\delta(Q)$.

Pela Fórmula de Decomposição de Mackey, $(eB)_{\delta(H)}$ é relativamente projetivo com relação à família de subgrupos consistindo da interseção de $\delta(H)$ com um conjugado de um vértice de um somando indecomponível de eB. Como nenhum vértice de um somando indecomponível de eB contém $\delta(Q)$, concluímos que a restrição $(eB)_{\delta(H)}$ também não possui um somando indecomponível com vértice contendo $\delta(Q)$. Utilizando o isomorfismo $H \cong \delta(H)$, podemos reescrever essa propriedade da seguinte forma: vendo eB como um kH-módulo onde os elementos de H agem por conjugação (isto é, $h \cdot x = hxh^{-1}$ para $h \in H$ e $x \in eB$), então eB não possui um somando indecomponível com vértice contendo Q. Vamos mostrar que o mesmo vale para o kH-módulo $eB \otimes eU$. De fato, se X é um somando indecomponível de eB e possui vértice R, então $X \otimes eU$ é somando direto de $eB \otimes eU$ e é relativamente R-projetivo pelo Exercício A.3.8. Variando X sobre todos os somandos indecomponíveis de eB, obtemos que $eB \otimes eU$ é a soma direta desses módulos $X \otimes eU$ e então é relativamente projetivo com relação à família desses vértices R. Mas nenhum R contém Q, então nenhum somando indecomponível de $eB \otimes eU$ pode possuir vértice contendo Q, como afirmamos.

Como V pertence a b e $V \mid U_H$, temos $V = eV \mid eU$. Agora, iremos mostrar que eU é somando direto de $eB \otimes eU$. Isso concluirá a demonstração, pois implicará que V é um somando indecomponível de $eB \otimes eU$ com vértice Q, contradizendo o que demonstramos acima. Para provar o que resta, procederemos de modo análogo ao início da demonstração do Teorema 4.2.2.

Como $eB \subseteq kG$ e U é um kG-módulo, podemos construir uma transformação linear $\varphi : eB \otimes eU \to eU$ que leva $x \otimes w$ em xw, para $x \in eB$ e $w \in eU$. Veja que φ está bem definida porque $xw \in eU$ (já que $x \in eB$) e porque a função $(x, w) \mapsto xw$ é bilinear. Da mesma forma que mostramos no Teorema 4.2.2, podemos demonstrar que φ é homomorfismo de kH-módulos. Por outro lado, se E é a unidade de B, podemos definir a transformação linear $\psi : eU \to eB \otimes eU$

dada por $\psi(w) = eE \otimes w$ para $w \in eU$. Como e e E comutam com todos os elementos de kH, o mesmo argumento dado no Teorema 4.2.2 mostra que ψ é um homomorfismo de kH-módulos. Por fim, se $w \in eU$, então temos $ew = w$ e, como U pertence a B, também temos $Ew = w$. Por isso,

$$\varphi(\psi(w)) = \phi(eE \otimes w) = eEw = ew = w$$

para todo $w \in eU$, provando que ψ é um homomorfismo injetor que cinde. Logo, eU é somando direto de $eB \otimes eU$, como desejado. □

O Segundo Teorema Principal de Brauer já nos fornece diversos corolários importantes. O primeiro deles clarifica a relação com a Correspondência de Green que havíamos mencionado anteriormente.

Corolário 4.3.5. Sejam Q um p-subgrupo de G e H um subgrupo de G contendo $N_G(Q)$. Seja também U um kG-módulo indecomponível de vértice Q e tome V como sendo o kH-módulo correspondente na Correspondência de Green. Se U pertence ao bloco B de kG e se V pertence ao bloco b de kH, então b^G está definido e $B = b^G$.

Demonstração: Como H contém o normalizador de Q, em particular, H contém o centralizador de Q. Além disso, pela definição da Correspondência de Green, $V \mid U_H$. Dessa forma, o corolário segue diretamente do Segundo Teorema Principal de Brauer. □

O próximo resultado complementa o Teorema 4.2.2 e nos dá uma caracterização interessante: um grupo de defeito de um bloco B de kG é exatamente um vértice de cardinalidade máxima dentre todos os vértices de kG-módulos indecomponíveis pertencentes a B!

Corolário 4.3.6. Se B é um bloco de kG com grupo de defeito D, então existe um kG-módulo indecomponível pertencente a B com vértice D.

Demonstração: Seja b o bloco de $kN_G(D)$ correspondente a B. Seja S um $kN_G(D)$-módulo simples pertencente a b. Como D é um p-subgrupo normal de $N_G(D)$ e como S é simples, sabemos que D age trivialmente em S pela Proposição 1.3.14. Dessa forma, podemos utilizar a projeção $N_G(D) \to N_G(D)/D$ (que nos dá uma projeção $kN_G(D) \to k[N_G(D)/D]$) para considerar S como um $k[N_G(D)/D]$-módulo. Note que S ainda é simples como um $k[N_G(D)/D]$-módulo, pois essa passagem de $N_G(D)$ para o quociente preserva submódulos. Assim, seja V o $k[N_G(D)/D]$-módulo que é a cobertura projetiva do $k[N_G(D)/D]$-módulo S. Como V é projetivo e indecomponível, V é somando direto do módulo regular $k[N_G(D)/D]$. Restringindo escalares através da projeção anterior, podemos ver V e $k[N_G(D)/D]$ como $kN_G(D)$-módulos. Observe que V ainda é indecomponível porque submódulos são preservados. Pelo Exemplo 3.1.8, $k[N_G(D)/D] \cong (k_D)^{N_G(D)}$ como $kN_G(D)$-módulos, onde k denota o kG-módulo trivial. Por isso, V é relativamente D-projetivo. Além disso, como D é normal em $N_G(D)$, o Exemplo 3.1.14 nos dá

$$((k_D)^{N_G(D)})_D \cong \bigoplus_{g \in [N_G(D)/D]} {}^g(k_D) \cong \bigoplus_{g \in [N_G(D)/D]} k_D,$$

logo, V_D é a soma de kD-módulos triviais. Pelo Lema 3.2.18, V_D possui um somando indecomponível com o mesmo vértice de V, mas o único vértice de k_D é o próprio D. Por isso, V possui D como vértice. Assim, podemos aplicar a Correspondência de Green para obter um kG-módulo indecomponível U de vértice D que corresponde a V. Agora, como S pertence a b e é fator de composição do $kN_G(D)$-módulo indecomponível V, então V também pertence a b. Por fim, pelo Corolário 4.3.5, U pertence a B e a demonstração está concluída. □

Finalmente, podemos explicar por que o grupo de defeito mede o quão longe um bloco está de ser uma álgebra semissimples! Vamos complementar o Corolário 4.2.3:

Corolário 4.3.7. Se B é um bloco de kG, então as seguintes afirmações são equivalentes:

(1) B possui defeito zero.

(2) B é um álgebra semissimples (e, portanto, simples).

(3) Existe um kG-módulo simples e projetivo que pertence a B.

Demonstração: (1) $\implies$ (2). Provamos essa implicação no Corolário 4.2.3.

(2) $\implies$ (3). Como B é semissimples, todo B-módulo é projetivo pelo Exercício A.2.4. Em particular, existe um B-módulo simples e projetivo. Utilizando o Exercício A.4.3, podemos enxergar esse B-módulo como um kG-módulo simples e projetivo que pertence a B.

(3) $\implies$ (1). Seja S um kG-módulo simples e projetivo que pertence a B. Vamos mostrar que S é o único kG-módulo indecomponível pertencente a B a menos de isomorfismo. De fato, se S é um fator de composição de um kG-módulo indecomponível U, então o Corolário 2.3.15 nos diz que $S \mid U$ e então $S \cong U$. Pela caracterização (2) do Teorema 4.1.17, concluímos que S é o único (a menos de isomorfismo) kG-módulo simples que pertence a B. Mas então qualquer kG-módulo indecomponível pertencente a B possui apenas S como fator de composição e, pelo que acabamos de ver, é isomorfo a S, como queríamos. Agora, pelo Corolário 4.3.6, existe um kG-módulo indecomponível pertencente a B cujos vértices são os grupos de defeito de B. Esse módulo indecomponível é necessariamente isomorfo a S e, como S é projetivo, seu único vértice é o grupo trivial. Concluímos que B possui grupo de defeito trivial, ou seja, B possui defeito zero. □

Observação 4.3.8. Como demonstramos acima, um bloco de defeito zero possui apenas uma única classe de isomorfismo de módulos simples. A recíproca desta propriedade não vale. Por exemplo, se P é um p-grupo não trivial, então kP é um bloco e possui um único módulo simples, porém seu grupo de defeito é P, que não é trivial. Pelo Exemplo 4.1.20, $\mathrm{SL}_2(2)$ e $\mathrm{SL}_2(3)$ (em característica 2 e 3, respectivamente) também nos dão exemplos de blocos de defeito positivo que possuem apenas um único módulo simples.

Como último corolário, demonstraremos uma versão mais fraca do Terceiro Teorema Principal de Brauer. O enunciado e a prova da versão "verdadeira" serão dados na Seção 4.5.

Corolário 4.3.9. Seja H um subgrupo de G e seja b um bloco de kH com grupo de defeito D. Se $N_G(D) \subseteq H$, então

$$b \text{ é o bloco principal de } kH \iff b^G \text{ é o bloco principal de } kG.$$

Demonstração: Como $C_G(D) \subseteq H$, sabemos que b^G está definido. A ideia da demonstração é notar que, se D é um p-subgrupo de Sylow de G, então k e k_H são correspondentes de Green (sendo k o kG-módulo trivial) e, assim, podemos aplicar o Corolário 4.3.5.

($\implies$) Suponha que b seja o bloco principal de kH. Como D é grupo de defeito de b, sabemos que D é um p-subgrupo de Sylow de H. Por isso, D é um vértice do kH-módulo trivial k_H e, como $N_G(D) \subseteq H$, o Teorema de Burry-Carlson-Puig nos diz que o kG-módulo trivial k é o correspondente de Green de k_H. Pelo Corolário 4.3.5, k pertence ao bloco b^G e, portanto, b^G é o bloco principal de kG.

($\impliedby$) Suponha que b^G seja o bloco principal de kG. Como $N_G(D) \subseteq H$, estamos nas condições da Correspondência de Brauer e podemos concluir que D também é grupo de defeito de b^G. Logo, D é um p-subgrupo de Sylow de G e então é um vértice do kG-módulo trivial k. Como o kH-módulo trivial k_H é o único somando indecomponível da restrição de k a H, sabemos que k_H é o correspondente de Green de k. Se b_0 é o bloco principal de kH, segue do Corolário 4.3.5 que $b_0^G = b^G$. Mas D é p-subgrupo de Sylow de H, então D também é grupo de defeito de b_0 e, voltando pela Correspondência de Brauer, concluímos que $b = b_0$, como queríamos. □

Observação 4.3.10. Na primeira parte da demonstração, vimos que D é p-subgrupo de Sylow de H. Se D não fosse p-subgrupo de Sylow de G, poderíamos encontrar um p-subgrupo D' de G com $D \subsetneq D'$ e D normal em D'. Dessa forma, teríamos $D' \not\subseteq H$ mas $D' \subseteq N_G(D)$, de onde obteríamos $N_G(D) \not\subseteq H$, uma contradição. Por isso, D também é p-subgrupo de Sylow de G e podemos proceder como em ($\Longleftarrow$) para mostrar que k é o correspondente de Green de k_H. Isso dá uma demonstração alternativa que utiliza mais teoria de grupos em troca do Teorema de Burry-Carlson-Puig.

Concluímos esta seção com um exemplo para ilustrar a Correspondência de Brauer em ação.

Exemplo 4.3.11. Tome k algebricamente fechado de característica $p > 2$ e $G = \mathrm{SL}_2(p)$. Já conseguimos determinar no Exemplo 4.1.20 que kG possui três blocos e encontramos a partição induzida nas classes de isomorfismo de kG-módulos simples. Porém, foi necessário conhecer a estrutura dos kG-módulos projetivos indecomponíveis, informação esta que não é fácil de ser obtida. Desta vez, vamos utilizar a Correspondência de Brauer para determinar de um modo alternativo os blocos de kG, sem precisar recorrer à estrutura de módulos indecomponíveis. O que se segue está baseado no começo do Exemplo 3.3.5.

Os p-subgrupos de Sylow de G são de ordem p e, por isso, os blocos de kG possuem defeito zero ou defeito um. Pelo Corolário 4.3.7, os blocos de defeito zero correspondem a kG-módulos simples e projetivos e, portanto, o único bloco de defeito zero é o que contém V_p. Além disso, sabemos que V_p é o único kG-módulo simples que pertence a esse bloco de defeito zero. Os demais blocos de kG possuem um p-subgrupo de Sylow como grupo de defeito.

Seja P o p-subgrupo de Sylow de G dado no Exemplo 3.3.5. Se L denota o normalizador de P em G, sabemos pela Correspondência de Brauer que os blocos de kG com grupo de defeito P estão em bijeção com os blocos de kL com esse mesmo grupo de defeito. Dessa forma, determinaremos quais são os blocos de kL.

No Exemplo 3.3.5, obtivemos uma família $\{S_j\}_{j\in\mathbb{Z}}$ de kL-módulos simples que representa todas as classes de isomorfismo de módulos simples e que satisfaz $S_{j_1} \cong S_{j_2}$ se, e somente se, $j_1 \equiv j_2 \pmod{p-1}$. Como P é p-subgrupo de Sylow cíclico e normal de L, podemos aplicar o Exercício A.4.7 (que segue do Exemplo 2.2.12 e do Teorema 4.1.17) para concluir que dois kL-módulos simples S_{j_1} e S_{j_2} pertencem ao mesmo bloco se, e somente se,

$$S_{j_1} \cong S_{j_2} \otimes W^{\otimes n}$$

para algum $n \geq 0$. Como vimos no Exemplo 3.3.5, o módulo W acima é isomorfo a S_{-2}. Assim, utilizando a identidade $S_{j_1} \otimes S_{j_2} \cong S_{j_1+j_2}$, concluímos que S_{j_1} e S_{j_2} pertencem ao mesmo bloco se, e somente se,

$$S_{j_1} \cong S_{j_2-2n}$$

para algum $n \geq 0$. Mas isso é equivalente a

$$j_1 \equiv j_2 - 2n \pmod{p-1}$$

para algum $n \geq 0$ e, como $p-1$ é par, isso é o mesmo que $j_1 \equiv j_2 \pmod 2$. Logo, kL possui exatamente dois blocos: o bloco principal b_1, que contém os kL-módulos simples

$$S_0, S_2, \ldots, S_{p-3},$$

e outro bloco b_2, que contém os kL-módulos simples

$$S_1, S_3, \ldots, S_{p-2}.$$

Como a dimensão de todos esses módulos simples não é divisível por p, sabemos do Corolário 2.2.9 que nenhum deles é projetivo e, consequentemente, b_1 e b_2 possuem defeito positivo. Assim, concluímos que b_1 e b_2 são blocos com grupo de defeito P.

Pela Correspondência de Brauer, os blocos de kG com grupo de defeito P são $B_1 := b_1^G$ e $B_2 := b_2^G$. Com isso, já descobrimos que kG possui exatamente três blocos! Mas ainda não sabemos como os kG-módulos simples $V_1, \dots, V_{p-1}$ se separam dentre os blocos B_1 e B_2. Vamos determinar isso agora! Vimos no Exemplo 3.3.5 que o correspondente de Green de V_i é $(V_i)_L$, se $1 \leq i \leq p-1$. Agora, vimos que $(V_i)_L$ é indecomponível e possui S_{i-1} como fator de composição, então $(V_i)_L$ pertence ao mesmo bloco de S_{i-1}. Pelo Corolário 4.3.5, os blocos de V_i e de S_{i-1} são correspondentes de Brauer se $1 \leq i \leq p-1$. A partir disso, concluímos que

$$V_1, V_3, \dots, V_{p-2}$$

pertencem a B_1 e que

$$V_2, V_4, \dots, V_{p-1}$$

pertencem a B_2. Observe que o que encontramos está de acordo com o Exemplo 4.1.20!

Algo interessante desse método é que, além de ser mais simples, ele justifica melhor o motivo de os kL-módulos simples V_i estarem separados nos blocos de acordo com a paridade de i, para $1 \leq i \leq p-1$. Isso ocorre porque P é cíclico, então conseguimos utilizar o Exemplo 2.2.12 e, coincidentemente, vale $W \cong S_{-2}$ e esse é o responsável por essa propriedade.

4.4 Blocos de subgrupos normais

Se H é um subgrupo de G, conseguimos estabelecer uma conexão interessante entre os blocos de kG e os blocos de kH, especialmente quando H é grande o suficiente para conter o normalizador de um p-subgrupo D. Nesse caso, como D é normal em $N_G(D)$, podemos estudar se há alguma relação a mais entre os blocos de kD e os de $kN_G(D)$. Por isso, vamos fazer teoria de Clifford para blocos! Ou seja, dedicaremos esta seção para estudar algumas relações entre os blocos de kG e os blocos de kN quando N é um subgrupo normal de G. Ao final, conseguiremos estender o Primeiro Teorema Principal de Brauer, fazendo aparecer não exatamente os blocos de kD, mas sim os blocos de $kDC_G(D)$.

Se N é um subgrupo normal de G, então G age naturalmente em N por conjugação. Essa ação se estende para a álgebra de grupo: a conjugação por um elemento $g \in G$ induz um automorfismo da álgebra kN. Logo, a conjugação preserva a estrutura de álgebra e, escrevendo kN como soma direta de blocos e conjugando por $g \in G$, conseguimos decompor kN como a soma dos conjugados dos blocos, que ainda são ideais indecomponíveis de kN. Mas, pelo Teorema 4.1.6, a decomposição de kN como soma de blocos é única, então concluímos que gbg^{-1} é um bloco para todo bloco b de kN. Ou seja, a conjugação permuta os blocos!

Se b é um bloco de kN, podemos ver b como um $k[N \times N]$-submódulo de kG e, assim, $kGbG$ é o $k[G \times G]$-submódulo gerado por b. Vamos começar estudando esses módulos. Para isso, iremos considerar dois grupos. O primeiro deles é o subgrupo $\mathrm{Stab}(b)$ de G formado pelos elementos $g \in G$ tais que $gbg^{-1} = b$, ou seja, é o estabilizador de b na ação de G por conjugação nos blocos de kN. O outro é o subgrupo $X = \delta(\mathrm{Stab}(b)) \cdot (N \times N)$ de $G \times G$. Como N é normal em G, então $N \times N$ é normal em $G \times G$ e, assim, X é de fato um subgrupo de $G \times G$. Vendo b dentro do $k[G \times G]$-módulo kG, note que b é invariante pela ação de $\delta(\mathrm{Stab}(b))$ e pela ação de $N \times N$, então b é um kX-módulo. Por abuso de notação, denotaremos tal módulo por b_X, como se estivéssemos restringindo a estrutura de b a X.

Lema 4.4.1. Sejam N um subgrupo normal de G e b um bloco de kN. Sejam $b_1 = b, b_2, \dots, b_n$ representantes das classes de conjugação, sob a ação de G, dos blocos de kN. Então valem as seguintes afirmações:

(1) O $k[G \times G]$-módulo kG é a soma direta dos submódulos kGb_iG, para $1 \leq i \leq n$.

(2) Como um kN-módulo, $kGbG$ é a soma dos somandos canônicos de kG associados aos blocos conjugados de b.

(3) Como um $k[N \times N]$-módulo, uma decomposição de $kGbG$ como soma direta de indecomponíveis é dada por

$$(kGbG)_{N\times N} = \bigoplus_{t\in[(G\times G)/X]} tb,$$

onde $X = \delta(\mathrm{Stab}(b)) \cdot (N \times N)$.

(4) Como um $k[G\times G]$-módulo, temos um isomorfismo $kGbG \cong (b_X)^{G\times G}$, onde X é como acima.

No item (2), os "somandos canônicos" são aqueles dados pela Proposição 4.1.15.

Demonstração: É imediato que kGb_iG contém todos os conjugados de b_i para $1 \leq i \leq n$. Logo, a soma desses módulos contém todos os blocos de kN e, portanto, contém kN. Como kN gera kG como um $k[G \times G]$-módulo, segue que kG é a soma dos $k[G \times G]$-submódulos kGb_iG, para $1 \leq i \leq n$. Se provarmos (2), concluiremos da Proposição 4.1.15 que essa soma é direta, demonstrando (1).

Pela Proposição 4.1.15 (e por sua demonstração), sabemos que a soma dos somandos canônicos do kN-módulo kG associados aos blocos conjugados de b é

$$\left(\sum_{g\in G} gbg^{-1}\right) kG.$$

Como $(gbg^{-1})kG$ está contido em $kGbG$ para todo $g \in G$, então o módulo acima está contido em $kGbG$. Por outro lado, $g_1bg_2 = (g_1bg_1^{-1})g_1g_2$ está contido no módulo acima para todos $g_1, g_2 \in G$, então este módulo contém $kGbG$. Logo, $kGbG$ é igual ao módulo em destaque acima e o item (2) está provado.

Para (3), seja $t \in [(G \times G)/X]$. Se $x \in b$ e $n_1, n_2 \in N$, então $t^{-1}(n_1, n_2)t \in N \times N$, já que $N \times N$ é normal em $G \times G$ e, consequentemente, $(t^{-1}(n_1, n_2)t) \cdot x \in b$ e

$$(n_1, n_2) \cdot tx = t \cdot (t^{-1}(n_1, n_2)t) \cdot x \in tb.$$

Portanto, o subespaço tb de $kGbG$ é um $k[N \times N]$-submódulo. Mais ainda, isso também prova que tb é isomorfo à conjugação ${}^tb$. Como b é um $k[N \times N]$-módulo indecomponível, segue do Exercício A.3.4 que tb também é indecomponível.

Agora, se $g_1, g_2 \in G$, então existem $t \in [(G \times G)/X]$ e $x \in X$ tais que $(g_1, g_2) = tx$, logo

$$(g_1, g_2) \cdot b = t \cdot (xb) = tb,$$

onde utilizamos que $xb = b$ pela definição de X. Como $kGbG$ é o $k[G \times G]$-módulo gerado por b, segue então que $kGbG$ é a soma dos $k[N \times N]$-submódulos tb onde t percorre os elementos de $[(G \times G)/X]$. Resta mostrar que essa soma é direta para demonstrar o item (3). Se ela não fosse direta, teríamos uma combinação linear não trivial entre elementos dos módulos envolvidos na soma e, multiplicando pelo inverso de um elemento apropriado $t \in [(G \times G)/X]$, seguiria que

$$b \cap \sum_{(g_1,g_2)\notin X} (g_1, g_2)b \neq 0.$$

Mostremos que isso não pode ocorrer. Como kN é a soma direta de seus blocos e kG é a soma direta de kN com o subespaço gerado pela diferença $G \setminus N$, basta mostrar que, se $(g_1, g_2) \notin X$, então $(g_1, g_2)b$ está contido em algum bloco de kN diferente de b ou está contido no subespaço gerado por $G \setminus N$. Como

$$(g_1, g_2)b = g_1bg_2^{-1} = g_1g_2^{-1}(g_2bg_2^{-1})$$

e $g_2bg_2^{-1} \subseteq kN$, se $g_1g_2^{-1} \notin N$, então $(g_1, g_2)b$ está contido no subespaço gerado por $G \setminus N$. Por outro lado, se $n = g_1g_2^{-1} \in N$, então

$$(g_1, g_2)b = n \cdot (g_2bg_2^{-1}) = g_2bg_2^{-1}$$

é um bloco de kN. Esse bloco não pode ser b porque valeria $g_2 \in \mathrm{Stab}(b)$, mas então $(g_2, g_2) \in \delta(\mathrm{Stab}(b))$ e

$$(g_1, g_2) = (g_1 g_2^{-1}, 1) \cdot (g_2, g_2) \in \delta(\mathrm{Stab}(b)) \cdot (N \times N) = X,$$

uma contradição. Isso termina o item (3).

Por fim, para (4), segue do item (3) que $kGbG$ é a soma direta dos subespaços

$$\{(g_1, g_2)b \mid (g_1, g_2) \in G \times G\}.$$

Além disso, no parágrafo anterior, acabamos mostrando que $(g_1, g_2)b = b$ se, e somente se, $(g_1, g_2) \in X$, então o Corolário 3.1.5 nos mostra que $kGbG \cong (b_X)^{G \times G}$, como queríamos. □

Seja b um bloco de kN. Anteriormente, nos perguntamos quando existe um bloco B de kG tal que $b \mid B_{N \times N}$ e quando esse bloco B é único. Essa unicidade nos permitia obter uma correspondência, mas apenas entre alguns dos blocos. Dessa vez, não vamos nos preocupar com a unicidade. Como veremos agora, se N é normal em G, ainda temos muita coisa interessante!

Proposição 4.4.2. Seja N um subgrupo normal de G. Se b é um bloco de kN e se B é um bloco de kG, então são equivalentes:

(1) $b \mid B_{N \times N}$.

(2) $B \mid kGbG$.

(3) Se U é um kG-módulo não nulo pertencente a B e se b' é um bloco de kN, então

$$b'U \neq 0 \iff b' \text{ é um conjugado de } b.$$

(4) Existe um kG-módulo U pertencente a B tal que U_N possui um somando direto não nulo pertencente a b.

Demonstração: Provaremos (1) $\iff$ (2) e depois (2) $\implies$ (3) $\implies$ (4) $\implies$ (2). Para auxiliar na demonstração, sejam $b_1, \ldots, b_n$ representantes das classes de conjugação dos blocos de kN e tome $b_1 = b$.

(1) $\implies$ (2). Pelo item (1) do Lema 4.4.1, kG é a soma direta dos $k[G \times G]$-submódulos kGb_iG para $1 \leq i \leq n$. Como a única decomposição do $k[G \times G]$-módulo kG como soma de indecomponíveis é a sua decomposição em blocos, sabemos que $B \mid kGb_iG$ para algum $1 \leq i \leq n$. Mas $b \mid B_{N \times N}$, então $bB \neq 0$ e também $b(kGb_iG) \neq 0$. Pelo item (2) do Lema 4.4.1, concluímos que b é conjugado de b_i e, portanto, devemos ter $i = 1$ e $B \mid kGb_1G = kGbG$, como desejado.

(2) $\implies$ (1). Pelo item (3) do Lema 4.4.1, podemos escrever

$$(kGbG)_{N \times N} = \bigoplus_{t \in [(G \times G)/X]} tb,$$

onde $X = \delta(\mathrm{Stab}(b)) \cdot (N \times N)$. Além disso, cada tb é um $k[N \times N]$-módulo indecomponível. Como $B \mid kGbG$, o Teorema de Krull-Schmidt implica que $tb \mid B_{N \times N}$ para algum elemento $t \in [(G \times G)/X]$. Mas vimos na demonstração do Lema 4.4.1 que $tb \cong {}^t b$, logo $b \cong {}^{t^{-1}}(tb)$ é um somando direto de

$${}^{t^{-1}}(B_{N \times N}) = \left({}^{t^{-1}}B\right)_{t^{-1}(N \times N)t} = \left({}^{t^{-1}}B\right)_{N \times N} \cong B_{N \times N},$$

como queríamos demonstrar. Acima, utilizamos os itens (d) e (c) do Exercício A.3.4 na primeira igualdade e no último isomorfismo, respectivamente.

(2) $\implies$ (3). Vimos que kG é a soma dos $k[G \times G]$-submódulos kGb_iG para $1 \leq i \leq n$ e também sabemos que cada bloco aparece só uma vez como somando indecomponível do $k[G \times G]$-módulo kG. Por isso, como $B \mid kGbG$, kGb_iG deve ser uma soma de blocos de kG diferentes de

B se $i > 1$. Também obtemos da unicidade da decomposição em blocos que $B \subseteq kGbG$ e que a soma anterior é interna, ou seja, kGb_iG é a soma de "verdadeiros" blocos de kG, não apenas de cópias isomorfas. Com isso em mãos, vamos prosseguir.

Seja $U \neq 0$ um kG-módulo pertencente a B e seja b' um bloco de kN. Se b' não é conjugado a b, então $b' = gb_ig^{-1}$ para algum $g \in G$ e algum $i > 1$. Como kGb_iG é soma de blocos de kG diferentes de B e como U pertence a B, vale $(kGb_iG)U = 0$. Em particular, $b'U = (gb_ig^{-1})U = 0$. Por outro lado, como $BU = U$ e $B \subseteq kGbG$, vale $(kGbG)U = U \neq 0$. Assim, existem $g_1, g_2 \in G$ tais que $(g_1bg_2)U \neq 0$ e disso segue que $bU \neq 0$, pois $g_2U = U$. Também concluímos que $(gbg^{-1})U \neq 0$ para todo $g \in G$, ou seja, se b' é conjugado de b, então $b'U \neq 0$. Em resumo, conseguimos demonstrar que

$$b'U \neq 0 \iff b' \text{ é um conjugado de } b,$$

como preciso.

(3) $\implies$ (4). Seja U um kG-módulo não nulo pertencente a B. Por (3), $bU \neq 0$ e, pela Proposição 4.1.15, bU é um somando direto de U_N pertencente a b.

(4) $\implies$ (2). Assim como fizemos no início da demonstração, podemos encontrar $1 \leq i \leq n$ tal que $B \mid kGb_iG$. Nesse caso, se $j \neq i$, sabemos que kGb_jG é uma soma de blocos de kG distintos de B. Agora, seja U um kG-módulo como em (4). Como U_N possui um somando direto não nulo pertencente a b, vale $bU \neq 0$ e, portanto, $(kGb_1G)U \neq 0$. Como U pertence a B, vale $(kGb_jG)U = 0$ se $j \neq i$, então concluímos que $i = 1$ e temos $B \mid kGbG$. □

Sejam b um bloco de kN e B um bloco de kG. Diremos que B **cobre** b ou que b **é coberto por** B se as condições equivalentes da Proposição 4.4.2 estiverem satisfeitas. Essa definição estende a correspondência estabelecida na seção anterior: se B corresponde a b então, em particular, B cobre b. Observe que, pela Proposição 4.4.2, há uma relação entre os kG-módulos pertencentes a B e os kN-módulos pertencentes a b!

Observação 4.4.3. Como apontamos na Observação 4.3.2, para todo bloco b de kN existe um bloco B de kG que cobre b. Reciprocamente, se B é um bloco de kG, então vimos na demonstração da Proposição 4.4.2 que existe um bloco b de kN tal que $B \mid kGbG$ e, portanto, B cobre b.

Vamos demonstrar algumas propriedades da definição que acabamos de dar:

Teorema 4.4.4. Seja N um subgrupo normal de G e seja B um bloco de kG que cobre um bloco b de kN. Então:

(1) Os blocos de kN cobertos por B são exatamente os conjugados de b.

(2) Se o centralizador em G de um grupo de defeito de b está contido em N, então $B = b^G$ e B é o único bloco de kG cobrindo b.

(3) Existe um grupo de defeito de B contido em $\mathrm{Stab}(b)$.

(4) Todo grupo de defeito de b é a interseção de um grupo de defeito de B com N.

(5) Existe um bloco B' de kG cobrindo b que possui um grupo de defeito D' contendo um grupo de defeito de cada bloco de kG que cobre b. Se k for algebricamente fechado, também vale

$$[D' : D' \cap N] = [\mathrm{Stab}(b) : N]_p.$$

Acima, o subíndice p em $[\mathrm{Stab}(b) : N]_p$ (ou em qualquer inteiro positivo) indica que esta é a maior potência de p que divide $[\mathrm{Stab}(b) : N]$.

No item (2), note que b^G está definido pelo Lema 4.3.1. Em (4), é importante ressaltar que nem sempre a interseção de um grupo de defeito de B com N é um grupo de defeito de b, mas, como grupos de defeito são conjugados, essa interseção é conjugada em G a algum grupo de defeito de b. No item (5), como $D' \cap N$ é conjugado a um grupo de defeito de b, essa fórmula diz que $|D'|$ é o produto da ordem de um grupo de defeito de b com $[\mathrm{Stab}(b) : N]_p$. Além disso, sob as hipóteses de (2), veja que $B' = b^G$ e, dessa forma, temos uma relação entre a ordem de um grupo de defeito de b e a ordem de um grupo de defeito de b^G.

Demonstração: A afirmação (3) da Proposição 4.4.2 nos dá que B cobre todos os conjugados de b. Ela também diz que, se b' não é conjugado a b, então não existe um kG-módulo U pertencente a B tal que U_N possui um somando direto pertencente a b', mostrando que B não cobre b'. Isso prova (1).

Sob as hipóteses de (2), sabemos que b^G está definido. Logo, b^G é o único bloco de kG satisfazendo $b \mid (b^G)_{N\times N}$, ou seja, b^G é o único bloco de kG cobrindo b. Disso segue que $B = b^G$ e concluímos a unicidade desejada.

Pelo Lema 4.4.1, vale $kGbG \cong (b_X)^{G\times G}$, onde $X = \delta(\mathrm{Stab}(b))\cdot(N\times N)$. Como B cobre b, vale $B \mid kGbG$ e, por isso, B é relativamente X-projetivo. Assim, existe um vértice de B contido em X. Se D é um grupo de defeito de B, então temos $g_1, g_2 \in G$ tais que $(g_1, g_2)\delta(D)(g_1, g_2)^{-1} \subseteq X$. Como $N \subseteq \mathrm{Stab}(b)$, vale $X \subseteq \mathrm{Stab}(b) \times \mathrm{Stab}(b)$ e, olhando para a primeira coordenada de $(g_1, g_2)\delta(D)(g_1, g_2)^{-1}$, obtemos $g_1 D g_1^{-1} \subseteq \mathrm{Stab}(b)$. Concluímos que $g_1 D g_1^{-1}$ é um grupo de defeito de B contido em $\mathrm{Stab}(b)$, demonstrando (3).

Como $b \mid B_{N\times N}$, podemos argumentar como na demonstração do Lema 4.3.1 para concluir que todo grupo de defeito de b está contido em algum grupo de defeito de B. Como b é bloco de kN, segue então que todo grupo de defeito de b está contido na interseção de algum grupo de defeito de B com N. Para mostrar a igualdade, basta mostrar que esses grupos possuem a mesma ordem. Mas sabemos que os grupos de defeito de b possuem todos a mesma ordem e que $|D \cap N|$ é constante para todo grupo de defeito D de B (pois grupos de defeito são conjugados e N é normal), então basta mostrar que algum grupo de defeito de b contém (e, portanto, tem ordem maior ou igual à ordem de) $D \cap N$ para algum grupo de defeito D de B.

Observe primeiramente que B possui fonte trivial: isso segue do Exercício A.3.13, já que $B \mid kG \cong (k_{\delta(G)})^{G\times G}$ (esse último isomorfismo foi provado na Proposição 4.2.1). Logo, pelo Lema 3.2.21, $B_{N\times N}$ possui um somando indecomponível com um vértice contendo $\delta(D)\cap(N\times N)$ para algum grupo de defeito D de B. Repare que essa interseção é igual a $\delta(D\cap N)$. Mas $B_{N\times N} \mid kGbG$, então o Lema 4.4.1 (e sua demonstração) nos diz que cada somando indecomponível de $B_{N\times N}$ é da forma ${}^t b$ para algum $t \in G\times G$. Assim, existe $t \in G\times G$ tal que ${}^t b$ possui um vértice contendo $\delta(D\cap N)$ e, pelo Exercício A.3.9, b possui um vértice contendo $t^{-1}\delta(D\cap N)t$. Olhando para a primeira coordenada, concluímos que algum conjugado de $D\cap N$ está contido em algum grupo de defeito de b, terminando a demonstração de (4).

Vamos para o item (5). Pela Proposição 4.4.2, os blocos de kG que cobrem b são os somandos indecomponíveis de $kGbG$. Mas $kGbG \cong (b_X)^{G\times G}$, então cada bloco de kG cobrindo b possui um vértice contido em um vértice de b_X. Por outro lado, b_X é um somando da restrição de $(b_X)^{G\times G}$ a X, então existe um bloco B' de kG cobrindo b tal que $b_X \mid B'_X$. Argumentando com a Fórmula de Decomposição de Mackey (como fizemos no início da demonstração do Lema 4.3.1), segue que um vértice de b_X está contido em um vértice de B'. Por questões de ordem, concluímos que existe um vértice de B' que é um vértice de b_X e, pelo que vimos no início desse parágrafo, ele contém um vértice de cada bloco de kG cobrindo b. Olhando para a primeira coordenada, encontramos um grupo de defeito D' de B' que contém um grupo de defeito de cada bloco de kG que cobre b. Isso prova a primeira afirmação em (5).

Agora, suponha que k seja algebricamente fechado. Tome $Q \subseteq X$ um vértice de b_X. Como a restrição de b_X ao subgrupo normal $N\times N$ é o módulo indecomponível b, o Lema 3.2.22 mostra

que $Q(N \times N)/(N \times N)$ é um p-subgrupo de Sylow de $X/(N \times N)$. Portanto,

$$[Q : Q \cap (N \times N)] = \left| \frac{Q}{Q \cap (N \times N)} \right| = \left| \frac{Q(N \times N)}{N \times N} \right| = \left| \frac{X}{N \times N} \right|_p = [X : N \times N]_p.$$

Mas também vale

$$\begin{aligned}[X : N \times N] = \left| \frac{\delta(\mathrm{Stab}(b))(N \times N)}{N \times N} \right| &= \left| \frac{\delta(\mathrm{Stab}(b))}{\delta(\mathrm{Stab}(b)) \cap (N \times N)} \right| \\ &= [\delta(\mathrm{Stab}(b)) : \delta(N)] \\ &= [\mathrm{Stab}(b) : N].\end{aligned}$$

Agora, como Q e $\delta(D')$ são vértices de B' (veja o parágrafo anterior), eles são conjugados em $G \times G$. Assim, usando que $N \times N$ é normal em $G \times G$, obtemos

$$[Q : Q \cap (N \times N)] = [\delta(D') : \delta(D') \cap (N \times N)] = [\delta(D') : \delta(D' \cap N)] = [D' : D' \cap N].$$

Juntando tudo, chegamos em $[D' : D' \cap N] = [\mathrm{Stab}(b) : N]_p$, como queríamos. □

Estamos prontos para estender o Primeiro Teorema Principal de Brauer!

Teorema 4.4.5. Suponha que k seja algebricamente fechado. Se D é um p-subgrupo de G, então existe uma correspondência biunívoca entre os blocos de kG com grupo de defeito D e as classes de conjugação em $N_G(D)$ de blocos β de $k[DC_G(D)/D]$ com defeito zero tais que $[\mathrm{Stab}(\beta) : DC_G(D)]$ não é divisível por p.

O enunciado acima é complicado e ainda precisamos esclarecer alguns detalhes antes de prosseguir para a demonstração. Não é difícil verificar que D e $C_G(D)$ são subgrupos normais de $N_G(D)$ e, por isso, o produto $DC_G(D)$ é um subgrupo normal de $N_G(D)$. Assim, $N_G(D)$ age por conjugação em $DC_G(D)$. Mas, por definição, $N_G(D)$ fixa D nessa ação e então podemos descer a ação para o quociente $DC_G(D)/D$. Estendendo para a álgebra de grupo, podemos mostrar como no início da seção que $N_G(D)$ age por conjugação nos blocos de $k[DC_G(D)/D]$ e é essa ação ao qual o enunciado se refere. Se β é um bloco de $k[DC_G(D)/D]$, podemos definir de modo análogo $\mathrm{Stab}(\beta)$, que é um subgrupo de $N_G(D)$. Como os blocos de $k[DC_G(D)/D]$ são ideais dessa álgebra de grupo, eles são invariantes pela conjugação por um elemento de $DC_G(D)$. Portanto, $DC_G(D)$ é um subgrupo de $\mathrm{Stab}(\beta)$ e faz sentido tomar o índice $[\mathrm{Stab}(\beta) : DC_G(D)]$.

A demonstração se resume a uma composição de bijeções entre certos conjuntos de blocos. Pelo Primeiro Teorema Principal de Brauer, já temos uma correspondência entre os blocos de kG com grupo de defeito D e os blocos de $kN_G(D)$ com esse mesmo grupo de defeito. O próximo passo é demonstrar uma correspondência entre esses blocos de $kN_G(D)$ com as classes de conjugação em $N_G(D)$ de blocos β de $kDC_G(D)$ com grupo de defeito D tais que $[\mathrm{Stab}(\beta) : DC_G(D)]$ não é divisível por p. Por fim, passaremos ao quociente com uma nova correspondência. Estabeleceremos esses dois passos em dois lemas, que juntos provam o Teorema 4.4.5.

Lema 4.4.6. Suponha que k seja algebricamente fechado. Se D é um p-subgrupo de G, então existe uma correspondência biunívoca entre os blocos de $kN_G(D)$ com grupo de defeito D e as classes de conjugação em $N_G(D)$ de blocos β de $kDC_G(D)$ com grupo de defeito D tais que $[\mathrm{Stab}(\beta) : DC_G(D)]$ não é divisível por p.

Demonstração: Seja b um bloco de $kN_G(D)$ com grupo de defeito D. Como $DC_G(D)$ é normal em $N_G(D)$, b cobre uma classe de conjugação de blocos de $kDC_G(D)$ pelo item (1) do Teorema 4.4.4. Seja β um dos blocos dessa classe de conjugação. Como D é um p-subgrupo normal em $DC_G(D)$, o Corolário 4.2.9 mostra que D está contido em todo grupo de defeito de β. Por outro lado, pelo item (4) do Teorema 4.4.4, todo grupo de defeito de β é a interseção de um grupo de defeito de b com $DC_G(D)$ e, por isso, possui ordem $|D \cap DC_G(D)| = |D|$. Disso segue que D é

um grupo de defeito de β. Como $C_{N_G(D)}(D) = C_G(D) \subseteq DC_G(D)$, o item (2) do Teorema 4.4.4 nos diz que $\beta^{N_G(D)}$ está definido, $b = \beta^{N_G(D)}$ e este é o único bloco de $kN_G(D)$ que cobre β. Em particular, o bloco b cumpre o papel do bloco B' no item (5) do Teorema 4.4.4 e então vale

$$[\mathrm{Stab}(\beta) : DC_G(D)]_p = [D : D \cap DC_G(D)] = [D : D] = 1,$$

isto é, p não divide $[\mathrm{Stab}(\beta) : DC_G(D)]$. Dessa maneira, o mapa que leva um bloco b na classe de conjugação do bloco β é uma função do conjunto dos blocos de $kN_G(D)$ com grupo de defeito D no conjunto das classes de conjugação em $N_G(D)$ de blocos β de $kDC_G(D)$ com grupo de defeito D tais que $[\mathrm{Stab}(\beta) : DC_G(D)]$ não é divisível por p. Vimos acima que o único bloco cobrindo a classe de conjugação de β é b, então essa função é injetora.

Resta mostrar que a função do parágrafo anterior é sobrejetora. Seja β um bloco de $kDC_G(D)$ com grupo de defeito D tal que $[\mathrm{Stab}(\beta) : DC_G(D)]_p = 1$. Como $C_{N_G(D)}(D) \subseteq DC_G(D)$, o Lema 4.3.1 mostra que $b := \beta^{N_G(D)}$ está definido. Esse é o único bloco de $N_G(D)$ que cobre β. Pelo item (4) do Teorema 4.4.4, b possui um grupo de defeito D' satisfazendo $D = D' \cap N$. Mas pelo item (5) deste mesmo teorema, temos

$$\left|D'\right| = [\mathrm{Stab}(\beta) : DC_G(D)]_p \cdot \left|D' \cap N\right| = 1 \cdot |D| = |D|,$$

então deve valer $D' = D$. Ou seja, b é um bloco de $kN_G(D)$ com grupo de defeito D que cobre β. Desse modo, a função em questão leva b na classe de conjugação de β, como queríamos. □

Observação 4.4.7. Na demonstração anterior, utilizamos que k era algebricamente fechado para calcular $[\mathrm{Stab}(\beta) : DC_G(D)]_p$. Isso nos permitiu determinar a "imagem" da correspondência. Se k é um corpo qualquer, um argumento análogo ainda nos permite obter uma função injetora do conjunto dos blocos de $N_G(D)$ com grupo de defeito D no conjunto das classes de conjugação em $N_G(D)$ de blocos de $kDC_G(D)$ com grupo de defeito D, mas não temos mais o controle sobre a imagem.

Observação 4.4.8. Se B é um bloco de kG com grupo de defeito D, então B corresponde a um bloco b de $kN_G(D)$ com grupo de defeito D pela Correspondência de Brauer. Pela demonstração do Lema 4.4.6, se β é um bloco de $kDC_G(D)$ coberto por b, então β também possui grupo de defeito D e vale $\beta^{N_G(D)} = b$. Mas $C_G(D) \subseteq DC_G(D)$, então β^G também está definido. Pelo Lema 4.3.1, $\beta^G = (\beta^{N_G(D)})^G = b^G = B$. Essa é uma forma de recuperar B através de β sem passar pelo subgrupo $N_G(D)$.

A próxima e última parte da demonstração do Teorema 4.4.5 decorre do seguinte lema, que é mais geral do que de fato precisamos.

Lema 4.4.9. Se D é um p-subgrupo de G, então existe uma correspondência biunívoca entre os blocos de $kDC_G(D)$ e os blocos de $k[DC_G(D)/D]$. Se um bloco de $kDC_G(D)$ possui grupo de defeito Q, então Q contém D e o bloco correspondente de $k[DC_G(D)/D]$ possui grupo de defeito Q/D. Além disso, essa correspondência é compatível com a conjugação por elementos de $N_G(D)$.

Nessa nova correspondência, blocos de $kDC_G(D)$ com grupo de defeito de D são levados em blocos de $k[DC_G(D)/D]$ com grupo de defeito $D/D = \{1\}$, ou seja, com defeito zero. Como ela é compatível com a conjugação por elementos de $N_G(D)$, classes de conjugação de blocos e estabilizadores são preservados. Assim, esse resultado se aplica para concluir a prova do Teorema 4.4.5.

Demonstração: Como D é um p-subgrupo normal de $DC_G(D)$, sabemos pela Proposição 1.3.14 que D age trivialmente em todo $kDC_G(D)$-módulo simples. Logo, descendo ao quociente, podemos ver um $kDC_G(D)$-módulo simples S como um $k[DC_G(D)/D]$-módulo simples, que denotaremos por $\overline{S}$. Note que todo $k[DC_G(D)/D]$-módulo simples é obtido dessa forma. Para estabelecer

a correspondência, a ideia é mostrar que dois $kDC_G(D)$-módulos simples S e T pertencem ao mesmo bloco de $kDC_G(D)$ se, e somente se, $\overline{S}$ e $\overline{T}$ pertencem ao mesmo bloco de $k[DC_G(D)/D]$.

Suponha que $\overline{S}$ e $\overline{T}$ pertençam ao mesmo bloco e mostremos que S e T pertencem ao mesmo bloco. Podemos utilizar o Teorema 4.1.17 e reduzir a situação para o caso em que $\overline{S}$ e $\overline{T}$ não são isomorfos e existe uma sequência exata

$$0 \longrightarrow \overline{S} \longrightarrow \overline{U} \longrightarrow \overline{T} \longrightarrow 0$$

que não cinde, onde $\overline{U}$ é um $k[DC_G(D)/D]$-módulo. Restringindo escalares para $kDC_G(D)$, podemos ver $\overline{U}$ como um $kDC_G(D)$-módulo U e os homomorfismos da sequência acima podem ser vistos como homomorfismos de $kDC_G(D)$-módulos. Note que a sequência continua exata. Mostremos que ela também não cinde em $kDC_G(D)$. De fato, se $\varphi : S \to U$ denota o primeiro homomorfismo da sequência, suponha que exista $\psi : U \to S$ tal que $\psi\varphi = \mathrm{id}_S$. Como D age trivialmente em U e em S, podemos voltar para o quociente, obtendo homomorfismos de $k[DC_G(D)/D]$-módulos $\overline{\varphi} : \overline{S} \to \overline{U}$ e $\overline{\psi} : \overline{U} \to \overline{S}$ satisfazendo $\overline{\psi}\overline{\varphi} = \mathrm{id}_{\overline{S}}$. Mas isso é um absurdo porque a sequência original não cinde. Logo, pelo item (3) do Teorema 4.1.17, S e T pertencem ao mesmo bloco de $kDC_G(D)$.

Reciprocamente, suponha que S e T pertençam ao mesmo bloco e mostremos que $\overline{S}$ e $\overline{T}$ pertencem ao mesmo bloco. Como anteriormente, podemos reduzir a situação para o caso em que S e T não são isomorfos e existe uma sequência exata

$$0 \longrightarrow S \longrightarrow U \longrightarrow T \longrightarrow 0$$

que não cinde, onde U é um $kDC_G(D)$-módulo. Podemos proceder como no parágrafo anterior e encontrar uma sequência exata no quociente que não cinde, mas, para isso, precisamos mostrar primeiramente que D age trivialmente em U para descer ao quociente. Assim que provarmos isso, seguirá que $\overline{S}$ e $\overline{T}$ pertencem ao mesmo bloco. Inicialmente, note que, se $\varphi : S_{C_G(D)} \to T_{C_G(D)}$ é um isomorfismo de $kC_G(D)$-módulos, então φ também é um isomorfismo de $kDC_G(D)$-módulos, pois D age trivialmente em S e em T e então sua ação comuta com φ. Como estamos supondo $S \ncong T$, devemos ter $S_{C_G(D)} \ncong T_{C_G(D)}$. Além disso, $S_{C_G(D)}$ e $T_{C_G(D)}$ ainda são $kC_G(D)$-módulos simples, porque D deixa invariante qualquer um de seus $kC_G(D)$-submódulos e então eles são $kDC_G(D)$-submódulos. Restringindo a sequência exata acima para $kC_G(D)$, concluímos que $U_{C_G(D)}$ possui exatamente dois fatores de composição e eles não são isomorfos. Sabendo disso, vamos calcular $\mathrm{End}_{kC_G(D)}(U)$. Temos dois casos:

(i) $U_{C_G(D)}$ é semissimples: nesse caso, deve valer $U_{C_G(D)} \cong S_{C_G(D)} \oplus T_{C_G(D)}$. Portanto, como $S_{C_G(D)}$ e $T_{C_G(D)}$ não são isomorfos, o Corolário 1.2.6 nos dá

$$\mathrm{End}_{kC_G(D)}(U) \cong \mathrm{End}_{kC_G(D)}(S) \times \mathrm{End}_{kC_G(D)}(T).$$

Pelo Lema de Schur, segue que $\mathrm{End}_{kC_G(D)}(U)$ é o produto de duas álgebras de divisão.

(ii) $U_{C_G(D)}$ não é semissimples: como este módulo possui apenas dois fatores de composição, ele dever ser unisseriado. Nesse caso, o seu radical é isomorfo a $S_{C_G(D)}$ e o quociente pelo radical é isomorfo a $T_{C_G(D)}$. Mostremos que $\mathrm{End}_{kC_G(D)}(U)$ é uma álgebra de divisão. Se $\varphi : U_{C_G(D)} \to U_{C_G(D)}$ é um homomorfismo não nulo, então sua imagem é igual a $\mathrm{rad}(U_{C_G(D)})$ ou a $U_{C_G(D)}$, já que $\mathrm{rad}(U_{C_G(D)})$ é o único submódulo não trivial do módulo unisseriado $U_{C_G(D)}$. Se a imagem fosse o radical de $U_{C_G(D)}$, o núcleo de φ seria um submódulo próprio não trivial de $U_{C_G(D)}$ e então também seria o radical de $U_{C_G(D)}$. Pelo Teorema do Isomorfismo, obteríamos $S_{C_G(D)} \cong T_{C_G(D)}$, uma contradição. Por isso, φ deve ser sobrejetor e, consequentemente, é um isomorfismo, como queríamos.

Em qualquer caso, decorre do Exercício A.1.5 que qualquer subálgebra de $\mathrm{End}_{kC_G(D)}(U)$ é semissimples[1]. Agora, cada elemento de D induz um operador linear em U e, como os elementos

[1]Se k é algebricamente fechado, então $\mathrm{End}_{kC_G(D)}(U)$ é isomorfo a k ou a $k \times k$. Nesse caso, é mais fácil verificar essa afirmação sem o uso do Exercício A.1.5.

de D comutam com os elementos de $C_G(D)$, esse operador linear é na verdade um elemento de $\mathrm{End}_{kC_G(D)}(U)$. Isso nos dá uma transformação linear $\varphi : kD \to \mathrm{End}_{kC_G(D)}(U)$ e não é difícil verificar que φ é um homomorfismo de álgebras. A imagem de φ é uma subálgebra de $\mathrm{End}_{kC_G(D)}(U)$ e, como acabamos de ver, é semissimples. Portanto, $kD/\ker\varphi$ é semissimples. Pelo Teorema 1.1.8, temos $\mathrm{rad}(kD) \subseteq \ker\varphi$. Mas D é um p-subgrupo, então sabemos do Exercício A.1.14 que o radical de kD é o ideal de aumento de kD, que é maximal. Assim, deve valer $\ker\varphi = \mathrm{rad}(kD)$. Se $d \in D$, então $d-1$ está no ideal de aumento de kD e vale $\varphi(d-1) = 0$. Isso diz que $d-1$ anula U, ou seja, d age trivialmente em U para todo $d \in D$, como era preciso demonstrar.

Com isso, podemos definir a correspondência. Se b é um bloco de $kDC_G(D)$, escolha um $kDC_G(D)$-módulo simples S pertencente a b e defina o correspondente $\overline{b}$ como sendo o bloco de $k[DC_G(D)/D]$ ao qual $\overline{S}$ pertence. Pelo que fizemos anteriormente, a definição de $\overline{b}$ não depende da escolha de S e a função $b \mapsto \overline{b}$ é injetora. Como todo bloco contém um módulo simples e como todo $k[DC_G(D)/D]$-módulo simples é da forma $\overline{S}$ para algum $kDC_G(D)$-módulo simples, a função $b \mapsto \overline{b}$ também é sobrejetora. Isso estabelece a correspondência. Vamos provar que ela possui as propriedades desejadas.

Seja b um bloco de $kDC_G(D)$. Para encurtar a notação, escreveremos[1] "b-módulo" para nos referir a um $kDC_G(D)$-módulo pertencente a b. Analogamente, "$\overline{b}$-módulo" significará um $k[DC_G(D)/D]$-módulo pertencente a $\overline{b}$. Se U é um b-módulo no qual D age trivialmente, então seus fatores de composição pertencem a b e podemos descer ao quociente para obter um $k[DC_G(D)/D]$-módulo $\overline{U}$ cujos fatores de composição pertencem a $\overline{b}$. Assim, $\overline{U}$ é um $\overline{b}$-módulo. Note que todo $\overline{b}$-módulo pode ser obtido dessa forma.

Agora, suponha que o bloco b de $kDC_G(D)$ possua grupo de defeito Q. Como D é um p-subgrupo normal de $DC_G(D)$, o Corolário 4.2.9 mostra que $D \subseteq Q$. Vamos provar que $\overline{b}$ possui Q/D como grupo de defeito. Se mostrarmos que todo $\overline{b}$-módulo indecomponível é relativamente Q/D-projetivo, então todo $\overline{b}$-módulo indecomponível possuirá um vértice contido em Q/D e o Corolário 4.3.6 nos dará que Q/D contém um grupo de defeito de $\overline{b}$. Seja então $\overline{U}$ um $\overline{b}$-módulo indecomponível, onde U é um b-módulo. Como D age trivialmente em U, todo b-submódulo de U corresponde a um $\overline{b}$-submódulo de $\overline{U}$ e, usando isso, vemos que U é indecomponível. Mas Q é um grupo de defeito de b, então o Teorema 4.2.2 mostra que U é relativamente Q-projetivo e vale $U \mid (U_Q)^{DC_G(D)}$. Vamos estudar esse módulo induzido. Observe que D age trivialmente nele. De fato, utilizando a identificação

$$(U_Q)^{DC_G(D)} = kDC_G(D) \otimes_{kQ} U_Q,$$

todo elemento desse módulo induzido é uma soma de tensores da forma $x \otimes u$, onde $x \in DC_G(D)$ e $u \in U$. Como $D \subseteq Q$, vemos que um elemento $d \in D$ age em um desses tensores da seguinte maneira:

$$d \cdot (x \otimes u) = x(x^{-1}dx) \otimes u = x \otimes (x^{-1}dx)u = x \otimes u.$$

Aqui utilizamos que D é normal em $DC_G(D)$, então $x^{-1}dx \in D \subseteq Q$ e pode ser "passado" pelo produto tensorial, e que D age trivialmente em U. Dessa forma, podemos olhar $(U_Q)^{DC_G(D)}$ como um $k[DC_G(D)/D]$-módulo, que possui um $k[Q/D]$-submódulo isomorfo a $\overline{U}_{Q/D}$ e é gerado por ele. Por questões de dimensão, segue do Corolário 3.1.6 que

$$\overline{(U_Q)^{DC_G(D)}} \cong (\overline{U}_{Q/D})^{DC_G(D)/D}.$$

Com isso, segue que $\overline{U} \mid (\overline{U}_{Q/D})^{DC_G(D)/D}$, ou seja, $\overline{U}$ é relativamente Q/D-projetivo.

Já sabemos que Q/D contém um grupo de defeito de $\overline{b}$. Para mostrar que Q/D é um grupo de defeito de $\overline{b}$, é suficiente encontrar um $\overline{b}$-módulo indecomponível com vértice Q/D pelo Teorema 4.2.2. Para isso, adaptaremos a demonstração do Corolário 4.3.6. Aplicando a Correspondência de Brauer para $DC_G(D)$, seja β o bloco de $kN_{DC_G(D)}(Q)$ que é o correspondente de Brauer de

[1] Com algumas identificações, sabemos que b-módulos são exatamente $kDC_G(D)$-módulos pertencentes a b, então essa notação não é ruim.

b. Como na demonstração a qual nos referimos, podemos encontrar um $kN_{DC_G(D)}(Q)$-módulo indecomponível V pertencente a β com vértice Q e tal que Q age trivialmente em V. Aplicando a Correspondência de Green para $DC_G(D)$, podemos tomar U como sendo um $kDC_G(D)$-módulo indecomponível que é o correspondente de Green de V. Note que U possui vértice Q, $U \mid V^{DC_G(D)}$ e, pelo Corolário 4.3.5, U pertence a b. Como $D \subseteq Q$ age trivialmente em V, podemos imitar o argumento do parágrafo anterior para mostrar que D age trivialmente em $V^{DC_G(D)}$. Mas $U \mid V^{DC_G(D)}$, então D também age trivialmente em U e podemos descer ao quociente, formando o $\overline{b}$-módulo $\overline{U}$. Como U é indecomponível, o mesmo vale para $\overline{U}$. Sabemos do parágrafo anterior que $\overline{U}$ possui um vértice contido em Q/D. Se $\overline{U}$ for relativamente Q'/D-projetivo para algum $D \leq Q' < Q$, então $\overline{U} \mid (\overline{U}_{Q'/D})^{DC_G(D)/D}$. Como D age trivialmente em U, podemos argumentar como no parágrafo anterior para obter que D age trivialmente em $(U_{Q'})^{DC_G(D)}$ e vale

$$\overline{(U_{Q'})^{DC_G(D)}} \cong (\overline{U}_{Q'/D})^{DC_G(D)/D}.$$

Mas então

$$\overline{U} \mid (\overline{U}_{Q'/D})^{DC_G(D)/D} \cong \overline{(U_{Q'})^{DC_G(D)}} \implies U \mid (U_{Q'})^{DC_G(D)},$$

o que não pode ocorrer, pois U possui vértice Q e $Q' \subsetneq Q$. Portanto, concluímos que $\overline{U}$ é um $\overline{b}$-módulo indecomponível com vértice Q/D, como queríamos. Isso prova a afirmação do enunciado que diz respeito a grupos de defeito.

Resta verificar que a correspondência é compatível com a conjugação por elementos de $N_G(D)$, ou seja, devemos mostrar que se b é um bloco de $kDC_G(D)$ e $g \in N_G(D)$, então $\overline{gbg^{-1}} = g\overline{b}g^{-1}$. Seja S um $kDC_G(D)$-módulo simples pertencente a b. Se $g \in N_G(D)$, então afirmamos que a conjugação ${}^gS$ pertence ao bloco gbg^{-1}. De fato, um elemento $gxg^{-1} \in kDC_G(D)$ (com $x \in kDC_G(D)$) age num elemento $s \in {}^gS$ por $gxg^{-1} \cdot s = xs$. Logo, se b' é um bloco de $kDC_G(D)$, então os espaços vetoriais $(gb'g^{-1}) \cdot {}^gS$ e $b'S$ são iguais e segue facilmente que ${}^gS$ pertence a gbg^{-1}. Agora, podemos fazer isso no quociente também. Pela correspondência, $\overline{S}$ pertence a $\overline{b}$. Além disso, D também age trivialmente em ${}^gS$ e podemos formar $\overline{{}^gS}$, que, pelo que vimos, pertence a $\overline{gbg^{-1}}$. Mas um elemento $g\overline{x}g^{-1} \in k[DC_G(D)/D]$ (com $\overline{x} \in k[DC_G(D)/D]$ e lembrando que $N_G(D)$ age nessa álgebra de grupo) age num elemento $s \in \overline{{}^gS}$ por $g\overline{x}g^{-1} \cdot s = \overline{x}s$. Com isso, se β é um bloco de $k[DC_G(D)/D]$, então os espaços $(g\beta g^{-1}) \cdot \overline{{}^gS}$ e $\beta\overline{S}$ são iguais, mostrando como antes que $\overline{{}^gS}$ pertence a $g\overline{b}g^{-1}$. Mas $\overline{{}^gS}$ só pode pertencer a um bloco, então devemos ter $\overline{gbg^{-1}} = g\overline{b}g^{-1}$, concluindo a demonstração. □

Na situação usual da Correspondência de Brauer, dada pelo Primeiro Teorema Principal de Brauer, não há de fato uma correspondência se o grupo de defeito D for normal em G, porque então temos $N_G(D) = G$. Com essa versão estendida dada pelo Teorema 4.4.5, esse problema é corrigido e agora podemos relacionar os blocos de kG com grupo de defeito D com os blocos de $k[DC_G(D)/D]$ de defeito zero. Note que $DC_G(D)/D$ sempre tem ordem menor do que a ordem de G se D não for trivial. Nesse sentido, descobrir os blocos de kG equivale a entender os seus blocos de defeito zero e os blocos de defeito zero de alguns grupos menores do que G. Por outro lado, a situação agora é mais complicada e devemos entender como são as classes de conjugação e os estabilizadores de blocos de $k[DC_G(D)/D]$. Um método para isso se encontra ao final da demonstração do Lema 4.4.9: dado um $k[DC_G(D)/D]$-módulo simples $\overline{S}$ pertencente a um bloco β, podemos identificar a quais blocos pertencem os conjugados de $\overline{S}$ pela ação de $N_G(D)$ e estes serão os blocos conjugados de β.

Pelo Corolário 4.3.7, blocos de defeito zero estão em bijeção com classes de isomorfismo de módulos simples projetivos. Dessa forma, o Teorema 4.4.5 associa a cada bloco B de kG com grupo de defeito D um $k[DC_G(D)/D]$-módulo simples projetivo, chamado de **módulo canônico** do bloco B. Pelo que vimos, ele está definido a menos de isomorfismo e a menos de conjugação por um elemento de $N_G(D)$. Em certo sentido, ele também não depende da escolha do grupo de defeito D (veja o Exercício A.4.12). O módulo canônico também existe quando k não é algebricamente

fechado por conta da Observação 4.4.7, mas nesse caso não sabemos quais $k[DC_G(D)/D]$-módulos simples projetivos podem ser módulos canônicos de um bloco de kG.

Terminaremos a seção calculando o módulo canônico associado ao bloco principal.

Exemplo 4.4.10. Seja B o bloco principal de kG. Sabemos que B possui defeito máximo, então um p-subgrupo de Sylow P de G é um grupo de defeito de B. Pelo Corolário 4.3.9, o bloco principal b de $kN_G(P)$ é o correspondente de Brauer de B. Pelo Exercício A.4.9 (que decorre essencialmente do item (3) da Proposição 4.4.2), b cobre apenas o bloco principal β de $kPC_G(P)$ e este é o correspondente de b segundo o Lema 4.4.6. Finalmente, vendo o $kPC_G(P)$-módulo trivial como módulo sobre $k[PC_G(P)/P]$, obtemos também o módulo trivial e, com a notação do Lema 4.4.9, $\overline{\beta}$ é o bloco principal de $k[PC_G(P)/P]$. Com isso, concluímos que o módulo canônico associado ao bloco principal de kG é o $k[PC_G(P)/P]$-módulo trivial, como era de se esperar. Note que esse módulo não possui conjugados na ação por $N_G(P)$.

4.5 Subpares

Seja b um bloco de kH, onde $H \leq G$. Se b possui grupo de defeito D e $N_G(D) \subseteq H$, sabemos do Primeiro Teorema Principal de Brauer que b^G está definido e que seu grupo de defeito também é D. Por outro lado, para b^G estar definido, vimos no Lema 4.3.1 que basta exigir $C_G(D) \subseteq H$. O que podemos dizer sobre essa correspondência nesse caso mais geral? Como veremos, o subgrupo $DC_G(D)$ que apareceu na seção anterior será muito importante!

Começaremos com o Terceiro Teorema Principal de Brauer, cuja demonstração motivará o que faremos em seguida. Esse teorema nos diz a relação entre b e b^G quando estamos lidando com o bloco principal.

Teorema 4.5.1 (Terceiro Teorema Principal de Brauer)**.** Seja H um subgrupo de G e seja b um bloco de kH com grupo de defeito D. Se $C_G(D) \subseteq H$, então

$$b \text{ é o bloco principal de } kH \iff b^G \text{ é o bloco principal de } kG.$$

A versão fraca dada pelo Corolário 4.3.9 exige $N_G(D) \subseteq H$. Agora, a hipótese pede apenas $C_G(D) \subseteq H$, que é a condição que o Lema 4.3.1 nos dá para garantir que b^G está definido.

A implicação ($\Longrightarrow$) é mais fácil e segue sem muitas dificuldades do Segundo Teorema Principal de Brauer, como explicado abaixo. O maior problema é demonstrar a implicação ($\Longleftarrow$) e a ideia será a seguinte. Primeiramente, reduziremos o problema a $H = DC_G(D)$. Depois, essencialmente teremos duas ferramentas para descer do bloco principal de kG para o bloco principal de um subgrupo. A primeira delas é através do Primeiro Teorema Principal de Brauer, que nos permite passar do bloco principal de kG para o bloco principal de $kN_G(P)$ onde P é um p-subgrupo de Sylow de G. Em seguida, é possível aplicar o Exercício A.4.9 e descer para $kPC_G(P)$. Então teremos que subir: encontramos $P' \subsetneq P$ com $PC_G(P) \subseteq N_G(P')$ e aplicamos ($\Longrightarrow$) para chegar no bloco principal de $kN_G(P')$. Como antes, conseguimos descer para $kP'C_G(P')$. Então tomamos $P'' \subsetneq P'$ com $P'C_G(P') \subseteq N_G(P'')$, repetimos os dois últimos passos e chegamos em $kP''C_G(P'')$, e assim em diante. Fazendo esse "zigue-zague", chegamos em $kDC_G(D)$ em algum momento.

Notação 4.5.2. Denotaremos por $b_0(G)$ o bloco principal de kG para um grupo qualquer G.

Demonstração: ($\Longrightarrow$) Se k denota o kG-módulo trivial, então a restrição k_H é o kH-módulo trivial. Assim, os vértices de k_H são os p-subgrupos de Sylow de H. Mas $b = b_0(H)$, então o grupo de defeito D é um p-subgrupo de Sylow de H e, consequentemente, é um vértice de k_H. Como $C_G(D) \subseteq H$, o Segundo Teorema Principal de Brauer implica que k pertence a b^G, isto é, $b^G = b_0(G)$, como preciso.

($\Longleftarrow$) Suponha que $b^G = b_0(G)$. Vamos reduzir o problema trocando H por $DC_G(D)$. Vejamos como fazer isso. Pela Observação 4.4.8, existe um bloco β de $kDC_H(D)$ com grupo de

defeito D tal que β^H está definido e é igual a b. Como $C_G(D) \subseteq H$, note que $C_H(D) = C_G(D)$. Assim, β é um bloco de $kDC_G(D)$ com grupo de defeito D e então o item (3) do Lema 4.3.1 mostra que β^G também está definido. Pelo item (2) desse mesmo lema, deve valer

$$\beta^G = (\beta^H)^G = b^G = b_0(G).$$

Se provarmos que $\beta = b_0(DC_G(D))$, então seguirá da implicação ($\Longrightarrow$) que $\beta^H = b$ é o bloco principal de kH, como queremos. Dessa forma, reduzimos o problema a mostrar que, se β é um bloco de $kDC_G(D)$ com grupo de defeito D e satisfazendo $\beta^G = b_0(G)$, então $\beta = b_0(DC_G(D))$.

Para provar a afirmação acima, vamos proceder por "indução de cima para baixo" na ordem do grupo de defeito D. Como base, suponha que D tenha tamanho máximo, isto é, que D seja um p-subgrupo de Sylow de G. Seja β um bloco de $kDC_G(D)$ com grupo de defeito D e satisfazendo $\beta^G = b_0(G)$. Note que $\beta^{N_G(D)}$ também está definido, satisfaz $(\beta^{N_G(D)})^G = \beta^G = b_0(G)$ e possui um grupo de defeito contendo D, tudo isso pelo Lema 4.3.1. Mas D é um p-subgrupo de Sylow e então $\beta^{N_G(D)}$ deve possuir D como grupo de defeito. Por outro lado, $b_0(N_G(D))$ também deve ter o p-subgrupo de Sylow D como grupo de defeito e, por ($\Longrightarrow$), vale $b_0(N_G(D))^G = b_0(G)$. Pelo Primeiro Teorema Principal de Brauer,

$$(\beta^{N_G(D)})^G = b_0(G) = b_0(N_G(D))^G \implies \beta^{N_G(D)} = b_0(N_G(D)).$$

É importante ressaltar que esse argumento funciona justamente porque ambos os blocos $\beta^{N_G(D)}$ e $b_0(N_G(D))$ de $kN_G(D)$ possuem grupo de defeito D e, para mostrar isso, era preciso assumir que D era p-subgrupo de Sylow. Agora, como $DC_G(D)$ é normal em $N_G(D)$, sabemos que $\beta^{N_G(D)} = b_0(N_G(D))$ é o único bloco de $kN_G(D)$ que cobre β. Mas o Exercício A.4.9 (que segue do item (3) da Proposição 4.4.2) diz que $b_0(N_G(D))$ cobre apenas $b_0(DC_G(D))$, de onde concluímos que $\beta = b_0(DC_G(D))$, como preciso.

Agora, suponha que D não seja um p-subgrupo de Sylow de G. Como hipótese de indução, suponha também que, se E é um p-subgrupo de G contendo D propriamente e se γ é um bloco de $kEC_G(E)$ com grupo de defeito E e com $\gamma^G = b_0(G)$, então $\gamma = b_0(EC_G(E))$. Seja β um bloco de $kDC_G(D)$ com grupo de defeito D e com $\beta^G = b_0(G)$. Mostremos que $\beta = b_0(DC_G(D))$. Pelo Lema 4.3.1, $\beta^{N_G(D)}$ possui um grupo de defeito E contendo D. Afirmamos que E contém D propriamente. De fato, se $E = D$, então poderíamos aplicar o Primeiro Teorema Principal de Brauer para obter que $(\beta^{N_G(D)})^G = \beta^G = b_0(G)$ possui D como grupo de defeito, o que é impossível já que D não é p-subgrupo de Sylow de G. Agora, aplicando a Observação 4.4.8 para o grupo $N_G(D)$, existe um bloco γ de $kEC_{N_G(D)}(E)$ com grupo de defeito E e com $\gamma^{N_G(D)} = \beta^{N_G(D)}$. Como $D \subseteq E$, temos $C_G(E) \subseteq C_G(D) \subseteq N_G(D)$, então $C_{N_G(D)}(E) = C_G(E)$ e γ é um bloco de $kEC_G(E)$. Mas

$$\gamma^G = (\gamma^{N_G(D)})^G = (\beta^{N_G(D)})^G = \beta^G = b_0(G),$$

então a hipótese de indução nos dá $\gamma = b_0(EC_G(E))$. Por ($\Longrightarrow$), $\beta^{N_G(D)} = \gamma^{N_G(D)} = b_0(N_G(D))$. Por fim, como $DC_G(D)$ é normal em $N_G(D)$, sabemos que $\beta^{N_G(D)} = b_0(N_G(D))$ é o único bloco de $kN_G(D)$ que cobre β, então o Exercício A.4.9 implica $\beta = b_0(DC_G(D))$, concluindo a prova. □

Para essa demonstração, foi importante estudar pares da forma (Q, b), onde Q é um p-subgrupo de G e b é um bloco de $kQC_G(Q)$ com grupo de defeito Q. Esses são os **pares de Brauer**. O restante da seção lidará com uma definição mais fraca que nos permitirá obter resultados bem interessantes!

Definição 4.5.3. Dizemos que (Q, b) é um **subpar** de G se Q é um p-subgrupo de G e se b é um bloco de $kQC_G(Q)$.

Observe que não estamos fazendo nenhuma restrição a respeito do grupo de defeito de b. Mas porque estudar os blocos de $QC_G(Q)$? O primeiro motivo é que podemos passar de blocos de kG para blocos de $kQC_G(Q)$ através do Lema 4.4.6. Vimos isso em prática na demonstração do Terceiro Teorema Principal de Brauer, por exemplo. Mas também há outro motivo interessante: todo

bloco de $kQC_G(Q)$ possui um correspondente em kH para todo subgrupo H contendo $QC_G(Q)$! De fato, se b é um bloco de $QC_G(Q)$ e possui grupo de defeito D, então $Q \subseteq D$ pelo Corolário 4.2.9, porque Q é normal em $QC_G(Q)$. Assim,

$$C_H(D) \subseteq C_H(Q) \subseteq C_G(Q) \subseteq QC_G(Q) \subseteq H$$

e, pelo Lema 4.3.1, b^H está definido. Em particular, se (Q, b) é um subpar de G, então $B := b^G$ está definido. Nesse caso, dizemos que o subpar (Q, b) é um **B-subgrupo** de G. Os próximos teoremas mostrarão que B-subgrupos se comportam de modo bem parecido com p-subgrupos!

Precisamos de mais algumas definições. Se (Q, b_Q) e (R, b_R) são subpares de G, então dizemos que (R, b_R) **é normal em** (Q, b_Q) (e denotamos $(R, b_R) \lhd (Q, b_Q)$) se valem as seguintes condições:

(1) R é subgrupo normal de Q.

(2) b_R é invariante sob conjugação por Q.

(3) $(b_R)^{QC_G(R)} = (b_Q)^{QC_G(R)}$.

As condições (1) e (2) são bem naturais, mas é preciso dar alguma motivação para (3). Como R é normal em Q, vale $Q \subseteq N_G(R)$. Assim, dentro de $N_G(R)$, podemos formar o produto entre o subgrupo Q e o subgrupo normal $C_G(R)$. Isso mostra que $QC_G(R)$ é de fato um subgrupo de G. Além disso, como $R \subseteq Q$, temos a inclusão contrária $C_G(Q) \subseteq C_G(R)$ e com isso obtemos que $QC_G(R)$ é o menor subgrupo de G que contém $QC_G(Q)$ e $RC_G(R)$. Logo, a condição (3) faz sentido e nos dá uma compatibilidade: b_R e b_Q "quase" são correspondentes. Além disso, podemos subir (3) para G, obtendo $b_R^G = b_Q^G$. Isso mostra que, se $(R, b_R) \lhd (Q, b_Q)$, então (R, b_R) e (Q, b_Q) são B-subgrupos de um mesmo bloco B de kG. Essa condição também garante algumas unicidades. Por exemplo, se $(Q, b_Q) \lhd (Q, b'_Q)$, então (3) está dizendo que $b_Q = b'_Q$, o que é algo agradável. Outro tipo de unicidade aparecerá no Teorema 4.5.5.

Tendo posto a definição de subpar normal, conseguimos definir a continência de subpares. Se (Q, b_Q) e (R, b_R) são subpares de G, então dizemos que (R, b_R) **está contido em** (Q, b_Q) (e denotamos $(R, b_R) \subseteq (Q, b_Q)$) se existem subpares (R_i, b_i), para $1 \leq i \leq n$, tais que

$$(R, b_R) = (R_1, b_1) \lhd (R_2, b_2) \lhd \cdots \lhd (R_{n-1}, b_{n-1}) \lhd (R_n, b_n) = (Q, b_Q).$$

Pelo parágrafo anterior, sabemos que, se $(R, b_R) \subseteq (Q, b_Q)$, então estes subpares são B-subgrupos para um mesmo bloco B de kG. Essa definição é motivada pelas propriedades de p-grupos: lembre que um subgrupo R de um p-grupo Q é sempre *subnormal*, isto é, existe uma cadeia de subgrupos indo de R a Q onde cada subgrupo é normal em seu sucessor.

Agora, seja B um bloco de kG. Vamos definir o análogo de um p-subgrupo de Sylow para B-subgrupos! Se (Q, b_Q) é um B-subgrupo de G, então os grupos de defeito de b_Q contêm Q e, pelo Lema 4.3.1, algum grupo de defeito de B também deve conter Q. Dizemos que (Q, b_Q) é um **B-subgrupo de Sylow** de G se Q é um grupo de defeito de B. Nesse caso, (Q, b_Q) é maximal com respeito à inclusão de subpares. De fato, se $(Q, b_Q) \subseteq (R, b_R)$, então (R, b_R) é um B-subgrupo e, além disso, R contém Q e está contido em um grupo de defeito de B. Como Q já é um grupo de defeito de B, devemos ter $R = Q$ e, como vimos anteriormente, $(R, b_R) = (Q, b_Q)$.

Será que todo B-subgrupo maximal é um B-subgrupo de Sylow? A resposta é sim! O próximo teorema mostra que B-subgrupos de Sylow se comportam como p-subgrupos de Sylow.

Teorema 4.5.4. Se B é um bloco de kG, então todos os B-subgrupos de Sylow são conjugados. Além disso, se k é algebricamente fechado, todo B-subgrupo de G está contido em um B-subgrupo de Sylow.

Para o enunciado acima fazer sentido, é preciso definir a conjugação para B-subgrupos. Anteriormente, havíamos definido a conjugação de blocos apenas para blocos de subgrupos normais, mas é possível estender um pouco. De fato, se $H \leq G$, a conjugação por um elemento $g \in G$ induz

um isomorfismo de álgebras entre kH e $k[gHg^{-1}]$, então, pelos mesmos motivos do caso onde H é normal, ela leva blocos de kH em blocos de $k[gHg^{-1}]$. Com isso em mente, diremos que dois subpares (Q, b_Q) e (R, b_R) são conjugados se existir $g \in G$ tal que $R = gQg^{-1}$ e $b_R = gb_Qg^{-1}$ (pelo Exercício A.4.12, $RC_G(R)$ é o conjugado de $QC_G(Q)$ por g, então gb_Qg^{-1} é de fato um bloco de $kRC_G(R)$). Não é difícil mostrar que subpares conjugados são B-subgrupos para um mesmo bloco B de kG e, em particular, todo conjugado de um B-subgrupo de Sylow também é um B-subgrupo de Sylow (veja o Exercício A.4.14).

Demonstração: Sejam (D, b_1) e (D', b_2) dois B-subgrupos de Sylow de G e mostremos que eles são conjugados. Como D e D' são grupos de defeito de B, eles são conjugados. Assim, usando que um conjugado de um B-subgrupo de Sylow ainda é um B-subgrupo de Sylow (Exercício A.4.14), podemos assumir que $D = D'$. Como D é normal em $DC_G(D)$, os grupos de defeito de b_1 e b_2 devem conter D. Mas os grupos de defeito de $b_1^G = b_2^G = B$ possuem a ordem de D e devem conter algum grupo de defeito de b_1 e algum de b_2. Concluímos assim que D é o grupo de defeito de b_1 e de b_2. Como $b_1^{N_G(D)}$ está entre b_1 e b_1^G, um argumento similar mostra que $b_1^{N_G(D)}$ também possui grupo de defeito D e, analogamente, $b_2^{N_G(D)}$ também possui esse mesmo grupo de defeito. Logo, estamos nas condições de aplicar o Primeiro Teorema Principal de Brauer e, como $(b_1^{N_G(D)})^G = B = (b_2^{N_G(D)})^G$, deve valer $b_1^{N_G(D)} = b_2^{N_G(D)}$. Mas $DC_G(D)$ é normal em $N_G(D)$, então $b_1^{N_G(D)}$ é o único bloco de $kN_G(D)$ que cobre b_1 e $b_2^{N_G(D)}$ é o único bloco de $kN_G(D)$ que cobre b_2. Concluímos que b_1 e b_2 são cobertos por um mesmo bloco e, pelo Teorema 4.4.4, existe $g \in N_G(D)$ com $b_2 = gb_1g^{-1}$. Por isso, $g(D, b_1)g^{-1} = (gDg^{-1}, gb_1g^{-1}) = (D, b_2)$, provando que (D, b_1) e (D, b_2) são conjugados.

A segunda parte do teorema é mais complicada. Seja (Q, b_Q) um B-subgrupo maximal com respeito à inclusão de subpares. Devemos mostrar que (Q, b_Q) é um B-subgrupo de Sylow. Como $QC_G(Q)$ é normal em $N_G(Q)$, podemos considerar o estabilizador $\mathrm{Stab}(b_Q)$ de b_Q em $N_G(Q)$. Vamos trabalhar dentro de $\mathrm{Stab}(b_Q)$. Seja H um subgrupo de $\mathrm{Stab}(b_Q)$ contendo $QC_G(Q)$ e tal que $H/QC_G(Q)$ seja um p-subgrupo de Sylow de $\mathrm{Stab}(b_Q)/QC_G(Q)$. Como b_Q^H está definido e $QC_G(Q)$ é normal em H, sabemos que b_Q^H cobre b_Q e, pelo Teorema 4.4.4, possui um grupo de defeito E tal que $R \coloneqq E \cap QC_G(Q)$ é um grupo de defeito de b_Q. Note que H estabiliza b_Q (pois $H \subseteq \mathrm{Stab}(b_Q)$), então, como estamos supondo k algebricamente fechado, segue do Teorema 4.4.4 que

$$[E : R] = [E : E \cap QC_G(Q)] = [H : QC_G(Q)]_p = [H : QC_G(Q)],$$

onde a última igualdade segue do fato de $H/QC_G(Q)$ ser um p-grupo. Manipulando essa igualdade, chegamos em

$$|EQC_G(Q)| = \frac{|E| \cdot |QC_G(Q)|}{|E \cap QC_G(Q)|} = \frac{|E| \cdot |QC_G(Q)|}{|R|} = |H|$$

e então $H = EQC_G(Q)$. Como Q é normal em $QC_G(Q)$, vale $Q \subseteq R$ e então $Q \subseteq E$. Com isso, podemos escrever $H = EC_G(Q)$.

Agora, aplicando a Observação 4.4.8 ao bloco b_Q^H de kH, podemos encontrar um bloco b_E de $kEC_H(E)$ com grupo de defeito E tal que $b_E^H = b_Q^H$ e, como $H = EC_G(Q)$, podemos escrever isso como $b_E^{EC_G(Q)} = b_Q^{EC_G(Q)}$. Como $Q \subseteq E$, então

$$C_G(E) \subseteq C_G(Q) \subseteq QC_G(Q) \subseteq H$$

e vale $C_H(E) = C_G(E)$, de onde segue que $EC_H(E) = EC_G(E)$ e (E, b_E) é um subpar de G. Por construção, todos os grupos obtidos até agora estão contidos em $\mathrm{Stab}(b_Q) \subseteq N_G(Q)$, então vemos que Q é subgrupo normal de E e E estabiliza b_Q. Como $b_E^{EC_G(Q)} = b_Q^{EC_G(Q)}$, obtemos $(Q, b_Q) \lhd (E, b_E)$. Mas (Q, b_Q) é maximal com relação à inclusão de subpares, de onde obtemos $Q = E$. Com isso, concluímos que $Q = R$, logo Q é um grupo de defeito de b_Q, e que $H = EC_G(Q) = QC_G(Q)$, então

$$[\mathrm{Stab}(b_Q) : QC_G(Q)]_p = [H : QC_G(Q)] = 1.$$

Pela demonstração do Lema 4.4.6, $b_Q^{N_G(Q)}$ é um bloco de $kN_G(Q)$ com grupo de defeito Q, então podemos aplicar o Primeiro Teorema Principal de Brauer para concluir que $B = b_Q^G = (b_Q^{N_G(Q)})^G$ possui Q como um grupo de defeito. Isso prova que (Q, b_Q) é um B-subgrupo de Sylow, como queríamos. □

O Teorema 4.5.4 possui uma interpretação interessante para o cálculo do grupo de defeito de b^G, que explicaremos agora. Seja H um subgrupo de G e seja b um bloco de kH com grupo de defeito Q. Suponha que $C_G(Q) \subseteq H$, de modo que $B = b^G$ está definido. Para calcular o grupo de defeito de B, podemos proceder da seguinte forma. Com o Lema 4.4.6, encontramos um bloco b_Q de $kQC_G(Q)$ (note que $C_G(Q) = C_H(Q)$, pois $C_G(Q) \subseteq H$) com grupo de defeito Q e tal que $b_Q^H = b$. Como $b_Q^G = b^G = B$, o subpar (Q, b_Q) é um B-subgrupo de G. Pelo Teorema 4.5.4 (e por sua demonstração), conseguimos encontrar um B-subgrupo de Sylow (D, b_D) que contém (Q, b_Q). Assim, D é um grupo de defeito de B. Observe que apenas precisamos conhecer a estrutura local de G para determinar D! Até o correspondente de Brauer de B é determinado localmente, pois $b_D^{N_G(D)}$ possui grupo de defeito D e satisfaz $(b_D^{N_G(D)})^G = b_D^G = B$, então $b_D^{N_G(D)}$ é o correspondente de Brauer de B.

Seja (Q, b_Q) um B-subgrupo de G, onde B é um bloco de kG. Pelo Teorema 4.5.4, podemos encontrar um grupo de defeito D de B e um bloco b_D de $kDC_G(D)$ tal que $(Q, b_Q) \subseteq (D, b_D)$. Mas, se tomarmos um p-subgrupo R com $Q \subseteq R \subseteq D$, existe um B-subgrupo (R, b_R) tal que $(Q, b_Q) \subseteq (R, b_R)$? Ou então se $R \subseteq Q$, existe um B-subgrupo (R, b_R) com $(R, b_R) \subseteq (Q, b_Q)$? O próximo resultado responde afirmativamente essas perguntas e, em alguns casos, ainda diz que (R, b_R) é único!

Teorema 4.5.5. Se (P, b_P) é um subpar de G e Q é um subgrupo de P, então existe um único bloco de b_Q de $kQC_G(Q)$ tal que $(Q, b_Q) \subseteq (P, b_P)$. Além disso, se Q é normal em P, então $(Q, b_Q) \lhd (P, b_P)$.

Mostremos como esse teorema responde as perguntas anteriores. Com a notação de antes, se $R \subseteq Q$, então o teorema acima diz que existe um único subpar (R, b_R) contido em (Q, b_Q). Por outro lado, se $Q \subseteq R \subseteq D$, então existe um único subpar (R, b_R) contido em (D, b_Q) e, aplicando o teorema mais uma vez, encontramos um único subpar (Q, b'_Q) contido em (R, b_R). Mas então (Q, b_Q) e (Q, b'_Q) são ambos subpares contidos em (D, b_D) e, pela unicidade do teorema, $b_Q = b'_Q$, mostrando que (Q, b_Q) está contido em (R, b_R), como queríamos. Nesse segundo caso, o teorema não garante a unicidade de (R, b_R) (só conseguimos a unicidade pedindo que $(R, b_R) \subseteq (D, b_D)$ também).

Também temos uma consequência interessante quando olhamos para o bloco principal. Se Q é um p-subgrupo de G, então $(Q, b_0(QC_G(Q)))$ é um subpar. Mais ainda, pelo Terceiro Teorema Principal de Brauer, $b_0(QC_G(Q))^G = b_0(G)$ e então $(Q, b_0(QC_G(Q)))$ é um $b_0(G)$-subgrupo de G. Por outro lado, se (Q, b) é um $b_0(G)$-subgrupo, a outra direção do Terceiro Teorema Principal de Brauer nos dá $b = b_0(QC_G(Q))$. Ou seja, existe uma bijeção entre $b_0(G)$-subgrupos e p-subgrupos! Além disso, se $Q \subseteq P$, então o Teorema 4.5.5 junto com o que acabamos de ver mostra que $(Q, b_0(QC_G(Q))) \subseteq (P, b_0(PC_G(P)))$. Logo, $Q \subseteq P$ se e só se $(Q, b_0(QC_G(Q))) \subseteq (P, b_0(PC_G(P)))$ e essa bijeção preserva inclusões! Pela segunda parte do Teorema 4.5.5, ela também preserva normalidade. Isso mostra que $b_0(G)$-subgrupos são essencialmente p-subgrupos!

Para provar o Teorema 4.5.5, vamos começar com um lema:

Lema 4.5.6. Seja (P, b_P) um subpar de G.

(1) Se Q é um subgrupo normal de P, então existe um único bloco b_Q de $kQC_G(Q)$ tal que $(Q, b_Q) \lhd (P, b_P)$.

(2) Se R e Q são subgrupos de P com $R \subseteq Q$ e se (R, b_R) e (Q, b_Q) são subpares normais em (P, b_P), então $(R, b_R) \lhd (Q, b_Q)$.

Demonstração: Vamos começar com (1). Como Q é normal em P, então $QC_G(Q)$ é normal em $PC_G(Q)$. De fato, é imediato que $gQC_G(Q)g^{-1} = QC_G(Q)$ se $g \in C_G(Q)$ e, por outro lado, o Exercício A.4.12 nos dá

$$gQC_G(Q)g^{-1} = (gQg^{-1})C_G(gQg^{-1}) = QC_G(Q)$$

se $g \in P$, já que $gQg^{-1} = Q$ por Q ser normal em P. Assim, o bloco $b_P^{PC_G(Q)}$ cobre algum bloco b_Q de $kQC_G(Q)$. Como $b_Q^{PC_G(Q)}$ está definido, este é o único bloco de $kPC_G(Q)$ que cobre b_Q e devemos ter $b_Q^{PC_G(Q)} = b_P^{PC_G(Q)}$. Dessa forma, para mostrar que $(Q, b_Q) \lhd (P, b_P)$, resta mostrar que P estabiliza b_Q. Como P é normal em $PC_G(P)$, então P está contido em um grupo de defeito de b_P. Logo, P também está contido em algum grupo de defeito de $b_P^{PC_G(Q)} = b_Q^{PC_G(Q)}$ e, pelo item (3) do Teorema 4.4.4, P possui um conjugado em $PC_G(Q)$ que está contido no estabilizador $\mathrm{Stab}(b_Q)$ de b_Q em $PC_G(Q)$. Seja $g \in PC_G(Q)$ tal que $gPg^{-1} \subseteq \mathrm{Stab}(b_Q)$. Escrevendo g como o produto de um elemento de $C_G(Q)$ por um elemento de P, sabemos que P é invariante pela conjugação por esse elemento de P, então podemos supor que $g \in C_G(Q)$. Logo, para todo $x \in P$, vale

$$gxg^{-1}b_Qgx^{-1}g^{-1} = b_Q \implies x(g^{-1}b_Qg)x^{-1} = g^{-1}b_Qg \implies xb_Qx^{-1} = b_Q,$$

onde utilizamos que $g^{-1}b_Qg = b_Q$ porque $g^{-1} \in C_G(Q) \subseteq QC_G(Q) \subseteq \mathrm{Stab}(b_Q)$. Isso mostra que P estabiliza b_Q, como preciso.

Com isso, mostramos que existe um subpar (Q, b_Q) normal em (P, b_P). Mais ainda, mostramos que P e $C_G(Q)$ estão contidos em $\mathrm{Stab}(b_Q)$, que por sua vez é um subgrupo de $PC_G(Q)$. Logo, deve valer $\mathrm{Stab}(b_Q) = PC_G(Q)$ e segue que b_Q não possui outros conjugados na ação por $PC_G(Q)$. Portanto, b_Q é o único bloco de $kQC_G(Q)$ coberto por $b_Q^{PC_G(Q)}$. Assim, se (Q, b'_Q) é outro subpar normal em (P, b_P), então b'_Q é coberto por $(b'_Q)^{PC_G(Q)}$ e, pela hipótese da normalidade, isso é igual a $b_P^{PC_G(Q)} = b_Q^{PC_G(Q)}$. Como b_Q é o único bloco coberto por $b_Q^{PC_G(Q)}$, concluímos que $b_Q = b'_Q$. Com isso, provamos que b_Q é o único bloco de $kQC_G(Q)$ de modo que $(Q, b_Q) \lhd (P, b_Q)$. Isso conclui o item (1).

Vamos para o item (2). Como $(R, b_R) \lhd (P, b_P)$, então R é normal em P e P estabiliza b_R. Como $Q \subseteq P$, segue que R é normal em Q e Q estabiliza b_R. Logo, para provar que $(R, b_R) \lhd (Q, b_Q)$, resta verificar que $b_R^{QC_G(R)} = b_Q^{QC_G(R)}$. Primeiramente, note que $QC_G(R)$ é normal em $PC_G(R)$. Para mostrar isso, basta proceder como no início da demonstração e usar que R e Q são normais em P. Vamos mostrar que $b_R^{QC_G(R)}$ e $b_Q^{QC_G(R)}$ não possuem conjugados em $PC_G(R)$. Provaremos isso apenas para $b_R^{QC_G(R)}$, já que para o outro bloco será análogo. Como $b_R^{QC_G(R)}$ é um bloco de $kQC_G(R)$, ele é certamente estabilizado por $C_G(R)$. Vejamos que ele também é estabilizado por P. Seja $x \in P$. Como P estabiliza b_R, vale $xb_Rx^{-1} = b_R$. Logo, utilizando a definição da correspondência de blocos e o item (a) do Exercício A.4.14, temos:

$$b_R = xb_Rx^{-1} \cong {}^{(x,x)}b_R \mid {}^{(x,x)}(B_S) = \left({}^{(x,x)}B\right)_S \cong (xBx^{-1})_S,$$

onde B denota $b_R^{QC_G(R)}$ e S denota $RC_G(R) \times RC_G(R)$. Segue então que xBx^{-1} corresponde a b_R, ou seja, o conjugado de $b_R^{QC_G(R)}$ por x é ele mesmo, como queríamos. Assim, como $b_R^{QC_G(R)}$ não possui conjugados em $PC_G(R)$, então ele é o único bloco de $kQC_G(R)$ coberto por

$$(b_R^{QC_G(R)})^{PC_G(R)} = b_R^{PC_G(R)}.$$

Analogamente, $b_Q^{QC_G(R)}$ é o único bloco de $kQC_G(R)$ coberto por $b_Q^{PC_G(R)}$. Por isso, para mostrar que $b_R^{QC_G(R)} = b_Q^{QC_G(R)}$, basta verificar que $b_R^{PC_G(R)} = b_Q^{PC_G(R)}$. De fato, por um lado temos

$$b_R^{PC_G(R)} = b_P^{PC_G(R)},$$

pois $(R, b_R) \lhd (P, b_P)$. Por outro lado, utilizando que $(Q, b_Q) \lhd (P, b_P)$, temos

$$b_Q^{PC_G(R)} = (b_Q^{PC_G(Q)})^{PC_G(R)} = (b_P^{PC_G(Q)})^{PC_G(R)} = b_P^{PC_G(R)},$$

concluindo a demonstração. □

Agora, conseguimos demonstrar o Teorema 4.5.5.

Demonstração: O item (1) do Lema 4.5.6 mostra a segunda afirmação do Teorema 4.5.5. Agora, se Q é um subgrupo do p-subgrupo P de G, então Q é subnormal em P, ou seja, existe uma cadeia de subgrupos indo de Q até P onde cada subgrupo é normal em seu sucessor. Portanto, repetidas aplicações do item (1) do Lema 4.5.6 garante a existência de um bloco b_Q de $kQC_G(Q)$ tal que $(Q, b_Q) \subseteq (P, b_P)$. Resta mostrar que b_Q é único.

Provaremos a unicidade de b_Q por indução no índice $[P : Q]$. Se $[P : Q] = 1$, ou seja, se $P = Q$, então mostramos logo após a definição de normalidade de subpares que $(Q, b_Q) \subseteq (Q, b_P)$ implica em $b_Q = b_P$ e, portanto, existe um único bloco b_Q com $(Q, b_Q) \subseteq (Q, b_P)$. Suponha agora que $[P : Q] > 1$ e que o resultado seja válido para índices menores do que $[P : Q]$. Sejam b_Q e b'_Q blocos de $kQC_G(Q)$ tais que (Q, b_Q) e (Q, b'_Q) estão contidos em (P, b_P). Como Q está contido propriamente em P, segue da definição de continência de subpares que podemos encontrar subpares (R, b_R) e $(R', b_{R'})$ satisfazendo $Q \subseteq R, R' \subsetneq P$ e

$$(Q, b_Q) \subseteq (R, b_R) \lhd (P, b_P) \quad \text{e} \quad (Q, b'_Q) \subseteq (R', b_{R'}) \lhd (P, b_P).$$

Como R e R' são normais em P, então $S := R \cap R'$ também é. Pelo item (1) do Lema 4.5.6, existe um subpar (S, b_S) normal em (P, b_P). Pelo item (2) desse mesmo lema, também sabemos que (S, b_S) está contido e é normal em (R, b_R) e em $(R', b_{R'})$. Como $Q \subseteq S$, o primeiro parágrafo garante a existência de um subpar (Q, b''_Q) contido em (S, b_S). Logo, como (Q, b_Q) e (Q, b''_Q) estão contidos em (R, b_R) e $[R : Q] < [P : Q]$, a hipótese de indução nos dá $b_Q = b''_Q$. Da mesma maneira, como (Q, b'_Q) e (Q, b''_Q) estão contidos em $(R', b_{R'})$ e $[R' : Q] < [P : Q]$, a hipótese de indução também nos dá $b'_Q = b''_Q$. Concluímos que $b_Q = b'_Q$ e a unicidade do enunciado está provada. □

Observação 4.5.7. Se B é um bloco de kG com grupo de defeito D, então a Observação 4.4.8 garante a existência de um B-subgrupo (D, b_D). O teorema que acabamos de demonstrar nos permite descer ainda mais: dado um subgrupo Q de D, existe um B-subgrupo (Q, b_Q). Isso nos permite conectar o bloco B com blocos de vários subgrupos de G diferentes de $DC_G(D)$! Podemos utilizar isso, por exemplo, para obter uma generalização de um resultado comentado anteriormente: para todo subgrupo Q de D, existe um kG-módulo indecomponível pertencente a B com vértice Q. Para uma demonstração, veja a solução do Exercício A.4.15.

Capítulo 5

Blocos com grupo de defeito cíclico

Este capítulo se dedica à demonstração de um dos grandes resultados da teoria de representações modulares: a descrição da estrutura das representações de blocos com grupo de defeito cíclico.

Já vimos no Corolário 4.3.7 que um bloco com grupo de defeito trivial é precisamente um bloco simples como álgebra, ou seja, isomorfo a uma álgebra de matrizes sobre uma álgebra de divisão. O próximo passo é entender os blocos com defeito um ou, um pouco mais geralmente, os blocos com grupo de defeito cíclico. Conseguimos demonstrar um resultado muito análogo ao Teorema 3.2.7: esses são precisamente os blocos com tipo de representação finito! Esse teorema motiva a busca de uma classificação de todos os módulos indecomponíveis sobre um desses blocos, já que há um número finito de módulos a se encontrar. Nesse sentido, como veremos, tais blocos são *álgebras de Brauer*.

Após introduzir as álgebras de Brauer, a primeira seção mostra como quase todos os exemplos retratados anteriormente são casos particulares desse novo conceito. Enunciamos o nosso objetivo final, o Teorema 5.1.7, e apresentamos um roteiro de sua prova, que será executada nas seções posteriores. Será uma demonstração bem longa e utilizaremos quase todas as ferramentas e os resultados elaborados até agora. Mesmo assim, há muita coisa interessante no meio do caminho e, de sobra, terminamos o material com um teorema que reflete um pouco da beleza da teoria de representações modulares de grupos finitos!

5.1 Considerações iniciais

Observação 5.1.1. A partir de agora e até o fim, assumiremos que o corpo k é algebricamente fechado. Precisamos dessa hipótese para provar o resultado que almejamos.

Já vimos alguns exemplos de como o grupo de defeito pode controlar a complexidade de um bloco. De certa forma, o grupo de defeito de um bloco se comporta como um "p-subgrupo de Sylow" do bloco. Por exemplo, se os p-subgrupos de Sylow de G são triviais, então p não divide $|G|$ e kG é semissimples pelo Teorema de Maschke. No caso dos blocos, temos um resultado análogo: se um bloco possui um grupo de defeito trivial, então ele é uma álgebra semissimples. O Teorema 3.2.7 também possui um análogo para blocos se trocarmos os p-subgrupos de Sylow por grupos de defeito!

Proposição 5.1.2. Seja B um bloco de kG com grupo de defeito D. Então B tem tipo de representação finito se, e somente se, D é cíclico.

A demonstração a seguir é baseada nos livros [3] e [23].

Demonstração. ($\Longleftarrow$) Suponha que D seja cíclico. Se U é um kG-módulo indecomponível pertencente a B, então U possui um vértice Q contido em D pelo Teorema 4.2.2. Assim, como U é relativamente Q-projetivo, U também é relativamente D-projetivo e podemos tomar um kD-módulo indecomponível S tal que $U \mid S^G$ (para encontrar S, utiliza-se o argumento usual

para se encontrar uma fonte). Isso mostra que todo kG-módulo indecomponível pertencente a B é somando direto da indução de um kD-módulo indecomponível. Como D é cíclico, então kD tem tipo de representação finito pelo Exemplo 2.1.12. Como existe um número finito de kD-módulos indecomponíveis e como a indução de cada um desses módulos possui um número finito de somandos indecomponíveis, concluímos que há um número finito de kG-módulos indecomponíveis pertencentes a B. Pelo Exercício A.4.3, B tem tipo de representação finito.

($\Longrightarrow$) Suponha que D não seja cíclico. A ideia para mostrar que B não possui tipo de representação finito é análoga à do Teorema 3.2.7, mas devemos tomar cuidado para construir módulos indecomponíveis que pertençam a B e, por isso, a prova será mais complicada. Pelo Exercício A.3.7, existe um subgrupo normal N de D tal que $D/N \cong C_p \times C_p$. Agora, pelo Exemplo 2.1.14, $k[C_p \times C_p]$ não possui tipo de representação finito. Como todo subgrupo próprio de $C_p \times C_p$ é cíclico, podemos argumentar como no parágrafo anterior para mostrar que há apenas um número finito de $k[C_p \times C_p]$-módulos indecomponíveis com vértice propriamente contido em $C_p \times C_p$. Isso mostra que existem infinitos $k[C_p \times C_p]$-módulos indecomponíveis não isomorfos cujo vértice é $C_p \times C_p$.

Seja $\overline{U}$ um $k[C_p \times C_p]$-módulo indecomponível com vértice $C_p \times C_p$. Como $D/N \cong C_p \times C_p$, podemos ver $\overline{U}$ como um kD-módulo no qual N age trivialmente. Denotaremos esse kD-módulo por U. Note que U é indecomponível, já que essa passagem preserva submódulos. Provaremos que U possui D como vértice. Se Q é um vértice de U, então U é relativamente Q-projetivo e vale $U \mid (U_Q)^D$. Vamos mostrar que $N \subseteq Q$. De fato, pela Fórmula de Decomposição de Mackey,

$$((U_Q)^D)_N \cong \bigoplus_{g \in [N\backslash D/Q]} (({}^g(U_Q))_{N \cap gQg^{-1}})^N.$$

Pelo Exercício A.3.4,

$$({}^g(U_Q))_{N \cap gQg^{-1}} = {}^g((U_Q)_{g^{-1}Ng \cap Q}) = {}^g(U_{N \cap Q}),$$

onde utilizamos que N é normal em D. Mas N age trivialmente em U, então $U_{N\cap Q} \cong (k_{N\cap Q})^n$, onde $n := \dim_k U$. Conjugar o módulo trivial ainda fornece um módulo trivial, então concluímos que

$$((U_Q)^D)_N \cong \bigoplus_{g \in [N\backslash D/Q]} \bigoplus_{i=1}^{n} (k_{N \cap gQg^{-1}})^N.$$

Mas N é um p-grupo, então o Corolário 3.2.17 implica que a decomposição acima é a decomposição de $((U_Q)^D)_N$ como soma de indecomponíveis. Como $U \mid (U_Q)^D$, então U_N é somando direto de $((U_Q)^D)_N$. Como N age trivialmente em U, segue que $k_N \mid ((U_Q)^D)_N$ e, pelo Teorema de Krull-Schmidt,

$$k_N \cong (k_{N \cap gQg^{-1}})^N$$

para algum $g \in D$. Comparando dimensões, obtemos $N \cap gQg^{-1} = N$, isto é, $N \subseteq gQg^{-1}$ e então $N = g^{-1}Ng \subseteq Q$, como desejado.

Agora, como $N \subseteq Q$, N é normal em D e N age trivialmente em U, podemos imitar o argumento dado no Lema 4.4.9 para mostrar que N age trivialmente em $(U_Q)^D$. Logo, podemos ver $(U_Q)^D$ como um $k[C_p \times C_p]$-módulo e ele é isomorfo a

$$(\overline{U}_{\overline{Q}})^{C_p \times C_p},$$

onde $\overline{Q}$ denota o subgrupo de $C_p \times C_p \cong D/N$ correspondente a Q/N. Com isso tudo, concluímos que

$$\overline{U} \mid (\overline{U}_{\overline{Q}})^{C_p \times C_p}$$

e então $\overline{U}$ é relativamente $\overline{Q}$-projetivo. Mas $C_p \times C_p$ é vértice de $\overline{U}$, então obtemos que $\overline{Q} = C_p \times C_p$. Como $N \subseteq Q$, concluímos que $Q = D$, ou seja, D é um vértice de U. Como existem infinitos

$k[C_p \times C_p]$-módulos indecomponíveis não isomorfos com vértice $C_p \times C_p$, isso mostra que existem infinitos kD-módulos indecomponíveis não isomorfos com vértice D e resta levantar esses módulos para kG-módulos indecomponíveis pertencentes a B.

Seja U um kD-módulo indecomponível com vértice D. Como D é um p-grupo, o soco de U contém um submódulo isomorfo ao módulo trivial k_D. Portanto, $U^{N_G(D)}$ contém um submódulo isomorfo a $(k_D)^{N_G(D)}$ que, por sua vez, é isomorfo a $k[N_G(D)/D]$ visto como um $kN_G(D)$-módulo (veja o Exemplo 3.1.8). Como D é p-subgrupo normal de $N_G(D)$, a Proposição 1.3.14 mostra que D age trivialmente em todo $kN_G(D)$-módulo simples, então todo $kN_G(D)$-módulo simples pode ser visto como um $k[N_G(D)/D]$-módulo simples e é fator de composição de $k[N_G(D)/D]$. Isso mostra que todo $kN_G(D)$-módulo simples é fator de composição de $U^{N_G(D)}$ e, dessa forma, nenhum bloco de $kN_G(D)$ pode anular $U^{N_G(D)}$.

Logo, se b é o correspondente de Brauer de B (em $kN_G(D)$), então $U^{N_G(D)}$ possui um somando indecomponível U' pertencente a b. Como D é normal em $N_G(D)$, o Exemplo 3.1.14 mostra que $(U^{N_G(D)})_D$ é uma soma de conjugados de U em $N_G(D)$ e, como U possui D como vértice, cada um desses conjugados tem esse mesmo vértice. Pelo Exercício A.3.10, U' possui vértice D e, pelo item (3) do Teorema 3.2.12, suas fontes são os conjugados de U em $N_G(D)$.

Em resumo, dado um kD-módulo indecomponível U com vértice D, é possível encontrar um $kN_G(D)$-módulo indecomponível U' pertencente a b com vértice D e cujas fontes são os conjugados de U em $N_G(D)$. Mas U possui um número finito de conjugados e existem infinitos kD-módulos indecomponíveis não isomorfos com vértice D. Concluímos então que existem infinitos $kN_G(D)$-módulos indecomponíveis não isomorfos pertencentes a b e com vértice D. Aplicando a Correspondência de Green e utilizando o Corolário 4.3.5, encontramos infinitos kG-módulos indecomponíveis não isomorfos pertencentes a B, provando que B não possui tipo de representação finito. □

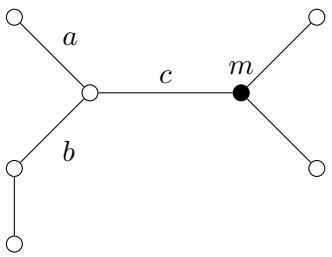
Por conta deste resultado, temos uma esperança maior de conseguir classificar os blocos com grupo de defeito cíclico. E isso é possível! Não saberemos dizer exatamente a qual álgebra "canônica" o bloco é isomorfo, mas conseguiremos descrever em detalhes os módulos projetivos indecomponíveis pertencentes ao bloco!

Precisaremos definir o que é uma álgebra de Brauer e, para isso, vamos introduzir um conceito preliminar. Uma **árvore de Brauer** é um grafo finito, conexo e acíclico munido de mais duas informações:

(1) Uma ordenação circular das arestas emanando de cada vértice.

(2) Um inteiro positivo, chamado de **multiplicidade**, associado a um dos vértice do grafo, chamado de **vértice excepcional**.

Vamos esclarecer algumas dessas propriedades. Um grafo acíclico é um grafo que não possui ciclos, isto é, não existe um caminho passando por arestas distintas que começa e termina em um mesmo vértice. Equivalentemente, um grafo finito conexo é acíclico se dados dois vértices do grafo existe um único caminho que os liga sem repetir arestas. Graficamente, um grafo finito, conexo e acíclico é uma árvore, como esta:



Se $e_1, \ldots, e_n$ são as arestas que incidem em um dado vértice, então a ordenação circular é apenas uma ordenação dessas arestas onde não se fixa a aresta inicial. Por exemplo, podemos

determinar que depois de e_1 vem e_2, depois e_3, depois e_4, e assim em diante, até chegarmos em e_n, que tem como sucessor a aresta e_1. Um jeito útil de lembrar essa ordenação é desenhar a árvore de Brauer de modo que a ordem circular das arestas corresponda exatamente a percorrer as arestas no desenho em sentido anti-horário. Se o desenho anterior representa uma árvore de Brauer desenhada respeitando a ordenação, então as arestas a, b e c incidem sobre o mesmo vértice e a ordem delas é a, depois b, depois c e então retornamos para a.

Sempre é possível desenhar a árvore de Brauer dessa forma. De fato, comece com um vértice qualquer e desenhe as arestas que incidem sobre ele na ordem correta e de modo que fiquem igualmente espaçadas. Em seguida, escolha um outro vértice que é um extremo de uma aresta já desenhada e repita o processo. Provavelmente você terá que desenhar as novas arestas muito mais curtas para que elas não choquem com o resto do desenho. Prosseguindo assim, a árvore estará desenhada com a ordenação correta. Ela não estará visualmente agradável, então basta "deslizar" e "esticar" algumas arestas para deixar o desenho mais bonito. Portanto, dar a ordenação é equivalente a desenhar a árvore no plano e, a partir de agora, a ordenação que consideraremos nos exemplos sempre será dada pelo desenho.

Por fim, representaremos o vértice excepcional com uma bola preenchida. A depender do caso, deixaremos a multiplicidade indicada no desenho. No exemplo, o vértice excepcional possui multiplicidade m. Quando o vértice excepcional tiver multiplicidade 1, não o marcaremos no desenho, porque, como veremos, um vértice com multiplicidade 1 se comporta como um vértice qualquer e não há necessidade de distingui-lo.

Agora podemos definir as álgebras que queríamos. Uma álgebra de dimensão finita A é chamada uma **álgebra de Brauer** se existem uma árvore de Brauer e uma bijeção entre as arestas da árvore e as classes de isomorfismo de A-módulos simples de modo que a árvore determine a estrutura dos A-módulos projetivos indecomponíveis segundo um algoritmo que agora explicaremos. Se S é um A-módulo simples e a sua cobertura projetiva é P, então vale $P/\operatorname{rad}(P) \cong \operatorname{soc}(P) \cong S$ e $\operatorname{soc}(P) \subseteq \operatorname{rad}(P)$. Além disso, $\operatorname{rad}(P)/\operatorname{soc}(P)$ é a soma de dois módulos unisseriados, cujos fatores são determinados do seguinte modo: sejam v e w os extremos da aresta correspondente a S e sejam $T_1, \ldots, T_n$ e $U_1, \ldots, U_{n'}$ os A-módulos simples correspondentes às arestas incidindo sobre v e w, respectivamente, sem contar com S. Suponha também que a ordenação das arestas seja tal que, em v, S é seguido por T_1, depois por T_2, $\ldots$, depois por T_n e então voltamos para S e, em w, S é seguido por U_1, depois por U_2, $\ldots$, depois por $U_{n'}$ e então voltamos para S. Então $\operatorname{rad}(P)/\operatorname{soc}(P)$ é a soma direta dos A-módulos unisseriados P_v e P_w, onde os fatores de composição de P_v são dados (em ordem e começando com $P_v/\operatorname{rad}(P_v)$) por

$$T_1, T_2, T_3, \ldots, T_n$$

e os fatores de composição de P_w são dados (em ordem e começando com $P_w/\operatorname{rad}(P_w)$) por

$$U_1, U_2, U_3, \ldots, U_{n'}.$$

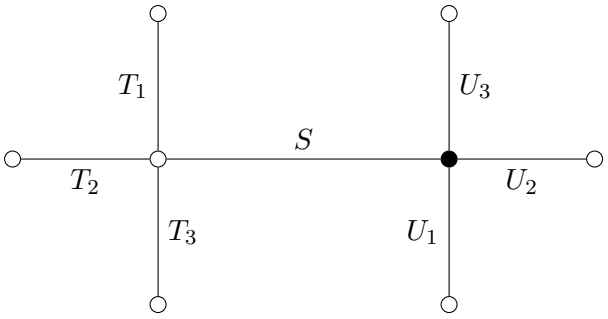
Devemos fazer algumas modificações em alguns casos especiais. Se v possui apenas a aresta de S incidindo sobre ele, então $P_v = 0$. Por outro lado, se v é o vértice excepcional e possui multiplicidade m, então os fatores de composição de P_v são, na verdade,

$$T_1, T_2, \ldots, T_n, S, T_1, T_2, \ldots, T_n, S, T_1, \ldots \quad \ldots, T_n, S, T_1, T_2, \ldots, T_n,$$

onde S aparece $m-1$ vezes e cada T_i aparece m vezes (se $m = 1$, note que isso é o mesmo que o caso usual).

Para esclarecer, vamos dar um exemplo e explicar melhor como é esse algoritmo. Suponha

que A seja uma álgebra de Brauer com a seguinte árvore de Brauer:



Já nomeamos cada aresta de acordo com o módulo simples associado. Vamos determinar a estrutura da cobertura projetiva P do módulo S. Sejam v e w os vértices de S, onde w denota o vértice excepcional à direita, que possui multiplicidade m. Segundo o algoritmo, P_v é unisseriado e seus fatores de composição são

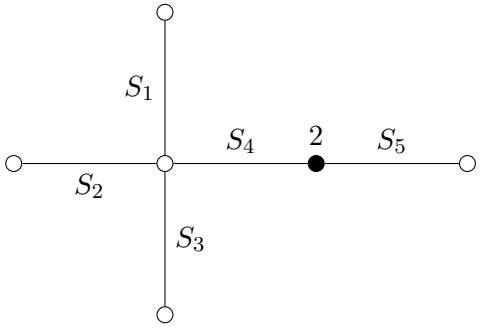
$$T_1, T_2, T_3,$$

nessa ordem. Observe que estamos dando uma volta torno do vértice v, começando imediatamente após S e terminando imediatamente antes de S. No caso do vértice w, que é excepcional, faremos esse mesmo processo, mas dessa vez daremos m voltas em torno de w, começando imediatamente após S e terminando imediatamente antes de S. Por exemplo, se $m = 3$, damos três voltas e obtemos que P_w é unisseriado com fatores de composição

$$U_1, U_2, U_3, S, U_1, U_2, U_3, S, U_1, U_2, U_3,$$

nessa ordem. Assim, vale $P/\operatorname{rad}(P) \cong \operatorname{soc}(P) \cong S$ e $\operatorname{rad}(P)/\operatorname{soc}(P) \cong P_v \oplus P_w$.

Daremos mais um exemplo hipotético. Suponha que A seja uma álgebra de Brauer com a seguinte árvore de Brauer:



Seja P a cobertura projetiva de S_5 e sejam v e w os extremos de S_5, onde v é o vértice excepcional. Então $P_w = 0$ e P_v é unisseriado com fatores de composição

$$S_4, S_5, S_4.$$

Note que demos duas voltas em torno de v, pois sua multiplicidade é 2. Logo, P é unisseriado com fatores de composição

$$S_5, S_4, S_5, S_4, S_5.$$

Podemos colocar essa informação numa figura:

$$\begin{matrix} S_5 \\ S_4 \\ S_5 \\ S_4 \\ S_5 \end{matrix}$$

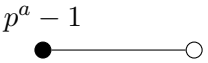
Analogamente, as figuras que representam a estrutura das coberturas projetivas de S_1, S_2, S_3 e S_4 são, respectivamente,

$$\begin{array}{cccc} S_1 & S_2 & S_3 & \\ S_2 & S_3 & S_4 & \\ S_3, & S_4, & S_1 & \text{e} \\ S_4 & S_1 & S_2 & \\ S_1 & S_2 & S_3 & \end{array} \qquad \begin{array}{ccc} & S_4 & \\ S_1 & & S_5 \\ S_2 & \oplus & S_4. \\ S_3 & & S_5 \\ & S_4 & \end{array}$$

A última representação simboliza que, se Q denota a cobertura projetiva de S_4, então $\operatorname{soc}(Q) \subseteq \operatorname{rad}(Q)$ e $\operatorname{rad}(Q)/\operatorname{soc}(Q)$ é a soma direta de um módulo unisseriado com fatores de composição S_1, S_2 e S_3 com um módulo unisseriado com fatores de composição S_5, S_4 e S_5.

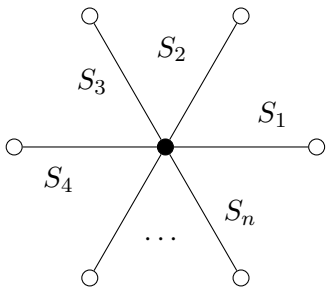
Chegamos nos exemplos concretos!

Exemplo 5.1.3. Seja $G = C_n$ o grupo cíclico de ordem n e escreva $n = p^a m$, onde m não é divisível por p. Suponha que $a \geq 1$. Vimos no Exemplo 2.2.10 como é a estrutura dos kC_n-módulos projetivos indecomponíveis. Note que cada kC_n-módulo simples é fator de composição apenas de sua cobertura projetiva, então módulos simples não isomorfos pertencem a blocos distintos. Além disso, a cobertura projetiva de um módulo simples é unisseriada de comprimento p^a. Com isso, conseguimos concluir que cada bloco de kC_n é uma álgebra de Brauer! A árvore de Brauer correspondente é:



De fato, se P é a cobertura projetiva do único módulo simples S representado pela árvore e se v e w são os vértices acima, onde v é excepcional, então o algoritmo diz que $P_w = 0$ e que P_v é unisseriado com comprimento $p^a - 2$ e seu único fator de composição é S. Acrescentando $P/\operatorname{rad}(P)$ e $\operatorname{soc}(P)$, temos que P é unisseriado de comprimento p^a e S é o seu único fator de composição, como deveria ser.

Exemplo 5.1.4. Generalizando o exemplo anterior, suponha que G possua um p-subgrupo de Sylow normal e cíclico. Pelo Exemplo 2.2.12, existe um kG-módulo W de dimensão 1 cujas potências tensoriais nos permitem encontrar os fatores de composição dos kG-módulos projetivos indecomponíveis, que são unisseriados. Com isso, se B é um bloco de kG, então os kG-módulos simples $S_1, \ldots, S_n$ pertencentes a B podem ser listados de modo que $S_i \otimes W \cong S_{i+1}$, se $1 \leq i < n$, e $S_n \otimes W \cong S_1$. Isso segue do Exercício A.4.7 e do fato de que $W^{\otimes n'} \cong k$ para algum $n' \geq 1$. Note que isso nos dá uma ordenação circular destes módulos e, pelo Exemplo 2.2.12, os fatores de composição dos projetivos indecomponíveis são dados percorrendo essa ordenação! Assim, B é uma álgebra de Brauer e a árvore de Brauer associada é uma **estrela**:



A árvore possui n arestas e o vértice excepcional possui multiplicidade $m = (p^a - 1)/n$, onde p^a é a ordem de um p-subgrupo de Sylow de G.

Vamos verificar com mais detalhes que B é de fato uma álgebra de Brauer com esta árvore de Brauer. Observe que, pelo Exemplo 2.2.12, $S_1 \otimes W^{\otimes p^a - 1}$ é isomorfo ao soco da cobertura projetiva de S_1, então vale $S_1 \otimes W^{\otimes p^a - 1} \cong S_1$ pelo Teorema 2.3.17. Mas a sequência dada

por $S_1, S_1 \otimes W, S_1 \otimes W^{\otimes 2}$, e assim em diante, é a sequência $S_1, S_2, S_3, \ldots$, que é "circular" de comprimento n. Por isso, o número n de módulos simples pertencentes a B deve dividir $p^a - 1$ e o vértice excepcional da árvore possui uma multiplicidade inteira. Segundo o algoritmo dado para álgebras de Brauer, a cobertura projetiva de S_1 deveria ser unisseriada (pois um dos extremos de S_1 não está conectado a outra aresta) e seus fatores de composição deveriam ser, em ordem,

$$S_1, S_2, S_3, \ldots, S_n, S_1, S_2, \ldots \quad \ldots S_n, S_1, S_2, \ldots, S_n, S_1.$$

Descontando as cópias de S_1 nas pontas, sabemos que S_1 aparece $m-1$ vezes e cada S_i aparece m vezes, se $i \neq 1$. Logo, o comprimento da cobertura projetiva deveria ser

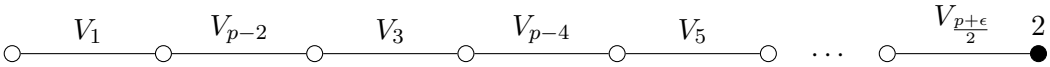
$$2 + (m-1) + (n-1)m = 1 + mn = 1 + (p^a - 1) = p^a$$

e cada fator de composição deveria ser isomorfo ao produto tensorial do anterior com W. Mas essa é a descrição dada no Exemplo 2.2.12! Então o algoritmo descreve corretamente a estrutura da cobertura projetiva de S_1. Verifica-se analogamente que, para as outras coberturas projetivas, o algoritmo também está de acordo com o Exemplo 2.2.12.

Para um exemplo mais concreto, considere $G = D_{15}$ e $p = 5$, como no Exemplo 2.3.22. Olhando a estrutura dos projetivos indecomponíveis, encontramos dois blocos: um contendo os módulos simples k e k_{sgn} e outro contendo o módulo simples U. Pelo que vimos anteriormente, ambos os blocos são álgebras de Brauer e suas árvores de Brauer são

respectivamente.

Exemplo 5.1.5. Tome $G = \mathrm{SL}_2(p)$. Lidaremos primeiramente com o caso $p > 2$. No Exemplo 4.1.20, mostramos que kG possui três blocos. Um deles é o que contém o kG-módulo simples projetivo V_p e então, pelo Corolário 4.3.7, possui defeito zero. Vamos mostrar que os outros dois blocos são álgebras de Brauer! Vamos começar com o bloco principal B_1, que contém os módulos simples V_i para i ímpar satisfazendo $1 \leq i \leq p-2$. Provemos que B_1 é uma álgebra de Brauer cuja árvore de Brauer é o seguinte **caminho**:



onde $\epsilon = (-1)^{\frac{p-1}{2}}$, ou seja, $\epsilon = 1$ se $p \equiv 1 \pmod 4$ ou $\epsilon = -1$ se $p \equiv 3 \pmod 4$. Primeiramente, vamos explicar como estão enumeradas as arestas. Observe que a aresta consecutiva à direita de V_i é $V_{p-i\pm 1}$ e o sinal desse "± 1" vai se alternando. Ou seja, começamos em V_1, depois vamos para $V_{p-1-1} = V_{p-2}$, depois vamos para $V_{p-(p-2)+1} = V_3$, depois vamos para $V_{p-3-1} = V_{p-4}$, e assim em diante. Note que o sucessor do sucessor de V_i é V_{i+2} ou V_{i-2} a depender do valor de i. Dessa forma, os índices percorrem a lista de números

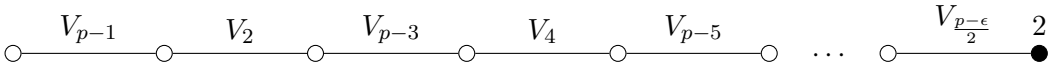
$$1, 3, 5, \ldots, p-4, p-2$$

de "fora para dentro": começamos do menor número, depois vamos para o maior, depois vamos para o segundo menor, depois vamos para o segundo maior, e assim em diante, até esgotar a lista. Não é difícil ver que o último índice depende da paridade da quantidade de números na lista acima. Deixamos a cargo do leitor conferir que este índice é de fato $(p+\epsilon)/2$.

Seja i um número ímpar entre 1 e $p-2$ e considere a cobertura projetiva P_i do módulo simples V_i. Segundo a árvore, se $i = 1$, então P_1 deveria ser unisseriado (pois um dos extremos da aresta V_1 é uma folha da árvore) e deveria valer $\mathrm{rad}(P_1)/\mathrm{soc}(P_1) \cong V_{p-2}$. Pelo Exemplo 2.4.14, isso de fato acontece! Agora, se $i > 1$ e $i \neq (p+\epsilon)/2$, a árvore indica que $\mathrm{soc}(P_i) \subseteq \mathrm{rad}(P_i)$ e $\mathrm{rad}(P_i)/\mathrm{soc}(P_i) \cong V_{p-i-1} \oplus V_{p-i+1}$ (para isso, note que os vizinhos de V_i são, em alguma ordem,

V_{p-i-1} e V_{p-i+1} pela definição da enumeração que demos). Isso também está de acordo com o Exemplo 2.4.14! Mas esse mesmo exemplo diz que $P_{\frac{p+\epsilon}{2}}$ também tem essa estrutura, então por que a árvore é diferente nesse ponto? O motivo é que $i = (p+\epsilon)/2$ é o único índice ímpar i tal que $p-i-1$ ou $p-i+1$ é igual a i. Nesse caso, como não há outra aresta indexada por V_i na árvore, é preciso colocar o vértice excepcional com multiplicidade 2 para o algoritmo conseguir contabilizar o próprio V_i em $\operatorname{rad}(P_i)/\operatorname{soc}(P_i)$. Isso confirma que B_1 é uma álgebra de Brauer com a árvore de Brauer indicada!

Se B_2 é o bloco ao qual pertence o módulo V_2, então um argumento análogo prova que B_2 é uma álgebra de Brauer com a seguinte árvore de Brauer:

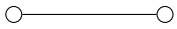


onde ϵ é como antes. Novamente os índices estão percorrendo a lista

$$2, 4, 6, \ldots, p-3, p-1$$

de "fora para dentro", mas agora começamos pelo maior número. A multiplicidade 2 aparece no último vértice porque, desta vez, $i = (p-\epsilon)/2$ é o único índice par i tal que $p-i-1$ ou $p-i+1$ é igual a i, então, como antes, a multiplicidade garante que a aresta seja contada no algoritmo como fator de composição de $\operatorname{rad}(P_i)/\operatorname{soc}(P_i)$.

Por fim, quando $p = 2$, sabemos que kG possui apenas dois blocos. Já vimos que o bloco não principal é de defeito zero, já que contém o módulo simples projetivo V_2. Por outro lado, o bloco principal contém apenas o módulo trivial V_1 e a sua cobertura projetiva é unisseriada de comprimento dois e fator de composição V_1. Assim como ocorreu no Exemplo 5.1.3, concluímos que o bloco principal de kG é uma álgebra de Brauer e sua árvore de Brauer é:

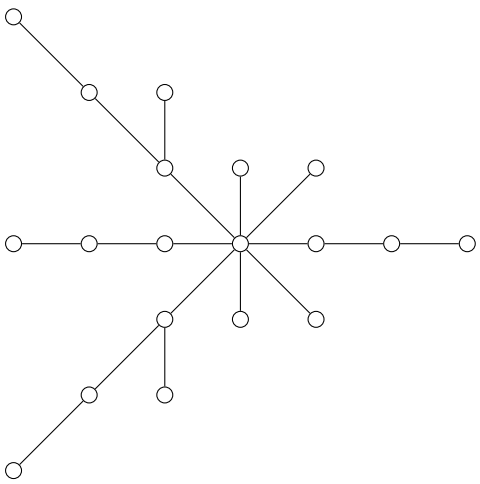


(Como o vértice excepcional não está indicado, entendemos que sua multiplicidade é 1 e, portanto, ele é indistinguível dos demais.)

Exemplo 5.1.6. Seja G o grupo simples esporádico de Thompson. Sabe-se que[1]

$$|G| = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$$

e, portanto, os 19-subgrupos de Sylow de G são cíclicos. Além disso, o bloco principal de kG em característica 19 é uma álgebra de Brauer! Sua árvore de Brauer é:



Note que o vértice excepcional não está em destaque porque a sua multiplicidade é 1. A determinação desta árvore foi finalizada no artigo [6].

[1] Consulte, por exemplo, a página 177 do livro [5].

O que todos os exemplos anteriores têm em comum para tantas álgebras de Brauer terem aparecido? Como é de se esperar pelo nome do capítulo, todos os grupos considerados possuem p-subgrupos de Sylow cíclicos e, por isso, os grupos de defeito de seus blocos são triviais ou cíclicos!

Vamos agora enunciar o teorema cuja prova será o objetivo deste capítulo. Iremos fixar algumas notações que serão utilizadas até o fim da demonstração[1]. Primeiramente, lembre que estamos considerando k algebricamente fechado. Seja B um bloco de kG com grupo de defeito D que é cíclico e de ordem p^n para algum $n \geq 1$. Seja b o bloco de $kN_G(D)$ que é o correspondente de Brauer de B. Se β é um bloco de[2] $kC_G(D)$ coberto por b e se $\mathrm{Stab}(\beta) \subseteq N_G(D)$ é o seu estabilizador, então $e \coloneqq [\mathrm{Stab}(\beta) : C_G(D)]$ é o **índice inercial** do bloco B. Como os blocos cobertos por b são conjugados, os seus estabilizadores também são conjugados e a definição de e não depende da escolha de β.

Teorema 5.1.7. Se B é um bloco de kG com grupo de defeito não trivial e cíclico, então B é uma álgebra de Brauer. Além disso, se e denota o índice inercial de B e se p^n denota a ordem do seu grupo de defeito, então a árvore de Brauer associada possui e arestas e seu vértice excepcional tem multiplicidade $(p^n - 1)/e$.

Antes de prosseguir, vejamos que $p^n - 1$ realmente é divisível por e. Pela definição de índice inercial, podemos ver que e divide $[N_G(D) : C_G(D)]$. Ademais, podemos identificar $N_G(D)/C_G(D)$ como um subgrupo de $\mathrm{Aut}(D)$! De fato, dado um elemento $x \in N_G(D)$, podemos definir o automorfismo $\varphi_x : D \to D$ dado por $\varphi_x(d) = xdx^{-1}$ para todo $d \in D$. Isso nos dá um homomorfismo $N_G(D) \to \mathrm{Aut}(D)$ cujo núcleo é $C_G(D)$, então podemos aplicar o Teorema do Isomorfismo para concluir o que queremos. Como D é cíclico, cada um de seus automorfismos corresponde a um de seus geradores e, portanto,

$$|\mathrm{Aut}(D)| = \phi(|D|) = p^{n-1}(p-1),$$

onde ϕ denota a função "phi" de Euler. Dessa forma, e é um divisor de $p^{n-1}(p-1)$. Por outro lado, o argumento dado no início do Lema 4.4.6 mostra que e não é divisível por p, então deve valer $e \mid (p-1)$. Em particular, e também divide $p^n - 1$. Deixaremos este fato anotado como um lema:

Lema 5.1.8. O índice inercial e divide $p - 1$.

A prova do Teorema 5.1.7 é bem longa, mas podemos dar um pequeno roteiro do que será feito ao longo do capítulo. Seja D_1 o único subgrupo de ordem p de D. Note que $N_G(D) \subseteq N_G(D_1)$ justamente por D_1 ser o único subgrupo de ordem p de D, então podemos formar o bloco $b_1 = b^{N_G(D_1)}$ de $kN_G(D_1)$. Observe que $b_1^G = B$, porque $b^G = B$, e b_1 possui D como grupo de defeito, já que um de seus grupos de defeito contém o grupo de defeito D de b e está contido em algum grupo de defeito de B pelo Lema 4.3.1. Como $C_G(D_1)$ é normal em $N_G(D_1)$, podemos tomar um bloco β_1 de $kC_G(D_1)$ coberto por b_1. Nas próximas seções, faremos os seguintes passos:

(1) Mostraremos que β_1 é uma álgebra de Brauer cuja árvore de Brauer possui apenas uma aresta e um vértice excepcional de multiplicidade $p^n - 1$.

(2) Em seguida, provaremos que b_1 é uma álgebra de Brauer cuja árvore de Brauer é uma estrela com e arestas e com vértice excepcional de multiplicidade $(p^n - 1)/e$.

(3) Para passar a estrutura de b_1 para B, teremos primeiro que fazer uma digressão para estudar coberturas projetivas de módulos não necessariamente simples. Nessa parte, definiremos o operador de Heller e veremos as suas propriedades.

[1] As notações e hipóteses feitas neste capítulo se encontram na tabela de notações no início do trabalho.
[2] Note que $DC_G(D) = C_G(D)$, porque D é abeliano e então $D \subseteq C_G(D)$!

(4) Com as ferramentas anteriores, demonstraremos que B possui e módulos simples e estudaremos as suas extensões.

(5) Entenderemos os B-módulos projetivos indecomponíveis e mostraremos que B é uma álgebra de Brauer "generalizada", isto é, permitimos que o seu "grafo de Brauer" possua ciclos e mais de um vértice excepcional.

(6) Finalmente, provaremos que o grafo de Brauer de B é de fato uma árvore de Brauer e determinaremos a multiplicidade do vértice excepcional.

Um ponto importante é que a demonstração do teorema será feita por indução em n. A hipótese de indução será aplicada nos passos (1) e (2). A base da indução será o caso dos blocos com grupo de defeito trivial, que já lidamos no Corolário 4.3.7. Fique com isso em mente sempre que ler um "por hipótese de indução" a partir de agora.

Para terminar esta seção introdutória, faremos uma observação. O Teorema 5.1.7 nos dá muita informação sobre as representações de um bloco com grupo de defeito cíclico, mas ele não determina a qual álgebra o bloco é isomorfo. Isso acontece porque a definição de uma álgebra de Brauer não é uma construção, mas sim apenas uma caracterização.

Dada uma árvore de Brauer, é possível construir uma álgebra de Brauer com essa árvore. Isso pode ser feito considerando-se álgebras de caminhos com relações, como comentado nas páginas 118 e 119 de [7] e como demonstrado na Proposição 5.10.8 de [23]. Além disso, essa álgebra de Brauer é única a menos de equivalência de Morita, ou seja, a menos de equivalência da categoria de módulos. Por isso, no quesito do estudo de representações, o Teorema 5.1.7 é bem forte.

Uma outra pergunta natural é se toda árvore de Brauer está associada a algum bloco de uma álgebra de grupo com grupo de defeito cíclico. Esse não é o caso, mas o artigo [11] mostra que o problema de determinar as possíveis árvores de Brauer se reduz a determinar as árvores de Brauer para grupos *quase-simples*. Esse novo problema ainda não foi completamente resolvido, mas já se tem uma boa ideia de como são as árvores de Brauer desses grupos!

5.2 O caso local

Nesta seção, iremos cumprir os passos (1) e (2) do roteiro dado para a demonstração do Teorema 5.1.7. O primeiro deles se resume à prova do seguinte teorema:

Teorema 5.2.1. O bloco β_1 de $kC_G(D_1)$ é uma álgebra de Brauer cuja árvore de Brauer possui apenas uma aresta e um vértice excepcional de multiplicidade $p^n - 1$.

Note que a conjugação entre blocos induz isomorfismos de álgebras. Logo, para provar o resultado acima, podemos escolher um bloco β_1 coberto por b_1 de modo conveniente. Pelo item (4) do Teorema 4.4.4, um grupo de defeito de um bloco coberto por b_1 é conjugado a $D \cap C_G(D_1) = D$ em $N_G(D_1)$. Assim, desfazendo a conjugação, encontramos outro bloco coberto por b_1 que possui D como grupo de defeito (aqui nós aplicamos o Exercício A.4.13). Por isso, iremos assumir a partir de agora que D é um grupo de defeito de β_1.

Da mesma forma que fizemos no Exemplo 5.1.3, devemos mostrar que β_1 possui um único módulo simples e que a sua cobertura projetiva é unisseriada de comprimento p^n. Provaremos cada uma dessas propriedades em um lema. Lembramos mais uma vez que a prova do Teorema 5.1.7 está sendo realizada por indução, então usaremos a hipótese de indução em alguns momentos.

Lema 5.2.2. A menos de isomorfismo, existe um único $kC_G(D_1)$-módulo simples pertencente a β_1.

Demonstração. Vamos começar mostrando que o índice inercial de β_1 é 1. Como β_1 possui D como grupo de defeito, observamos na prova do Lema 5.1.8 que o seu índice inercial divide $[N_{C_G(D_1)}(D) : C_{C_G(D_1)}(D)]$ mas não é múltiplo de p. Note que $N_{C_G(D_1)}(D) = N_G(D) \cap C_G(D_1)$

e $C_{C_G(D_1)}(D) = C_G(D)$, então basta mostrar que $[N_G(D) \cap C_G(D_1) : C_G(D)]$ é uma potência de p para concluir o que desejamos. Com efeito, imitando a prova do Lema 5.1.8, vemos que $(N_G(D) \cap C_G(D_1))/C_G(D)$ é isomorfo a um subgrupo de $\mathrm{Aut}(D)$ que age trivialmente em D_1. Pelo Exercício A.5.3, a ordem desse quociente é de fato uma potência de p e, assim, o índice inercial de β_1 é de fato 1.

Agora, seja $\overline{\beta_1}$ o bloco de $k[C_G(D_1)/D_1]$ que corresponde a β_1 pelo Lema 4.4.9. Ele possui D/D_1 como grupo de defeito. Como o normalizador de D/D_1 em $C_G(D_1)/D_1$ é igual ao quociente $(N_G(D) \cap C_G(D_1))/D_1$ e como o centralizador de D/D_1 em $C_G(D_1)/D_1$ contém $C_G(D)/D_1$, obtemos que o índice inercial de $\overline{\beta_1}$ divide

$$[(N_G(D) \cap C_G(D_1))/D_1 : C_G(D)/D_1] = [N_G(D) \cap C_G(D_1) : C_G(D)],$$

que é uma potência de p pelo que vimos acima. Logo, o índice inercial de $\overline{\beta_1}$ também é 1.

Se $D = D_1$, então $\overline{\beta_1}$ possui defeito zero e, consequentemente, possui uma única classe de isomorfismo de módulos simples. Por outro lado, de $D \neq D_1$, então D/D_1 é um subgrupo cíclico não trivial de $C_G(D_1)/D_1$ e, pela hipótese de indução do Teorema 5.1.7, $\overline{\beta_1}$ também possui uma única classe de isomorfismo de módulos simples, já que seu índice inercial é 1. Por fim, como os módulos simples de β_1 são exatamente os módulos simples de $\overline{\beta_1}$, concluímos que, a menos de isomorfismo, existe um único $kC_G(D_1)$-módulo simples pertencente a β_1. □

Como β_1 possui grupo de defeito cíclico, a Proposição 5.1.2 diz que β_1 possui tipo de representação finito. Dessa forma, podemos utilizar o resultado anterior com a próxima proposição para concluir que β_1 é uma álgebra de Brauer:

Proposição 5.2.3. Seja A uma k-álgebra com tipo de representação finito. Se existe uma única classe de isomorfismo de A-módulos simples, então A é uma álgebra semissimples ou uma álgebra de Brauer.

Demonstração. Sejam S o único A-módulo simples e P a sua cobertura projetiva. Assim, ${}_AA \cong P^d$ para algum $d \geq 1$. Se $\mathrm{rad}(P) = 0$, então $\mathrm{rad}(A) \cong \mathrm{rad}(P)^d = 0$ e A é semissimples. Então podemos supor que $\mathrm{rad}(P) \neq 0$. Dessa forma, $\mathrm{rad}(P)/\mathrm{rad}^2(P)$ é um A-módulo semissimples não nulo e, por isso, é uma soma de cópias de S.

Suponha inicialmente que $\mathrm{rad}(P)/\mathrm{rad}^2(P) \cong S$. Vamos utilizar um argumento semelhante ao do Exemplo 2.2.12 para mostrar que P é unisseriado. Se $R := \mathrm{rad}(P)$, então $R/\mathrm{rad}(R) \cong S$ e, pelo Lema 2.2.5, R é um quociente de P. Segue que $\mathrm{rad}(R)/\mathrm{rad}^2(R)$ é quociente de $\mathrm{rad}(P)/\mathrm{rad}^2(P) \cong S$ e, por isso, $\mathrm{rad}(R)/\mathrm{rad}^2(R) = \mathrm{rad}^2(P)/\mathrm{rad}^3(P)$ é igual a 0 ou isomorfo a S. Prosseguindo assim, obtemos que $\mathrm{rad}^i(P)/\mathrm{rad}^{i+1}(P)$ é igual a 0 ou isomorfo a S para todo $i \geq 0$, mostrando que as camadas radicais de P são simples. Concluímos que P é unisseriado e, portanto, A é uma álgebra de Brauer (cuja árvore de Brauer possui uma única aresta e multiplicidade um a menos do que o comprimento de P).

Resta verificar o que acontece quando $\mathrm{rad}(P)/\mathrm{rad}^2(P) \cong S^r$ para algum $r \geq 2$. Vamos mostrar que esse caso não pode acontecer. Ou melhor, vejamos que se isso acontece, então A não pode ter tipo de representação finito. Considere o ideal $\mathrm{rad}^2(A) = \mathrm{rad}(A)^2$ de A e defina $\overline{A} := A/\mathrm{rad}^2(A)$. Observe que $\mathrm{rad}(\overline{A}) = \mathrm{rad}(A)/\mathrm{rad}^2(A)$: isso segue de imediato da definição de radical porque A e $\overline{A}$ possuem os mesmos módulos simples (já que $\mathrm{rad}^2(A) \subseteq \mathrm{rad}(A)$). Se $Q := P/\mathrm{rad}^2(P)$, então Q é anulado por $\mathrm{rad}^2(A)$ e pode ser visto como um $\overline{A}$-módulo. Nesse caso,

$$\mathrm{rad}(Q) = \mathrm{rad}(\overline{A}) \cdot Q = \frac{\mathrm{rad}(A)}{\mathrm{rad}^2(A)} \cdot \frac{P}{\mathrm{rad}^2(P)} = \frac{\mathrm{rad}(P)}{\mathrm{rad}^2(P)} \cong S^r$$

e

$$\frac{Q}{\mathrm{rad}(Q)} \cong \frac{P/\mathrm{rad}^2(P)}{\mathrm{rad}(P)/\mathrm{rad}^2(P)} \cong \frac{P}{\mathrm{rad}(P)} \cong S.$$

Pelo Exemplo 2.1.11, Q é indecomponível e, como ${}_{\overline{A}}\overline{A} \cong Q^d$, Q é projetivo. Logo, Q é a cobertura projetiva de S como $\overline{A}$-módulo, que é o único $\overline{A}$-módulo simples. Mas todo $\overline{A}$-módulo indecomponível também é um A-módulo indecomponível, logo, se mostrarmos que $\overline{A}$ não possui tipo de representação finito, A também não possuirá. Isso nos permite trabalhar apenas com $\overline{A}$. Para não carregar a notação, podemos trabalhar com A e supor simplesmente que $\operatorname{rad}^2(P) = 0$ e que $\operatorname{rad}(P) \cong S^r$.

Como ${}_AA \cong P^d$, temos

$$A^{\mathrm{op}} \cong \operatorname{End}_A({}_AA) \cong \operatorname{End}_A(P^d) \cong M_d(\operatorname{End}_A(P)),$$

onde utilizamos o Lema 1.2.3 e o Corolário 1.2.7. Por isso, será importante estudar a álgebra $E \coloneqq \operatorname{End}_A(P)$. Vamos encontrar uma base para essa nova álgebra. Escreva $\operatorname{rad}(P) = S_1 \oplus \cdots \oplus S_r$, onde cada S_i é um submódulo de $\operatorname{rad}(P)$ isomorfo a S. Defina $\varphi_i : P \to P$ como sendo a composição da projeção $P \to P/\operatorname{rad}(P) \cong S$ junto com um isomorfismo $S \to S_i$ e com as inclusões $S_i \to \operatorname{rad}(P)$ e $\operatorname{rad}(P) \to P$. Observe que φ_i é um elemento de E cujo núcleo é $\operatorname{rad}(P)$ e cuja imagem é S_i. Provaremos que $\mathrm{id}_P, \varphi_1, \ldots, \varphi_r$ formam uma base de E sobre k.

Como P é um A-módulo indecomponível, E é uma álgebra local pelo Corolário 2.1.8. Em particular, $E/\operatorname{rad}(E)$ é uma k-álgebra de divisão e, como estamos supondo k algebricamente fechado, $E/\operatorname{rad}(E) \cong k$. Logo, $\operatorname{rad}(E)$ possui codimensão 1 em E. Como $\mathrm{id}_P \notin \operatorname{rad}(E)$, basta mostrar que $\varphi_1, \ldots, \varphi_r$ formam uma base de $\operatorname{rad}(E)$. Pela Proposição 2.1.4, $\operatorname{rad}(E)$ é formado pelos elementos não inversíveis de E. Como $\operatorname{im}\varphi_i = S_i \subseteq \operatorname{rad}(P) = \ker\varphi_i$, vale $\varphi_i^2 = 0$ e então $\varphi_i \in \operatorname{rad}(E)$ para todo $1 \leq i \leq r$. Além disso, como os subespaços $S_1, \ldots, S_r$ estão em soma direta, os endomorfismos $\varphi_1, \ldots, \varphi_r$ são linearmente independentes. Resta mostrar que $\operatorname{rad}(E)$ possui dimensão r. De fato, $\operatorname{rad}(E)$ é formado pelos endomorfismos de P que não são inversíveis, ou seja, cujas imagens são submódulos próprios de P. Mas $\operatorname{rad}(P)$ é o único submódulo maximal de P, de onde concluímos que $\operatorname{rad}(E)$ é formado pelos endomorfismos cuja imagem está contida em $\operatorname{rad}(P)$. Portanto,

$$\dim_k \operatorname{rad}(E) = \dim_k \operatorname{Hom}_A(P, \operatorname{rad}(P)) = \dim_k \operatorname{Hom}_A(S, S^r) = r \cdot \dim_k \operatorname{End}_A(S) = r,$$

como preciso. Acima, utilizamos que $\operatorname{Hom}_A(P, \operatorname{rad}(P))$ é isomorfo a $\operatorname{Hom}_A(P/\operatorname{rad}(P), \operatorname{rad}(P))$ na segunda igualdade, já que $\operatorname{rad}(P)$ é semissimples, e usamos o Lema de Schur na última igualdade.

Até agora, descobrimos que E possui $\mathrm{id}_P, \varphi_1, \ldots, \varphi_r$ como base. É fácil entender o produto da álgebra E através dessa base, porque id_P é a identidade e $\varphi_i\varphi_j = 0$ para todos $1 \leq i, j \leq r$. A partir dessas informações, demonstraremos que E não possui tipo de representação finito. O que se segue apenas funciona porque $r \geq 2$. Através das relações anteriores, não é difícil verificar que o subespaço I gerado por $\varphi_3, \ldots, \varphi_r$ é um ideal de E (se $r = 2$, então $I = 0$). O quociente E/I possui dimensão 3 e é gerado por elementos $1, X$ e Y, onde 1 é a identidade e X e Y satisfazem as relações $X^2 = XY = YX = Y^2 = 0$. Comparando dimensões, vemos que esse quociente é a álgebra gerada[1] por elementos X e Y com as relações $X^2 = XY = YX = Y^2 = 0$. Assim, podemos imitar o que fizemos no Exemplo 2.1.14 e construir infinitos E/I-módulos indecomponíveis dois a dois não isomorfos. Restringindo escalares para E, conseguimos construir infinitos E-módulos indecomponíveis dois a dois não isomorfos, provando que E não possui tipo de representação finito.

Pelas relações do início do parágrafo anterior, é imediato que E é uma álgebra comutativa. Desse modo,

$$A \cong (A^{\mathrm{op}})^{\mathrm{op}} \cong M_d(E)^{\mathrm{op}} \cong M_d(E^{\mathrm{op}}) \cong M_d(E).$$

Sabendo que E não possui tipo de representação finito, mostraremos que $M_d(E)$ também não possui, o que concluirá a prova por conta do isomorfismo acima. Se U é um E-módulo, então podemos considerar o espaço U_d dos vetores-coluna de comprimento d com entradas em U. Imitando

[1] Por esta expressão queremos dizer que essa álgebra é o quociente da álgebra livre em duas variáveis pelas relações apresentadas.

a multiplicação de matrizes, é fácil verificar que U_d é naturalmente um $M_d(E)$-módulo. Para obter o que queremos, provaremos que U é indecomponível se e só se U_d é indecomponível. Como E possui representações indecomponíveis de dimensão arbitrariamente grande, o mesmo ocorrerá para $M_d(E)$. Por sua vez, pelo Corolário 2.1.8, basta mostrar que a álgebra de endomorfismos do E-módulo U é isomorfa à álgebra de endomorfismos do $M_d(E)$-módulo U_d. Faremos isso agora.

Como espaço vetorial, U_d é isomorfo à soma direta de d cópias de U. Logo, aplicando o Corolário 1.2.7 com a k-álgebra k, vemos que a álgebra de operadores lineares sobre U_d é isomorfa à álgebra M de matrizes $d \times d$ cujas entradas são operadores lineares em U. Além disso, sabemos como esse isomorfismo é dado: cada elemento de M define uma transformação linear em U_d dada pela "multiplicação" de matrizes. Se $x \in E$, denote por $\overline{x}$ a transformação linear que x induz no E-módulo U. Se (x_{ij}) é uma matriz de $M_d(E)$, então a transformação linear induzida no $M_d(E)$-módulo U_d é a mesma induzida pela matriz $(\overline{x_{ij}})$ de M. Dessa forma, concluímos que $\mathrm{End}_{M_d(E)}(U_d)$ é isomorfa à subálgebra de M formadas pelas matrizes que comutam com todos os elementos de $M_d(\overline{E})$, que denota o conjuntos das matrizes cujas entradas são da forma $\overline{x}$ para $x \in E$. Mas um elemento de M que comuta com os elementos de $M_d(\overline{E})$ necessariamente comuta com as matrizes elementares, cujas entradas são 0 exceto em uma única coordenada, onde vale a identidade em U. Isso facilmente implica que os elementos de $\mathrm{End}_{M_d(E)}(U_d)$ correspondem a matrizes "escalares" de M. Mais do que isso, uma matriz escalar de M (cujo elemento na diagonal principal é uma transformação linear f) comuta com todas as matrizes escalares de $M_d(\overline{E})$ se e só se f comuta com $\overline{x}$ para todo $x \in E$, ou seja, se e só se $f \in \mathrm{End}_E(U)$. Como $M_d(\overline{E})$ é gerado pelas matrizes elementares e por suas matrizes escalares, concluímos que $\mathrm{End}_{M_d(E)}(U_d)$ é isomorfa à subálgebra de M formada pelas matrizes diagonais cujos elementos da diagonal principal são todos iguais a um elemento de $\mathrm{End}_E(U)$. Com isso, rapidamente concluímos que $\mathrm{End}_{M_d(E)}(U_d) \cong \mathrm{End}_E(U)$, terminando a demonstração. □

Observação 5.2.4. Ao final da demonstração, relacionamos algumas propriedades dos E-módulos e dos $M_d(E)$-módulos. Um fato interessante é que E e $M_d(E)$ são Morita equivalentes, ou seja, as suas categorias de módulos são equivalentes! Poderíamos ter utilizado isso para concluir a demonstração, mas demos um argumento direto. Para mais algumas propriedades relacionadas, veja o Exercício A.5.4.

Outra observação é que o resultado anterior é mais geral do que precisamos. Inclusive, podemos utilizar ele para concluir que, se B possui um único módulo simples, então B é uma álgebra de Brauer cuja árvore de Brauer possui uma única aresta! Isso segue do resultado anterior e da Proposição 5.1.2, já que B possui grupos de defeito cíclicos.

Com isso, já sabemos que β_1 possui um único módulo simples e que a sua cobertura projetiva é unisseriada. Resta mostrar que o comprimento dessa cobertura projetiva é p^n para terminar a prova do Teorema 5.2.1. Também precisaremos da hipótese de indução para isso. Como vimos na prova do Lema 5.2.2, se $\overline{\beta_1}$ é o bloco de $k[C_G(D_1)/D_1]$ que corresponde a β_1, então D/D_1 é um grupo de defeito de $\overline{\beta_1}$ e o índice inercial desse bloco é 1. Se $n = 1$, então $D = D_1$ e $\overline{\beta_1}$ possui defeito zero, de modo que seu único módulo simples é projetivo e, portanto, de comprimento $1 = p^{n-1}$. Por outro lado, se $n > 1$, então D/D_1 é cíclico não trivial e a hipótese de indução do Teorema 5.1.7 mostra que o único $\overline{\beta_1}$-módulo projetivo indecomponível também possui comprimento p^{n-1}. Para passar essa propriedade de $\overline{\beta_1}$ para β, temos mais um resultado:

Proposição 5.2.5. Seja N um p-subgrupo normal de G e defina $\overline{G} = G/N$. Se S é um kG-módulo simples, seja P_S a sua cobertura projetiva. Também podemos considerar S como $k\overline{G}$-módulo simples, então seja $\overline{P_S}$ o $k\overline{G}$-módulo projetivo indecomponível correspondente. Nessas condições, existe uma série de submódulos

$$P_S = P_S^0 \supseteq P_S^1 \supseteq \cdots \supseteq P_S^r = 0,$$

onde r é o comprimento radical da álgebra kN, de modo que

$$\frac{P_S^i}{P_S^{i+1}} \cong \overline{P_S} \otimes \frac{\mathrm{rad}^i(kN)}{\mathrm{rad}^{i+1}(kN)}$$

para todo $0 \leq i < r$. Aqui estamos considerando kN como um kG-módulo por conjugação e então os quocientes radicais acima são de fato kG-módulos.

Vejamos como isso finaliza a demonstração do Teorema 5.2.1. Tomamos G na proposição acima como $C_G(D_1)$ e N como D_1. Como D_1 está no centro de $C_G(D_1)$, então $C_G(D_1)$ age trivialmente em kD_1. Logo, o quociente radical no resultado acima é um módulo trivial e obtemos

$$\frac{P_S^i}{P_S^{i+1}} \cong \overline{P_S} \otimes k^{t_i} \cong \overline{P_S}^{t_i},$$

onde t_i é a dimensão da camada radical em questão e onde P_S e $\overline{P_S}$ denotam o único β_1-módulo projetivo indecomponível e o único $\overline{\beta_1}$-módulo projetivo indecomponível, respectivamente. Com isso, vemos que o comprimento de P_S é o comprimento de $\overline{P_S}$ vezes

$$t_0 + t_1 + \cdots + t_{r-1} = \dim_k kD_1 = |D_1| = p,$$

ou seja, o comprimento de P_S é $p^{n-1} \cdot p = p^n$, como necessário.

Demonstração. Antes de começar, esclareceremos alguns detalhes do enunciado. Como N é um p-subgrupo normal de G, sabemos da Proposição 1.3.14 que N age trivialmente em S, então de fato podemos ver S como um $k\overline{G}$-módulo. Ademais, como N é normal em G, é fácil ver que G age por conjugação em kN e este se torna um kG-módulo. Se R denota $\mathrm{rad}(kN)$, como a conjugação em kN fornece um automorfismo de álgebra, vemos que $gR^ig^{-1} = R^i$ para todo $g \in G$ e para todo $i \geq 1$. Por isso, cada R^i é um submódulo do kG-módulo kN e então os quocientes radicais do enunciado são de fato kG-módulos.

A série do enunciado é a série radical de P_S, mas quando visto como um kN-módulo, ou seja, $P_S^i = R^iP_S$ para todo $i \geq 0$. Como $gR^ig^{-1} = R^i$ para todo $g \in G$, cada P_S^i é um kG-submódulo de P_S. Além disso, como N é um p-grupo, sabemos do Exercício A.1.14 que $x - 1 \in R$ para todo $x \in N$, logo $(x-1)P_S^i \subseteq P_S^{i+1}$ para todo $x \in N$ e então N age trivialmente em P_S^i/P_S^{i+1}. Portanto, cada P_S^i/P_S^{i+1} é um $k\overline{G}$-módulo. Reciprocamente, se V é um submódulo de P_S^i tal que N age trivialmente em P_S^i/V, então $(x-1)P_S^i \subseteq V$ para todo $x \in N$. Mas os elementos da forma $x - 1$ com $x \in N$ geram R, de modo que $P_S^{i+1} = RP_S^i \subseteq V$. Isso mostra que P_S^{i+1} é o menor submódulo de P_S^i cujo quociente é um $k\overline{G}$-módulo.

Como $P_S/\mathrm{rad}(P_S) \cong S$ pode ser visto como um $k\overline{G}$-módulo, segue que $P_S^0 = P_S \supseteq \mathrm{rad}(P_S) \supseteq P_S^1$. Por isso, o radical de P_S^0/P_S^1 é $\mathrm{rad}(P_S)/P_S^1$ e o respectivo quociente também é isomorfo a S. Pelo Exemplo 2.1.11, P_S^0/P_S^1 é indecomponível. Afirmamos que $P_S^0/P_S^1 \cong \overline{P_S}$. Para mostrar isso, basta verificar que P_S^0/P_S^1 é um $k\overline{G}$-módulo projetivo. Utilizaremos a caracterização (3) da Proposição 2.2.1. Sejam $\varphi : U \to V$ um homomorfismo sobrejetor de $k\overline{G}$-módulos e $\psi : P_S^0/P_S^1 \to V$ um homomorfismo de $k\overline{G}$-módulos qualquer. Se $\pi : P_S \to P_S^0/P_S^1$ é a projeção canônica, então $\psi\pi$ é um homomorfismo de P_S em V. Como P_S é projetivo, conseguimos encontrar um homomorfismo de kG-módulos $\sigma : P_S \to U$ que faz o seguinte diagrama comutar:

$$\begin{array}{ccc} P_S & \xrightarrow{\pi} & P_S^0/P_S^1 \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\psi} \\ U & \xrightarrow[\varphi]{} & V \end{array}$$

Como U é um $k\overline{G}$-módulo, então $P_S/\ker\sigma$ também é um $k\overline{G}$-módulo e vale $P_S^1 \subseteq \ker\sigma$. Por isso, podemos descer σ ao quociente e obter um homomorfismo $\rho : P_S^0/P_S^1 \to U$ satisfazendo $\rho\pi = \sigma$.

Desse modo, $\varphi\rho\pi = \varphi\sigma = \psi\pi$ e, como π é sobrejetor, $\varphi\rho = \psi$. Como conseguimos garantir a existência desse homomorfismo ρ dados φ e ψ quaisquer, concluímos que P_S^0/P_S^1 é de fato um $k\overline{G}$-módulo projetivo. Logo, $P_S^0/P_S^1 \cong \overline{P_S}$.

Finalmente, vamos provar que

$$\frac{P_S^i}{P_S^{i+1}} \cong \frac{P_S^0}{P_S^1} \otimes \frac{R^i}{R^{i+1}} \cong \overline{P_S} \otimes \frac{R^i}{R^{i+1}}$$

para todo $i \geq 0$, onde estamos vendo R e suas potências como kG-módulos através da conjugação. Se $x \in R^j$ e $v \in P_S^t$, então é imediato das definições que $xv \in P_S^{j+t}$. Em particular, conseguimos obter uma transformação linear de $(P_S^0/P_S^1) \otimes (R^i/R^{i+1})$ em P_S^i/P_S^{i+1} dada por

$$(v + P_S^1) \otimes (x + R^{i+1}) \longmapsto xv + P_S^{i+1}.$$

Não é difícil verificar que essa transformação linear está de fato bem definida. Note que ela é sobrejetora, já que $R^i P_S^0 = P_S^i$, e também é um homomorfismo de kG-módulos: se $g \in G$, então

$$g \cdot ((v + P_S^1) \otimes (x + R^{i+1})) = (gv + P_S^1) \otimes (gxg^{-1} + R^{i+1})$$

e este elemento é levado em

$$(gxg^{-1})(gv) + P_{i+1} = gxv + P_{i+1} = g \cdot (xv + P_{i+1}).$$

Logo, encontramos um homomorfismo sobrejetor de $(P_S^0/P_S^1) \otimes (R^i/R^{i+1})$ em P_S^i/P_S^{i+1}. Em particular, a dimensão de um deles é maior ou igual à do outro, então podemos somar sobre os índices $i \geq 0$ e obter

$$\dim_k P_S = \sum_{i\geq 0} \dim_k P_S^i/P_S^{i+1} \leq \dim_k \overline{P_S} \cdot \sum_{i\geq 0} \dim_k R^i/R^{i+1} = \dim_k \overline{P_S} \cdot |N|.$$

Se a desigualdade acima for na verdade uma igualdade, então todos os homomorfismos sobrejetores que construímos serão isomorfismos, concluindo a demonstração. De fato, repetindo a prova e variando S sobre todos os kG-módulos simples, o Corolário 2.2.6 (junto com o Corolário 1.2.9, já que k é algebricamente fechado), nos dá

$$|G| = \sum_S \dim_k S \cdot \dim_k P_S \leq |N| \cdot \sum_S \dim_k S \cdot \dim_k \overline{P_S} = |N| \cdot \left|\overline{G}\right| = |G|$$

e então a desigualdade é necessariamente uma igualdade, como desejado. □

Conseguimos provar o Teorema 5.2.1 e concluir o passo (1): β_1 é uma álgebra de Brauer cuja árvore de Brauer possui apenas uma aresta e tem $p^n - 1$ como multiplicidade!

A meta agora é provar o passo (2):

Teorema 5.2.6. O bloco b_1 de $kN_G(D_1)$ é uma álgebra de Brauer cuja árvore de Brauer é uma estrela com e arestas e com vértice excepcional no centro de multiplicidade $(p^n - 1)/e$.

Como sempre, e é o índice inercial do bloco B. Esta parte da prova é longa e a nomenclatura é um pouco carregada, já que diversos subgrupos entram em cena. Para tentar ajudar, simplificaremos algumas notações. Denotaremos

$$N \coloneqq N_G(D), \quad N_1 \coloneqq N_G(D_1), \quad C \coloneqq C_G(D) \quad \text{e} \quad C_1 \coloneqq C_G(D_1).$$

Seja também β_1 o bloco de kC_1 coberto por b_1 e com grupo de defeito D, como lidamos anteriormente. Denote $I_1 \coloneqq \mathrm{Stab}(\beta_1)$, que é um subgrupo de N_1 contendo C_1.

Inicialmente, demonstraremos o Teorema 5.2.6 mas trocando o bloco b_1 de kN_1 pelo bloco $\beta_1^{I_1}$ de kI_1. Necessitamos de alguns lemas.

Lema 5.2.7. Vale a igualdade $[I_1 : C_1] = e$.

Demonstração. Seja γ o correspondente de Brauer do bloco β_1 de kC_1 (em $kN_{C_1}(D)$). Como $N_{C_1}(D) = N \cap C_1$, então γ é um bloco de $k[N \cap C_1]$ com grupo de defeito D e satisfazendo $\gamma^{C_1} = \beta_1$. Como C é normal em N e $C \subseteq C_1$, segue que C é um subgrupo normal de $N \cap C_1$. Logo, se β é um bloco de kC coberto por γ, então β possui um grupo de defeito contendo D (pois D é p-subgrupo normal de C) e de cardinalidade $|D \cap C| = |D|$ (pelo Teorema 4.4.4), ou seja, β possui D como grupo de defeito. Como C é o centralizador de D, segue que $\beta^{N \cap C_1}$ está definido e é necessariamente igual a γ. Portanto,

$$\beta^G = (\beta^{N \cap C_1})^G = \gamma^G = (\gamma^{C_1})^G = \beta_1^G = (\beta_1^{N_1})^G = b_1^G = B$$

e, em particular, $(\beta^N)^G = B$ e β^N possui D como grupo de defeito (algum grupo de defeito de β^N contém o grupo de defeito D de β e está contido em algum grupo de defeito de B, que possui a ordem de D). Pelo Primeiro Teorema de Brauer, β^N é o correspondente de Brauer de B, ou seja, $\beta^N = b$. Assim, β é coberto por b e então, se $I := \mathrm{Stab}(\beta)$, a definição de índice inercial diz que $e = [I : C]$. Logo, se demonstramos que

$$\frac{I}{C} \cong \frac{I_1}{C_1},$$

o lema estará provado. Para isso, mostraremos que $I \cap C_1 = C$ e $IC_1 = I_1$, pois então seguirá do Segundo Teorema do Isomorfismo que

$$\frac{I}{C} = \frac{I}{I \cap C_1} \cong \frac{IC_1}{C_1} = \frac{I_1}{C_1},$$

como queremos.

Vamos começar com a igualdade $I \cap C_1 = C$. Vimos na demonstração do Lema 5.2.2 que $(N \cap C_1)/C$ é um p-grupo. Por outro lado, a ordem de I/C é um índice inercial e, pelo Lema 5.1.8, não é múltipla de p. Portanto,

$$\frac{N \cap C_1}{C} \cap \frac{I}{C} = \{1\},$$

ou seja, $N \cap C_1 \cap I = C$. Como $I \subseteq N$, segue que $I \cap C_1 = C$.

Para mostrar que $IC_1 = I_1$, começamos com a inclusão $IC_1 \subseteq I_1$, que é equivalente às inclusões $I \subseteq I_1$ e $C_1 \subseteq I_1$. Como I_1 é o estabilizador de β_1, que é um bloco de kC_1, a inclusão $C_1 \subseteq I_1$ é imediata. Para a outra inclusão, seja $x \in I$. Como $\beta^{C_1} = \beta_1$, vamos imitar um argumento dado na demonstração do Lema 4.5.6 para mostrar que x estabiliza β_1. Pelo item (a) do Exercício A.4.14, $x\beta x^{-1}$ é isomorfo a ${}^{(x,x)}\beta$ como $k[C \times C]$-módulos (note que $xCx^{-1} = C$ porque $x \in I \subseteq N$). Mas $x\beta x^{-1} = \beta$, já que I é o estabilizador de β, então segue de $\beta \mid (\beta_1)_{C \times C}$ que

$$\beta = x\beta x^{-1} \cong {}^{(x,x)}\beta \mid {}^{(x,x)}((\beta_1)_{C \times C}) = \left({}^{(x,x)}\beta_1\right)_{C \times C} \cong (x\beta_1 x^{-1})_{C \times C},$$

onde utilizamos o Exercício A.4.14 mais uma vez. Como $xC_1x^{-1} = C_1$, já que $x \in I \subseteq N \subseteq N_1$, vemos que $x\beta_1 x^{-1}$ é um bloco de kC_1. Mas β^{C_1} está definido e é igual a β_1, então da definição dessa correspondência devemos ter $\beta_1 = x\beta_1 x^{-1}$, mostrando que $x \in I_1$. Isso prova a inclusão $I \subseteq I_1$.

Finalmente, provemos que $I_1 \subseteq IC_1$. Seja $x \in I_1$. Como $x^{-1}\beta_1 x = \beta_1$ e D é um grupo de defeito de β_1, segue do Exercício A.4.13 que $x^{-1}Dx$ também é um grupo de defeito de β_1. Mas grupos de defeito de β_1 são conjugados em C_1, então existe $z \in C_1$ tal que $x^{-1}Dx = z^{-1}Dz$. Logo, se $y = xz^{-1}$, então $y \in N$ e, como $x \in I_1$ e $z \in C_1 \subseteq I_1$, $y \in I_1$. Desse modo, se mostrarmos que $N \cap I_1 \subseteq IC_1$, então teremos $x = yz \in IC_1$, como desejado.

Seja $y \in N \cap I_1$ e demonstremos que $y \in IC_1$. Vamos começar mostrando que y estabiliza γ. Primeiramente, isso faz sentido porque γ é um bloco de $k[N \cap C_1]$ e $N \cap C_1$ é normal em $N \cap I_1$.

Como $y \in N$, então o Exercício A.4.13 diz que $D = yDy^{-1}$ é um grupo de defeito do bloco $y\gamma y^{-1}$ de $k[N \cap C_1]$. Como γ^{C_1} está definido e é igual a β_1, podemos proceder como anteriormente para mostrar que $(y\gamma y^{-1})^{C_1}$ está definido e é igual a $y\beta_1 y^{-1} = \beta_1$. Como $\gamma^{C_1} = (y\gamma y^{-1})^{C_1}$, o Primeiro Teorema Principal de Brauer implica em $\gamma = y\gamma y^{-1}$, ou seja, y estabiliza γ, como queríamos.

Agora, como C é normal em $N \cap I_1$, $y\beta y^{-1}$ é ainda um bloco de kC. Como $\beta^{N\cap C_1}$ está definido e é igual a γ, procedemos como antes para obter que $(y\beta y^{-1})^{N\cap C_1}$ está definido e é igual a $y\gamma y^{-1} = \gamma$. Isso mostra que $y\beta y^{-1}$ ainda é coberto por γ. Mas podemos repetir esse argumento trocando β por qualquer bloco de kC coberto por γ, então concluímos que $\langle y\rangle$ age por conjugação nos blocos de kC cobertos por γ. Vamos estudar essa ação.

Pelo Teorema 4.4.4, os blocos de kC cobertos por γ são os conjugados de β em $N \cap C_1$. Como o estabilizador de β em $N \cap C_1$ é $I \cap (N \cap C_1) = I \cap C_1 = C$, sabemos que o número de blocos de kC cobertos por γ é $q \coloneqq [N \cap C_1 : C]$. Já observamos anteriormente que q é uma potência de p. Por outro lado, N/C é isomorfo a um subgrupo de $\mathrm{Aut}(D)$, que é abeliano porque D é cíclico. Desse modo, como $C \subseteq I \subseteq N$ e N/C é abeliano, vemos que I é normal em N. Logo, se $g \in N \cap C_1$, então o estabilizador de $g\beta g^{-1}$ em $N \cap C_1$ é $gIg^{-1} = I$. Isso mostra que o estabilizador em $\langle y\rangle$ de cada bloco de kC coberto por γ é $I \cap \langle y\rangle$. Em particular, todas as órbitas possuem tamanho igual a $[\langle y\rangle : I \cap \langle y\rangle]$ e, como existem q elementos na ação, esse índice divide q. Mais do que isso, o Teorema da Órbita e do Estabilizador diz que a ação de $\langle y\rangle$ em uma órbita é equivalente à sua ação por translação à esquerda no quociente $\langle y\rangle/(I \cap \langle y\rangle)$. Assim, vemos que y^q age em cada órbita assim como $y^q(I \cap \langle y\rangle)$ age em $\langle y\rangle/(I \cap \langle y\rangle)$. Mas esse quociente é um grupo e q é múltiplo de sua ordem, então $y^q(I \cap \langle y\rangle) = (y(I \cap \langle y\rangle))^q$ é a identidade e concluímos que y^q age trivialmente nos blocos de kC cobertos por γ. Em particular, y^q estabiliza β e $y^q \in I$. Agora, como I_1/C_1 é um subgrupo de N_1/C_1 que é isomorfo a um subgrupo de $\mathrm{Aut}(D_1)$ (que possui ordem $p-1$), temos que p não divide $[I_1 : C_1]$ e então q é coprimo com esse índice. Por isso, no quociente I_1/C_1, yC_1 e y^qC_1 geram o mesmo subgrupo. Logo, $y \in \langle y^q\rangle C_1$ e, como $y^q \in I$, concluímos que $y \in IC_1$, provando que $N \cap I_1 \subseteq IC_1$ e terminando a demonstração. □

Lema 5.2.8. Se S é um kC_1-módulo simples pertencente a β_1, então S possui exatamente e extensões para um kI_1-módulo. Além disso, essas extensões pertencem a $\beta_1^{I_1}$ e formam todos os kI_1-módulos simples deste bloco.

Acima, dizemos que um kI_1-módulo T estende o kC_1-módulo S se vale $T_{C_1} = S$.

Demonstração. O primeiro passo é mostrar que existe ao menos uma extensão de S para um kI_1-módulo. Veja que o quociente I_1/C_1 é um grupo cíclico por ser isomorfo a um subgrupo de $\mathrm{Aut}(D_1)$, que é cíclico. Tome $x \in I_1$ tal que xC_1 seja um gerador de I_1/C_1. Pelo Lema 5.2.7, a ordem de I_1/C_1 é e, então $y \coloneqq x^e \in C_1$. Além disso, todo elemento de I_1 se escreve de modo único na forma x^ic, onde $0 \leq i < e$ e $c \in C_1$. Agora, veja a estrutura de módulo de S como uma representação $\rho : C_1 \to \mathrm{GL}(S)$. Por enquanto, suponha que exista um operador linear inversível $t : S \to S$ tal que $t^e = \rho(y)$ e

$$t^{-1}\rho(c)t = \rho(x^{-1}cx)$$

para todo $c \in C_1$ (lembre que $x^{-1}cx \in C_1$ porque C_1 é normal em I_1). A partir disso, defina $\tilde{\rho} : I_1 \to \mathrm{GL}(S)$ por

$$\tilde{\rho}(x^ic) = t^i\rho(c)$$

para todos $0 \leq i < e$ e $c \in C_1$. É imediato que $\tilde{\rho}$ estende ρ, então basta mostrarmos que $\tilde{\rho}$ é um homomorfismo de grupos para obter uma extensão de S para um kI_1-módulo. Se x^ic e x^jd são elementos de I_1, onde $0 \leq i, j < e$ e $c, d \in C_1$, então temos

$$x^ic \cdot x^jd = x^{i+j} \cdot (x^{-j}cx^j)d$$

e note que $x^{-j}cx \in C_1$. Se $i+j < e$, então temos

$$\begin{aligned}\tilde{\rho}(x^i c \cdot x^j d) &= \tilde{\rho}(x^{i+j} \cdot (x^{-j}cx^j)d) \\ &= t^{i+j} \cdot \rho(x^{-j}cx^j)\rho(d) \\ &= t^{i+j} \cdot (t^{-j}\rho(c)t^j)\rho(d) \\ &= t^i\rho(c) \cdot t^j\rho(d) \\ &= \tilde{\rho}(x^i c) \cdot \tilde{\rho}(x^j d).\end{aligned}$$

Por outro lado, se $i+j \geq e$, então $0 \leq i+j-e < e$ e vale

$$\begin{aligned}\tilde{\rho}(x^i c \cdot x^j d) &= \tilde{\rho}(x^{i+j-e} \cdot y(x^{-j}cx^j)d) \\ &= t^{i+j-e} \cdot \rho(y)\rho(x^{-j}cx^j)\rho(d) \\ &= t^{i+j-e} \cdot t^e(t^{-j}\rho(c)t^j)\rho(d) \\ &= t^i\rho(c) \cdot t^j\rho(d) \\ &= \tilde{\rho}(x^i c) \cdot \tilde{\rho}(x^j d).\end{aligned}$$

Isso mostra que $\tilde{\rho}$ é de fato um homomorfismo.

Para garantir a existência da extensão de S, resta encontrar o operador linear t com as propriedades desejadas. A principal observação para encontrar t é notar que a conjugação ${}^{x^{-1}}S$ é um kC_1-módulo simples pertencente ao bloco $x^{-1}\beta_1 x$, que é igual a β_1 já que I_1 é o estabilizar deste bloco. Mas vimos no Teorema 5.2.1 que existe um único β_1-módulo simples, de onde concluímos $S \cong {}^{x^{-1}}S$. Um isomorfismo entre esses módulos é um operador linear inversível $u : S \to S$ que satisfaz

$$u((x^{-1}cx) \cdot s) = c \cdot u(s)$$

para todos $s \in S$ e $c \in C_1$, então temos

$$u\rho(x^{-1}cx) = \rho(c)u \implies u^{-1}\rho(c)u = \rho(x^{-1}cx)$$

para todo $c \in C_1$. Como todo múltiplo de u ainda satisfaz a propriedade acima, é suficiente encontrar um múltiplo de u cuja e-ésima potência seja igual y. Aplicando a propriedade acima repetidas vezes, obtemos

$$u^{-e}\rho(c)u^e = \rho(x^{-e}cx^e) = \rho(y^{-1}cy) = \rho(y)^{-1}\rho(c)\rho(y) \implies \rho(c)(u^e\rho(y)^{-1}) = (u^e\rho(y)^{-1})\rho(c)$$

para todo $c \in C_1$. Isso significa que $u^e\rho(y)^{-1}$ é um automorfismo do módulo S. Como k é algebricamente fechado, o Lema de Schur nos dá um escalar $\lambda \in k$ não nulo tal que

$$u^e\rho(y)^{-1} = \lambda \,\mathrm{id}_S \implies u^e = \lambda\rho(y).$$

Utilizando mais uma vez que k é algebricamente fechado, encontramos $\mu \in k$ tal que $\mu^e = \lambda^{-1}$, logo, se definirmos $t \coloneqq \mu u$, então

$$t^e = \mu^e u^e = \lambda^{-1} \cdot \lambda\rho(y) = \rho(y).$$

Desse modo, o operador t que acabamos de construir satisfaz as propriedades necessárias.

Vamos provar as outras afirmações do enunciado. Seja T uma extensão de S para I_1, que agora sabemos que existe. Como $T_{C_1} = S$ é simples, certamente T também é simples. Considerando o módulo induzido S^{I_1}, note que

$$S^{I_1} = (T_{C_1})^{I_1} \cong (T_{C_1} \otimes k)^{I_1} \cong T \otimes k^{I_1},$$

onde k é o módulo trivial de kC_1 e o último isomorfismo é dado pelo item (5) do Lema 3.1.10. Veja que C_1 age trivialmente em k^{I_1}, porque o Exemplo 3.1.14 nos dá

$$(k^{I_1})_{C_1} \cong \bigoplus_{g\in[I_1/C_1]} {}^g k \cong k^e,$$

então podemos ver k^{I_1} como um $k[I_1/C_1]$-módulo. Mas I_1/C_1 é um grupo cíclico de ordem e e e não é divisível por p. Logo, k^{I_1} é semissimples e, como os $k[I_1/C_1]$-módulos simples são unidimensionais, k^{I_1} é a soma direta de e kI_1-módulos unidimensionais, que denotaremos por $W_1, \ldots, W_e$. Assim, S^{I_1} é semissimples porque

$$S^{I_1} \cong T \otimes k^{I_1} = T \otimes \left(\bigoplus_{i=1}^{e} W_i\right) \cong \bigoplus_{i=1}^{e} (T \otimes W_i)$$

e, como $(T \otimes W_i)_{C_1} = T_{C_1} \otimes (W_i)_{C_1} \cong S \otimes k \cong S$, cada um dos somandos acima é simples e é (isomorfo a) uma extensão de S para I_1. Pela Reciprocidade de Frobenius e pelo Lema de Schur, temos

$$\dim_k \operatorname{Hom}_{kI_1}(T, S^{I_1}) = \dim_k \operatorname{Hom}_{kC_1}(T_{C_1}, S) = \dim_k \operatorname{Hom}_{kC_1}(S, S) = 1,$$

ou seja, T aparece uma única vez como somando direto de S^{I_1}. Mas, inicialmente, T era uma extensão qualquer de S para I_1, então acabamos de mostrar que S^{I_1} é a soma direta de e extensões distintas de S e toda extensão é isomorfa a exatamente uma delas.

Falta provarmos a última afirmação do enunciado. Se T é uma extensão de S para I_1, então $T_{C_1} = S$ e o item (4) da Proposição 4.4.2 mostra que o bloco de kI_1 ao qual T pertence cobre o bloco β_1. Mas $\beta_1^{I_1}$ está definido e então este é o único bloco de kI_1 que cobre β_1, de onde segue que T pertence a $\beta_1^{I_1}$. Logo, as extensões de S são módulos simples pertencentes a $\beta_1^{I_1}$. Por outro lado, suponha que U seja um kI_1-módulo simples pertencente a $\beta_1^{I_1}$. Como I_1 estabiliza o bloco β_1, o item (3) da Proposição 4.4.2 mostra que U_{C_1} pertence ao bloco β_1. Pelo Teorema de Clifford, U_{C_1} é semissimples e, portanto, é a soma direta de cópias de S, já que S é o único kC_1-módulo simples pertencente a β_1. Mas

$$\dim_k \operatorname{Hom}_{kC_1}(U_{C_1}, S) = \dim_k \operatorname{Hom}_{kI_1}(U, S^{I_1})$$

e essa última dimensão é no máximo 1, porque U é simples e S^{I_1} é a soma direta de módulos simples distintos. Então devemos ter $\dim_k \operatorname{Hom}_{kC_1}(U_{C_1}, S) = 1$ e S aparece com multiplicidade 1 em U_{C_1}, logo $U_{C_1} \cong S$. Concluímos que U é (isomorfo a) uma extensão de S, como preciso. □

Lema 5.2.9. Se U é um kI_1-módulo pertencente a $\beta_1^{I_1}$, então $\operatorname{rad}(U) = \operatorname{rad}(U_{C_1})$.

Demonstração. Comecemos verificando que, se V é um kI_1-módulo pertencente a $\beta_1^{I_1}$, então

$$V \text{ é semissimples} \iff V_{C_1} \text{ é semissimples.}$$

Uma das implicações segue do Teorema de Clifford, pois C_1 é normal em I_1. Reciprocamente, suponha que V_{C_1} seja semissimples. Como S é o único β_1-módulo simples, vale $V_{C_1} \cong S^r$ para algum $r \geq 1$. Como D é um grupo de defeito de $\beta_1^{I_1}$ (porque $\beta_1^{I_1}$ está "entre" β_1 e B, que possuem D como grupo de defeito), o Teorema 4.2.2 diz que V é relativamente D-projetivo. Como $D \subseteq C_1$, V também é relativamente C_1-projetivo e temos

$$V \mid (V_{C_1})^{I_1} \cong (S^r)^{I_1} \cong (S^{I_1})^r.$$

Pela prova do Lema 5.2.8, S^{I_1} é semissimples, então V também é semissimples, como desejado.

Seja U um kI_1-módulo pertencente a $\beta_1^{I_1}$. Como $\operatorname{rad}(U_{C_1}) = \operatorname{rad}(kC_1)U$ e como $\operatorname{rad}(kC_1)$ é invariante por conjugação por I_1, já que C_1 é normal em I_1, sabemos que $\operatorname{rad}(U_{C_1})$ é um kI_1-submódulo de U. Como a restrição de $U/\operatorname{rad}(U_{C_1})$ é $U_{C_1}/\operatorname{rad}(U_{C_1})$, que é semissimples, o parágrafo anterior implica que $U/\operatorname{rad}(U_{C_1})$ é semissimples e temos $\operatorname{rad}(U) \subseteq \operatorname{rad}(U_{C_1})$. Por outro lado, como $U/\operatorname{rad}(U)$ é semissimples, a sua restrição a C_1 também o é e obtemos $\operatorname{rad}(U_{C_1}) \subseteq \operatorname{rad}(U)$. Concluímos que $\operatorname{rad}(U) = \operatorname{rad}(U_{C_1})$, como queríamos. □

Juntando os lemas anteriores, conseguimos provar a seguinte proposição:

Proposição 5.2.10. O bloco $\beta_1^{I_1}$ de kI_1 é uma álgebra de Brauer cuja árvore de Brauer é uma estrela com e arestas e com vértice excepcional no centro de multiplicidade $(p^n-1)/e$.

Demonstração. Pelo Lema 5.2.8, $\beta_1^{I_1}$ possui exatamente e módulos simples e cada um deles é uma extensão do único β_1-módulo simples S para I_1. Vamos analisar a cobertura projetiva deles. Seja T uma extensão de S para um kI_1-módulo e seja P a sua cobertura projetiva. Pelo Lema 5.2.9, $\operatorname{rad}(P) = \operatorname{rad}(P_{C_1})$, então

$$\frac{P_{C_1}}{\operatorname{rad}(P_{C_1})} = \left(\frac{P}{\operatorname{rad}(P)}\right)_{C_1} \cong T_{C_1} = S.$$

Pelo Exemplo 2.1.11, P_{C_1} é indecomponível e, pela Proposição 2.2.7, P_{C_1} também é projetivo. Desse modo, P_{C_1} é a cobertura projetiva de S. Pelo Teorema 5.2.1, P_{C_1} é unisseriado de comprimento p^n e cada um de seus fatores de composição é isomorfo a S. Mas o Lema 5.2.9 mostra que a série radical de P é igual à série radical de P_{C_1}, então também concluímos que P é unisseriado de comprimento p^n e cada um de seus fatores de composição é isomorfo a uma extensão de S para I_1. Em particular, pela prova do Lema 5.2.8, $\operatorname{rad}(P)/\operatorname{rad}^2(P)$ é da forma $T \otimes W$ para algum $k[I_1/C_1]$-módulo unidimensional W. Assim, $V \coloneqq P/\operatorname{rad}^2(P)$ é uma extensão de T por $T \otimes W$ que não cinde. Usaremos esse módulo V logo abaixo.

Até agora, demonstramos que todo kI_1-módulo projetivo indecomponível pertencente a $\beta_1^{I_1}$ é unisseriado de comprimento p^n e cada um de seus fatores de composição é isomorfo a uma extensão de S para I_1. Vamos verificar que o módulo W do parágrafo anterior é "comum" a todas essas coberturas, ou seja, veremos que, se Q é a cobertura projetiva de um $\beta_1^{I_1}$-módulo simples U, então $\operatorname{rad}(Q)/\operatorname{rad}^2(Q) \cong U \otimes W$. Como U é uma extensão de S para I_1, a demonstração do Lema 5.2.8 nos dá um $k[I_1/C_1]$-módulo unidimensional L tal que $U \cong T \otimes L$. Logo, utilizando as propriedades do produto tensorial dadas no Corolário 2.4.2, $V \otimes L$ é uma extensão do módulo simples $T \otimes L \cong U$ pelo módulo simples $T \otimes W \otimes L \cong U \otimes W$. Veja que essa extensão não cinde: se ela cindisse, $V \otimes L$ seria semissimples, mas então, se L' denota o inverso de L no grupo dual de I_1/C_1 (como definimos na Seção 2.4), teríamos que $V \cong (V \otimes L) \otimes L'$ também seria semissimples, uma contradição. Em particular, $(V \otimes L)/\operatorname{rad}(V \otimes L) \cong U$ e, pelo Lema 2.2.5, $V \otimes L$ é um quociente de Q. Segue que $\operatorname{rad}(V \otimes L)/\operatorname{rad}^2(V \otimes L) \cong U \otimes W$ é um quociente de $\operatorname{rad}(Q)/\operatorname{rad}^2(Q)$. Como Q é unisseriado, $\operatorname{rad}(Q)/\operatorname{rad}^2(Q)$ é simples, então obtemos $\operatorname{rad}(Q)/\operatorname{rad}^2(Q) \cong U \otimes W$, como queríamos.

Desse modo, mostramos que o segundo fator de composição de um $\beta_1^{I_1}$-módulo projetivo indecomponível é sempre isomorfo ao produto tensorial de seu primeiro fator de composição com W. Imitando o último parágrafo do Exemplo 2.2.12, concluímos que os fatores de composição da cobertura projetiva de um $\beta_1^{I_1}$-módulo simples T são, em ordem,

$$T,\ T \otimes W,\ T \otimes W \otimes W,\ \ldots,\ T \otimes W^{\otimes p^n - 1} \cong T.$$

O último isomorfismo acima segue do Teorema 2.3.17 ou então do fato de que a ordem do grupo dual de I_1/C_1 é e (porque I_1/C_1 é cíclico e e não divide a característica p de k, que é algebricamente fechado) e de que e divide $p^n - 1$ pelo Lema 5.1.8.

Fixando um $\beta_1^{I_1}$-módulo simples T, defina

$$T_i \coloneqq T \otimes W^{\otimes i-1}$$

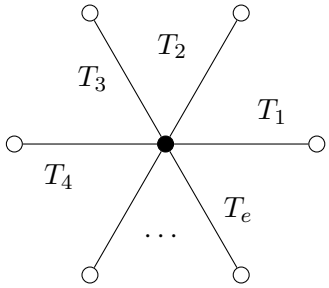
para $i \geq 1$. Note que $T_{i+1} \cong T_i \otimes W$ e que cada T_i é um kI_1-módulo simples pertencente a $\beta_1^{I_1}$, porque C_1 age trivialmente nas potências de W e então cada T_i é uma extensão de S para I_1. Vamos provar que $T_1, \ldots, T_e$ são dois a dois não isomorfos e que $T_{e+1} \cong T_1$. Como W possui um inverso no grupo dual e como o produto tensorial de um módulo simples com um unidimensional continua simples, vemos que tomar o produto tensorial por W permuta as e classes de isomorfismo de $\beta_1^{I_1}$-módulos simples. Devemos mostrar que há apenas uma órbita. De

fato, pelo que demonstramos, os fatores de composição da cobertura projetiva de um $\beta_1^{I_1}$-módulo simples estão todos numa mesma órbita da ação por W. Mas, pelo Teorema 4.1.17, dados dois $\beta_1^{I_1}$-módulos simples, conseguimos encontrar uma sequência de módulos simples conectando os dois de modo que módulos consecutivos na sequência são fatores de composição do mesmo projetivo indecomponível e, então, estão na mesma órbita da ação de W. Como resultado, todo os $\beta_1^{I_1}$-módulos simples devem estar na mesma órbita. Logo, os fatores de composição da cobertura projetiva de um $\beta_1^{I_1}$-módulo simples T_i são, em ordem,

$$T_i, T_{i+1}, \ldots, T_e, T_1, T_2, \ldots, T_e, T_1, T_2, \ldots, T_i,$$

onde há p^n módulos na lista acima.

Podemos concluir a demonstração! Considere a seguinte árvore de Brauer:



A multiplicidade do vértice excepcional é $(p^n - 1)/e$. Tomando uma álgebra de Brauer associada à árvore, o algoritmo mostra que a cobertura projetiva de T_i é unisseriada de comprimento

$$1 + (e-1) \cdot \frac{p^n - 1}{e} + \left(\frac{p^n - 1}{e} - 1 \right) + 1 = p^n$$

e a ordem dos fatores de composição segue a ordem dos índices. Mas essa é exatamente a estrutura dos $\beta_1^{I_1}$-módulos projetivos indecomponíveis, como acabamos de provar! Concluímos que $\beta_1^{I_1}$ é uma álgebra de Brauer para a árvore de Brauer acima. □

Para concluir o Teorema 5.2.6, iremos mostrar que b_1 e $\beta_1^{I_1}$ são Morita equivalentes! O que estabelece a equivalência é o seguinte lema:

Lema 5.2.11. Se V é um kI_1-módulo pertencente a $\beta_1^{I_1}$, então V^{N_1} é um kN_1-módulo pertencente a b_1. Além disso, todo b_1-módulo é isomorfo a um desses módulos induzidos e, se V_1 e V_2 são $\beta_1^{I_1}$-módulos, então a indução define um isomorfismo de $\mathrm{Hom}_{kI_1}(V_1, V_2)$ em $\mathrm{Hom}_{kN_1}(V_1^{N_1}, V_2^{N_1})$.

Demonstração. Sejam $g_1 = 1, g_2, \ldots, g_r$ representantes das classes laterais à esquerda de I_1 em N_1. Defina também $\beta_i := g_i \beta_1 g_i^{-1}$ para $1 < i \leq r$. Como I_1 é o estabilizador de β_1 em N_1, os blocos $\beta_1, \ldots, \beta_r$ são os diferentes conjugados de β_1 em N_1. Seja V um kI_1-módulo pertencente a $\beta_1^{I_1}$. Como β_1 não possui conjugados em I_1, ele é o único bloco de kC_1 coberto por $\beta_1^{I_1}$, então o item (3) da Proposição 4.4.2 mostra que V_{C_1} pertence a β_1. Como I_1 é normal em N_1 (já que I_1/C_1 é subgrupo do grupo cíclico N_1/C_1), o Exemplo 3.1.14 nos dá

$$(V^{N_1})_{C_1} = ((V^{N_1})_{I_1})_{C_1} \cong ({}^{g_1}V)_{C_1} \oplus \cdots \oplus ({}^{g_r}V)_{C_1} = {}^{g_1}(V_{C_1}) \oplus \cdots \oplus {}^{g_r}(V_{C_1}).$$

Note que o conjugado ${}^{g_i}(V_{C_1})$ pertence ao bloco β_i. Desse modo, todo somando indecomponível de V^{N_1} pertence a um bloco que cobre os blocos $\beta_1, \ldots, \beta_r$. Mas $\beta_1^{N_1}$ está definido e é igual a b_1, logo este é o único bloco de kN_1 que cobre os conjugados de β_1 e segue que V^{N_1} pertence a b_1.

Por outro lado, seja W um kN_1-módulo pertencente a b_1. Como b_1 cobre β_1, o item (3) da Proposição 4.4.2 nos dá a seguinte decomposição de W_{C_1} com relação ao blocos de kC_1:

$$W_{C_1} = \beta_1 W \oplus \cdots \oplus \beta_r W.$$

Como I_1 é o estabilizador de β_1, não é difícil ver que $\beta_1 W$ é um kI_1-submódulo de W. Além disso, se $g \in N_1$, então podemos escrever $g = g_i x$ para algum $1 \leq i \leq r$ e $x \in I_1$ e temos

$$g \cdot \beta_1 W = g_i \cdot (x\beta_1 x^{-1})(xW) = g_i \cdot \beta_1 W = (g_i \beta_1 g_i^{-1})(g_i W) = \beta_i W.$$

Isso mostra que W é a soma direta das translações $g \cdot \beta_1 W$ ($g \in N_1$) e que o estabilizador do subespaço $\beta_1 W$ é precisamente I_1. Pelo Corolário 3.1.5, $W \cong (\beta_1 W)^{N_1}$, onde $\beta_1 W$ está sendo visto com um kI_1-módulo. Além disso, como $(\beta_1 W)_{C_1}$ pertence a β_1, que é coberto apenas por $\beta_1^{I_1}$, esse kI_1-módulo $\beta_1 W$ pertence a $\beta_1^{I_1}$. Isso prova que todo b_1-módulo é isomorfo à indução de um $\beta_1^{I_1}$-módulo a N_1.

Vamos para a última afirmação. Se $\varphi \in \mathrm{Hom}_{kI_1}(V_1, V_2)$, vimos no Lema 3.1.11 como definir naturalmente um homomorfismo induzido $\varphi^{N_1} \in \mathrm{Hom}_{kN_1}(V_1^{N_1}, V_2^{N_1})$. Se identificarmos V_1 e V_2 do modo canônico como kI_1-submódulos de $V_1^{N_1}$ e $V_2^{N_1}$, respectivamente, segue que φ^{N_1} é uma extensão de φ, então a transformação linear de $\mathrm{Hom}_{kI_1}(V_1, V_2)$ em $\mathrm{Hom}_{kN_1}(V_1^{N_1}, V_2^{N_1})$ que leva φ em φ^{N_1} é injetora. É essa transformação linear que define o isomorfismo do enunciado. Para mostrar que ela é sobrejetora, temos de verificar que os espaços envolvidos possuem a mesma dimensão. Pela Reciprocidade de Frobenius,

$$\mathrm{Hom}_{kN_1}(V_1^{N_1}, V_2^{N_1}) \cong \mathrm{Hom}_{kI_1}(V_1, (V_2^{N_1})_{I_1}) \cong \mathrm{Hom}_{kI_1}(V_1, \beta_1^{I_1}(V_2^{N_1})_{I_1}),$$

onde usamos o Exercício A.4.2 e que V_1 pertence a $\beta_1^{I_1}$. Basta mostramos que $\beta_1^{I_1}(V_2^{N_1})_{I_1} \cong V_2$. Sabemos que $(V_2^{N_1})_{I_1}$ é a soma direta dos conjugados ${}^{g_1}V_2, \ldots, {}^{g_r}V_2$. Como fizemos no primeiro parágrafo, $({}^{g_i}V_2)_{C_1}$ pertence ao bloco β_i, então, se $i > 1$, nenhum somando indecomponível de ${}^{g_i}V_2$ pode pertencer a $\beta_1^{I_1}$, já que $\beta_1^{I_1}$ apenas cobre o bloco β_1. Logo, os somandos indecomponíveis de $(V_2^{N_1})_{I_1}$ pertencentes a $\beta_1^{I_1}$ são os somandos indecomponíveis de ${}^{g_1}V_2 = V_2$ pertencentes a esse bloco. Como o próprio V_2 pertence a $\beta_1^{I_1}$, concluímos que $\beta_1^{I_1}(V_2^{N_1})_{I_1} \cong V_2$, como preciso. □

Com isso em mãos, conseguimos ver que $\beta_1^{I_1}$-módulos e b_1-módulos se comportam de modo muito parecido:

Lema 5.2.12. Se U, V, W, V_1, V_2 são $\beta_1^{I_1}$-módulos, se $\varphi \in \mathrm{End}_{kI_1}(V)$ e se $\psi \in \mathrm{Hom}_{kI_1}(V_1, V_2)$, então valem as seguintes afirmações:

(1) φ é a identidade se, e somente se, φ^{N_1} é a identidade.

(2) ψ é injetor (sobrejetor) se, e somente se, ψ^{N_1} é injetor (sobrejetor).

(3) V é simples (semissimples, projetivo) se, e somente se, V^{N_1} é simples (semissimples, projetivo).

(4) Se $\alpha \in \mathrm{Hom}_{kI_1}(U, V)$ e $\lambda \in \mathrm{Hom}_{kI_1}(V, W)$, então a sequência

$$0 \longrightarrow U \xrightarrow{\alpha} V \xrightarrow{\lambda} W \longrightarrow 0$$

é exata se, e somente se, a sequência

$$0 \longrightarrow U^{N_1} \xrightarrow{\alpha^{N_1}} V^{N_1} \xrightarrow{\lambda^{N_1}} W^{N_1} \longrightarrow 0$$

é exata.

(5) Temos isomorfismos $\mathrm{rad}(V^{N_1}) \cong \mathrm{rad}(V)^{N_1}$ e $(V/\mathrm{rad}(V))^{N_1} \cong V^{N_1}/\mathrm{rad}(V^{N_1})$.

Os itens (1), (2) e (4) também são válidos em um contexto mais geral e seguem facilmente do Lema 3.1.11 e de sua demonstração. Eles até poderiam ser apresentados anteriormente. Estamos listando-os aqui para juntar alguns resultados úteis em um só lema.

Demonstração. Se $\psi \in \mathrm{Hom}_{kI_1}(V_1, V_2)$, então ψ^{N_1} é dado por

$$\psi^{N_1}\left(\sum_{s\in[N_1/I_1]} s\otimes v_s\right) = \sum_{s\in[N_1/I_1]} s\otimes\psi(v_s),$$

como observado no Lema 3.1.11. Como todo elemento de $V_1^{N_1}$ e de $V_2^{N_1}$ se escreve de maneira única como soma de tensores da forma acima, não é difícil ver que

$$\operatorname{im}\psi^{N_1} = \sum_{s\in[N_1/I_1]} s\otimes\operatorname{im}\psi \quad \text{e} \quad \ker\psi^{N_1} = \sum_{s\in[N_1/I_1]} s\otimes\ker\psi.$$

Disso segue facilmente o item (2) e, sem muito mais esforço, também obtemos o item (4). Note que essa demonstração é geral e poderia ter sido colocada no Lema 3.1.11.

Para o item (1), se φ é a identidade, então é imediato da descrição de φ^{N_1} (que é análoga à de ψ^{N_1} do parágrafo anterior) que este homomorfismo também é a identidade. Como a função que leva φ em φ^{N_1} é injetora, também vale a recíproca. Mais uma vez, essa demonstração independe do contexto considerado.

Consideremos o item (3). Veja que um módulo é simples se, e somente se, qualquer homomorfismo saindo dele é nulo ou injetor. Supondo V simples, vamos utilizar isso para mostrar que V^{N_1} também é simples. Se $\psi' : V^{N_1} \to W'$ é um homomorfismo de b_1-módulos, então podemos assumir pelo Lema 5.2.11 que $W' = W^{N_1}$ para algum $\beta_1^{I_1}$-módulo W e que $\psi' = \psi^{N_1}$ para algum homomorfismo $\psi : V \to W$. Como V é simples, ψ é nulo ou injetor, então o item (2) garante que ψ^{N_1} é nulo ou injetor. Isso mostra que V^{N_1} é simples. De modo análogo, o item (2) também nos permite mostrar que, se V^{N_1} é simples, então V também é simples.

Agora suponha que V seja semissimples. Então existem $\beta_1^{I_1}$-módulos simples $S_1, \ldots, S_r$ tais que $V \cong S_1 \oplus \cdots \oplus S_r$. Em termos de morfismos, isso quer dizer que existem homomorfismos $\pi_i : V \to S_i$ e $\mu_i : S_i \to V$ para $1 \le i \le r$ tais que

$$\sum_{i=1}^{r} \mu_i\pi_i = \mathrm{id}_V$$

e

$$\pi_i\mu_i = \mathrm{id}_{S_i} \quad \text{e} \quad \pi_i\mu_j = 0 \ (i \neq j).$$

Essas condições garantem que V é a soma de cópias dos S_i's e que essa soma é direta. Induzindo para N_1 e aplicando o item (1), obtemos homomorfismos $\pi_i^{N_1} : V^{N_1} \to S_i^{N_1}$ e $\mu_i^{N_1} : S_i^{N_1} \to V^{N_1}$ para $1 \le i \le r$ tais que

$$\sum_{i=1}^{r} \mu_i^{N_1}\pi_i^{N_1} = \mathrm{id}_{V^{N_1}}$$

e

$$\pi_i^{N_1}\mu_i^{N_1} = \mathrm{id}_{S_i^{N_1}} \quad \text{e} \quad \pi_i^{N_1}\mu_j^{N_1} = 0 \ (i \neq j).$$

Mas isso diz que V^{N_1} é a soma direta das imagens dos homomorfismos injetores $\mu_i^{N_1}$. Logo, $V^{N_1} \cong S_1^{N_1} \oplus \cdots \oplus S_r^{N_1}$ e, pelo parágrafo anterior, V^{N_1} é semissimples. Reciprocamente, se V^{N_1} é semissimples, então o Lema 5.2.11 e o parágrafo anterior garantem a existência de $\beta_1^{I_1}$-módulos simples $S_1, \ldots, S_r$ tais que $V^{N_1} \cong S_1^{N_1} \oplus \cdots \oplus S_r^{N_1}$. Esse mesmo lema também nos permite encontrar homomorfismos $\pi_i : V \to S_i$ e $\mu_i : S_i \to V$ tais que $\pi_i^{N_1}$ e $\mu_i^{N_1}$ satisfazem as relações acima. Usando a injetividade da transformação $\psi \mapsto \psi^{N_1}$ e o item (1), concluímos que π_i e μ_i também satisfazem as relações anteriores e temos $V \cong S_1 \oplus \cdots \oplus S_r$, comprovando que V também é semissimples.

Finalmente, suponha que V seja projetivo e mostremos que V^{N_1} também o é. Seja $\varphi' : U' \to W'$ um homomorfismo sobrejetor de b_1-módulos e $\psi' : V^{N_1} \to W'$ um homomorfismo de

b_1-módulos qualquer. Pelo Lema 5.2.11, podemos assumir que $U' = U^{N_1}$ e $W' = W^{N_1}$ para certos $\beta_1^{I_1}$-módulos U e W, e que $\varphi' = \varphi^{N_1}$ e $\psi' = \psi^{N_1}$ para certos homomorfismos $\varphi : U \to W$ e $\psi : V \to W$. Pelo item (2), φ é sobrejetor e, como V é projetivo, existe um homomorfismo $\rho : V \to U$ tal que $\varphi\rho = \psi$. Induzindo para N_1, obtemos $\varphi^{N_1}\rho^{N_1} = \psi^{N_1}$. Segue da Proposição 2.2.1 que V^{N_1} é de fato projetivo. Reciprocamente, um argumento análogo utilizando o item (2) e o Lema 5.2.11 mostra que, se V^{N_1} é projetivo, então o mesmo vale para V. Isso conclui o item (3).

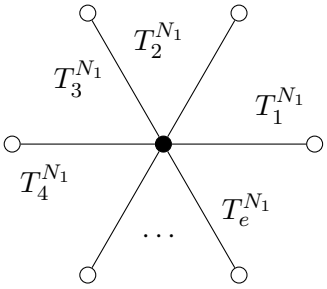
Vamos para o último item. Pelo item (4), se U e V são $\beta_1^{I_1}$-módulos e $U \leq V$, então U^{N_1} é canonicamente isomorfo a um submódulo de V^{N_1} e temos $(V/U)^{N_1} \cong V^{N_1}/U^{N_1}$. Em particular, tomando $U = \operatorname{rad}(V)$, vemos que

$$\left(\frac{V}{\operatorname{rad}(V)}\right)^{N_1} \cong \frac{V^{N_1}}{\operatorname{rad}(V)^{N_1}}.$$

Como $V/\operatorname{rad}(V)$ é semissimples, o item (3) mostra que o módulo acima é semissimples e então, após identificar $\operatorname{rad}(V)^{N_1}$ como submódulo de V^{N_1}, temos $\operatorname{rad}(V^{N_1}) \subseteq \operatorname{rad}(V)^{N_1}$. Por outro lado, pelo Lema 5.2.11, $\operatorname{rad}(V^{N_1}) \cong U^{N_1}$ para algum $\beta_1^{I_1}$-módulo U. Como $\operatorname{rad}(V^{N_1}) \subseteq V^{N_1}$, podemos assumir pelo item (2) que $U \leq V$ e, identificando U^{N_1} como submódulo de V^{N_1}, também podemos supor que $\operatorname{rad}(V^{N_1}) = U^{N_1}$. Como $V^{N_1}/\operatorname{rad}(V^{N_1}) \cong (V/U)^{N_1}$ é semissimples, o item (3) mostra que V/U é semissimples e então $\operatorname{rad}(V) \subseteq U$, de onde segue $\operatorname{rad}(V)^{N_1} \subseteq U^{N_1} = \operatorname{rad}(V^{N_1})$. Concluímos que $\operatorname{rad}(V)^{N_1} = \operatorname{rad}(V^{N_1})$ e, pelo isomorfismo em destaque acima, $(V/\operatorname{rad}(V))^{N_1} \cong V^{N_1}/\operatorname{rad}(V^{N_1})$. A demonstração está concluída. □

Observação 5.2.13. A prova dos itens (3) e (5) é bem "funtorial" e não depende do uso explícito da definição de indução, apenas de suas propriedades. Isso é interessante, porque evidencia que as propriedades obtidas vêm do simples fato de haver uma equivalência das categorias de módulos, que pode ser qualquer. No Exercício A.5.8, são apresentadas algumas ideias de como utilizar essa abordagem mais funtorial para provar os outros itens.

Iremos demonstrar o Teorema 5.2.6! Sejam $T_1, \ldots, T_e$ os $\beta_1^{I_1}$-módulos simples. O item (3) do Lema 5.2.12 mostra que $T_1^{N_1}, \ldots, T_e^{N_1}$ são os b_1-módulos simples. Se $P_1, \ldots, P_e$ são as coberturas projetivas dos módulos $T_1, \ldots, T_e$, respectivamente, então o item (3) desse mesmo lema implica que cada $P_i^{N_1}$ é projetivo e, pelo item (5), $P_i^{N_1}/\operatorname{rad}(P_i^{N_1}) \cong T_i^{N_1}$, então $P_i^{N_1}$ é a cobertura projetiva de $T_i^{N_1}$. Se $T_1, \ldots, T_e$ estão listados na ordenação circular dada pela árvore de Brauer de $\beta_1^{I_1}$, então cada P_i é unisseriado de comprimento p^n e seus fatores de composição são T_i, T_{i+1}, T_{i+2}, e assim em diante, seguindo a ordenação. Pelo item (5) do Lema 5.2.12, os quocientes radicais de $P_i^{N_1}$ são, em ordem, $T_i^{N_1}, T_{i+1}^{N_1}, T_{i+2}^{N_1}, \ldots$, de onde segue que $P_i^{N_1}$ é unisseriado de comprimento p^n e com esses fatores de composição. Desse modo, a estrutura dos b_1-módulos projetivos indecomponíveis é semelhante à dos $\beta_1^{I_1}$-módulos projetivos indecomponíveis e concluímos que b_1 é uma álgebra de Brauer cuja árvore de Brauer é:



A multiplicidade é $(p^n - 1)/e$.

Para concluir a seção, vamos enunciar mais um resultado:

Corolário 5.2.14. Todo b_1-módulo indecomponível é quociente de um único b_1-módulo indecomponível projetivo. Em particular, existem exatamente ep^n classes de isomorfismo de b_1-módulos indecomponíveis e cada um deles é unisseriado.

A demonstração é muito análoga ao que fizemos no Exemplo 2.3.20.

Observação 5.2.15. Quando D é normal em G, vale $N = G$. Como N_1 contém N, também temos $N_1 = G$. Ou seja, b_1 é um bloco de G. Mas sabemos que $b_1^G = B$, então $b_1 = B$. Logo, o Teorema 5.2.6 já nos permite descrever a estrutura de qualquer bloco com grupo de defeito normal e cíclico! Observe que temos mais informação do que o Teorema 5.1.7, porque sabemos que a árvore de Brauer deve ser uma estrela neste caso. Repare como esta é uma generalização dos Exemplos 2.2.12 e 2.3.20 e também como o grupo de defeito substitui o papel antes exercido pelo p-subgrupo de Sylow.

5.3 Coberturas projetivas e envolventes injetivas

Vamos esquecer um pouco sobre os blocos com grupo de defeito cíclico para introduzir algumas ideias importantes de álgebra homológica. Iremos estudar melhor a relação entre módulos projetivos e módulos quaisquer, generalizando o que vimos no Teorema 2.2.4. Esta seção deveria estar no Capítulo 2, mas vamos deixá-la aqui porque é neste capítulo que usaremos os resultados abordados.

Seja A uma k-álgebra de dimensão finita qualquer (apenas nesta seção, k não precisa ser algebricamente fechado). Se $\varphi : U \to V$ é um homomorfismo sobrejetor de A-módulos, então diremos que φ é um **epimorfismo essencial** se $\varphi(U') \subsetneq V$ para todo submódulo próprio $U' < U$. Intuitivamente, nesse caso, V é um quociente de U, mas é preciso toda a informação de U para "montar" V. Em algum sentido, φ é "minimal". Também é possível dar uma caracterização em termos de homomorfismos:

Lema 5.3.1. Um homomorfismo sobrejetor de A-módulos $\varphi : U \to V$ é um epimorfismo essencial se, e somente se, para todo homomorfismo $\psi : W \to U$ vale a implicação

$$\varphi\psi \text{ é sobrejetor} \implies \psi \text{ é sobrejetor.}$$

Demonstração. ($\implies$) Suponha que φ seja um epimorfismo essencial e seja $\psi : W \to U$ um homomorfismo. Mostremos a contrapositiva da implicação do enunciado. Se ψ não é sobrejetor, então $\operatorname{im}\psi$ é um submódulo próprio de U e, como φ é epimorfismo essencial, $\varphi(\operatorname{im}\psi) = \operatorname{im}\varphi\psi$ é um submódulo próprio de V, provando que $\varphi\psi$ não é sobrejetor.

($\impliedby$) Suponha que φ não seja um epimorfismo essencial. Logo, existe um submódulo próprio U' de U tal que $\varphi(U') = V$. Defina $\psi : U' \to U$ como sendo a inclusão. Desse modo, $\varphi\psi$ é sobrejetor mas ψ não o é. Logo, a implicação do enunciado não pode ser verdadeira. □

Mas como encontrar exemplos de epimorfismos essenciais? A melhor fonte é o Lema de Nakayama! Esse lema é bem mais geral e possui diversas versões. Apenas enunciaremos o que será preciso no nosso contexto.

Lema 5.3.2 (Nakayama)**.** Se U é um A-módulo, então a projeção canônica $U \to U/\operatorname{rad}(U)$ é um epimorfismo essencial. Equivalentemente, se V é um submódulo de U satisfazendo $V + \operatorname{rad}(U) = U$, então $V = U$.

Demonstração. Seja V um submódulo próprio de U. Por questões de dimensão, conseguimos encontrar um submódulo maximal M de U contendo V. Como $\operatorname{rad}(U)$ é a interseção dos submódulos maximais de U, segue que $\operatorname{rad}(U) \subseteq M$ e, por isso, $V + \operatorname{rad}(U) \subseteq M$. Assim,

$$\pi(V) = \frac{V + \operatorname{rad}(U)}{\operatorname{rad}(U)} \subseteq \frac{M}{\operatorname{rad}(U)} \subsetneq \frac{U}{\operatorname{rad}(U)},$$

provando que o homomorfismo sobrejetor $U \to U/\operatorname{rad}(U)$ é um epimorfismo essencial. □

Temos algumas propriedades importantes:

Proposição 5.3.3. Valem as seguintes afirmações:

(1) Sejam $\varphi : U \to V$ e $\psi : V \to W$ homomorfismos. Se dois homomorfismos dentre φ, ψ e $\psi\varphi$ são epimorfismos essenciais, então o mesmo vale para o terceiro.

(2) Se $\varphi : U \to V$ é um homomorfismo de A-módulos, então φ é um epimorfismo essencial se e só se o homomorfismo induzido $U/\operatorname{rad}(U) \to V/\operatorname{rad}(V)$ é um isomorfismo.

(3) Se $\varphi : U_1 \to V_1$ e $\psi : U_2 \to V_2$ são homomorfismos, então φ e ψ são epimorfismos essenciais se e somente se
$$(\varphi \oplus \psi) : U_1 \oplus U_2 \to V_1 \oplus V_2$$
é um epimorfismo essencial.

Demonstração. Para mostrar (1), sejam $\varphi : U \to V$ e $\psi : V \to W$ homomorfismos. Temos de considerar três casos. Primeiramente, suponha que φ e ψ sejam epimorfismos essenciais. Logo, a composição $\psi\varphi$ é um homomorfismo sobrejetor. Além disso, se U' é um submódulo próprio de U, então $\varphi(U')$ é um submódulo próprio de V e, consequentemente, $\psi\varphi(U')$ é um submódulo próprio de W. Isso garante que $\psi\varphi$ é epimorfismo essencial.

Agora, suponha que φ e $\psi\varphi$ sejam epimorfismos essenciais. Como $\psi\varphi$ é sobrejetor, certamente o mesmo vale para ψ. Se V' é um submódulo próprio de V, então $\varphi^{-1}(V')$ é um submódulo de U que é necessariamente próprio, já que φ é sobrejetor. Novamente pela sobrejetividade de φ, temos $\varphi(\varphi^{-1}(V')) = V'$ e, como $\psi\varphi$ é epimorfismo essencial, obtemos que $\psi(V') = \psi\varphi(\varphi^{-1}(V'))$ é um submódulo próprio de W. Logo, ψ é um epimorfismo essencial.

Por fim, para concluir (1), suponha que ψ e $\psi\varphi$ sejam epimorfismos essenciais. Pelo Lema 5.3.1, φ é sobrejetor. Se U' é um submódulo próprio de U, então $\psi\varphi(U')$ é submódulo próprio de W porque $\psi\varphi$ é epimorfismo essencial. Mas ψ é sobrejetor, então $\varphi(U')$ deve ser submódulo próprio de V, de onde deduzimos que φ é epimorfismo essencial.

Para (2), considere o seguinte diagrama comutativo:

$$\begin{array}{ccc} U & \xrightarrow{\quad\varphi\quad} & V \\ \downarrow & & \downarrow \\ U/\operatorname{rad}(U) & \xrightarrow{\quad\overline{\varphi}\quad} & V/\operatorname{rad}(V) \end{array}$$

Aqui, os mapas verticais são as projeções canônicas e $\overline{\varphi}$ é o homomorfismo induzido por φ no quociente. Pelo Lema de Nakayama, os mapas verticais são epimorfismos essenciais, então o item (1) mostra que φ é epimorfismo essencial se, e somente se, $\overline{\varphi}$ o é. Se $\overline{\varphi}$ é isomorfismo, então ele certamente é epimorfismo essencial. Por outro lado, como $U/\operatorname{rad}(U)$ é semissimples, podemos escrever $U/\operatorname{rad}(U) = \ker\overline{\varphi} \oplus W$ para algum submódulo W de $U/\operatorname{rad}(U)$. Logo, como $\overline{\varphi}(W) = V/\operatorname{rad}(V)$, se $\overline{\varphi}$ é epimorfismo essencial, então deve valer $\ker\overline{\varphi} = 0$ e $\overline{\varphi}$ é um isomorfismo. Isso conclui (2).

Para (3), note que, pelo Exercício A.1.2, o homomorfismo
$$\frac{U_1 \oplus U_2}{\operatorname{rad}(U_1 \oplus U_2)} \to \frac{V_1 \oplus V_2}{\operatorname{rad}(V_1 \oplus V_2)}$$
induzido por $\varphi \oplus \psi$ pode ser identificado com
$$\overline{\varphi} \oplus \overline{\psi} : \frac{U_1}{\operatorname{rad}(U_1)} \oplus \frac{U_2}{\operatorname{rad}(U_2)} \to \frac{V_1}{\operatorname{rad}(V_1)} \oplus \frac{V_2}{\operatorname{rad}(V_2)},$$
onde $\overline{\varphi} : U_1/\operatorname{rad}(U_1) \to V_1/\operatorname{rad}(V_1)$ e $\overline{\psi} : U_2/\operatorname{rad}(U_2) \to V_2/\operatorname{rad}(V_2)$ são os homomorfismos induzidos por φ e ψ. É fácil ver que $\overline{\varphi}\oplus\overline{\psi}$ é um isomorfismo se e somente se $\overline{\varphi}$ e $\overline{\psi}$ são isomorfismos, então (3) é uma consequência de (2). □

Se U é um A-módulo qualquer, podemos nos perguntar se existe um maior A-módulo V tal que existe um epimorfismo essencial $V \to U$. Devemos esclarecer o que seria um "maior" módulo satisfazendo essa propriedade. Por exemplo, se $W \to V$ e $V \to U$ são epimorfismos essenciais, o item (1) da Proposição 5.3.3 mostra que a composição $W \to U$ também é um epimorfismo essencial. Nesse sentido, W é maior do que V. Assim, faz sentido estudar os módulos P tais que todo epimorfismo essencial $V \to P$ é um isomorfismo. Esses seriam os potenciais candidatos aos maiores módulos "cobrindo" U. Já conhecemos tais módulos!

Proposição 5.3.4. Seja P um A-módulo. Então todo epimorfismo essencial $\varphi : V \to P$ é um isomorfismo se, e somente se, P é um módulo projetivo.

Demonstração. Utilizaremos a caracterização (2) da Proposição 2.2.1.

($\implies$) Para mostrar que P é projetivo, tome um homomorfismo sobrejetor $\varphi : U \to P$ e mostremos que φ cinde. Podemos tomar um submódulo V de U tal que $\varphi(V) = P$ e que é minimal para essa propriedade. Da minimalidade de V, vemos que φ não leva nenhum submódulo próprio de V sobrejetivamente em P, então a restrição de φ a V é um epimorfismo essencial. Pela hipótese, essa restrição é um isomorfismo e, olhando para a inversa, conseguimos encontrar um homomorfismo $\psi : P \to U$ satisfazendo $\varphi\psi = \mathrm{id}_P$, provando que φ cinde.

($\impliedby$) Tome um epimorfismo essencial $\varphi : V \to P$. Se P é projetivo, então φ cinde e podemos escrever $V = \ker\varphi \oplus W$ para algum submódulo W de V. Como $\varphi(W) = \varphi(V) = P$, devemos ter $W = V$, ou seja, $\ker\varphi = 0$ e φ é um isomorfismo. □

Por isso, vamos estudar homomorfismos sobrejetores $\varphi : P \to U$ onde P é um A-módulo projetivo. Nesse caso, se φ é um epimorfismo essencial, dizemos que P (juntamente com φ) é uma **cobertura projetiva** de U. Essa definição generaliza a definição dada logo após o Teorema 2.2.4. De fato, se P é a cobertura projetiva de um A-módulo simples S como definido nesse capítulo anterior, então o Lema de Nakayama mostra que a projeção $P \to P/\operatorname{rad}(P) \cong S$ é um epimorfismo essencial e, portanto, P é uma cobertura projetiva de S como definimos agora.

Olhar para as coberturas projetivas é algo bem útil no estudo dos A-módulos, especialmente quando lidamos com o espaço $\overline{\mathrm{Hom}}_A(U, V)$ definido na Seção 3.3. Por exemplo, um resultado simples mas útil pode ser obtido diretamente da definição de módulos projetivos (faça o Exercício A.3.14):

Lema 5.3.5. Se $\psi : U \to V$ é um homomorfismo de A-módulos e se $\varphi : P \to V$ é uma cobertura projetiva, então ψ se fatora através de um projetivo se, e somente se, existe um homomorfismo $\alpha : U \to P$ tal que $\psi = \varphi\alpha$.

Não é imediato da definição que coberturas projetivas sempre existem, mas isso é verdade!

Proposição 5.3.6. Todo A-módulo admite uma cobertura projetiva.

Demonstração. Seja U um A-módulo. Como $U/\operatorname{rad}(U)$ é semissimples, podemos escrevê-lo como soma direta de módulos simples:

$$\frac{U}{\operatorname{rad}(U)} = S_1 \oplus \cdots \oplus S_r.$$

Para cada $1 \leq i \leq r$, seja $\varphi_i : P_i \to S_i$ a cobertura projetiva de S_i, cuja existência está garantida pelo Teorema 2.2.4. Como cada φ_i é um epimorfismo essencial, podemos aplicar o item (3) da Proposição 5.3.3 repetidas vezes para mostrar que

$$\varphi_1 \oplus \cdots \oplus \varphi_r : P_1 \oplus \cdots \oplus P_r \to U/\operatorname{rad}(U)$$

é um epimorfismo essencial. Mas $P_1 \oplus \cdots \oplus P_r$ é projetivo, então encontramos a cobertura projetiva! □

Observação 5.3.7. Aqui é essencial estar trabalhando com uma álgebra de dimensão finita. Sobre um anel qualquer, nem sempre existem coberturas projetivas!

Um ponto fundamental na hora de lidar com coberturas projetivas é que elas são únicas!

Proposição 5.3.8. Seja $\varphi : P \to U$ uma cobertura projetiva de um A-módulo U e seja $\psi : Q \to U$ um homomorfismo sobrejetor qualquer onde Q é um A-módulo projetivo. Então:

(1) Existe um homomorfismo sobrejetor $\rho : Q \to P$ tal que $\varphi\rho = \psi$.

(2) Podemos decompor $Q = R \oplus \ker \rho$ e a restrição de ψ a R é uma cobertura projetiva de U.

(3) O par formado por Q e ψ é uma cobertura projetiva de U se, e somente se, ρ é um isomorfismo.

Demonstração. Como φ é sobrejetor e como Q é projetivo, segue do item (3) da Proposição 2.2.1 a existência de um homomorfismo $\rho : Q \to P$ tal que $\varphi\rho = \psi$. Como φ é um epimorfismo essencial e como a composição $\varphi\rho = \psi$ é sobrejetora por hipótese, o Lema 5.3.1 mostra que ρ é sobrejetor. Isso mostra (1).

Como P é projetivo e $\rho : Q \to P$ é sobrejetor, sabemos que ρ cinde e, por isso, podemos escrever $Q = R \oplus \ker \rho$ para algum submódulo R de Q. Como $R \cong Q/\ker \rho \cong P$, R é projetivo, então basta verificarmos que a restrição de ψ a R é um epimorfismo essencial para mostrar que ela é uma cobertura projetiva de U. De fato, a restrição de ψ a R é a composição da restrição de ρ a R, que é um isomorfismo, com φ, que é um epimorfismo essencial. Pelo item (1) da Proposição 5.3.3, a restrição de ψ a R é um epimorfismo essencial, provando (2).

Vamos para o último item. Se ρ é um isomorfismo, então $\ker \rho = 0$ e $R = Q$, de onde concluímos do item (2) que Q e ψ formam uma cobertura projetiva de U. Reciprocamente, se ψ é uma cobertura projetiva de U, então $\psi = \varphi\rho$ e φ são epimorfismos essenciais. Logo, o item (1) da Proposição 5.3.3 nos mostra que ρ também é um epimorfismo essencial. Mas P é projetivo, então concluímos que ρ é um isomorfismo pela Proposição 5.3.4. □

Se $\varphi : P \to U$ é uma cobertura projetiva de U, o resultado acima mostra que o módulo projetivo P é único a menos de isomorfismo. Assim, definiremos PU como sendo uma cobertura projetiva de U, o que está bem definido a menos de isomorfismo. Além disso, o mapa φ também é único! De fato, se $\psi : Q \to U$ é outra cobertura projetiva, podemos encontrar um isomorfismo $\rho : Q \to P$ tal que $\psi = \varphi\rho$. Logo, faz sentido escolher um epimorfismo essencial $\pi_U : PU \to U$ para a cobertura projetiva de U. Uma outra consequência disso é que o isomorfismo ρ leva o núcleo de ψ no núcleo de φ e então esses módulos são isomorfos! Dessa forma, podemos definir ΩU como sendo o núcleo de π_U, que não depende da particular escolha de PU ou de π_U. Note que temos uma sequência exata

$$0 \longrightarrow \Omega U \longrightarrow PU \longrightarrow U \longrightarrow 0$$

e que $\Omega U = 0$ se e só se U é projetivo. Podemos ver Ω como sendo uma "função" que atua nos A-módulos, que chamaremos de **operador de Heller**. Esse operador é muito importante e precisaremos dele para continuar a demonstração do Teorema 5.1.7.

Corolário 5.3.9. Se $\psi : Q \to U$ é um homomorfismo sobrejetor, onde Q é um A-módulo projetivo, então $\ker \psi \cong \Omega U \oplus K$, onde K é um A-módulo projetivo. Além disso, Q é uma cobertura projetiva de U se, e somente se, $K = 0$.

Demonstração. Se $\varphi : P \to U$ é uma cobertura projetiva de U, então podemos encontrar um homomorfismo sobrejetor $\rho : Q \to P$ pela Proposição 5.3.8. Além disso, podemos escrever $Q = R \oplus \ker \rho$ e a restrição de ψ a R é uma cobertura projetiva de U. Note que $\ker \rho$ está contido em $\ker \psi$ porque $\psi = \varphi\rho$, então é fácil ver que $\ker \psi$ é a soma direta de $\ker \rho$ com o núcleo da restrição

de ψ a R, que é isomorfo a ΩU. Por isso, se tomarmos $K \coloneqq \ker \rho$, então K é projetivo por ser somando direto de Q e temos $\ker \psi \cong \Omega U \oplus K$. Também sabemos que Q é cobertura projetiva de U se e só se ρ é um isomorfismo, ou seja, se e só se $K = \ker \rho = 0$. □

Para deduzir mais propriedades do operador de Heller, especificaremos para o caso das álgebras de grupo. Nesse caso, como kG-módulos projetivos e injetivos são a mesma coisa, será muito importante introduzir o conceito dual da cobertura projetiva. Começaremos lidando com álgebras de dimensão finita quaisquer, porém não elaboramos ferramentas suficientes para lidar com módulos injetivos no caso geral e alguns resultados enunciaremos apenas para álgebras de grupo. Ademais, a maioria das demonstrações é muito análoga às demonstrações que já demos, então explicaremos melhor apenas aquelas onde aparece algo diferente.

Seja $\varphi : U \to V$ um homomorfismo injetor. Dualizando o conceito de epimorfismo essencial, diremos que φ é um **monomorfismo essencial** se $\varphi^{-1}(V') \neq 0$ para todo submódulo não nulo V' de V. Isso significa exatamente que a imagem de φ intersecta não trivialmente qualquer submódulo não nulo de V. Nesse sentido, é como se U fosse uma "componente essencial" para formar V, ou então como se V "envolvesse" U de um modo "econômico". Também temos uma caracterização em termos de homomorfismos:

Lema 5.3.10. Um homomorfismo injetor de A-módulos $\varphi : U \to V$ é um monomorfismo essencial se, e somente se, para todo homomorfismo $\psi : V \to W$ vale a implicação

$$\psi\varphi \text{ é injetor} \implies \psi \text{ é injetor.}$$

No caso dos monomorfismos essenciais, também temos uma fonte canônica de exemplos: se U é um A-módulo, então a inclusão $\operatorname{soc}(U) \to U$ é um monomorfismo essencial. De fato, isso é equivalente a dizer que $\operatorname{soc}(U)$ intersecta não trivialmente qualquer submódulo não nulo de U. Isso é imediato, porque se U' é um submódulo não nulo de U, então $\operatorname{soc}(U') \subseteq \operatorname{soc}(U)$ e $\operatorname{soc}(U') \neq 0$.

Também temos propriedades importantes análogas às dos epimorfismos essenciais:

Proposição 5.3.11. Valem as seguintes afirmações:

(1) Sejam $\varphi : U \to V$ e $\psi : V \to W$ homomorfismos. Se dois homomorfismos dentre φ, ψ e $\psi\varphi$ são monomorfismos essenciais, então o mesmo vale para o terceiro.

(2) Se $\varphi : U \to V$ é um homomorfismo de A-módulos, então φ é um monomorfismo essencial se e só se o homomorfismo induzido $\operatorname{soc}(U) \to \operatorname{soc}(V)$ é um isomorfismo.

(3) Se $\varphi : U_1 \to V_1$ e $\psi : U_2 \to V_2$ são homomorfismos, então φ e ψ são monomorfismos essenciais se e somente se
$$(\varphi \oplus \psi) : U_1 \oplus U_2 \to V_1 \oplus V_2$$
é um monomorfismo essencial.

Se U é um A-módulo qualquer, dessa vez queremos saber se existe um maior A-módulo V tal que existe um monomorfismo essencial $U \to V$. Portanto, devemos olhar para os módulos I tais que todo monomorfismo essencial $I \to V$ é um isomorfismo. Esses seriam os potenciais candidatos aos maiores módulos "envolvendo" U. Você provavelmente já deduziu quais são esses módulos:

Proposição 5.3.12. Seja I um A-módulo. Então todo monomorfismo essencial $\varphi : I \to V$ é um isomorfismo se, e somente se, I é um módulo injetivo.

Desse modo, vamos estudar homomorfismos injetores $\varphi : U \to I$ onde I é um A-módulo injetivo. Nesse caso, se φ é um monomorfismo essencial, dizemos que I (juntamente com φ) é uma **envolvente injetiva** de U. Também veremos como essa definição é útil. Para aquecer, enunciamos o análogo do Lema 5.3.5:

Lema 5.3.13. Se $\psi : U \to V$ é um homomorfismo de A-módulos e se $\varphi : U \to I$ é uma envolvente injetiva, então ψ se fatora através de um injetivo se, e somente se, existe um homomorfismo $\alpha : I \to V$ tal que $\psi = \alpha\varphi$.

Ainda devemos garantir que envolventes injetivas existem. É a partir de agora que tomaremos $A = kG$. Se S é um kG-módulo simples e se P é a sua cobertura projetiva, então o Teorema 2.3.17 mostra que $S \cong \operatorname{soc}(P)$, logo o homomorfismo $S \cong \operatorname{soc}(P) \to P$ é um monomorfismo essencial. Pelo Teorema 2.3.14, P é injetivo, então encontramos a envolvente injetiva de S. Com o item (3) da Proposição 5.3.11, podemos adaptar a demonstração da Proposição 5.3.6 para provar o seguinte resultado:

Proposição 5.3.14. Todo kG-módulo admite uma envolvente injetiva.

Para demonstrar a proposição conforme indicamos, devemos utilizar que uma soma direta finita de kG-módulos injetivos é injetiva. Essa propriedade vale em geral para módulos sobre qualquer anel. No nosso caso, isso segue facilmente quando lembramos que kG-módulos injetivos e projetivos são a mesma coisa.

Observação 5.3.15. Surpreendentemente, a proposição não é um caso particular de kG-módulos. Na verdade, a envolvente injetiva se comporta melhor do que a cobertura projetiva: todo R-módulo admite uma envolvente injetiva, seja qual for o anel R! Veja, por exemplo, o Lema 3.29 na página 75 do livro [16].

A Proposição 5.3.14 também segue da Proposição 5.3.6 a partir do seguinte resultado:

Proposição 5.3.16. Se $\varphi : U \to V$ é um homomorfismo de kG-módulos e se $\varphi^* : V^* \to U^*$ é a sua transposta, então

$$\varphi \text{ é um epimorfismo essencial} \iff \varphi^* \text{ é um monomorfismo essencial,}$$

e vice-versa. Em particular, o dual de uma cobertura projetiva é uma envolvente injetiva, e vice-versa.

Demonstração. Se φ é um epimorfismo essencial, então temos um isomorfismo induzido $\overline{\varphi} : U/\operatorname{rad}(U) \to V/\operatorname{rad}(V)$. Tomando a transposta, temos um isomorfismo $\overline{\varphi}^* : (V/\operatorname{rad}(V))^* \to (U/\operatorname{rad}(U))^*$. Pela Proposição 2.3.9, temos isomorfismos

$$\operatorname{soc}(U^*) \cong \left(\frac{U}{\operatorname{rad}(U)}\right)^* \quad \text{e} \quad \operatorname{soc}(V^*) \cong \left(\frac{V}{\operatorname{rad}(V)}\right)^*.$$

Mais do que isso, seguindo a definição explícita desse isomorfismo dada no Lema 2.3.6, podemos verificar que o seguinte diagrama é comutativo:

$$\begin{array}{ccc} \left(\frac{V}{\operatorname{rad}(V)}\right)^* & \xrightarrow{\overline{\varphi}^*} & \left(\frac{U}{\operatorname{rad}(U)}\right)^* \\ \uparrow & & \uparrow \\ \operatorname{soc}(V^*) & \xrightarrow{\widetilde{\varphi^*}} & \operatorname{soc}(U^*) \end{array}$$

O homomorfismo $\widetilde{\varphi^*}$ acima é o homomorfismo induzido por φ^*. Segue que $\widetilde{\varphi^*}$ é um isomorfismo e, consequentemente, φ^* é um monomorfismo essencial. Analogamente, se φ é um monomorfismo essencial, então φ^* é um epimorfismo essencial.

Reciprocamente, se φ^* é um monomorfismo essencial, então o parágrafo anterior mostra que φ^{**} é um epimorfismo essencial. Utilizando o isomorfismo canônico do Lema 2.3.4 e a Observação 2.3.5, concluímos que φ é um epimorfismo essencial também. Do mesmo modo, se φ^* é um

epimorfismo essencial, obtemos que φ é um monomorfismo essencial. Isso prova as equivalências do enunciado.

A última afirmação segue do que acabamos de provar juntamente com o Corolário 2.3.12 e com o Teorema 2.3.14. □

Também temos uma unicidade para envolventes injetivas!

Proposição 5.3.17. Seja $\varphi : U \to I$ uma envolvente injetiva de um kG-módulo U e seja $\psi : U \to J$ um homomorfismo injetor qualquer onde J é um kG-módulo injetivo. Então:

(1) Existe um homomorfismo injetor $\rho : I \to J$ tal que $\rho\varphi = \psi$.

(2) Podemos decompor $J = V \oplus \operatorname{im}\rho$. Além disso, $\operatorname{im}\psi \subseteq \operatorname{im}\rho$ e, restringindo o contradomínio de ψ a $\operatorname{im}\rho$, ψ se torna uma envolvente injetiva de U.

(3) O par formado por J e ψ é uma envolvente injetiva de U se, e somente se, ρ é um isomorfismo.

Desse modo, assim como fizemos antes, podemos definir para cada kG-módulo U uma envolvente injetiva IU, o que está bem definido a menos de isomorfismo. Mais do que isso, se $\varphi : U \to I$ e $\psi : U \to J$ são envolventes injetivas, então temos um isomorfismo $\rho : I \to J$ tal que $\psi = \rho\varphi$. Assim, podemos escolher um monomorfismo essencial $\lambda_U : U \to IU$ para a envolvente injetiva de U. Como ρ leva a imagem de φ na imagem de ψ, os *conúcleos* (ou seja, os quocientes dos contradomínios pelas imagens) das envolventes injetivas de U são isomorfos! Denotaremos o conúcleo de λ_U por $\Omega^{-1}U$ e, novamente, isso não depende da escolha de IU e de λ_U. Note que temos uma sequência exata

$$0 \longrightarrow U \longrightarrow IU \longrightarrow \Omega^{-1}U \longrightarrow 0$$

e que $\Omega^{-1}U = 0$ se e só se U é injetivo (projetivo). Como veremos em breve, o "operador" Ω^{-1} se comporta como um inverso do operador de Heller! Esse é o motivo para a notação apresentada.

Corolário 5.3.18. Se $\psi : U \to J$ é um homomorfismo injetor, onde J é um kG-módulo injetivo, então $J/\operatorname{im}\psi \cong \Omega^{-1}U \oplus V$, onde V é um kG-módulo injetivo. Além disso, J é uma envolvente injetiva de U se, e somente se, $V = 0$.

A demonstração desse corolário é análoga à do Corolário 5.3.9. Dessa vez, V aparecerá como um somando direto de um módulo injetivo. É um resultado geral que, nesse caso, V é injetivo, mas, com o que desenvolvemos, é mais prático aplicar o Teorema 2.3.14.

Vamos começar a relacionar coberturas projetivas com envolventes injetivas e o operador Ω com o operador Ω^{-1}!

Lema 5.3.19. Seja $\alpha : U \to V$ um homomorfismo que se fatora por um projetivo, onde U e V são kG-módulos não nulos. Se α é sobrejetor, então U possui um somando direto projetivo não nulo. Analogamente, se α é injetor, então V possui um somando direto projetivo não nulo.

Demonstração. Inicialmente, suponha que α seja sobrejetor. Pelo Lema 5.3.5, existe um homomorfismo $\rho : U \to PV$ tal que $\alpha = \pi_V\rho$. Como π_V é um epimorfismo essencial e a composição $\pi_V\rho = \alpha$ é sobrejetora, o Lema 5.3.1 mostra que ρ é sobrejetor. Mas PV é projetivo, então ρ cinde e U possui um somando direto isomorfo a PV, que é projetivo.

Agora, suponha que α seja injetor. Como kG-módulos injetivos são projetivos, α se fatora por um injetivo. Pelo Lema 5.3.13, existe um homomorfismo $\rho : IU \to V$ tal que $\alpha = \rho\lambda_U$. Como λ_U é um monomorfismo essencial e a composição $\rho\lambda_U = \alpha$ é injetora, o Lema 5.3.10 mostra que ρ é injetor. Mas IU é injetivo, então ρ cinde e V possui um somando direto isomorfo a IU, que é projetivo pelo Teorema 2.3.14. □

Como evidente no resultado anterior, é interessante estudar os somandos diretos projetivos de um dado módulo. Na verdade, é ainda mais importante olhar para os somandos diretos que não são projetivos! Módulos que não possuem somandos diretos projetivos não nulos são chamados **projetivamente livres**. Por simplicidade (ou por vacuidade), diremos que o módulo nulo é projetivamente livre. Se U é um kG-módulo qualquer, podemos escrever U como a soma direta de um módulo projetivo com um módulo projetivamente livre. Se definirmos $\Omega^0 U$ como sendo esse somando projetivamente livre, o Teorema de Krull-Schmidt garante que $\Omega^0 U$ está definido a menos de isomorfismo.

Como é de se esperar das notações, temos o seguinte resultado:

Lema 5.3.20. Se U é um kG-módulo, então temos os seguintes isomorfismos:

(1) $\Omega\Omega^0 U \cong \Omega U \cong \Omega^0\Omega U$.

(2) $\Omega^{-1}\Omega^0 U \cong \Omega^{-1} U \cong \Omega^0\Omega^{-1} U$.

(3) $\Omega\Omega^{-1} U \cong \Omega^0 U \cong \Omega^{-1}\Omega U$.

Demonstração. Vamos começar com o primeiro isomorfismo de (1) e com o primeiro isomorfismo de (2). Por simplicidade, denote $V \coloneqq \Omega^0 U$. Escreva $U = V \oplus Q$ para algum módulo projetivo Q. Pelo item (3) da Proposição 5.3.3, $\pi_V \oplus \mathrm{id}_Q : PV \oplus Q \to U$ é um epimorfismo essencial e, como $PV \oplus Q$ é projetivo, esta é uma cobertura projetiva de U. Logo,

$$\Omega U \cong \ker(\pi_V \oplus \mathrm{id}_Q) \cong \ker \pi_V = \Omega V = \Omega\Omega^0 U.$$

Analogamente, pelo item (3) da Proposição 5.3.11, $\lambda_V \oplus \mathrm{id}_Q : U \to IV \oplus Q$ é um monomorfismo essencial e, como $IV \oplus Q$ é injetivo (por ser projetivo), esta é uma envolvente injetiva de U. Logo,

$$\Omega^{-1} U \cong \frac{IV \oplus Q}{\mathrm{im}(\lambda_V \oplus \mathrm{id}_Q)} \cong \frac{IV}{\mathrm{im}\,\lambda_V} \oplus \frac{Q}{Q} \cong \Omega^{-1} V = \Omega^{-1}\Omega^0 U.$$

Em vista do que acabamos de demonstrar, basta mostrarmos que $\Omega\Omega^{-1} V \cong V \cong \Omega^{-1}\Omega V$ para provar (3). Considere a inclusão $\Omega V \to PV$. Como PV também é injetivo, o Corolário 5.3.18 mostra que $PV/\Omega V \cong \Omega^{-1}\Omega V \oplus W$ para algum módulo projetivo W. Mas $PV/\Omega V \cong V$ e, como V é projetivamente livre, devemos ter $W = 0$ e $V \cong \Omega^{-1}\Omega V$, como desejado. Além disso, como $W = 0$, esse corolário também diz que $\Omega V \to PV$ é uma envolvente injetiva!

Por outro lado, podemos considerar a projeção $IV \to \Omega^{-1} V$. Como IV também é projetivo, o Corolário 5.3.9 mostra que o núcleo da projeção é isomorfo a $\Omega\Omega^{-1} V \oplus K$ para algum módulo projetivo K. Mas o núcleo da projeção é a imagem de λ_V, que é isomorfa a V. Como V é projetivamente livre, devemos ter $K = 0$ e $V \cong \Omega\Omega^{-1} V$, como preciso. Mais uma vez, como $K = 0$, a projeção $IV \to \Omega^{-1} V$ é uma cobertura projetiva!

Para concluir, observe que

$$\Omega^0\Omega U \cong (\Omega\Omega^{-1})\Omega U = \Omega(\Omega^{-1}\Omega U) \cong \Omega\Omega^0 U \cong \Omega U,$$

mostrando o segundo isomorfismo em (1). Semelhantemente, prova-se o segundo isomorfismo em (2). □

Com isso, note que ΩU e $\Omega^{-1} U$ sempre são projetivamente livres e então não podemos esperar que Ω e Ω^{-1} sejam inversos um do outro. Porém, se nos restringirmos a módulos projetivamente livres, esses operadores são de fato um o inverso do outro! Também obtivemos algo muito interessante durante a demonstração acima, que anotaremos como um corolário:

Corolário 5.3.21. Seja V um kG-módulo projetivamente livre. Então a inclusão canônica $\Omega V \to PV$ é uma envolvente injetiva e a projeção canônica $IV \to \Omega^{-1} V$ é uma cobertura projetiva.

O operador de Heller permuta os módulos projetivamente livres e podemos restringir essa permutação aos módulos indecomponíveis! Além disso, a inversa dessa permutação é dada por Ω^{-1}. Esse é o conteúdo do próximo resultado.

Teorema 5.3.22. Sejam U_1, U_2 e V kG-módulos indecomponíveis e não projetivos. Então:

(1) ΩV também é indecomponível e não projetivo.

(2) Se $\Omega U_1 \cong \Omega U_2$, então $U_1 \cong U_2$.

(3) Existe um kG-módulo indecomponível e não projetivo U tal que $\Omega U \cong V$.

Demonstração. Suponha por absurdo que ΩV não seja indecomponível. Escreva $\Omega V = M_1 \oplus M_2$ onde M_1 e M_2 são não nulos. Pelo Lema 5.3.20, vale $\Omega^0 \Omega V \cong \Omega V$, ou seja, ΩV é projetivamente livre. Por isso, M_1 e M_2 não são projetivos e vale $\Omega^{-1} M_1 \neq 0$ e $\Omega^{-1} M_2 \neq 0$. Por sua vez, podemos utilizar que V é projetivamente livre e o Exercício A.5.9 para obter

$$V = \Omega^0 V \cong \Omega^{-1}\Omega V \cong \Omega^{-1} M_1 \oplus \Omega^{-1} M_2,$$

o que contradiz o fato de V ser indecomponível. Dessa contradição, concluímos que ΩV é indecomponível e o item (1) está provado.

Para o item (2), se $\Omega U_1 \cong \Omega U_2$, segue do fato de U_1 e U_2 serem projetivamente livres e do Lema 5.3.20 que

$$U_1 = \Omega^0 U_1 \cong \Omega^{-1}(\Omega U_1) \cong \Omega^{-1}(\Omega U_2) \cong \Omega^0 U_2 = U_2,$$

como desejado.

Por fim, podemos argumentar como no primeiro parágrafo para mostrar que $U := \Omega^{-1} V$ é um kG-módulo indecomponível e, pelo Lema 5.3.20, vale $V = \Omega^0 V \cong \Omega\Omega^{-1} V = \Omega U$. □

Homomorfismos também são preservados (a menos de fatoração por projetivos) pelo operador de Heller:

Proposição 5.3.23. Se U e V são kG-módulos, então

$$\overline{\mathrm{Hom}}_{kG}(U, V) \cong \overline{\mathrm{Hom}}_{kG}(\Omega U, \Omega V).$$

Demonstração. Escreva $U = \Omega^0 U \oplus Q$ e $V = \Omega^0 V \oplus R$, onde Q e R são kG-módulos projetivos. Pelo Exercício A.3.15, temos

$$\overline{\mathrm{Hom}}_{kG}(U, V) \cong \overline{\mathrm{Hom}}_{kG}(\Omega^0 U, \Omega^0 V).$$

Pelo Lema 5.3.20, $\Omega U \cong \Omega\Omega^0 U$ e $\Omega V \cong \Omega\Omega^0 V$, então também vale

$$\overline{\mathrm{Hom}}_{kG}(\Omega U, \Omega V) \cong \overline{\mathrm{Hom}}_{kG}(\Omega\Omega^0 U, \Omega\Omega^0 V).$$

Isso mostra que é suficiente provar o isomorfismo do enunciado onde trocamos U por $\Omega^0 U$ e V por $\Omega^0 V$. Mais simplesmente, podemos assumir que U e V são projetivamente livres para provar o resultado.

Se $\alpha \in \mathrm{Hom}_{kG}(U, V)$, vamos construir um diagrama comutativo como a seguir:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega U & \xrightarrow{i_U} & PU & \xrightarrow{\pi_U} & U & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \Omega\alpha} & & \downarrow{\scriptstyle P\alpha} & & \downarrow{\scriptstyle \alpha} & & \\
0 & \longrightarrow & \Omega V & \xrightarrow{i_V} & PV & \xrightarrow{\pi_V} & V & \longrightarrow & 0
\end{array}$$

Os homomorfismos i_U e i_V são as inclusões canônicas e note que as duas sequências horizontais do diagrama são exatas. Vamos construir os mapas $\Omega\alpha$ e $P\alpha$. Como $\alpha\pi_U$ é um homomorfismo

de PU em V, podemos encontrar $P\alpha : PU \to PV$ tal que $\pi_V(P\alpha) = \alpha\pi_U$, pois PU é projetivo e π_V é sobrejetor. Agora, veja que $P\alpha(\Omega U) \subseteq \Omega V$ porque

$$\pi_V(P\alpha)(\Omega U) = \alpha\pi_U(\Omega U) = \alpha(0) = 0,$$

então podemos definir $\Omega\alpha : \Omega U \to \Omega V$ de modo que o diagrama acima comute. O homomorfismo $P\alpha$ não é necessariamente único, então $\Omega\alpha$ depende tanto de α quanto da escolha de $P\alpha$.

Reciprocamente, todo homomorfismo de ΩU em ΩV pode ser construído a partir de algum $\alpha \in \mathrm{Hom}_{kG}(U, V)$ como acima. Vejamos o porquê. A ideia vem do Corolário 5.3.21, que nos permite dualizar o argumento anterior. Seja $\beta : \Omega U \to \Omega V$ um homomorfismo. Como $i_V\beta$ é um homomorfismo de ΩU em PV, podemos encontrar $I\beta : PU \to PV$ tal que $(I\beta)i_U = i_V\beta$, pois PV é injetivo e i_U é injetor. Agora, note que ΩU está contido no núcleo de de $\pi_V(I\beta)$, já que $\pi_V(I\beta)i_U = \pi_V i_V\beta = 0$. Logo, pelo Teorema do Homomorfismo, podemos descer ao quociente, obtendo um homomorfismo $\Omega^{-1}\beta : U \to V$ tal que $(\Omega^{-1}\beta)\pi_U = \pi_V(I\beta)$. Se tomarmos $\alpha \coloneqq \Omega^{-1}\beta$, podemos tomar $P\alpha = I\beta$ na construção anterior e obtemos $\Omega\alpha = \beta$, como desejado.

Provaremos que α se fatora através de um projetivo se e só se o mesmo acontece para $\Omega\alpha$. Comecemos supondo que α se fatora através de um projetivo. Pelo Corolário 5.3.5, existe um homomorfismo $\delta : U \to PV$ tal que $\pi_V\delta = \alpha$. Observe que a imagem de $P\alpha - \delta\pi_U$ cai em ΩV, porque

$$\pi_V(P\alpha - \delta\pi_U) = \pi_V(P\alpha) - (\pi_V\delta)\pi_U = \pi_V(P\alpha) - \alpha\pi_U = 0.$$

Além disso,

$$(P\alpha - \delta\pi_U)i_U = (P\alpha)i_U - 0 = i_V(\Omega\alpha).$$

Por isso, vendo $\gamma \coloneqq P\alpha - \delta\pi_U$ como um mapa de PU para ΩV, vale $\gamma i_U = \Omega\alpha$, logo $\Omega\alpha$ se fatora através do projetivo PU, como desejado.

Reciprocamente, suponha que $\Omega\alpha$ se fatore por um projetivo. Pelo Corolário 5.3.21, $i_U : \Omega U \to PU$ é uma envolvente injetiva, então o Lema 5.3.13 garante a existência de um homomorfismo $\gamma : PU \to \Omega V$ tal que $\gamma i_U = \Omega\alpha$. Desse modo,

$$(P\alpha - i_V\gamma)i_U = (P\alpha)i_U - i_V(\gamma i_U) = (P\alpha)i_U - i_V(\Omega\alpha) = 0$$

e ΩU está contido no núcleo de $P\alpha - i_V\gamma$. Pelo Teorema do Homomorfismo, podemos descer ao quociente, obtendo um homomorfismo $\delta : U \to PV$ tal que $P\alpha - i_V\gamma = \delta\pi_U$. Como PV é projetivo, basta mostrar que $\pi_V\delta = \alpha$ para mostrar que α se fatora por um projetivo. De fato, vale

$$\pi_V\delta\pi_U = \pi_V(P\alpha - i_V\gamma) = \pi_V(P\alpha) - 0 = \alpha\pi_U$$

e, como π_U é sobrejetor, obtemos a condição que queríamos.

Finalmente, terminemos a demonstração. Se $\alpha, \alpha' \in \mathrm{Hom}_{kG}(U, V)$, então podemos escolher homomorfismos $P\alpha$ e $P\alpha'$ e construir os homomorfismos $\Omega\alpha$ e $\Omega\alpha'$ de modo que as triplas $(\alpha, P\alpha, \Omega\alpha)$ e $(\alpha', P\alpha', \Omega\alpha')$ façam o diagrama comutar. Isso implica que a tripla

$$(\alpha - \alpha', P\alpha - P\alpha', \Omega\alpha - \Omega\alpha')$$

também faz o diagrama comutar. Em particular, se $\alpha = \alpha'$, então $\alpha - \alpha' = 0$ se fatora através de um projetivo e os parágrafos anteriores mostram que $\Omega\alpha - \Omega\alpha'$ também se fatora através de um projetivo. Ou seja, a menos de fatoração por projetivo, $\Omega\alpha$ está unicamente determinado por α! Logo, podemos definir uma função f de $\mathrm{Hom}_{kG}(U, V)$ em $\overline{\mathrm{Hom}}_{kG}(\Omega U, \Omega V)$ que leva α na classe à qual pertencem todas as escolhas de $\Omega\alpha$. Além disso, se $\lambda \in k$, então $(\lambda\alpha, \lambda P\alpha, \lambda\Omega\alpha)$ faz o diagrama comutar e o mesmo vale para

$$(0, \lambda P\alpha - P(\lambda\alpha), \lambda\Omega\alpha - \Omega(\lambda\alpha)),$$

mostrando que $\lambda\Omega\alpha$ é igual a $\Omega(\lambda\alpha)$ módulo fatoração por projetivo. Da mesma forma, pode-se mostrar que $\Omega(\alpha + \beta)$ é igual a $\Omega\alpha + \Omega\beta$ módulo fatoração por projetivo, então concluímos que a

função f é na verdade uma transformação linear! Como todo homomorfismo de ΩU em ΩV é da forma $\Omega\alpha$ para algum $\alpha \in \mathrm{Hom}_{kG}(U,V)$, obtemos que f é sobrejetora. Por fim, um homomorfismo α está no núcleo de f exatamente quando $\Omega\alpha$ se fatora por um projetivo, o que ocorre se e só se α se fatora por um projetivo. Logo, pelo Teorema do Isomorfismo, f induz um isomorfismo entre $\overline{\mathrm{Hom}}_{kG}(U,V)$ e $\overline{\mathrm{Hom}}_{kG}(\Omega U, \Omega V)$. □

Concluiremos a seção com um resultado relacionando o operador de Heller e a Correspondência de Green.

Proposição 5.3.24. Seja U um kG-módulo indecomponível e não projetivo. Então:

(1) Os kG-módulos U e ΩU possuem os mesmos vértices.

(2) Se V é o correspondente de Green de U, então ΩV é o correspondente de Green de ΩU.

Demonstração. Seja H um subgrupo de G e suponha que U seja relativamente H-projetivo. Logo, existe um kH-módulo W tal que $U \mid W^G$. Vejamos que ΩU também é relativamente H-projetivo mostrando que $\Omega U \mid (\Omega W)^G$. Temos a seguinte sequência exata de kH-módulos:

$$0 \longrightarrow \Omega W \xrightarrow{i_W} PW \xrightarrow{\pi_W} W \longrightarrow 0$$

Induzindo para G, o Lema 3.1.11 nos fornece uma sequência exata de kG-módulos:

$$0 \longrightarrow (\Omega W)^G \xrightarrow{i_W^G} (PW)^G \xrightarrow{\pi_W^G} W^G \longrightarrow 0$$

Por hipótese, $W^G \cong U \oplus X$ para algum kG-módulo X. Pelo item (3) da Proposição 5.3.3, $\pi_U \oplus \pi_X : PU \oplus PX \to U \oplus X$ é uma cobertura projetiva. Pelo Lema 3.1.10, $(PW)^G$ é projetivo, então a Proposição 5.3.8 nos dá um homomorfismo sobrejetor $\rho : (PW)^G \to PU \oplus PX$ fazendo o seguinte diagrama comutar:

$$\begin{array}{ccc} (PW)^G & \xrightarrow{\pi_W^G} & W^G \\ \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \wr} \\ PU \oplus PX & \xrightarrow{\pi_U \oplus \pi_X} & U \oplus X \end{array}$$

A Proposição 5.3.8 também diz que $(PW)^G = R \oplus \ker\rho$ para algum submódulo R, logo podemos decompor ρ como a composição de um isomorfismo de $(PW)^G \to PU \oplus PX \oplus \ker\rho$ (que aplica ρ em R e a identidade em $\ker\rho$) seguido da projeção canônica $PU \oplus PX \oplus \ker\rho \to PU \oplus PX$. Assim, temos um novo diagrama comutativo

$$\begin{array}{ccc} (PW)^G & \xrightarrow{\pi_W^G} & W^G \\ \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \wr} \\ PU \oplus PX \oplus \ker\rho & \longrightarrow & U \oplus X \end{array}$$

onde os mapas verticais são isomorfismos. Portanto, os núcleos dos mapas horizontais são isomorfos, ou seja, $(\Omega W)^G$ é isomorfo a $\Omega U \oplus \Omega X \oplus \ker\rho$, de onde concluímos que ΩU é um somando direto de $(\Omega W)^G$, como desejado.

Vamos mostrar a recíproca. Suponha que ΩU seja relativamente H-projetivo e desta vez denote por W um kH-módulo tal que $\Omega U \mid W^G$. Vamos mostrar que $U \mid (\Omega^{-1}W)^G$ para garantir que U também é relativamente H-projetivo. Temos a seguinte sequência exata de kH-módulos:

$$0 \longrightarrow W \xrightarrow{\lambda_W} IW \xrightarrow{\psi_W} \Omega^{-1}W \longrightarrow 0$$

Induzindo para G, o Lema 3.1.11 nos fornece uma sequência exata de kG-módulos:

$$0 \longrightarrow W^G \xrightarrow{\lambda_W^G} (IW)^G \xrightarrow{\psi_W^G} (\Omega^{-1}W)^G \longrightarrow 0$$

Por hipótese, $W^G \cong \Omega U \oplus X$ para algum kG-módulo X. Pelo item (3) da Proposição 5.3.11, $\lambda_{\Omega U} \oplus \lambda_X : \Omega U \oplus X \to I(\Omega U) \oplus IX$ é uma envolvente injetiva. Pelo Lema 3.1.10 e pelo Teorema 2.3.14, $(IW)^G$ é injetivo, então a Proposição 5.3.17 nos fornece um homomorfismo injetor $\rho : I(\Omega U) \oplus IX \to (IW)^G$ fazendo o seguinte diagrama comutar:

$$\begin{array}{ccc} W^G & \xrightarrow{\lambda_W^G} & (IW)^G \\ \wr\uparrow & & \uparrow\rho \\ \Omega U \oplus X & \xrightarrow{\lambda_{\Omega U}\oplus\lambda_X} & I(\Omega U) \oplus IX \end{array}$$

A Proposição 5.3.17 também diz que $(IW)^G = \operatorname{im}\rho \oplus R$ para algum submódulo R, logo podemos decompor ρ como a composição da inclusão canônica $I(\Omega U) \oplus IX \to I(\Omega U) \oplus IX \oplus R$ seguida de um isomorfismo $I(\Omega U) \oplus IX \oplus R \to (IW)^G$ (que aplica ρ em $I(\Omega U) \oplus IX$ e a identidade em R). Assim, temos um novo diagrama comutativo

$$\begin{array}{ccc} W^G & \xrightarrow{\lambda_W^G} & (IW)^G \\ \wr\uparrow & & \wr\uparrow \\ \Omega U \oplus X & \longrightarrow & I(\Omega U) \oplus IX \oplus R \end{array}$$

onde os mapas verticais são isomorfismos. Por isso, os conúcleos dos mapas horizontais são isomorfos, ou seja, $(\Omega^{-1}W)^G$ é isomorfo a $\Omega^{-1}\Omega U \oplus \Omega^{-1}X \oplus R$. Como U é projetivamente livre, o Lema 5.3.20 mostra que $\Omega^{-1}\Omega U \cong \Omega^0 U = U$ e concluímos que $U \mid (\Omega^{-1}W)^G$. Desse modo, demonstramos que U e ΩU são relativamente projetivos para os mesmos subgrupos de G, então esses módulos devem possuir os mesmos vértices.

Vamos para o item (2). Suponha que um p-subgrupo $Q \leq G$ é um vértice de U e seja $L \leq G$ um subgrupo contendo $N_G(Q)$. Assim, podemos considerar o kL-módulo indecomponível V que é o correspondente de Green de U. Como U não é projetivo, Q não é trivial. Por isso, V também não é projetivo, já que também possui Q como vértice. Pelo Teorema 5.3.22, ΩV e ΩU são indecomponíveis e, pelo item (1), ambos possuem Q como vértice. Assim, para mostrar que ΩV e ΩU são correspondentes de Green, basta provar que $\Omega U \mid (\Omega V)^G$. Mas, como $U \mid V^G$, podemos imitar o argumento dado no primeiro parágrafo e, consequentemente, a demonstração está concluída. □

5.4 Módulos simples e suas extensões

Finalmente iremos começar a estudar os B-módulos! Utilizaremos a estrutura dos b_1-módulos indecomponíveis que descobrimos anteriormente, mas precisamos de uma forma de conectar b_1-módulos e B-módulos. Faremos isso a partir da Correspondência de Green!

Teorema 5.4.1. Existe uma bijeção entre as classes de isomorfismo de B-módulos indecomponíveis e não projetivos e as classes de isomorfismo de b_1-módulos indecomponíveis e não projetivos. Se U e V são módulos sobre B e sobre b_1, respectivamente, que se correspondem, então

$$V^G \cong U \oplus X \quad \text{e} \quad U_{N_1} \cong V \oplus Y,$$

onde X é um kG-módulo projetivo e Y é a soma direta de um kN_1-módulo projetivo com módulos pertencentes a blocos de kN_1 diferentes de b_1.

Demonstração. Vamos aplicar a Correspondência de Green na forma do Corolário 3.4.6. O p-subgrupo em questão será D e o tomaremos o subgrupo L como sendo N_1, que contém o normalizador N de D. Vamos descrever as famílias $\mathfrak{X}, \mathfrak{Y}$ e $\mathfrak{Z}$. Seja $g \in G$ e suponha que $D \cap gDg^{-1} \neq \{1\}$. Essa interseção é um subgrupo do grupo cíclico D, então contém o seu único subgrupo minimal D_1. Da mesmo forma, ela é subgrupo do grupo cíclico gDg^{-1} e também deve conter o seu único subgrupo minimal, que é gD_1g^{-1}. Mas $D \cap gDg^{-1}$ também é um p-grupo cíclico e contém um único subgrupo de ordem p, de onde obtemos $D_1 = gD_1g^{-1}$, ou seja, $g \in N_1$. Como

$$\mathfrak{X} = \{D \cap gDg^{-1} \mid g \in G, g \notin N_1\},$$

isso mostra que o único subgrupo em $\mathfrak{X}$ é $\{1\}$. Como

$$\mathfrak{Z} = \{R \subseteq D \mid R \not\subseteq_G \mathfrak{X}\},$$

também obtemos que $\mathfrak{Z}$ consiste de todos os subgrupos de D diferentes do trivial. Pelo Corolário 3.4.6, já sabemos que há uma bijeção entre kG-módulos e kN_1-módulos indecomponíveis não projetivos com vértice contido em D e que, se V é um kN_1-módulo indecomponível não projetivo com vértice em D, então V^G é a soma direta de um indecomponível não projetivo com um módulo relativamente $\mathfrak{X}$-projetivo, ou seja, com um módulo projetivo.

Vamos analisar $\mathfrak{Y}$ agora. Seja $g \in G$ e suponha que $N_1 \cap gDg^{-1} \neq \{1\}$. Se $N_1 \cap gDg^{-1}$ possui um conjugado em N_1 que intersecta não trivialmente um subgrupo de D, então existe $x \in N_1$ tal que

$$D_1 \subseteq x(N_1 \cap gDg^{-1})x^{-1} = xN_1x^{-1} \cap xgDg^{-1}x^{-1} = N_1 \cap xgD(xg)^{-1}.$$

Logo,

$$D \cap xgD(xg)^{-1} \supseteq D_1 \implies D \cap xgD(xg)^{-1} \neq \{1\}.$$

Como fizemos no parágrafo anterior, isso implica que $xg \in N_1$ e, portanto, $g \in N_1$. Vejamos qual informação isso nos dá. Como

$$\mathfrak{Y} = \{N_1 \cap gDg^{-1} \mid g \in G, g \notin N_1\},$$

concluímos que nenhum conjugado (em N_1) de um subgrupo em $\mathfrak{Y}$ pode conter um subgrupo não trivial de D. Pelo Teorema 4.2.2, D contém um vértice de todo b_1-módulo indecomponível, logo, se Y é um kN_1-módulo indecomponível relativamente $\mathfrak{Y}$-projetivo, então Y é projetivo ou então Y não é projetivo e, nesse caso, não pode pertencer a b_1 (já que possui um vértice não trivial contido em um subgrupo de $\mathfrak{Y}$).

O Corolário 3.4.6 já fez quase tudo para nós! Como D é um grupo de defeito de B e de b_1, o Teorema 4.2.2 mostra que todos os B-módulos e b_1-módulos indecomponíveis não projetivos aparecem nessa correspondência. A única coisa que resta para terminar a prova do teorema é verificar que o correspondente de Green de um B-módulo indecomponível não projetivo é um b_1-módulo, e vice-versa. Uma das direções é mais fácil: suponha que V seja um b_1-módulo indecomponível não projetivo e seja U o seu correspondente de Green. Pelo Teorema 4.2.2, V possui um vértice contido em D. Esse vértice deve ser não nulo, porque V não é projetivo, então ele contém D_1. Em particular, o centralizador desse vértice está contido em $C_G(D_1) \subseteq N_1$. Como $V \mid U_{N_1}$, podemos aplicar o Segundo Teorema Principal de Brauer para concluir que U pertence ao bloco $b_1^G = B$.

Reciprocamente, suponha que U seja um B-módulo indecomponível não projetivo e seja V o seu correspondente de Green, que pertence a algum bloco b' de kN_1. Devemos mostrar que $b' = b_1$. Como V possui o mesmo vértice de U e D é um grupo de defeito de B, segue como no parágrafo anterior que um vértice de V contém D_1 e, por isso, o centralizador desse vértice está contido em N_1. Pelo Segundo Teorema Principal de Brauer, concluímos como antes que $(b')^G$ está definido e é igual a B. Seja D' um grupo de defeito de b'. Como $(b')^G = B$, o Lema 4.3.1 nos diz que D' é conjugado a um subgrupo de D e então D' é cíclico. Como D_1 é um p-subgrupo

normal de N_1, o Corolário 4.2.9 mostra que $D_1 \subseteq D'$. Logo, D_1 é o único subgrupo de ordem p do grupo cíclico D' e segue que $N_G(D') \subseteq N_1$. Pelo Primeiro Teorema Principal de Brauer, segue que D' é um grupo de defeito de $(b')^G = B$, então existe $g \in G$ tal que $gD'g^{-1} = D$. Como D_1 é o único subgrupo de ordem p de D e de D', concluímos que $gD_1g^{-1} = D_1$, ou seja, $g \in N_1$. Mas então D é conjugado a D' em N_1 e, por isso, D também é um grupo de defeito de b'. Como $(b')^G = B = b_1^G$ e os blocos b' e b_1 possuem D como grupo de defeito, segue do Primeiro Teorema Principal de Brauer que $b' = b_1$, como preciso. □

De certa forma, esta seção inteira é um estudo profundo dessa correspondência entre B-módulos e b_1-módulos. Porém, é preciso entender o que é preservado quando passamos de um lado para o outro. O primeiro resultado nessa linha é um análogo do Corolário 3.3.4:

Corolário 5.4.2. Se U_1 e U_2 são B-módulos indecomponíveis não projetivos e V_1 e V_2 são os b_1-módulos correspondentes, então

$$\overline{\mathrm{Hom}}_{kG}(U_1, U_2) \cong \overline{\mathrm{Hom}}_{kN_1}(V_1, V_2).$$

Demonstração. Pelo Teorema 5.4.1, existe um kG-módulo projetivo X_1, um kN_1-módulo projetivo Y_2 e um kN_1-módulo Y_2' cujos somandos indecomponíveis estão em blocos diferentes de b_1 tais que

$$V_1^G \cong U_1 \oplus X_1 \quad \text{e} \quad (U_2)_{N_1} \cong V_2 \oplus Y_2 \oplus Y_2'.$$

Como X_1 é projetivo, vale

$$\overline{\mathrm{Hom}}_{kG}(U_1, U_2) \cong \overline{\mathrm{Hom}}_{kG}(U_1 \oplus X_1, U_2) \cong \overline{\mathrm{Hom}}_{kG}(V_1^G, U_2) \cong \overline{\mathrm{Hom}}_{kN_1}(V_1, (U_2)_{N_1}),$$

onde o primeiro isomorfismo segue do Exercício A.3.15 e o terceiro é o mesmo que demonstramos no Corolário 3.3.4. Também temos

$$\overline{\mathrm{Hom}}_{kN_1}(V_1, (U_2)_{N_1}) \cong \overline{\mathrm{Hom}}_{kN_1}(V_1, V_2) \oplus \overline{\mathrm{Hom}}_{kN_1}(V_1, Y_2) \oplus \overline{\mathrm{Hom}}_{kN_1}(V_1, Y_2').$$

Como Y_2 é projetivo, $\overline{\mathrm{Hom}}_{kN_1}(V_1, Y_2) = 0$. Por sua vez, como os somandos indecomponíveis de Y_2' pertencem a blocos distintos do bloco ao qual pertence V_1, segue do Exercício A.4.2 que não há homomorfismos não nulos entre esses módulos e, em particular, $\overline{\mathrm{Hom}}_{kN_1}(V_1, Y_2') = 0$. Isso termina a prova do resultado. □

São preservados homomorfismos apenas a menos de fatoração por projetivo. É por isso que demos tanta importância às coberturas projetivas e ao operador de Heller na seção anterior! Com isso, já conseguimos dar uma descrição dos B-módulos simples! Mas primeiro vamos introduzir algumas notações.

Pelo Teorema 5.2.6, b_1 é uma álgebra de Brauer e a sua árvore de Brauer é uma estrela com e arestas. Sejam $V_0, V_1, \ldots, V_{e-1}$ os b_1-módulos simples ordenados de acordo com a árvore. Para simplificar alguns argumentos, dado um inteiro i qualquer, V_i denotará o módulo V_t, onde t é o único inteiro tal que $0 \leq t < e$ e $i \equiv t \pmod{e}$. Pelo Corolário 5.2.14, sabemos como são todos os b_1-módulos indecomponíveis: cada um deles é unisseriado e unicamente determinado por seu comprimento e por sua primeira camada radical. Assim, dados i inteiro e $1 \leq s \leq q := p^n$, denote por V_{is} o b_1-módulo indecomponível de comprimento s tal que $V_{is}/\operatorname{rad}(V_{is}) \cong V_i$. Observe que os seus fatores de composição são, em ordem,

$$V_i, V_{i+1}, \ldots, V_{i+s-1}.$$

Teorema 5.4.3. Existem e classes de isomorfismo de B-módulos simples. Todo b_1-módulo simples é um quociente do correspondente de Green de exatamente um B-módulo simples e é um submódulo do correspondente de Green de exatamente um B-módulo simples.

Demonstração. Sejam S_1 e S_2 dois B-módulos simples não isomorfos. Como B não é de defeito zero, esses módulos não são projetivos e então possuem correspondentes de Green T_1 e T_2. Comecemos mostrando que $T_1/\operatorname{rad}(T_1)$ e $T_2/\operatorname{rad}(T_2)$ não são isomorfos. Suponha, por absurdo, que tais quocientes sejam isomorfos. Como T_1 e T_2 são indecomponíveis e como sabemos a estrutura dos b_1-módulos indecomponíveis, segue que $T_1/\operatorname{rad}(T_1)$ e $T_2/\operatorname{rad}(T_2)$ são isomorfos a algum b_1-módulo simples V_i. Portanto, existem $1 \leq s, t < q$ tais que $T_1 \cong V_{is}$ e $T_2 \cong V_{it}$. Como S_1 e S_2 não são isomorfos, T_1 e T_2 também não são e vale $s \neq t$. Sem perda de generalidade, vamos assumir que $s < t$. Assim, T_2 possui um quociente de comprimento s que necessariamente é isomorfo a T_1, o que nos dá um homomorfismo sobrejetor $T_2 \to T_1$. É importante observar que esse homomorfismo não pode se fatorar por um projetivo, pois, caso se fatorasse, o Lema 5.3.19 nos diria que T_2 possuiria um somando direto não nulo projetivo, o que não pode acontecer porque T_2 é indecomponível e não projetivo. Em particular, $\overline{\operatorname{Hom}}_{kN_1}(T_1, T_2) \neq 0$. Pelo Corolário 5.4.2,

$$\overline{\operatorname{Hom}}_{kG}(S_1, S_2) \neq 0 \implies \operatorname{Hom}_{kG}(S_1, S_2) \neq 0,$$

o que é um absurdo, já que S_1 e S_2 são simples não isomorfos. Logo, de fato deve valer $T_1/\operatorname{rad}(T_1) \ncong T_2/\operatorname{rad}(T_2)$. Como existem e b_1-módulos simples, isso mostra que existem no máximo e B-módulos simples.

Um argumento análogo mostra que $\operatorname{soc}(T_1) \ncong \operatorname{soc}(T_2)$. Com efeito, se esses módulos fossem isomorfos, conseguiríamos utilizar a descrição dos b_1-módulos indecomponíveis para mostrar que T_1 é submódulo de T_2 ou vice-versa. Novamente pelo Lema 5.3.19, essa inclusão não poderia se fatorar por um projetivo e então obteríamos $\overline{\operatorname{Hom}}_{kN_1}(T_1, T_2) \neq 0$ (ou então $\overline{\operatorname{Hom}}_{kN_1}(T_2, T_1) \neq 0$). A partir disso, conseguimos usar o Corolário 5.4.2 para chegar numa contradição.

Agora, para cada $0 \leq i < e$, vamos encontrar um B-módulo simples S cujo correspondente de Green T satisfaz $T/\operatorname{rad}(T) \cong V_i$. Para isso, seja U o B-módulo que é o correspondente de Green de V_i. Tome S como sendo um submódulo simples de $\operatorname{soc}(U)$. Como U é indecomponível não projetivo, o Lema 5.3.19 garante que a inclusão $S \to U$ não se fatora através de um projetivo. Logo, $\overline{\operatorname{Hom}}_{kG}(S, U) \neq 0$ e, pelo Corolário 5.4.2, $\overline{\operatorname{Hom}}_{kN_1}(T, V_i) \neq 0$, onde T é o correspondente de Green de S. Em particular, existe algum homomorfismo não nulo de T em V_i e, como V_i é simples, ele é sobrejetor. Por isso, V_i é um quociente de $T/\operatorname{rad}(T)$ e, como $T/\operatorname{rad}(T)$ é simples (pela descrição dos b_1-módulos indecomponíveis), vale $T/\operatorname{rad}(T) \cong V_i$, como queríamos. Isso prova que existem exatamente e B-módulos simples e também demonstra a primeira metade da segunda afirmação do enunciado. A outra metade segue de modo análogo, apenas dualizando o argumento acima: desta vez, tomamos S como um quociente simples de $U/\operatorname{rad}(U)$ e prosseguimos de modo semelhante para encontrar um homomorfismo injetor de V_i em T, obtendo $V_i \cong \operatorname{soc}(T)$. □

A partir disso, podemos estabelecer mais uma notação. Sejam $S_0, S_1, \ldots, S_{e-1}$ os B-módulos simples, ordenados de modo que $T_i/\operatorname{rad}(T_i) \cong V_i$, onde T_i é o correspondente de Green de S_i para todo $0 \leq i < e$. Também sabemos que existe uma permutação π do conjunto $\{0, 1, \ldots, e-1\}$ tal que $\operatorname{soc}(T_i) \cong V_{\pi(i)}$ para todo $0 \leq i < e$. Essa permutação será importante.

Lema 5.4.4. Se $0 \leq i, j < e$, então vale $\dim_k \overline{\operatorname{Hom}}_{kN_1}(T_i, T_j) = \delta_{ij}$.

Demonstração. Pelo Corolário 5.4.2 e pelo Lema 5.3.19, temos

$$\overline{\operatorname{Hom}}_{kN_1}(T_i, T_j) \cong \overline{\operatorname{Hom}}_{kG}(S_i, S_j) \cong \operatorname{Hom}_{kG}(S_i, S_j),$$

de onde o resultado segue porque S_i e S_j são simples. □

Isso está indicando que os módulos $T_0, T_1, \ldots, T_{e-1}$ não podem ser quaisquer. Vamos explorar as suas propriedades para depois conseguir obter informações a respeito dos B-módulos simples. Para os próximos resultados, denotaremos por $l(V)$ o comprimento de um b_1-módulo V.

Lema 5.4.5. Se $\theta : V_{is} \to V_{jt}$ é um homomorfismo não nulo, então θ se fatora através de um projetivo se, e somente se,

$$l(\operatorname{im}\theta) \leq s + t - q.$$

Demonstração. Sejam $Y \coloneqq \operatorname{im}\theta$ e $r \coloneqq l(Y)$. Note que V_{jq} é projetivo e possui V_{jt} como quociente. Como os quocientes radicais de V_{jq} e V_{jt} são isomorfos, a projeção $\varphi : V_{jq} \to V_{jt}$ induz um isomorfismo nos quocientes radicais, de onde concluímos que V_{jq} e φ formam uma cobertura projetiva de V_{jt}. Seja $X \coloneqq \varphi^{-1}(Y)$. Pelo Teorema do Isomorfismo, obtemos $V_{jq}/X \cong V_{jt}/Y$, então

$$q - l(X) = l(V_{jq}) - l(X) = l(V_{jq}/X) = l(V_{jt}/Y) = l(V_{jt}) - l(Y) = t - r,$$

ou seja, $l(X) = q - t + r$.

Suponha que θ se fatore através de um projetivo. Pelo Lema 5.3.5, existe um homomorfismo $\rho : V_{is} \to V_{jq}$ tal que $\theta = \varphi\rho$. Nesse caso, devemos ter $\operatorname{im}\rho \subseteq X$. Por outro lado, como V_{jq} é unisseriado, $\operatorname{im}\rho \subseteq \ker\varphi$ ou $\ker\varphi \subseteq \operatorname{im}\rho$. Como θ é um homomorfismo não nulo, a primeira dessas inclusões não pode valer, logo $\ker\varphi \subseteq \operatorname{im}\rho$. Como $\varphi(\operatorname{im}\rho) = Y = \varphi(X)$ e tanto $\operatorname{im}\rho$ como X contêm $\ker\varphi$, segue do Teorema da Correspondência que $X = \operatorname{im}\rho$. Assim, X é um quociente de V_{is} e vale

$$l(X) \leq l(V_{is}) \implies q - t + r \leq s \implies r \leq s + t - q,$$

como desejado.

Reciprocamente, suponha que $r \leq s + t - q$. Vamos mostrar que θ se fatora através de um projetivo por indução em r. Como veremos na demonstração, o caso base acontecerá essencialmente quando $r = 0$, ou seja, quando $\theta = 0$. Como Y é não nulo e é um quociente de V_{is}, deve valer $Y/\operatorname{rad}(Y) \cong V_i$. Logo, como Y é quociente de X, V_i é quociente de $X/\operatorname{rad}(X)$. Mas X é unisseriado, então $X/\operatorname{rad}(X)$ é simples e, consequentemente, isomorfo a V_i. Agora, como $r \leq s+t-q$, obtemos como no parágrafo anterior que $l(X) \leq l(V_{is})$. Da descrição dos b_1-módulos indecomponíveis, concluímos que X é um quociente de V_{is} e existe um homomorfismo sobrejetor $\rho : V_{is} \to X$. Podemos ver a composta $\varphi\rho$ como um homomorfismo sobrejetor de V_{is} em Y. Gostaríamos que valesse $\theta = \varphi\rho$, mas não há motivos para isso acontecer. Porém, note que θ e $\varphi\rho$ possuem o mesmo núcleo, já que possuem a mesma imagem e V_{is} é unisseriado. Encarando o mapa $\varphi\rho$ como sendo um mapa quociente de V_{is} em Y, podemos utilizar o Teorema do Isomorfismo para encontrar um isomorfismo $\alpha : Y \to Y$ tal que $\alpha(\varphi\rho) = \theta$. Se α se estendesse a um automorfismo de V_{jt}, então $\alpha\varphi$ seria um homomorfismo de V_{jq} em V_{jt} satisfazendo $(\alpha\varphi)\rho = \theta$ e, assim, θ se fatoraria por um projetivo. Pensando nisso, tentaremos trocar α por um automorfismo de V_{jt}. Como k é algebricamente fechado, α possui um autovalor, ou seja, podemos encontrar $\lambda \in k$ tal que $\alpha - \lambda\operatorname{id}_Y$ não é inversível. Portanto, a imagem de $\alpha - \lambda\operatorname{id}_Y$ está propriamente contida em Y e o mesmo acontece para a composição

$$(\alpha - \lambda\operatorname{id}_Y)\varphi\rho = \alpha(\varphi\rho) - \lambda\varphi\rho = \theta - \lambda\varphi\rho.$$

Note que $\lambda\varphi$ agora é um homomorfismo de V_{jq} em V_{jt}, então $\lambda\varphi\rho$ é um homomorfismo de V_{is} em V_{jt} que se fatora por um projetivo. Se o homomorfismo em destaque acima for nulo, então $\theta = \lambda\varphi\rho$ e θ se fatora através de um projetivo. Se ele não for nulo, então sua imagem está propriamente contida em Y e podemos aplicar a hipótese de indução para deduzir que $\theta - \lambda\varphi\rho$ se fatora por um projetivo, logo a soma $(\theta - \lambda\varphi\rho) + \lambda\varphi\rho = \theta$ também se fatora através de um projetivo. □

Esse último lema nos permitirá dar uma boa estimativa do comprimento de cada T_i. Para fazer essa estimativa, precisaremos lidar com ΩT_i. Vejamos em geral como é ΩV para um b_1-módulo indecomponível e não projetivo V. Pela descrição dos indecomponíveis, podemos supor $V = V_{jt}$ para algum $0 \leq j < e$ e $1 \leq t < q$. Como vimos na demonstração anterior, V_{jq} é a cobertura projetiva de V_{jt}. Em particular, $l(\Omega V_{jt})$ possui comprimento $q - t$. Mas V_{jq} possui um único submódulo de comprimento $q - t$. Como os t primeiros fatores de composição de V_{jq} são

$$V_j, V_{j+1}, \ldots, V_{j+t-1},$$

segue que os fatores de composição de ΩV_{jt} são, em ordem,

$$V_{j+t}, V_{j+t+1}, \ldots, V_{j+q-1}.$$

Pela descrição dos indecomponíveis, concluímos que $\Omega V_{jt} \cong V_{j+t,q-t}$.

Diremos que um b_1-módulo indecomponível V é **baixo** se $l(V) \leq e$ e **alto** se $l(V) \geq q - e$. Observe que, pelo parágrafo anterior, se V é baixo (alto) então ΩV é alto (baixo), e vice-versa.

Lema 5.4.6. Cada módulo T_i é baixo ou alto.

Demonstração. Se $q \leq 2e$, então todo b_1-módulo é baixo ou alto. Suponha que $q > 2e$, de modo que tenhamos as desigualdades

$$e < \frac{q}{2} < q - e.$$

Primeiramente, suponha por absurdo que $e < l(T_i) \leq q/2$. Como $l(T_i) > e$ e os fatores de composição de T_i seguem a ordem V_i, V_{i+1}, V_{i+2} e assim em diante, sabemos que V_{i+e} aparece nessa lista, ou seja, V_i aparece novamente como fator de composição de T_i. Por conta dessa descrição circular dos fatores de composição, sabemos que um submódulo de T_i com quociente radical V_i é necessariamente um quociente de T_i. Em particular, conseguimos encontrar um homomorfismo não nulo e não inversível de T_i em T_i. Portanto, a dimensão de $\mathrm{Hom}_{kN_1}(T_i, T_i)$ é pelo menos 2. Porém, observe que

$$l(T_i) + l(T_i) - q \leq \frac{q}{2} + \frac{q}{2} - q = 0,$$

então o Lema 5.4.5 diz que nenhum homomorfismo não nulo de T_i em T_i pode se fatorar por um projetivo. Desse modo, $\mathrm{Hom}_{kN_1}(T_i, T_i) \cong \overline{\mathrm{Hom}}_{kN_1}(T_i, T_i)$. Mas $\overline{\mathrm{Hom}}_{kN_1}(T_i, T_i)$ possui dimensão 1 pelo Lema 5.4.4, o que é uma contradição.

Agora, suponha por absurdo que $q/2 \leq l(T_i) < q - e$. Como $l(\Omega T_i) = q - l(T_i)$, concluímos que $e < l(\Omega T_i) \leq q/2$. Argumentando como no parágrafo anterior, concluímos que a dimensão de $\overline{\mathrm{Hom}}_{kN_1}(\Omega T_i, \Omega T_i)$ é pelo menos 2. Mas a Proposição 5.3.23 nos dá um isomorfismo

$$\overline{\mathrm{Hom}}_{kN_1}(\Omega T_i, \Omega T_i) \cong \overline{\mathrm{Hom}}_{kN_1}(T_i, T_i),$$

então novamente chegamos em uma contradição pelo Lema 5.4.4. Dessas contradições, concluímos que $l(T_i) \leq e$ ou $l(T_i) \geq q - e$, isto é, T_i é baixo ou alto. □

Por conta disso, o próximo resultado é válido para os módulos T_i:

Lema 5.4.7. Se V é um b_1-módulo indecomponível que é baixo ou alto e se W é um b_1-módulo indecomponível qualquer, então cada um dos espaços vetoriais

$$\overline{\mathrm{Hom}}_{kN_1}(V, W), \quad \overline{\mathrm{Hom}}_{kN_1}(W, V), \quad \overline{\mathrm{Hom}}_{kN_1}(\Omega V, W), \quad \overline{\mathrm{Hom}}_{kN_1}(W, \Omega V)$$

é nulo ou unidimensional.

Demonstração. Suponha inicialmente que V seja baixo. Vamos mostrar que $\mathrm{Hom}_{kN_1}(V, W)$ e $\mathrm{Hom}_{kN_1}(W, V)$ possuem dimensão no máximo 1. Seja $0 \leq i < e$ tal que $V/\operatorname{rad}(V) \cong V_i$. Se W não possui nenhum fator de composição isomorfo a V_i, então devemos ter $\mathrm{Hom}_{kN_1}(V, W) = 0$. Suponha então que W possua um fator de composição isomorfo a V_i. Vejamos que W possui um único submódulo baixo Y tal que $Y/\operatorname{rad}(Y) \cong V_i$. Escolha Y de modo que $Y/\operatorname{rad}(Y)$ seja o último fator de composição de W isomorfo a V_i. Como os fatores de composição de Y seguem a ordem V_i, V_{i+1}, V_{i+2} e assim em diante, e como Y possui um único fator de composição isomorfo a V_i, segue que $V_{i+e} = V_i$ não pode aparecer nessa lista e temos $l(Y) \leq e$, ou seja, Y é baixo. Além disso, se $Z \neq Y$ é outro submódulo de W com $Z/\operatorname{rad}(Z) \cong V_i$, então Z deve conter Y propriamente e, pela estrutura "circular" de W, vale $l(Z/Y) \geq e$, então $l(Z) > e$ e Z não é baixo. Logo, a nossa afirmação sobre Y é válida. Como todo quociente não nulo de V é baixo e possui quociente radical isomorfo a V_i, concluímos que, se φ e θ são homomorfismos não nulos de V em W, então vale $\operatorname{im}\varphi = Y = \operatorname{im}\theta$. Argumentando exatamente como na demonstração do Lema 5.4.5, encontramos $\lambda \in k$ tal que $\varphi - \lambda\theta$ possui imagem propriamente contida em Y. Mas $\varphi - \lambda\theta$

ainda é um homomorfismo de V em W e, como sua imagem não é Y, ele deve ser nulo e chegamos em $\varphi = \lambda\theta$. Isso comprova que $\mathrm{Hom}_{N_1}(V, W)$ possui dimensão no máximo 1.

De modo análogo, conseguimos limitar a dimensão de $\mathrm{Hom}_{kN_1}(W, V)$. Se $W/\operatorname{rad}(W) \cong V_j$, então temos dois casos: ou V_j não é fator de composição de V e vale $\mathrm{Hom}_{kN_1}(W, V) = 0$, ou V possui um único submódulo X tal que $X/\operatorname{rad}(X) \cong V_j$ e, nesse caso, X é a imagem de qualquer homomorfismo não nulo de W em V, de onde concluímos como antes que $\mathrm{Hom}_{kN_1}(W, V)$ possui dimensão no máximo 1.

Se W é projetivo, então $\overline{\mathrm{Hom}}_{kN_1}(\Omega V, W) = 0$. Se W não é projetivo, então $W = \Omega^0 W \cong \Omega\Omega^{-1}W$ e, pela Proposição 5.3.23,

$$\overline{\mathrm{Hom}}_{kN_1}(\Omega V, W) \cong \overline{\mathrm{Hom}}_{kN_1}(\Omega V, \Omega\Omega^{-1}W) \cong \overline{\mathrm{Hom}}_{kN_1}(V, \Omega^{-1}W).$$

Pelo Teorema 5.3.22, $\Omega^{-1}W$ é indecomponível, então concluímos do primeiro parágrafo que a dimensão de $\overline{\mathrm{Hom}}_{kN_1}(\Omega V, W)$ é no máximo 1. Trocando ΩV e W de posição, um argumento simétrico garante que o mesmo vale para $\overline{\mathrm{Hom}}_{kN_1}(W, \Omega V)$.

Agora, suponha que V seja alto. Se V é projetivo, então todos os espaços do enunciado são nulos. Se V não é projetivo, podemos escrever

$$V = \Omega^0 V \cong \Omega\Omega^{-1}V = \Omega V',$$

onde $V' := \Omega^{-1}V$, que é indecomponível pelo Teorema 5.3.22. Como $\Omega V' \cong V$ é alto, V' deve ser baixo. Assim, já sabemos que o enunciado é verdadeiro se trocarmos V por V'. Se W é projetivo, então $\overline{\mathrm{Hom}}_{kN_1}(V, W) = 0$. Caso contrário, podemos imitar o parágrafo anterior para obter

$$\overline{\mathrm{Hom}}_{kN_1}(V, W) \cong \overline{\mathrm{Hom}}_{kN_1}(V', \Omega^{-1}W)$$

e, como V' é baixo e $\Omega^{-1}W$ é indecomponível, concluímos que $\overline{\mathrm{Hom}}_{kN_1}(V, W)$ possui dimensão no máximo 1. Analogamente, o mesmo vale para $\overline{\mathrm{Hom}}_{kN_1}(W, V)$. Por fim, copiando o parágrafo anterior, concluímos que $\overline{\mathrm{Hom}}_{kN_1}(\Omega V, W)$ e $\overline{\mathrm{Hom}}_{kN_1}(W, \Omega V)$ também são nulos ou unidimensionais. □

Conseguimos obter uma propriedade muito interessante dos B-módulos indecomponíveis!

Proposição 5.4.8. Se U é um B-módulo indecomponível, então $\operatorname{soc}(U)$ e $U/\operatorname{rad}(U)$ são livres de multiplicidade.

Por "livres de multiplicidade" queremos dizer que os módulos semissimples $\operatorname{soc}(U)$ e $U/\operatorname{rad}(U)$ são uma soma direta de módulos simples dois a dois não isomorfos.

Demonstração. Se U é projetivo, isso segue dos Teoremas 2.2.4 e 2.3.17. Suponha então que U não seja projetivo. Pelo Exercício A.1.11 (e usando que k é algebricamente fechado), devemos mostrar que $\mathrm{Hom}_{kG}(S_j, U)$ e $\mathrm{Hom}_{kG}(U, S_j)$ possuem dimensão no máximo 1 para todo $0 \leq j < e$. Como U não é projetivo, podemos considerar o seu correspondente de Green V, então, pelo Lema 5.3.19 e pelo Corolário 5.4.2,

$$\mathrm{Hom}_{kG}(S_j, U) \cong \overline{\mathrm{Hom}}_{kG}(S_j, U) \cong \overline{\mathrm{Hom}}_{kN_1}(T_j, V).$$

Como T_j é baixo ou alto, o Lema 5.4.7 mostra que $\mathrm{Hom}_{kG}(S_j, U)$ é nulo ou unidimensional, como preciso. Um argumento análogo se aplica para $\mathrm{Hom}_{kG}(U, S_j)$, concluindo a demonstração. □

Observação 5.4.9. Essa propriedade é crucial para o que se segue. Muitos dos próximos resultados utilizam a Proposição 5.4.8 para mostrar que certos casos não podem acontecer, já que implicariam na existência de indecomponíveis com quociente radical ou soco não livres de multiplicidade. Um comentário interessante é que há um teorema relacionado, mas em outra direção: se A é uma álgebra de dimensão finita e todo A-módulo indecomponível possui soco livre de multiplicidade (ou se todo A-módulo indecomponível possui quociente radical livre de multiplicidade),

então A possui tipo de representação finito (veja o artigo [9] para uma prova). Note que, pela Proposição 5.1.2, os blocos de uma álgebra de grupo com grupo de defeito cíclico são exatamente aqueles que possuem tipo de representação finito, então podemos ver a Proposição 5.4.8 como uma recíproca do teorema deste artigo.

Estamos prontos para estudar as extensões dos B-módulos simples.

Proposição 5.4.10. Se U é um B-módulo indecomponível não projetivo e se $0 \leq j < e$, então existe, a menos de isomorfismo, no máximo uma sequência exata que não cinde da forma

$$0 \longrightarrow S_j \longrightarrow M \longrightarrow U \longrightarrow 0$$

Ademais, essa sequência existe se, e somente se,

$$\overline{\mathrm{Hom}}_{kN_1}(\Omega V, T_j) \neq 0,$$

onde V é o correspondente de Green de U.

A unicidade aqui significa que, se

$$0 \longrightarrow S_j \longrightarrow M' \longrightarrow U \longrightarrow 0$$

é outra sequência como no enunciado, então existem um isomorfismo $\theta : M \to M'$ e um automorfismo $\varphi : S_j \to S_j$ tais que o seguinte diagrama é comutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S_j & \longrightarrow & M & \longrightarrow & U & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}_U} & & \\ 0 & \longrightarrow & S_j & \longrightarrow & M' & \longrightarrow & U & \longrightarrow & 0 \end{array}$$

Portanto, M e M' são isomorfos e esse isomorfismo é compatível com o modo de que esses módulos são construídos.

Demonstração. Suponha que $\overline{\mathrm{Hom}}_{kN_1}(\Omega V, T_j) \neq 0$. Pela Proposição 5.3.24, o correspondente de Green de ΩV é ΩU, então o Corolário 5.4.2 implica em

$$\overline{\mathrm{Hom}}_{kN_1}(\Omega V, T_j) \cong \overline{\mathrm{Hom}}_{kG}(\Omega U, S_j).$$

Como todo homomorfismo não nulo de ΩU em S_j é sobrejetor e como ΩU é indecomponível não projetivo, o Lema 5.3.19 mostra que $\overline{\mathrm{Hom}}_{kG}(\Omega U, S_j)$ é isomorfo a $\mathrm{Hom}_{kG}(\Omega U, S_j)$. Pela hipótese inicial, concluímos que de fato existe um homomorfismo não nulo de ΩU em S_j e, por isso, S_j é um fator de composição de $\Omega U/\operatorname{rad}(\Omega U)$. Pela Proposição 5.4.8, $\Omega U/\operatorname{rad}(\Omega U)$ é livre de multiplicidade, então, se escrevermos esse quociente como soma direta de módulos simples, os submódulos desse quociente são precisamente as somas de um subconjunto de tais módulos simples. Concluímos que existe um único submódulo X de ΩU tal que $\Omega U/X \cong S_j$. Agora, se tomarmos a sequência exata canônica

$$0 \longrightarrow \Omega U \xrightarrow{i_U} PU \xrightarrow{\pi_U} U \longrightarrow 0$$

então $X \subseteq \Omega U = \ker \pi_U$ e podemos passar a sequência ao quociente:

$$0 \longrightarrow \Omega U/X \longrightarrow PU/X \longrightarrow U \longrightarrow 0$$

Afirmamos que essa sequência não cinde. Para isso, primeiro precisamos argumentar que $\Omega U \subseteq \operatorname{rad}(PU)$. De fato, como π_U é um epimorfismo essencial, a Proposição 5.3.3 diz que π_U induz

um isomorfismo de $PU/\operatorname{rad}(PU)$ em $U/\operatorname{rad}(U)$. Certamente esse isomorfismo leva o submódulo $(\Omega U + \operatorname{rad}(PU))/\operatorname{rad}(PU)$ em 0 porque $\Omega U = \ker \pi_U$ e, portanto, esse módulo é nulo, de onde obtemos $\Omega U \subseteq \operatorname{rad}(PU)$. Como $X \subseteq \Omega U$, então segue que $X \subseteq \operatorname{rad}(PU)$ e obtemos que o radical de PU/X é $\operatorname{rad}(PU)/X$. Agora, se a sequência em destaque cindisse, então $\Omega U/X$ seria um somando direto de PU/X e conseguiríamos escrever

$$\frac{PU}{X} = \frac{\Omega U}{X} \oplus Y$$

para algum submódulo Y de PU/X. Como $\Omega U/X \cong S_j$ é simples, ao tomarmos o radical dos dois lados da igualdade acima, nós obtemos $\operatorname{rad}(PU)/X = \operatorname{rad}(Y)$. Mas sabemos que $\Omega U/X \subseteq \operatorname{rad}(PU)/X$, então chegamos em $\Omega U/X \subseteq Y$, o que contradiz o fato de a soma acima ser direta. Isso garante a existência de uma sequência como no enunciado e prova uma das implicações apresentadas.

Vamos mostrar agora a outra implicação e a unicidade. Seja

$$0 \longrightarrow S_j \xrightarrow{\ i\ } M \xrightarrow{\ \pi'\ } U \longrightarrow 0$$

uma sequência exata que não cinde. Denote a imagem de S_j por i como sendo S. Vejamos que $S \subseteq \operatorname{rad}(M)$. Se isso não acontecesse, então $S \cap \operatorname{rad}(M) = 0$, porque S é simples. Agora, olhando dentro do módulo semissimples $M/\operatorname{rad}(M)$, podemos encontrar um submódulo da forma $N/\operatorname{rad}(M)$ (onde N é um submódulo de M contendo $\operatorname{rad}(M)$) tal que

$$\frac{M}{\operatorname{rad}(M)} = \frac{S + \operatorname{rad}(M)}{\operatorname{rad}(M)} \oplus \frac{N}{\operatorname{rad}(M)}.$$

Portanto, $(S + \operatorname{rad}(M)) + N = M$ e $(S + \operatorname{rad}(M)) \cap N = \operatorname{rad}(M)$. Como $S \cap \operatorname{rad}(M) = 0$ e como $\operatorname{rad}(M) \subseteq N$, obtemos

$$S + N = S + (\operatorname{rad}(M) + N) = (S + \operatorname{rad}(M)) + N = M$$

e $S \cap N = 0$, ou seja, N é um complemento de S em M. Mas isso diz que a sequência inicial cinde, um absurdo! Por isso, $S \subseteq \operatorname{rad}(M)$. Vamos usar isso para provar que π' é um epimorfismo essencial. Como π' é sobrejetor, podemos utilizar que $\operatorname{rad}(U) = \operatorname{rad}(A)U$ para mostrar que $\pi'(\operatorname{rad}(M)) = \operatorname{rad}(U)$. Mas $\operatorname{rad}(M)$ contém S, que é o núcleo de π', então obtemos $(\pi')^{-1}(\operatorname{rad}(U)) = \operatorname{rad}(M)$. Logo, pelo Teorema do Isomorfismo, π' induz um isomorfismo de $M/\operatorname{rad}(M)$ em $U/\operatorname{rad}(U)$ e a Proposição 5.3.3 mostra que π' é essencial.

Com as informações que temos, vamos encontrar um diagrama comutativo da forma

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega U & \xrightarrow{i_U} & PU & \xrightarrow{\pi_U} & U & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \mathrm{id}_U} & & \\
0 & \longrightarrow & S_j & \xrightarrow{\ i\ } & M & \xrightarrow{\ \pi'\ } & U & \longrightarrow & 0
\end{array}$$

onde δ e γ são sobrejetores. Como PU é projetivo e π' é sobrejetor, conseguimos encontrar $\gamma : PU \to M$ tal que $\pi'\gamma = \pi_U$. Como π' é epimorfismo essencial e a composição $\pi'\gamma = \pi_U$ é sobrejetora, o Lema 5.3.1 mostra que γ é sobrejetor. Como $\pi'(\gamma(\Omega U)) = \pi_U(\Omega U) = 0$, segue que $\gamma(\Omega U) \subseteq \ker \pi' = S = \operatorname{im} i$. Como i é injetor, podemos definir $\delta : \Omega U \to S_j$ tal que $\gamma i_U = i\delta$. Não é difícil verificar que δ é um homomorfismo. Além disso, δ é sobrejetor. Isso segue, por exemplo, do "Lema dos Quatro" de álgebra homológica, mas podemos mostrar isso utilizando dimensões: a dimensão de $\operatorname{im}\delta$ é igual à dimensão de $i(\operatorname{im}\delta) = \gamma(\Omega U)$, porque i é injetor. Agora, note que um elemento no núcleo de γ está certamente no núcleo de $\pi'\gamma = \pi_U$, que é ΩU, então vale $\ker\gamma \subseteq \Omega U$ e obtemos

$$\dim_k \gamma(\Omega U) = \dim_k \Omega U - \dim_k \ker \gamma.$$

Como γ é sobrejetor, a dimensão de $\ker\gamma$ é a dimensão de PU menos a dimensão de M, então o número acima vale

$$\dim_k M - (\dim_k PU - \dim_k \Omega U) = \dim_k M - \dim_k U = \dim_k S_j.$$

Segue que a dimensão da imagem de δ é a dimensão de S_j, então δ deve ser sobrejetor, como afirmado. Em particular, $\Omega U/\ker\delta \cong S_j$. Mas vimos no primeiro parágrafo que X é o único submódulo de ΩU cujo quociente é isomorfo a S_j, então $\ker\delta = X$. Observe que X está no núcleo de π_U (que é ΩU) e no núcleo de γ (porque $i\delta = \gamma i_U$), então podemos descer o diagrama ao quociente:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Omega U/X & \longrightarrow & PU/X & \longrightarrow & U & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & S_j & \longrightarrow & M & \longrightarrow & U & \longrightarrow & 0 \end{array}$$

Como os dois mapas verticais nas pontas são isomorfismos, segue do "Lema dos Cinco" que o mapa vertical no meio também é um isomorfismo. Isso também segue sabendo-se que o mapa vertical do meio é sobrejetor e que

$$\dim_k PU/X = \dim_k \Omega U/X + \dim_k U = \dim_k S_j + \dim_k U = \dim_k M.$$

Logo, mostramos que toda sequência como no enunciado é isomorfa à sequência que construímos no primeiro parágrafo! Ademais, durante essa prova, vimos que a existência de uma sequência como no enunciado garante que S_j é um quociente de ΩU, logo $\mathrm{Hom}_{kG}(\Omega U, S_j) \neq 0$. Pelos isomorfismos construídos no primeiro parágrafo, concluímos que $\overline{\mathrm{Hom}}_{kN_1}(\Omega V, T_j) \neq 0$. Assim, a demonstração está finalizada! □

Para prosseguir, vamos generalizar o Corolário 3.3.3. Aproveitaremos para destacar algumas observações a mais que não fizemos anteriormente.

Proposição 5.4.11. Sejam U_1 e U_2 B-módulos indecomponíveis não projetivos e sejam V_1 e V_2 os respectivos correspondentes de Green. Se existe uma sequência exata

$$0 \longrightarrow V_1 \longrightarrow V \longrightarrow V_2 \longrightarrow 0$$

que não cinde, então existe uma sequência exata

$$0 \longrightarrow U_1 \longrightarrow U \longrightarrow U_2 \longrightarrow 0$$

que não cinde. Além disso, se V for projetivo, podemos tomar U também projetivo, e se V for indecomponível não projetivo, então podemos tomar U como sendo a soma de um indecomponível não projetivo com um projetivo (possivelmente nulo). Reciprocamente, se existir uma sequência que não cinde como a segunda acima e se U for indecomponível, então conseguimos encontrar V tal que a primeira sequência não cinde. Nesse caso, se U for projetivo, podemos tomar V como sendo um indecomponível projetivo, e se U não for projetivo, então podemos tomar V como sendo a soma de um indecomponível não projetivo com um projetivo (possivelmente nulo).

Demonstração. Parte da demonstração é muito análoga ao que fizemos no Corolário 3.3.3, mas vamos entrar em alguns detalhes. Suponha inicialmente que exista uma sequência exata de b_1-módulos

$$0 \longrightarrow V_1 \longrightarrow V \longrightarrow V_2 \longrightarrow 0$$

que não cinde. Induzindo a G, o Lema 3.1.11 nos dá uma nova sequência exata

$$0 \longrightarrow V_1^G \longrightarrow V^G \longrightarrow V_2^G \longrightarrow 0$$

que também não cinde. Pelo Teorema 5.4.1, cada V_i^G é a soma direta de U_i com um módulo projetivo R_i. Estamos exatamente nas mesmas condições da demonstração do Corolário 3.3.3! Tomando um submódulo W de V^G contendo V_1^G e satisfazendo $V^G/W \cong R_2$ e $W/V_1^G \cong U_2$, conseguimos imitar a demonstração para obter uma sequência exata

$$0 \longrightarrow U_1 \longrightarrow W/R_1 \longrightarrow U_2 \longrightarrow 0$$

que não cinde. Note que $U := W/R_1$ pertence a B porque seus fatores de composição são os fatores de U_1 e de U_2, que pertencem a B. Agora, como $V^G/W \cong R_2$ é projetivo, a projeção canônica ao quociente cinde e W é um somando direto de V^G (com complemento isomorfo a R_2). Por outro lado, como R_1 é injetivo (Teorema 2.3.14), R_1 é um somando direto de W (com complemento isomorfo a W/R_1). Ou seja, temos um isomorfismo

$$V^G \cong W/R_1 \oplus R_1 \oplus R_2 = U \oplus R_1 \oplus R_2.$$

Se V é projetivo, então V^G também o é e concluímos que U é projetivo. Se V é indecomponível não projetivo, então podemos aplicar o Teorema 5.4.1 e obter que V^G é a soma direta de seu correspondente de Green com um projetivo. Como esse correspondente de Green é indecomponível e não projetivo, o Teorema de Krull-Schmidt mostra que U é isomorfo à soma direta desse indecomponível não projetivo com mais alguns projetivos. Isso mostra uma das implicações do enunciado.

Reciprocamente, suponha que exista uma sequência exata de B-módulos

$$0 \longrightarrow U_1 \longrightarrow U \longrightarrow U_2 \longrightarrow 0$$

que não cinde, onde U é indecomponível, e considere a restrição

$$0 \longrightarrow (U_1)_{N_1} \longrightarrow U_{N_1} \longrightarrow (U_2)_{N_1} \longrightarrow 0$$

que certamente é uma sequência exata. Como U_2 pertence a B, o Teorema 4.2.2 mostra que U_2 é relativamente D-projetivo e, como $D \subseteq N_1$, também é relativamente N_1-projetivo. Pela Proposição 3.2.1, se o mapa $U_{N_1} \to (U_2)_{N_1}$ cindisse, o mesmo valeria para o mapa $U \to U_2$, o que não é o caso já que estamos supondo que a sequência inicial não cinde. Logo, a sequência restrita também não cinde. Estamos prontos para copiar o Corolário 3.3.3! Mas devemos tomar um certo cuidado. Pelo Teorema 5.4.1, para cada $i = 1, 2$ podemos escrever

$$(U_i)_{N_1} \cong V_i \oplus V_i' \oplus R_i,$$

onde os somandos indecomponíveis de V_i' não pertencem a b_1 e onde R_i é um kN_1-módulo projetivo. Isso é um pouco diferente do que tínhamos no Corolário 3.3.3, mas o segredo é pensar em $V_i \oplus V_i'$ como um módulo só. Assim, podemos fazer como antes: tomamos um submódulo W de U_{N_1} contendo $(U_1)_{N_1}$ tal que $U_{N_1}/W \cong R_2$ e $W/(U_1)_{N_1} \cong V_2 \oplus V_2'$ e, a partir disso, obtemos uma sequência exata

$$0 \longrightarrow V_1 \oplus V_1' \longrightarrow W/R_1 \longrightarrow V_2 \oplus V_2' \longrightarrow 0$$

que não cinde. Resta "limpar" os módulos que não pertencem a b_1. Como na Proposição 4.1.15, podemos escrever W/R_1 como a soma direta de sua componente W_1 correspondente ao bloco b_1 com a soma W_1' das componentes correspondentes aos outros blocos. Vendo $V_1 \oplus V_1'$ como submódulo de W/R_1, a unicidade da Proposição 4.1.15 garante que $V_1 \subseteq W_1$ e $V_1' \subseteq W_1'$. Portanto,

$$V_2 \oplus V_2' \cong \frac{W/R_1}{V_1 \oplus V_1'} = \frac{W_1 \oplus W_1'}{V_1 \oplus V_1'} \cong \frac{W_1}{V_1} \oplus \frac{W_1'}{V_1'}.$$

Novamente pela unicidade da Proposição 4.1.15, devemos ter $V_2 \cong W_1/V_1$ e $V_2' \cong W_1'/V_1'$. Isso nos dá uma sequência exata

$$0 \longrightarrow V_1 \longrightarrow W_1 \longrightarrow V_2 \longrightarrow 0$$

mas não conseguimos garantir que essa sequência não cinde porque não temos controle sobre a outra sequência exata

$$0 \longrightarrow V_1' \longrightarrow W_1' \longrightarrow V_2' \longrightarrow 0$$

É aqui que precisaremos usar que U é indecomponível. Primeiramente, suponha que U não seja projetivo. Assim, podemos aplicar a Correspondência de Green para U, obtendo um b_1-módulo V_U indecomponível não projetivo. Pelo Teorema 5.4.1, $U_{N_1} \cong V_U \oplus V_U' \oplus R_U$, onde V_U' não possui somandos indecomponíveis pertencentes a b_1 e onde R_U é um kN_1-módulo projetivo. Por outro lado, como $U_{N_1}/W \cong R_2$ é projetivo, a projeção canônica ao quociente cinde e W é um somando direto de U_{N_1} (com complemento isomorfo a R_2). Ademais, como R_1 é injetivo, R_1 é um somando direto de W (com complemento isomorfo a W/R_1). Logo,

$$V_U \oplus V_U' \oplus R_U \cong U_{N_1} \cong W/R_1 \oplus R_1 \oplus R_2.$$

Tomando a componente associada ao bloco b_1, obtemos um isomorfismo

$$V_U \oplus Q \cong W_1 \oplus Q'$$

para certos b_1-módulos projetivos Q e Q'. Como V_U é indecomponível não projetivo, agora podemos aplicar o Teorema de Krull-Schmidt para obter

$$V_U \oplus Q'' \cong W_1$$

para certo b_1-módulo projetivo Q''. Se a sequência

$$0 \longrightarrow V_1 \longrightarrow W_1 \longrightarrow V_2 \longrightarrow 0$$

cindisse, então teríamos $W_1 \cong V_1 \oplus V_2$, ou seja, W_1 seria a soma de dois indecomponíveis não projetivos. Mas pelo isomorfismo anterior, W_1 é a soma de um indecomponível não projetivo com outro projetivo, contradizendo o Teorema de Krull-Schmidt. Por isso, a sequência em questão não cinde e podemos tomar $V \coloneqq W_1$. Observe que V é isomorfo à soma direta do indecomponível não projetivo V_U com o projetivo Q''.

O caso em que U é projetivo precisa ser considerado de um jeito totalmente diferente. Por conta da sequência

$$0 \longrightarrow U_1 \longrightarrow U \longrightarrow U_2 \longrightarrow 0,$$

a Proposição 5.3.8 e o Corolário 5.3.9 mostram que $U \cong PU_2 \oplus Q$ e $U_1 \cong \Omega U_2 \oplus Q$ para algum projetivo Q. Mas estamos supondo U indecomponível, então devemos ter $Q = 0$. Em particular, obtemos $U_1 \cong \Omega U_2$. Pela Proposição 5.3.24, $V_1 \cong \Omega V_2$ e então temos a sequência exata canônica

$$0 \longrightarrow V_1 \longrightarrow PV_2 \longrightarrow V_2 \longrightarrow 0.$$

Observe que essa sequência não cinde, já que V_1 e V_2 não são projetivos e então não podem ser somandos diretos de PV_2. Por isso, podemos tomar $V \coloneqq PV_2$. Note que V é projetivo e, como V_2 é indecomponível, temos V indecomponível (a partir da descrição dos b_1-módulos indecomponíveis, lembre que a cobertura projetiva de V_{is} é V_{iq}). □

Conseguimos dar uma boa descrição de como são as extensões de alguns B-módulos indecomponíveis!

Teorema 5.4.12. Seja U um B-módulo indecomponível não projetivo com $U/\operatorname{rad}(U)$ simples e com correspondente de Green isomorfo a V_{is}. Se $0 \leq j < e$, então existe uma sequência exata

$$0 \longrightarrow S_j \longrightarrow M \longrightarrow U \longrightarrow 0$$

que não cinde se, e somente se, ou

$$s + l(T_j) > q \quad \text{e} \quad i = \pi(j)$$

ou

$$s + l(T_j) \leq q \quad \text{e} \quad i + s \equiv j \pmod{e}.$$

Nesse caso, vale $M/\operatorname{rad}(M) \cong U/\operatorname{rad}(U)$ e M é indecomponível.

Acima, π é a permutação definida logo após o Teorema 5.4.3.

Demonstração. Começaremos pela última afirmação. Suponha que exista uma sequência como no enunciado. Como S_j é simples e a sequência não cinde, podemos argumentar exatamente como na demonstração da Proposição 5.4.10 e mostrar que a cópia de S_j em M está contida em $\operatorname{rad}(M)$ e, a partir disso, obter que $M/\operatorname{rad}(M) \cong U/\operatorname{rad}(U)$. Como o quociente radical de U é simples, então o mesmo vale para M e, pelo Exemplo 2.1.11, M é indecomponível.

Ainda supondo que a sequência existe, vamos mostrar que vale uma das condições do enunciado. Como M é indecomponível, podemos aplicar a Proposição 5.4.11! Logo, existe um b_1-módulo L e uma sequência exata

$$0 \longrightarrow T_j \longrightarrow L \longrightarrow V_{is} \longrightarrow 0$$

que não cinde. Vamos separar em dois casos a depender se M é projetivo ou não. Se M é projetivo, então L pode ser tomado como um projetivo indecomponível. Como $V_{is}/\operatorname{rad}(V_{is}) \cong V_i$ é um quociente de L, deve valer $L \cong V_{iq}$. Desse modo,

$$s + l(T_j) = l(V_{is}) + l(T_j) = l(L) = q.$$

Além disso, como L é unisseriado e seus fatores de composição são, em ordem,

$$V_i, V_{i+1}, \ldots, V_{i+q-1},$$

L possui um único submódulo de comprimento $l(T_j)$ e, descartando os s primeiros fatores de composição, segue que o quociente radical desse submódulo é V_{i+s}. Mas esse submódulo deve ser isomorfo a T_j, que possui quociente radical isomorfo a V_j. Logo, $V_{i+s} = V_j$, isto é, $i + s \equiv j \pmod{e}$.

Agora, suponha que M não seja projetivo. Pela Proposição 5.4.11, L pode ser tomado como a soma de um indecomponível não projetivo com um módulo projetivo (possivelmente nulo). Se esse módulo projetivo é não nulo, então seu comprimento é pelo menos q e vale $l(L) = s + l(T_j) > q$. Portanto, se $s + l(T_j) \leq q$, então esse somando projetivo é nulo e segue que L é um indecomponível não projetivo. Isso implica que o comprimento de L é estritamente menor do que q e temos $s + l(T_j) < q$. Prosseguindo como no parágrafo anterior, concluímos que $L \cong V_{i,s+l(T_j)}$ e que $i + s \equiv j \pmod{e}$.

Como último caso, suponha que $s + l(T_j) > q$. Nesse caso, o somando projetivo de L é não nulo. Observe que $s < q$ e $l(T_j) < q$, então o comprimento de L é menor do que $2q$ e esse somando projetivo deve ser de comprimento q e, portanto, é indecomponível. Escreva $L = L' \oplus P$, onde L' é um indecomponível não projetivo e P é um indecomponível projetivo. Vamos determinar L' e P. Identificando T_j como submódulo de L, a projeção de T_j na componente P não pode ser sobrejetora, já que o comprimento de T_j é menor do que o comprimento q de P. Mas P é unisseriado, então a imagem dessa projeção está contida em $\operatorname{rad}(P)$. Logo, $T_j \subseteq L' \oplus \operatorname{rad}(P)$ e concluímos que

$$\frac{L}{L' \oplus \operatorname{rad}(P)} = \frac{L' \oplus P}{L' \oplus \operatorname{rad}(P)} \cong \frac{P}{\operatorname{rad}(P)}$$

é um quociente de

$$\frac{L}{T_j} \cong V_{is}.$$

Mas o único quociente simples de V_{is} é V_i, logo $P/\operatorname{rad}(P) \cong V_i$ e P é a cobertura projetiva de V_i. Por isso, $P \cong V_{iq}$. Por outro lado, se a projeção de T_j na componente L' não fosse sobrejetora, então a imagem dessa projeção estaria contida em $\operatorname{rad}(L')$, porque L' é unisseriado, e teríamos que $T_j \subseteq \operatorname{rad}(L') \oplus \operatorname{rad}(P)$. Como antes, seguiria que

$$\frac{L'}{\operatorname{rad}(L')} \oplus \frac{P}{\operatorname{rad}(P)}$$

seria um quociente de V_{is}. Mas o único quociente semissimples de V_{is} é V_i, que é simples, gerando uma contradição. Logo, a projeção de T_j em L' é sobrejetora e L' é um quociente de T_j. O quociente radical de L' deve então ser um quociente de $T_j/\operatorname{rad}(T_j) \cong V_j$. Concluímos que $L' \cong V_{j,s+l(T_j)-q}$. Assim,

$$L \cong V_{iq} \oplus V_{j,s+l(T_j)-q}.$$

Resta mostrar que $i = \pi(j)$. Pela definição da permutação π, sabemos que $\operatorname{soc}(T_j) \cong V_{\pi(j)}$. Para provar que $i = \pi(j)$, é suficiente mostrar que a cópia de T_j em L intersecta P não trivialmente, pois assim $\operatorname{soc}(T_j)$ intersecta não trivialmente $\operatorname{soc}(P) \cong \operatorname{soc}(V_{iq}) \cong V_i$. Entretanto, se $T_j \cap P = 0$, então a projeção de T_j em L' seria injetora. Já vimos que ela é sobrejetora também, então valeria $T_j \cong L' \cong V_{j,s+l(T_j)-q}$. Mas $s < q$, porque V_{is} não é projetivo, então chegamos em $l(T_j) = s + l(T_j) - q < l(T_j)$, um absurdo! Isso termina a demonstração de uma das implicações.

Para provar a recíproca, pela Proposição 5.4.11, devemos construir uma sequência exata

$$0 \longrightarrow T_j \longrightarrow L \longrightarrow V_{is} \longrightarrow 0$$

que não cinde a partir das condições do enunciado. Vamos imitar as demonstrações dos Lemas 3.3.6 e 3.3.7. Suponha inicialmente que $s + l(T_j) \leq q$ e $i + s \equiv j \pmod{e}$. Tome $L = V_{i,s+l(T_j)}$, que é unisseriado e cujos fatores de composição são dados por

$$V_i, V_{i+1}, \ldots, V_{i+s+l(T_j)-1}.$$

Assim, L possui um único submódulo de comprimento que $l(T_j)$, que é unisseriado e possui quociente radical isomorfo a $V_{i+s} = V_j$ (aqui é onde usamos que $i + s \equiv j \pmod{e}$). Logo, esse submódulo deve ser isomorfo a T_j. Como o quociente de L por essa cópia de T_j é unisseriado e possui comprimento s e quociente radical isomorfo a V_i, ele é isomorfo a V_{is}. Isso nos dá uma sequência exata como acima e ela não cinde porque L é indecomponível.

Agora suponha que $s+l(T_j) > q$ e $i = \pi(j)$. Como $s < q$ e $l(T_j) < q$, temos $0 < s+l(T_j)-q < q$ e podemos definir

$$L = V_{iq} \oplus V_{j,s+l(T_j)-q}.$$

Como $\operatorname{soc}(T_j) \cong V_{\pi(j)} = V_i$ e como V_{iq} é um injetivo contendo V_i, podemos estender esse isomorfismo a um homomorfismo $T_j \to V_{iq}$, que é injetor por induzir um isomorfismo nos socos. Por outro lado, como $s < q$, temos $s + l(T_j) - q < l(T_j)$ e então $V_{j,s+l(T_j)-q}$ é um quociente de T_j, já que ambos possuem o mesmo quociente radical. Seja $\varphi : T_j \to V_{j,s+l(T_j)-q}$ um homomorfismo sobrejetor. Vendo T_j dentro de V_{iq}, defina $\psi : T_j \to L$ por

$$\pi(x) = (x, \varphi(x))$$

para todo $x \in T_j$. É fácil ver que ψ é um homomorfismo injetor, então a sua imagem W é isomorfa a T_j. Vamos mostrar que $L/W \cong V_{is}$, o que dará origem a uma sequência como a que precisamos construir. Pelo Teorema de Krull-Schmidt, $L \ncong T_j \oplus V_{is}$ (porque V_{iq} é projetivo mas T_j e V_{is} não o são) e então a sequência em questão não cinde, o que concluirá a prova.

Como o comprimento de L/W é s, basta mostrar que o quociente radical de L/W é isomorfo a V_i, pois seguirá do Exemplo 2.1.11 que L/W indecomponível e, pela descrição dos b_1-módulos indecomponíveis, deveremos ter $L/W \cong V_{is}$. Pelo Exercício A.1.3,

$$\operatorname{rad}(L/W) = \frac{\operatorname{rad}(L) + W}{W}.$$

Se mostrarmos que $\operatorname{rad}(L) + W = \operatorname{rad}(V_{iq}) \oplus V_{j,s+l(T_j)-q}$, então teremos

$$\frac{L/W}{\operatorname{rad}(L/W)} = \frac{L/W}{(\operatorname{rad}(L)+W)/W} \cong \frac{L}{\operatorname{rad}(L)+W} = \frac{V_{iq} \oplus V_{j,s+l(T_j)-q}}{\operatorname{rad}(V_{iq}) \oplus V_{j,s+l(T_j)-q}} \cong \frac{V_{iq}}{\operatorname{rad}(V_{iq})} \cong V_i,$$

como preciso. Como T_j não é projetivo, a cópia de T_j dentro de V_{iq} é um submódulo próprio e, por isso, está contida em $\operatorname{rad}(V_{iq})$. Logo, obtemos $\operatorname{rad}(L) + W \subseteq \operatorname{rad}(V_{iq}) \oplus V_{j,s+l(T_j)-q}$ porque temos

$$\operatorname{rad}(L) = \operatorname{rad}(V_{iq}) \oplus \operatorname{rad}(V_{j,s+l(T_j)-q}) \subseteq \operatorname{rad}(V_{iq}) \oplus V_{j,s+l(T_j)-q}$$

e, pela definição de W,

$$W \subseteq T_j \oplus V_{j,s+l(T_j)-q} \subseteq \operatorname{rad}(V_{iq}) \oplus V_{j,s+l(T_j)-q}.$$

Por outro lado, como $V_{iq} \subseteq L$, certamente vale $\operatorname{rad}(V_{iq}) \subseteq \operatorname{rad}(L)$. Além disso, se $v \in V_{j,s+l(T_j)-q}$, podemos tomar $x \in T_j$ com $\varphi(x) = v$, então

$$(0, v) = (x, v) - (x, 0) = \psi(x) - (x, 0) \in W + T_j,$$

mostrando que

$$V_{j,s+l(T_j)-q} \subseteq W + T_j \subseteq W + \operatorname{rad}(V_{iq}) \subseteq W + \operatorname{rad}(L).$$

Segue que de fato vale $\operatorname{rad}(L) + W = \operatorname{rad}(V_{iq}) \oplus V_{j,s+l(T_j)-q}$ e a demonstração está finalmente concluída. □

Na próxima seção, aplicaremos esse teorema repetidas vezes para construir módulos unisseriados com certos fatores de composição. Vamos anotar a base desse processo como um resultado à parte:

Corolário 5.4.13. Se $0 \leq i, j < e$, então existe uma sequência exata

$$0 \longrightarrow S_j \longrightarrow M \longrightarrow S_i \longrightarrow 0$$

que não cinde se, e somente se, ou

$$l(T_i) + l(T_j) > q \quad \text{e} \quad i = \pi(j)$$

ou

$$l(T_i) + l(T_j) \leq q \quad \text{e} \quad j \equiv \pi(i) + 1 \pmod{e}.$$

Demonstração. Isso segue do Teorema 5.4.12, já que o correspondente de Green de S_i é T_i, que é isomorfo a $V_{i,l(T_i)}$. A única parte que não é imediata é que $i + l(T_i) \equiv \pi(i) + 1 \pmod{e}$. De fato, como os fatores de composição de T_i são, em ordem,

$$V_i, V_{i+1}, \ldots, V_{i+l(T_i)-1},$$

obtemos $V_{\pi(i)} \cong \operatorname{soc}(T_i) \cong V_{i+l(T_i)-1}$ e então $\pi(i) \equiv i + l(T_i) - 1 \pmod{e}$. □

Fecharemos a seção com algumas observações. Se U é um B-módulo indecomponível não projetivo com $U/\operatorname{rad}(U)$ simples e com correspondente de Green isomorfo a V_{is}, o Teorema 5.4.12 nos dá condições necessárias e suficientes para a existência de uma extensão M de U por S_j que não cinde. Essa extensão é indecomponível e, pela Proposição 5.4.10, é única. Nesse sentido, podemos dizer que M é "a extensão indecomponível" de U por S_j.

A demonstração do Teorema 5.4.12 também indica algumas propriedades de M. Primeiramente, M é projetivo se, e só se, $s+l(T_j) = q$. Se $s+l(T_j) \neq q$, então M não é projetivo e podemos olhar para o seu correspondente de Green N. Se L é o módulo que aparece no Teorema 5.4.12, então a demonstração da Proposição 5.4.11 mostra que N é o único somando indecomponível não projetivo de L. Logo, temos dois casos:

(1) Se $s + l(T_j) > q$, então $N \cong V_{j,s+l(T_j)-q}$. Nesse caso, o quociente radical de N é isomorfo a V_j e o seu soco é isomorfo a

$$V_{j+s+l(T_j)-q-1}.$$

É possível simplificar a expressão acima: pelo Teorema 5.4.12, temos $i = \pi(j)$ e, como comentamos na demonstração do Corolário 5.4.13, $\pi(j) \equiv j + l(T_j) - 1 \pmod{e}$. Ademais, pelo Lema 5.1.8, $q = p^n \equiv 1 \pmod{e}$. Por conta dessas congruências, concluímos que o soco de N é isomorfo a V_{i+s-1}.

(2) Se $s + l(T_j) < q$, então $N \cong V_{i,s+l(T_j)}$. Nesse caso, o quociente radical de N é isomorfo a V_i e o seu soco é isomorfo a

$$V_{i+s+l(T_j)-1}.$$

O Teorema 5.4.12 garante que $i + s \equiv j \pmod{e}$ e, como antes, $j + l(T_j) - 1$ é congruente a $\pi(j)$. Ou seja, o soco de N é isomorfo a $V_{\pi(j)}$.

Isso conclui o passo (4) da demonstração do Teorema 5.1.7 e estamos prontos para considerar o passo (5).

5.5 Módulos projetivos indecomponíveis

Iremos descrever em detalhes como são os B-módulos projetivos indecomponíveis e demonstraremos que B está muito próximo de ser uma álgebra de Brauer.

Sejam ρ e σ as permutações do conjunto $\{0, 1, \ldots, e-1\}$ tais que $\rho = \pi^{-1}$ e $\sigma(i) \equiv \pi(i) + 1 \pmod{e}$ para todo $0 \leq i < e$. Note que as igualdades $j = \rho(i)$ e $j = \sigma(i)$ são as duas condições que aparecem no Corolário 5.4.13. A ideia principal será iterar o Teorema 5.4.12 e, consequentemente, iteraremos as permutações ρ e σ. Isso dará o caráter "circular" presente na definição de uma álgebra de Brauer.

Vamos associar um grafo a B (que acabará sendo a sua árvore de Brauer). Para cada órbita de ρ e para cada órbita de σ, teremos um vértice no grafo. Uma órbita de ρ é um **vértice de tipo** ρ, enquanto uma órbita de σ é um **vértice de tipo** σ. Para cada $0 \leq i < e$, existe um único vértice de tipo ρ e um único vértice de tipo σ que contêm i, então podemos formar uma aresta entre esses dois vértices e associá-la ao B-módulo simples S_i. Com isso, está definido um grafo de e arestas e cada uma destas arestas está associada a um B-módulo simples. Observe que não há arestas entre dois vértices de mesmo tipo. Há também uma ordenação circular natural das arestas emanando de cada vértice: se o vértice é de tipo ρ e contém um índice $i \in \{0, 1, \ldots, e-1\}$, então as arestas em torno desse vértice seguem a ordem S_i, $S_{\rho(i)}$, $S_{\rho^2(i)}$, e assim em diante. Podemos definir uma ordenação de modo semelhante caso o vértice seja de tipo σ.

A partir de agora, P_i denotará a cobertura projetiva do B-módulo simples S_i, para $0 \leq i < e$. O próximo teorema descreve a estrutura de cada um desses projetivos indecomponíveis. É importante observar que as ordenações circulares presentes no grafo construído acima aparecerão mais uma vez.

Teorema 5.5.1. Seja $0 \leq i < e$. Então o quociente $\operatorname{rad}(P_i)/\operatorname{soc}(P_i)$ é a soma direta de módulos unisseriados W_i^ρ e W_i^σ (possivelmente nulos) com as seguintes propriedades:

(1) Os fatores de composição de W_i^ρ são, em ordem,

$$S_{\rho(i)}, S_{\rho^2(i)}, \ldots, S_{\rho^a(i)},$$

onde a é um inteiro não negativo (que depende de i) e satisfaz $\rho^{a+1}(i) = i$.

(2) Os fatores de composição de W_i^σ são, em ordem,

$$S_{\sigma(i)}, S_{\sigma^2(i)}, \ldots, S_{\sigma^b(i)},$$

onde b é um inteiro não negativo (que depende de i) e satisfaz $\sigma^{b+1}(i) = i$.

(3) W_i^ρ e W_i^σ não possuem fatores de composição em comum.

Quase toda esta seção será dedicada à prova do resultado acima. Essencialmente, encontraremos módulos unisseriados como acima mas com um fator S_i a mais no início. Isso permitirá "colar" os módulos unisseriados para construir P_i. Então começaremos construindo tais módulos unisseriados.

Por enquanto, fixemos $0 \leq i < e$. Vamos lidar com a permutação σ primeiramente. Se $l(T_i) + l(T_{\sigma(i)}) < q$, a segunda condição do Corolário 5.4.13 está satisfeita e podemos formar a extensão indecomponível M_1 de S_i por $S_{\sigma(i)}$. Como vimos no Teorema 5.4.12 e nos comentários posteriores a ele, M_1 possui quociente radical simples, não é projetivo e seu correspondente de Green é $V_{i,l(T_i)+l(T_{\sigma(i)})}$. Veja que o comprimento deste último módulo é $s_1 \coloneqq l(T_i) + l(T_{\sigma(i)})$. Usando a identidade $j+l(T_j) \equiv \pi(j)+1 \equiv \sigma(j) \pmod e$ para todo $0 \leq j < e$, temos a congruência

$$i + s_1 = i + l(T_i) + l(T_{\sigma(i)}) \equiv \sigma(i) + l(T_{\sigma(i)}) \equiv \sigma^2(i) \pmod e.$$

Logo, se $l(T_i)+l(T_{\sigma(i)})+l(T_{\sigma^2(i)}) < q$, então a segunda condição do Teorema 5.4.12 está satisfeita e, como M_1 é indecomponível não projetivo com quociente radical simples, podemos formar a extensão indecomponível M_2 de M_1 por $S_{\sigma^2(i)}$. Mais uma vez, M_2 possui quociente radical simples, não é projetivo e seu correspondente de Green é $V_{i,l(T_i)+l(T_{\sigma(i)})+l(T_{\sigma^2(i)})}$. Se s_2 denota o comprimento deste correspondente de Green, temos, como antes, $i + s_2 \equiv \sigma^3(i) \pmod e$. Se também tivermos

$$l(T_i) + l(T_{\sigma(i)}) + l(T_{\sigma^2(i)}) + l(T_{\sigma^3(i)}) < q,$$

podemos similarmente construir a extensão indecomponível M_3 de M_2 por $S_{\sigma^3(i)}$. Procedendo assim, podemos tomar b como sendo o maior inteiro não negativo tal que

$$l(T_i) + l(T_{\sigma(i)}) + \cdots + l(T_{\sigma^b(i)}) < q$$

e construir um módulo indecomponível U_i^σ obtido realizando essas extensões sucessivas b vezes. Como ressaltamos ao longo do processo, U_i^σ possui quociente radical simples, não é projetivo e seu correspondente de Green possui quociente radical isomorfo a V_i e comprimento dado pela soma em destaque logo acima.

Agora é a vez de lidar com a permutação ρ. Se $l(T_i) + l(T_{\rho(i)}) > q$, então a primeira condição do Corolário 5.4.13 está satisfeita e podemos formar a extensão indecomponível M_1' de S_i por $S_{\rho(i)}$. Como antes, M_1' possui quociente radical simples, não é projetivo e seu correspondente de Green é

$$V_{\rho(i),l(T_i)+l(T_{\rho(i)})-q}.$$

Seja $s_1' \coloneqq l(T_i) + l(T_{\rho(i)}) - q$, que é o comprimento do módulo acima. Se $s_1' + l(T_{\rho^2(i)}) > q$, ou seja, se $l(T_i) + l(T_{\rho(i)}) + l(T_{\rho^2(i)}) > 2q$, então a primeira condição do Teorema 5.4.12 está satisfeita e, como M_1' é indecomponível não projetivo com quociente radical simples, podemos formar a extensão indecomponível M_2' de M_1' por $S_{\rho^2(i)}$. Mais uma vez, M_2' possui quociente radical simples, não é projetivo e seu correspondente de Green é

$$V_{\rho^2(i),s_1'+l(T_{\rho^2(i)})-q} = V_{\rho^2(i),l(T_i)+l(T_{\rho(i)})+l(T_{\rho^2(i)})-2q}.$$

Seja s_2' o comprimento do correspondente de Green acima. Se também tivermos $s_2' + l(T_{\rho^3(i)}) > q$, ou seja, se

$$l(T_i) + l(T_{\rho(i)}) + l(T_{\rho^2(i)}) + l(T_{\rho^3(i)}) > 3q,$$

podemos analogamente construir a extensão indecomponível M_3' de M_2' por $S_{\rho^3(i)}$. Procedendo assim, podemos tomar a como sendo o maior inteiro não negativo tal que

$$l(T_i) + l(T_{\rho(i)}) + \cdots + l(T_{\rho^a(i)}) > aq$$

e construir um módulo indecomponível U_i^ρ obtido realizando essas extensões sucessivas a vezes. Como $l(T_j) < q$ para todo $0 \leq j < e$, a diferença entre os dois membros da desigualdade acima é cada vez menor à medida que acrescentamos parcelas na soma, então de fato existe um maior inteiro não negativo a como acima. Além disso, sabemos que U_i^ρ possui quociente radical simples, não é projetivo e seu correspondente de Green possui quociente radical isomorfo a $V_{\rho^a(i)}$ e comprimento

$$l(T_i) + l(T_{\rho(i)}) + \cdots + l(T_{\rho^a(i)}) - aq.$$

O próximo resultado mostrará que U_i^ρ e U_i^σ são unisseriados:

Lema 5.5.2. Seja M um B-módulo de comprimento t com fatores de composição $S_{j_1}, \ldots, S_{j_t}$, onde cada índice varia entre 0 e $e-1$. Se $M/\operatorname{rad}(M)$ é simples e se vale

$$l(T_{j_1}) + \cdots + l(T_{j_t}) < q$$

ou

$$l(T_{j_1}) + \cdots + l(T_{j_t}) > (t-1)q,$$

então M é unisseriado.

Pelas construções de U_i^ρ e U_i^σ e pelas definições de a e b, as condições acima estão satisfeitas, garantindo que os módulos em questão são unisseriados. Por conta da ordem em que realizamos as extensões, U_i^ρ é unisseriado de comprimento $a+1$ com fatores de composição

$$S_i, S_{\rho(i)}, \ldots, S_{\rho^a(i)},$$

nessa ordem, enquanto U_i^σ é unisseriado de comprimento $b+1$ com fatores de composição

$$S_i, S_{\sigma(i)}, \ldots, S_{\sigma^b(i)},$$

nessa ordem. A partir desses dois módulos, conseguiremos deduzir a estrutura de P_i!

Demonstração. A prova será dada por indução em t. Se $t = 1$, não há o que fazer. Se $t = 2$, então o fato de $M/\operatorname{rad}(M)$ ser simples implica que M não é semissimples e, por ter comprimento 2, deve ser unisseriado.

Antes de lidar com o passo de indução, vamos analisar também o caso $t = 3$. Suponha que valha a condição

$$l(T_{j_1}) + l(T_{j_2}) + l(T_{j_3}) < q.$$

Como $M/\operatorname{rad}(M)$ é simples, $\operatorname{rad}(M)$ possui comprimento 2. Se $\operatorname{rad}(M)$ não é semissimples, então é necessariamente unisseriado. Assim, as camadas radicais de M são todas simples e M é unisseriado, como preciso. Vejamos que sempre caímos nesse caso. Suponha, por absurdo, que seja possível de $\operatorname{rad}(M)$ ser semissimples. Sem perda de generalidade, podemos assumir que $M/\operatorname{rad}(M) \cong S_{j_1}$ e $\operatorname{rad}(M) = M' \oplus M''$, onde M' e M'' são submódulos isomorfos a S_{j_2} e S_{j_3}, respectivamente. Note que M/M'' é uma extensão de S_{j_1} por S_{j_2} e ela não pode cindir porque, como $M'' \subseteq \operatorname{rad}(M)$, temos $\operatorname{rad}(M/M'') = \operatorname{rad}(M)/M'' \neq 0$. Como $l(T_{j_1}) + l(T_{j_2}) < q$, o Corolário 5.4.13 mostra que $j_2 = \sigma(j_1)$. Mas também temos $l(T_{j_1}) + l(T_{j_3}) < q$, então um argumento análogo também mostra que $j_3 = \sigma(j_1)$. Em particular, $j_2 = j_3$ e o soco de M não é livre de multiplicidade. Mas M é indecomponível, já que seu quociente radical é simples, então chegamos em uma contradição por conta da Proposição 5.4.8.

Ainda no caso $t = 3$, se dessa vez tivermos a condição

$$l(T_{j_1}) + l(T_{j_2}) + l(T_{j_3}) > 2q,$$

o mesmo argumento mostra que M não é unisseriado. Dessa vez, utilizamos a outra condição dada no Corolário 5.4.13. Para adaptar o argumento, é importante notar que $l(T_{j_1}) + l(T_{j_2}) > q$ e $l(T_{j_1}) + l(T_{j_3}) > q$, já que vale a condição em destaque acima e $l(T_j) < q$ para todo $0 \leq j < e$.

Agora, suponha que $t > 3$ e, como hipótese de indução, suponha que o resultado valha para módulos de comprimento $t-1$. Considere uma série de composição

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_{t-1} \supseteq M_t = 0.$$

Nesse caso, o quociente radical de M/M_{t-1} é quociente de $M/\operatorname{rad}(M)$, então ele é simples. Além disso, M/M_{t-1} tem comprimento $t-1$ e seus fatores de composição ainda satisfazem a condição do enunciado que lida com comprimentos, já que $0 < l(T_j) < q$ para todo $0 \leq j < e$. Por hipótese de indução, M/M_{t-1} é unisseriado. Sabendo disso, vamos mostrar que M é unisseriado se valer $\operatorname{rad}(M_{t-2}) = M_{t-1}$. Nesse caso, se $0 \leq j \leq t-2$, então

$$M_j \supseteq M_{t-2} \implies \operatorname{rad}(M_j) \supseteq \operatorname{rad}(M_{t-2}) = M_{t-1}.$$

Por isso, $\operatorname{rad}(M_j/M_{t-1}) = \operatorname{rad}(M_j)/M_{t-1}$. Mas M/M_{t-1} é unisseriado e a sua única série de composição deve ser dada por

$$M/M_{t-1} = M_0/M_{t-1} \supseteq M_1/M_{t-1} \supseteq \cdots \supseteq M_{t-2}/M_{t-1} \supseteq M_{t-1}/M_{t-1} = 0.$$

Logo, $\operatorname{rad}(M_j/M_{t-1}) = M_{j+1}/M_{t-1}$. Pelo Teorema da Correspondência, concluímos então que $\operatorname{rad}(M_j) = M_{j+1}$ para todo $0 \leq j \leq t-2$. Mas essa igualdade também vale para $j = t-1$, já que M_{t-1} é simples. Portanto, a série de composição considerada é a série radical de M. Pela Proposição 2.1.13, M é unisseriado, como queríamos.

Para concluir a demonstração, resta verificar que $\operatorname{rad}(M_{t-2}) = M_{t-1}$. Mostraremos essa igualdade por redução a um absurdo. Suponha que $\operatorname{rad}(M_{t-2}) \neq M_{t-1}$. Como M_{t-2}/M_{t-1} é simples, vale $\operatorname{rad}(M_{t-2}) \subseteq M_{t-1}$. Mas M_{t-1} é simples, então devemos ter $\operatorname{rad}(M_{t-2}) = 0$, isto é, M_{t-2} é semissimples. Em particular, M_{t-3} não é unisseriado. Os fatores de composição de M_{t-3} ainda satisfazem a condição do enunciado que lida com comprimentos, então podemos utilizar o caso particular do lema para comprimento 3 (que fizemos antes do passo de indução) para obter que o quociente radical de M_{t-3} não é simples. Por outro lado, como M_{t-3}/M_{t-2} é simples, vale $\operatorname{rad}(M_{t-3}) \subseteq M_{t-2}$ e essa inclusão deve ser estrita. Logo, conseguimos encontrar um submódulo M'_{t-1} de M_{t-2} contendo $\operatorname{rad}(M_{t-3})$ tal que M_{t-2}/M'_{t-1} seja simples. Em suma, encontramos uma nova série de composição para M:

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_{t-3} \supseteq M_{t-2} \supseteq M'_{t-1} \supseteq 0,$$

e agora temos M_{t-3}/M'_{t-1} semissimples (porque M'_{t-1} contém $\operatorname{rad}(M_{t-3})$). Do mesmo modo que mostramos que M/M_{t-1} é unisseriado, também temos M/M'_{t-1} unisseriado. Mas o soco de M/M'_{t-1} contém M_{t-3}/M'_{t-1}, que não é simples. Isso é uma contradição! □

Agora que sabemos que U_i^ρ e U_i^σ são unisseriados e começam com o mesmo fator de composição, a ideia será "colá-los" no "topo" e depois acrescentar um fator S_i na "base" para "arrematar as pontas soltas". Tudo isso será enunciado de forma precisa logo a diante. Porém, esse arremate final será feito através do Teorema 5.4.12 e precisaremos conhecer melhor os correspondentes de Green de U_i^ρ e U_i^σ, o que será feito no próximo lema. Aproveitaremos o momento para também demonstrar as propriedades de a e b dadas no Teorema 5.5.1 que ainda não foram verificadas.

Lema 5.5.3. Com as notações anteriores, valem $\rho^{a+1}(i) = i$ e $\sigma^{b+1}(i) = i$. Além disso, o correspondente de Green de U_i^ρ é o módulo simples $V_{\pi(i)}$, enquanto o correspondente de Green de U_i^σ é o módulo indecomponível $V_{i,q-1}$.

Demonstração. Como o quociente radical de U_i^ρ é isomorfo a S_i, basta nós verificarmos que $\operatorname{Hom}_{kG}(U_i^\rho, S_{\rho^{a+1}(i)}) \neq 0$ para mostrar que $\rho^{a+1}(i) = i$. Se V^ρ é o correspondente de Green de U_i^ρ, então o Corolário 5.4.2 mostra que

$$\overline{\operatorname{Hom}}_{kG}(U_i^\rho, S_{\rho^{a+1}(i)}) \cong \overline{\operatorname{Hom}}_{kN_1}(V^\rho, T_{\rho^{a+1}(i)}).$$

Sabemos que $l(V^\rho) = l(T_i)+l(T_{\rho(i)})+\cdots+l(T_{\rho^a(i)})-aq$, então não podemos ter $l(V^\rho)+l(T_{\rho^{a+1}(i)}) > q$, porque, se tivéssemos, valeria a desigualdade

$$l(T_i) + l(T_{\rho(i)}) + \cdots + l(T_{\rho^a(i)}) + l(T_{\rho^{a+1}(i)}) > (a+1)q,$$

contradizendo a definição de a. Por isso, $l(V^\rho) + l(T_{\rho^{a+1}(i)}) \leq q$ e, pelo Lema 5.4.5, o único homomorfismo de V^ρ em $T_{\rho^{a+1}(i)}$ que se fatora através de um projetivo é o homomorfismo nulo. Segue que

$$\overline{\mathrm{Hom}}_{kN_1}(V^\rho, T_{\rho^{a+1}(i)}) \cong \mathrm{Hom}_{kN_1}(V^\rho, T_{\rho^{a+1}(i)}).$$

Mas o quociente radical de V^ρ é isomorfo a $V_{\rho^a(i)}$ e o soco de $T_{\rho^{a+1}(i)}$ é isomorfo a $V_{\pi(\rho^{a+1}(i))} = V_{\rho^a(i)}$ (lembre que $\rho = \pi^{-1}$). Logo, temos um homomorfismo não nulo de $V^\rho/\operatorname{rad}(V^\rho)$ em $\operatorname{soc}(T_{\rho^{a+1}}(i))$. Compondo com os homomorfismos canônicos, obtemos um homomorfismo não nulo de V^ρ em $T_{\rho^{a+1}(i)}$ e, pelos isomorfismos acima,

$$\overline{\mathrm{Hom}}_{kG}(U_i^\rho, S_{\rho^{a+1}(i)}) \neq 0.$$

Em particular, há um homomorfismo não nulo de U_i^ρ em $S_{\rho^{a+1}(i)}$, como preciso.

Vejamos que $V^\rho \cong V_{\pi(i)}$. Primeiramente, o quociente radical de V^ρ é isomorfo a $V_{\rho^a(i)}$. Mas $\rho^{a+1}(i) = i$, então $\rho^a(i) = \rho^{-1}(i) = \pi(i)$. Resta mostrar que V^ρ é simples, isto é, que o seu comprimento é 1. Vimos anteriormente que tal comprimento é dado pela expressão

$$l(T_i) + l(T_{\rho(i)}) + \cdots + l(T_{\rho^a(i)}) - aq,$$

então o soco de V^ρ é

$$V_{\rho^a(i)+l(T_i)+l(T_{\rho(i)})+\cdots+l(T_{\rho^a(i)})-aq-1}.$$

Lembre da identidade $\pi(j)+1 \equiv j+l(T_j) \pmod e$ e, como $\rho = \pi^{-1}$, temos $j+1 \equiv \rho(j)+l(T_{\rho(j)}) \pmod e$, para todo $0 \leq j < e$. Aplicando isso na expressão acima, podemos trocar $\rho^a(i)+l(T_{\rho^a(i)})$ por $\rho^{a-1}(i)+1$. Depois, podemos trocar $\rho^{a-1}(i)+l(T_{\rho^{a-1}(i)})$ por $\rho^{a-2}(i)+1$. Prosseguindo assim e lembrando que $q \equiv 1 \pmod e$, obtemos que o soco de V^ρ é

$$V_{i+l(T_i)+a-aq-1} = V_{i+l(T_i)+a-a-1} = V_{i+l(T_i)-1} = V_{\pi(i)}.$$

Ou seja, o soco e quociente radical de V^ρ são isomorfos! Pela descrição dos b_1-módulos indecomponíveis, segue que $l(V^\rho) = 1+me$ para algum inteiro $m \geq 0$. Falta mostrarmos que $m = 0$. Para tanto, suponha que $m \geq 1$ e cheguemos em uma contradição. Pelo Lema 5.4.6, temos $l(T_i) \leq e$ ou $l(T_i) \geq q-e$. Se vale o primeiro caso, então temos

$$\begin{aligned}
1+e &\leq 1+me \\
&= l(V^\rho) \\
&= l(T_i) + l(T_{\rho(i)}) + \cdots + l(T_{\rho^a(i)}) - aq \\
&= l(T_i) + (l(T_{\rho(i)}) - q) + \cdots + (l(T_{\rho^a(i)}) - q) \\
&\leq l(T_i) \\
&\leq e,
\end{aligned}$$

um absurdo. Por outro lado, se vale o segundo caso, temos

$$l(V^\rho) + l(T_{\rho^{a+1}(i)}) = l(V^\rho) + l(T_i) = 1 + me + l(T_i) \geq 1 + e + q - e = q + 1 > q,$$

contradizendo a desigualdade $l(V^\rho)+l(T_{\rho^{a+1}(i)}) \leq q$ que havíamos encontrado no parágrafo anterior. Assim, de fato vale $m = 0$ e então $V^\rho \cong V_{\pi(i)}$.

Agora é a hora de lidar com a permutação σ. Como o quociente radical de U_i^σ é isomorfo a S_i, basta nós verificarmos que $\mathrm{Hom}_{kG}(U_i^\sigma, S_{\sigma^{b+1}(i)}) \neq 0$ para mostrar que $\sigma^{b+1}(i) = i$. Se V^σ é o correspondente de Green de U_i^σ, então o Corolário 5.4.2 e a Proposição 5.3.23 mostram que

$$\overline{\mathrm{Hom}}_{kG}(U_i^\sigma, S_{\sigma^{b+1}(i)}) \cong \overline{\mathrm{Hom}}_{kN_1}(V^\sigma, T_{\sigma^{b+1}(i)}) \cong \overline{\mathrm{Hom}}_{kN_1}(\Omega V^\sigma, \Omega T_{\sigma^{b+1}(i)}).$$

Sabemos que $l(V^\sigma) = l(T_i) + l(T_{\sigma(i)}) + \cdots + l(T_{\sigma^b(i)})$, então deve valer $l(V^\sigma) + l(T_{\sigma^{b+1}(i)}) \geq q$ para não contradizer a maximalidade de b. Lembre que $l(\Omega W) = q - l(W)$ para todo b_1-módulo indecomponível W, o que nos dá a igualdade $l(\Omega V^\sigma) + l(\Omega T_{\sigma^{b+1}(i)}) \leq q$. Como antes, o Lema 5.4.5 implica em

$$\overline{\mathrm{Hom}}_{kN_1}(\Omega V^\sigma, \Omega T_{\sigma^{b+1}(i)}) \cong \mathrm{Hom}_{kN_1}(\Omega V^\sigma, \Omega T_{\sigma^{b+1}(i)}).$$

Através desses isomorfismos, para garantir que há um homomorfismo não nulo de U_i^σ em $S_{\sigma^{b+1}(i)}$, basta garantir, como antes, que o quociente radical de ΩV^σ e o soco de $\Omega T_{\sigma^{b+1}(i)}$ são isomorfos. Vimos anteriormente que $\Omega V_{jt} \cong V_{j+t,q-t}$, então o quociente radical de ΩV^σ é isomorfo a

$$V_{i+l(V^\sigma)} = V_{i+l(T_i)+l(T_{\sigma(i)})+\cdots+l(T_{\sigma^b(i)})}.$$

Imitando uma conta dada logo antes da definição de U_i^σ, não é difícil verificar que o índice acima é congruente a $\sigma^{b+1}(i)$ módulo e, então o quociente radical de ΩV^σ é isomorfo a $V_{\sigma^{b+1}(i)}$. Por outro lado, o soco de $\Omega T_{\sigma^{b+1}(i)}$ é isomorfo ao soco da cobertura projetiva de $T_{\sigma^{b+1}(i)}$, que é isomorfo ao quociente radical dessa mesma cobertura projetiva. Mas isso é isomorfo ao quociente radical de $T_{\sigma^{b+1}(i)}$, que é $V_{\sigma^{b+1}(i)}$. Logo, o quociente radical de ΩV^σ é de fato isomorfo ao soco de $\Omega T_{\sigma^{b+1}(i)}$ e concluímos que $\sigma^{b+1}(i) = i$.

Finalmente, vejamos que $V^\sigma \cong V_{i,q-1}$. Já sabemos que o quociente radical de V^σ é isomorfo a V_i, então basta verificarmos que $l(V^\sigma) = q - 1$. Pela congruência utilizada no parágrafo anterior, sabemos que o soco de V^σ é isomorfo

$$V_{i+l(V^\sigma)-1} = V_{i+l(T_i)+l(T_{\sigma(i)})+\cdots+l(T_{\sigma^b(i)})-1} = V_{\sigma^{b+1}(i)-1} = V_{i-1}.$$

Pela descrição dos b_1-módulos indecomponíveis, a única forma de valer $V^\sigma/\operatorname{rad}(V^\sigma) \cong V_i$ e $\operatorname{soc}(V^\sigma) \cong V_{i-1}$ é se o comprimento de V^σ for um múltiplo de e. Como $q-1$ é um múltiplo de e, podemos escrever $l(V^\sigma) = q-1-me$ para algum inteiro m. Como o comprimento de V^σ é menor do que q, vale $m \geq 0$. Falta mostrarmos que $m = 0$. Para isso, suponha que $m \geq 1$ e cheguemos em uma contradição. Pelo Lema 5.4.6, temos $l(T_i) \leq e$ ou $l(T_i) \geq q - e$. Se vale o primeiro caso, então temos

$$l(V^\sigma) + l(T_{\sigma^{b+1}(i)}) = l(V^\sigma) + l(T_i) = q - 1 - me + l(T_i) \leq q - 1 - e + e = q - 1 < q,$$

contradizendo a desigualdade $l(V^\sigma) + l(T_{\sigma^{b+1}(i)}) \geq q$ que havíamos encontrado no parágrafo anterior. Por outro lado, se vale o segundo caso, temos

$$(q-e) - 1 \geq q - 1 - me = l(V^\sigma) = l(T_i) + l(T_{\sigma(i)}) + \cdots + l(T_{\sigma^b(i)}) \geq l(T_i) \geq q - e,$$

um absurdo. Por isso, de fato vale $m = 0$ e então $V^\sigma \cong V_{i,q-1}$. □

Estamos prontos para demonstrar o Teorema 5.5.1!

Demonstração. Supondo que a estrutura de P_i satisfaça os itens (1) e (2) do enunciado, é fácil mostrar que também vale o item (3). Vejamos o porquê. Se W_i^ρ e W_i^σ tivessem um fator de composição em comum, poderíamos encontrar $X \leq W_i^\rho$ e $Y \leq W_i^\sigma$ com quocientes radicais isomorfos. Assim, observe que o soco de $(W_i^\rho \oplus W_i^\sigma)/(\operatorname{rad}(X) \oplus \operatorname{rad}(Y))$ seria a soma direta de dois módulos simples isomorfos. Agora, como $W_i^\rho \oplus W_i^\sigma \cong \operatorname{rad}(P_i)/\operatorname{soc}(P_i)$, $\operatorname{rad}(X) \oplus \operatorname{rad}(Y)$ corresponderia a um submódulo Z de P_i contido em $\operatorname{rad}(P_i)$ e contendo $\operatorname{soc}(P_i)$. Como o quociente radical de P_i é simples, o mesmo valeria para P_i/Z, então P_i/Z seria indecomponível. Por outro lado, $\operatorname{soc}(P_i/Z)$

contém $\operatorname{soc}(\operatorname{rad}(P_i)/Z)$ e, nesse caso, $\operatorname{rad}(P_i)/Z \cong (W_i^\rho \oplus W_i^\sigma)/(\operatorname{rad}(X) \oplus \operatorname{rad}(Y))$. Isso prova que P_i/Z seria um indecomponível e seu soco não seria livre de multiplicidade, contradizendo a Proposição 5.4.8.

Agora, precisamos de fato construir P_i do modo desejado. Vamos começar "colando" U_i^ρ e U_i^σ. Sejam $W_i^\rho := \operatorname{rad}(U_i^\rho)$ e $W_i^\sigma := \operatorname{rad}(U_i^\sigma)$. Note que W_i^ρ e W_i^σ são como no enunciado do teorema. Como os quocientes radicais de U_i^ρ e U_i^σ são ambos isomorfos a S_i, podemos encontrar um isomorfismo

$$\varphi : \frac{U_i^\rho}{W_i^\rho} \to \frac{U_i^\sigma}{W_i^\sigma}.$$

Defina o seguinte subconjunto de $U_i^\rho \oplus U_i^\sigma$:

$$U := \{(x, y) \in U_i^\rho \oplus U_i^\sigma \mid \varphi(x + W_i^\rho) = y + W_i^\sigma\}.$$

Não é difícil verificar que U é um submódulo de $U_i^\rho \oplus U_i^\sigma$ contendo $W := W_i^\rho \oplus W_i^\sigma$. Além disso, U/W é o submódulo de

$$\frac{U_i^\rho \oplus U_i^\sigma}{W_i^\rho \oplus W_i^\sigma} \cong \frac{U_i^\rho}{W_i^\rho} \oplus \frac{U_i^\sigma}{W_i^\sigma}$$

constituído dos elementos da forma $(x + W_i^\rho, \varphi(x + W_i^\rho))$ $(x \in U_i^\rho)$, que é isomorfo a S_i. Dado $x \in U_i^\rho$ qualquer, sempre podemos tomar $y \in U_i^\sigma$ tal que $\varphi(x + W_i^\rho) = y + W_i^\sigma$, mostrando que a projeção $\pi_\rho : U \to U_i^\rho$ na primeira coordenada é sobrejetora. Se $\pi_\rho(x, y) = 0$, então $x = 0$ e obtemos $y + W_i^\sigma = \varphi(0 + W_i^\rho) = 0$, ou seja $y \in W_i^\sigma$. Disso obtemos que o núcleo de π_ρ é W_i^σ e então $U/W_i^\sigma \cong U_i^\rho$. Analogamente, trocando o papel de ρ e σ e usando que φ é inversível, obtemos $U/W_i^\rho \cong U_i^\sigma$.

Em resumo, encontramos um módulo U que possui $W = W_i^\rho \oplus W_i^\sigma$ como submódulo e satisfaz $U/W \cong S_i$, $U/W_i^\sigma \cong U_i^\rho$ e $U/W_i^\rho \cong U_i^\sigma$. Afirmamos que U possui a estrutura enunciada no teorema para $P_i/\operatorname{soc}(P_i)$. Para provar isso, devemos garantir que $\operatorname{rad}(U)$ é maximal em U e que $\operatorname{rad}(U) \cong W_i^\rho \oplus W_i^\sigma$. Assim, basta garantirmos que $\operatorname{rad}(U) = W$. Se $a = 0$ ou se $b = 0$, então $W_i^\rho = 0$ ou $W_i^\sigma = 0$ e os isomorfismos anteriores mostram que $U \cong U_i^\rho$ ou $U \cong U_i^\sigma$, de onde segue $\operatorname{rad}(U) = W$. Suponha então que $a > 0$ e $b > 0$. Como $U/W \cong S_i$ é simples, vale $\operatorname{rad}(U) \subseteq W$ e, como $W \subseteq U$, temos $\operatorname{rad}(W) \subseteq \operatorname{rad}(U)$. Com essa informação, para determinar $\operatorname{rad}(U)$, vamos encontrar os submódulos de W que contêm $\operatorname{rad}(W)$. Observe que

$$\frac{W}{\operatorname{rad}(W)} \cong \frac{W_i^\rho}{\operatorname{rad}(W_i^\rho)} \oplus \frac{W_i^\sigma}{\operatorname{rad}(W_i^\sigma)} \cong S_{\rho(i)} \oplus S_{\sigma(i)}.$$

Mas note que $\rho(i) \neq \sigma(i)$, porque as definições de a e b garantem que $l(T_i) + l(T_{\rho(i)}) > q$ enquanto $l(T_i) + l(T_{\sigma(i)}) < q$. Portanto, $W/\operatorname{rad}(W)$ é a soma direta de dois simples não isomorfos e, consequentemente, possui exatamente quatro submódulos. Assim, existem quatro submódulos de W que contêm $\operatorname{rad}(W)$ e não é difícil verificar que eles são $\operatorname{rad}(W)$, $W_i^\rho \oplus \operatorname{rad}(W_i^\sigma)$, $\operatorname{rad}(W_i^\rho) \oplus W_i^\sigma$ e W. Vamos determinar qual deles é $\operatorname{rad}(U)$. Veja que $U/(W_i^\rho \oplus \operatorname{rad}(W_i^\sigma))$ possui comprimento 2 e é um quociente de $U/W_i^\rho \cong U_i^\sigma$, que é unisseriado. Por isso, $U/(W_i^\rho \oplus \operatorname{rad}(W_i^\sigma))$ não pode ser semissimples e então $\operatorname{rad}(U) \not\subseteq W_i^\rho \oplus \operatorname{rad}(W_i^\sigma)$. Analogamente, $\operatorname{rad}(U) \not\subseteq \operatorname{rad}(W_i^\rho) \oplus W_i^\sigma$. A única opção que resta é $\operatorname{rad}(U) = W$, como desejado.

O próximo passo é mostrar que existe uma extensão de U por S_i que é indecomponível e projetiva. Nesse caso, S_i estará contido no soco dessa extensão e, por isso, ela será isomorfa a P_i e seu soco será exatamente essa cópia de S_i. Isso concluirá a demonstração, porque obteremos que o quociente de P_i por seu soco é isomorfo a U, que possui a estrutura indicada no enunciado. Para tanto, precisaremos conhecer o correspondente de Green de U.

Como $U/W_i^\rho \cong U_i^\sigma$, U é uma extensão de U_i^σ por W_i^ρ. Então, pela estrutura de W_i^ρ, U é obtido através de sucessivas extensões, começando por U_i^σ e adicionando $S_{\rho(i)}$, depois $S_{\rho^2(i)}$, e assim em diante, terminando em $S_{\rho^a(i)}$. Cada uma das extensões é um quociente de U e, por isso, cada uma possui quociente radical simples isomorfo a S_i e não pode cindir. Logo, todas

essas extensões podem ser descritas pelo Teorema 5.4.12. Vamos verificar que sempre caímos no primeiro caso dado no teorema. Se V^σ é o correspondente de Green de U_i^σ, então sabemos pelo Lema 5.5.3 que $l(V^\sigma) = q - 1$ e, em particular, $l(V^\sigma) \geq l(T_i)$. Desse modo,

$$l(V^\sigma) + l(T_{\rho(i)}) \geq l(T_i) + l(T_{\rho(i)}) > q,$$

onde a última desigualdade segue da definição de a. Isso garante que a primeira extensão cai no primeiro caso do Teorema 5.4.12. Como observado logo após a demonstração desse teorema, o correspondente de Green dessa primeira extensão possui comprimento $l(V^\sigma) + l(T_{\rho(i)}) - q$, então

$$(l(V^\sigma) + l(T_{\rho(i)}) - q) + l(T_{\rho^2(i)}) \geq l(T_i) + l(T_{\rho(i)}) + l(T_{\rho^2(i)}) - q > q.$$

Aqui utilizamos que

$$l(T_i) + l(T_{\rho(i)}) + l(T_{\rho^2(i)}) > 2q$$

mais uma vez pela definição de a. Como antes, a segunda extensão também deve cair no primeiro caso do Teorema 5.4.12 e o seu correspondente de Green possui comprimento

$$l(V^\sigma) + l(T_{\rho(i)}) + l(T_{\rho^2(i)}) - 2q.$$

Prosseguindo assim, sempre utilizando as desigualdades fornecidas pela definição de a, concluímos que todas as extensões caem no caso desejado. Também obtemos que o comprimento do correspondente de Green V de U é

$$l(V^\sigma) + l(T_{\rho(i)}) + \cdots + l(T_{\rho^a(i)}) - aq.$$

Lembrando que o comprimento do correspondente de Green V^ρ de U_i^ρ é

$$l(T_i) + l(T_{\rho(i)}) + \cdots + l(T_{\rho^a(i)}) - aq$$

e utilizando o Lema 5.5.3, concluímos que

$$l(V) = l(V^\sigma) + l(V^\rho) - l(T_i) = (q-1) + 1 - l(T_i) = q - l(T_i).$$

Por outro lado, como o quociente radical de V^σ é V_i e todas as extensões caem no primeiro caso do Teorema 5.4.12, segue que o quociente radical de V é $V_{\rho^a(i)} = V_{\pi(i)}$ (onde utilizamos que $\rho^{a+1}(i) = i$ e que $\pi = \rho^{-1}$). Em suma,

$$V \cong V_{\pi(i),q-l(T_i)}.$$

Como

$$l(T_i) + l(V) = l(T_i) + (q - l(T_i)) = q$$

e como

$$\pi(i) + l(V) \equiv (i + l(T_i) - 1) + (q - l(T_i)) = i + (q-1) \equiv i \pmod{e}$$

(lembre que e divide $q-1$), concluímos do Teorema 5.4.12 que existe uma extensão indecomponível de U por S_i e, como vale a igualdade $l(T_i)+l(V) = q$, essa extensão também é projetiva, finalizando a demonstração. □

Falta apenas um pequeno detalhe para concluirmos o passo (5) da demonstração do Teorema 5.1.7. Quando definimos o algoritmo que descreve os projetivos indecomponíveis de uma álgebra de Brauer, não foi preciso utilizar em nenhum momento que a árvore de Brauer era uma árvore nem que havia um único vértice excepcional com multiplicidade. Relaxaremos essas hipóteses: um **grafo de Brauer** é um grafo finito (não necessariamente conexo nem acíclico) munido de mais duas informações:

(1) Uma ordenação circular das arestas emanando de cada vértice.

(2) Um inteiro positivo (a multiplicidade) associado a cada um dos vértices do grafo.

Como observamos, o algoritmo dado na definição de uma álgebra de Brauer funciona se trocarmos a árvore de Brauer por um grafo de Brauer. Nesse sentido, diremos que uma álgebra A é uma **álgebra de Brauer generalizada** se existir um grafo de Brauer de modo que os A-módulos projetivos indecomponíveis sejam descritos por tal algoritmo. Isso nos leva ao último resultado desta seção:

Teorema 5.5.4. O bloco B é uma álgebra de Brauer generalizada e o seu grafo de Brauer possui e arestas.

Demonstração. No início desta seção, definimos um grafo a partir das permutações ρ e σ. Ele dará origem ao grafo de Brauer de B. Já associamos cada uma das arestas desse grafo a um B-módulo simples diferente e já determinamos uma ordenação circular em torno de cada vértice. Resta definirmos as multiplicidades adequadas. Vamos lidar com vértices de tipo ρ, sendo o caso de vértices de tipo σ completamente análogo. Considere um vértice de tipo ρ (ou seja, uma órbita da permutação ρ) que contenha um índice $0 \leq i < e$. Supondo que o algoritmo da álgebra de Brauer generalizada em torno deste vértice determine o unisseriado W_i^ρ dado pelo Teorema 5.5.1, devemos associar a multiplicidade[1] $(a+1)/t$ para esse vértice, onde a é o inteiro que aparece nesse teorema e t é o tamanho da órbita de i pela permutação ρ. O problema é que, a princípio, a depende do índice i. Para provar o resultado desejado, devemos garantir que, se $0 \leq j < e$ é outro índice que pertence à órbita de i, então o inteiro a associado a j é o mesmo inteiro a associado a i. Para isso, basta provar que W_i^ρ e W_j^ρ possuem o mesmo comprimento.

Vejamos que $l(W_i^\rho) \leq l(W_{\rho(i)}^\rho)$. Se $\rho(i) = i$, não há o que fazer. Por isso, suporemos $\rho(i) \neq i$. Por enquanto, isso já garante que W_i^ρ e $W_{\rho(i)}^\rho$ são ambos não nulos. Nesse caso, se $l(W_i^\rho) = 1$, então a desigualdade também é imediata. Assim, também prosseguiremos supondo que $l(W_i^\rho) \geq 2$, ou seja, que $\operatorname{rad}(W_i^\rho) \neq 0$.

Como o quociente radical de W_i^ρ é isomorfo a $S_{\rho(i)}$, W_i^ρ é um quociente de $P_{\rho(i)}$. Note que não pode valer $W_i^\rho \cong P_{\rho(i)}$: se isso valesse, W_i^ρ seria projetivo (ou seja, injetivo) e, como é submódulo $P_i/\operatorname{soc}(P_i)$, ele seria somando direto não trivial de $P_i/\operatorname{soc}(P_i)$, contradizendo a indecomponibilidade deste último módulo. Garantimos, pois, que W_i^ρ é um quociente próprio de $P_{\rho(i)}$ e, consequentemente, é um quociente de $P_{\rho(i)}/\operatorname{soc}(P_{\rho(i)})$. Tomando radicais, $\operatorname{rad}(W_i^\rho)$ é um quociente de

$$\frac{\operatorname{rad}(P_{\rho(i)})}{\operatorname{soc}(P_{\rho(i)})} \cong W_{\rho(i)}^\rho \oplus W_{\rho(i)}^\sigma.$$

Como $W_{\rho(i)}^\rho$ e $W_{\rho(i)}^\sigma$ não possuem fatores de composição em comum pelo item (3) do Teorema 5.5.1, cada submódulo de $W_{\rho(i)}^\rho \oplus W_{\rho(i)}^\sigma$ é a soma de um submódulo de $W_{\rho(i)}^\rho$ com um submódulo de $W_{\rho(i)}^\sigma$ (o argumento para demonstrar isso está feito na solução do Exercício A.5.1). Logo, a única forma do unisseriado $\operatorname{rad}(W_i^\rho)$ ser um quociente dessa soma direta é se ele for quociente de $W_{\rho(i)}^\rho$ ou de $W_{\rho(i)}^\sigma$. Agora, como $\operatorname{rad}(W_i^\rho)$ e $W_{\rho(i)}^\rho$ são não nulos, $S_{\rho^2(i)}$ é um fator de composição desses dois módulos, então $S_{\rho^2(i)}$ não pode aparecer como fator de composição de $W_{\rho(i)}^\sigma$ e concluímos que $\operatorname{rad}(W_i^\rho)$ é necessariamente um quociente de $W_{\rho(i)}^\rho$. Pelo Teorema 5.5.1,

$$\operatorname{soc}(\operatorname{rad}(W_i^\rho)) = \operatorname{soc}(W_i^\rho) \cong S_{\rho^{-1}(i)}$$

e

$$\operatorname{soc}(W_{\rho(i)}^\rho) \cong S_{\rho^{-1}(\rho(i))} = S_i$$

[1] Como $\rho^{a+1}(i) = i$, o número $(a+1)/t$ é de fato um inteiro positivo!

e, como $\rho(i) \neq i$, esses dois socos são diferentes. Consequentemente, $\operatorname{rad}(W_i^\rho)$ deve ser um quociente próprio de $W_{\rho(i)}^\rho$. Concluímos que

$$l(W_i^\rho) - 1 = l(\operatorname{rad}(W_i^\rho)) \leq l(W_{\rho(i)}^\rho) - 1 \implies l(W_i^\rho) \leq l(W_{\rho(i)}^\rho),$$

como desejado.

Agora é fácil terminar a demonstração. Aplicando repetidas vezes a igualdade $l(W_i^\rho) \leq l(W_{\rho(i)}^\rho)$, que vale para todo $0 \leq i < e$, obtemos

$$l(W_i^\rho) \leq l(W_{\rho(i)}^\rho) \leq l(W_{\rho^2(i)}^\rho) \leq \cdots \leq l(W_{\rho^t(i)}^\rho) = l(W_i^\rho)$$

para algum $t \geq 1$. Logo, todas essas desigualdades são igualdades. Se $0 \leq i, j < e$ são índices que pertencem à mesma órbita de ρ, isso prova que W_i^ρ e W_j^ρ possuem o mesmo comprimento, como preciso. □

5.6 Encontrando a árvore e a multiplicidade

Com o Teorema 5.5.4 em mãos, resta apenas demonstrar que o grafo de Brauer de B é uma árvore de Brauer e que a multiplicidade de seu vértice excepcional é $(p^n - 1)/e$. Esse é o objetivo desta seção, que concluirá a demonstração do Teorema 5.1.7!

Iniciaremos demonstrando que B é uma álgebra de Brauer usual. A ideia-chave para a prova é argumentar que, se o grafo de Brauer possuísse um ciclo ou mais de um vértice excepcional, então seria possível construir módulos indecomponíveis violando a Proposição 5.4.8. Os indecomponíveis que aparecerão serão mais complicados do que estamos habituados a lidar e precisaremos de um lema técnico para garantir a sua indecomponibilidade.

Lema 5.6.1. Seja A uma álgebra de dimensão finita. Sejam M um A-módulo e N um submódulo de M satisfazendo as seguintes condições:

(1) $M/\operatorname{rad}(M)$ é livre de multiplicidade.

(2) $N/\operatorname{rad}(N)$ é simples.

(3) $N \not\subseteq \operatorname{rad}(M)$.

(4) Existe um submódulo semissimples $S \leq \operatorname{rad}(M)$ tal que $M/\operatorname{rad}(M)$ e $\operatorname{rad}(M)/S$ não possuem fatores de composição em comum.

Com essas hipóteses, se temos uma decomposição $M = M_1 \oplus M_2$ em soma direta, então existe um índice $i \in \{1, 2\}$ tal que $N \cap S \subseteq M_i$ e $M_i/\operatorname{rad}(M_i)$ possui um quociente isomorfo a $N/\operatorname{rad}(N)$.

Demonstração. Dada a decomposição em soma direta de M, sejam N_1 e N_2 as projeções de N nos somandos M_1 e M_2, respectivamente. Suponha inicialmente que $N_2 = 0$, ou seja, que $N \subseteq M_1$. Vamos mostrar que podemos tomar $i = 1$. É imediato que $N \cap S \subseteq M_1$. Por outro lado, como $\operatorname{rad}(M_1) \subseteq \operatorname{rad}(M)$, a condição (3) do enunciado garante que $N \not\subseteq \operatorname{rad}(M_1)$. A inclusão $N \to M_1$ induz um homomorfismo $N/\operatorname{rad}(N) \to M_1/\operatorname{rad}(M_1)$, que é não nulo pela observação anterior. Mas $N/\operatorname{rad}(N)$ é simples, então esse homomorfismo é injetor e $N/\operatorname{rad}(N)$ é um fator de composição de $M_1/\operatorname{rad}(M_1)$. Como $M_1/\operatorname{rad}(M_1)$ é semissimples, concluímos que $N/\operatorname{rad}(N)$ é um quociente de $M_1/\operatorname{rad}(M_1)$, conforme diz o enunciado. O mesmo argumento funciona caso tenhamos $N_1 = 0$ e, nesse caso, devemos tomar $i = 2$.

Agora, suponha que $N_1 \neq 0$ e $N_2 \neq 0$. Como N_1 e N_2 são quocientes não nulos de N, a condição (2) nos dá

$$\frac{N_1}{\operatorname{rad}(N_1)} \cong \frac{N}{\operatorname{rad}(N)} \cong \frac{N_2}{\operatorname{rad}(N_2)}.$$

Se $N_1 \subseteq \operatorname{rad}(M_1)$ e $N_2 \subseteq \operatorname{rad}(M_2)$, então valeria

$$N \subseteq N_1 \oplus N_2 \subseteq \operatorname{rad}(M_1) \oplus \operatorname{rad}(M_2) = \operatorname{rad}(M),$$

contradizendo a condição (3), então uma das inclusões não pode valer. Sem perda de generalidade, assumiremos que $N_1 \not\subseteq \operatorname{rad}(M_1)$ e mostraremos que podemos tomar $i = 1$ no enunciado. Assim como fizemos no parágrafo anterior, garantimos que $N_1/\operatorname{rad}(N_1) \cong N/\operatorname{rad}(N)$ é um quociente de $M_1/\operatorname{rad}(M_1)$. Se também tivéssemos $N_2 \not\subseteq \operatorname{rad}(M_2)$, então o mesmo argumento mostraria que $N/\operatorname{rad}(N)$ é fator de composição de $M_2/\operatorname{rad}(M_2)$, violando a condição (1) do enunciado. Por isso, $N_2 \subseteq \operatorname{rad}(M_2)$ e, consequentemente, $N_2 \subseteq \operatorname{rad}(M)$. Vamos utilizar a condição (4) para refinar essa inclusão, provando que $N_2 \subseteq S$. Pelo Segundo Teorema do Isomorfismo, temos

$$\frac{N_2}{N_2 \cap S} \cong \frac{N_2 + S}{S} \leq \frac{\operatorname{rad}(M)}{S}.$$

Se $N_2 \cap S \subsetneq N_2$, então $N_2 \cap S \subseteq \operatorname{rad}(N_2)$, porque $N_2/\operatorname{rad}(N_2)$ é simples. Assim, $N_2/\operatorname{rad}(N_2) \cong N/\operatorname{rad}(N)$ seria um fator de composição de $N_2/(N_2 \cap S)$ e também de $\operatorname{rad}(M)/S$. Mas $N/\operatorname{rad}(N)$ já é fator de composição de $M/\operatorname{rad}(M)$, o que contradiz a condição (4). Logo, $N_2 \cap S = N_2$, isto é, $N_2 \subseteq S$, como desejado. Em particular, N_2 é semissimples e temos $\operatorname{rad}(N_2) = 0$. Para finalizar, observe que $N \cap S$ é um submódulo próprio de N, porque, se fossem iguais, teríamos $N = N \cap S \subseteq S \subseteq \operatorname{rad}(M)$, o que não é verdade por (3). Como $N/\operatorname{rad}(N)$ é simples, concluímos que

$$N \cap S \subseteq \operatorname{rad}(N) \subseteq \operatorname{rad}(N_1) + \operatorname{rad}(N_2) = \operatorname{rad}(N_1) + 0 \subseteq N_1 \subseteq M_1,$$

terminando a demonstração. □

Teorema 5.6.2. O grafo de Brauer do bloco B é uma árvore de Brauer.

Demonstração. O primeiro passo é notar que o grafo de Brauer de B é conexo. De fato, por conta do algoritmo da definição de uma álgebra de Brauer generalizada, não é difícil utilizar a caracterização (2) do Teorema 4.1.17 para verificar que dois B-módulos simples estão no mesmo bloco de B se e somente se as arestas correspondentes pertencem à mesma componente conexa do grafo de Brauer. Mas B é uma álgebra indecomponível e, portanto, é o seu único bloco. Segue que todos os B-módulos simples pertencem ao mesmo bloco e o grafo de Brauer possui apenas uma componente conexa, ou seja, é conexo.

Vejamos que o grafo de Brauer de B também é acíclico. Suponha, por absurdo, que exista um ciclo no grafo e considere um ciclo de tamanho mínimo. Lembre que o grafo é *bipartido*: podemos separar os seus vértices em tipo ρ e em tipo σ e só há arestas entre vértices de tipos distintos. Como consequência, esse ciclo minimal deve possuir comprimento par. Inicialmente, verifiquemos que esse comprimento não pode ser 2. Se fosse, existiriam dois vértices distintos e duas arestas R_1 e R_2 diferentes entre eles. Se P_1 é a cobertura projetiva de R_1, então o algoritmo para álgebras de Brauer generalizadas mostra que $\operatorname{rad}(P_1)/\operatorname{soc}(P_1)$ é a soma direta de dois módulos unisseriados, ambos possuindo o módulo simples R_2 como fator de composição. Mas o item (3) do Teorema 5.5.1 garante que isso não pode acontecer!

Dessa forma, o ciclo de tamanho mínimo deve possuir comprimento $2r$ com $r \geq 2$. Liste as suas arestas como $R_1, R_2, \ldots, R_{2r}$, na ordem em que são percorridas. Como anteriormente, estenderemos a notação para definir R_i para todo inteiro i e leremos os índices módulo $2r$. É importante notar que o vértice ligado a R_i e R_{i+1} não pode se conectar a nenhum outro R_j (com j não congruente a i nem $i+1$), porque senão poderíamos encurtar o ciclo e obter um comprimento ainda menor. Por esse motivo, para cada $1 \leq i \leq 2r$, a cobertura projetiva P_i de R_i possui um quociente N_i satisfazendo $N_i/\operatorname{rad}(N_i) \cong R_i$, $\operatorname{soc}(N_i) \cong R_{i-1} \oplus R_{i+1}$ e nenhum simples dentre $R_1, \ldots, R_{2r}$ é um fator de composição de $\operatorname{rad}(N_i)/\operatorname{soc}(N_i)$. Para encontrar N_i, escreva $\operatorname{rad}(P_i)/\operatorname{soc}(P_i)$ como soma direta de dois unisseriados, um contendo R_{i-1} como fator de composição e outro contendo R_{i+1}, considere o maior submódulo cujo quociente possui $R_{i-1} \oplus R_{i+1}$ como soco, e quociente P_i pelo correspondente desse submódulo.

Considere a seguinte soma direta:

$$N_1 \oplus N_3 \oplus \cdots \oplus N_{2r-1}.$$

Vamos formar um quociente especial dessa soma. Por construção, o soco de N_1 é isomorfo a $R_{2r} \oplus R_2$, o de N_3 é isomorfo a $R_2 \oplus R_4$, e assim em diante. Portanto, o soco da soma direta acima é isomorfo

$$R_{2r} \oplus (R_2 \oplus R_2) \oplus (R_4 \oplus R_4) \oplus \cdots \oplus (R_{2r-2} \oplus R_{2r-2}) \oplus R_{2r}.$$

Não agrupamos as duas aparições de R_{2r} propositalmente porque, logo em seguida, iremos identificar apenas os pares destacados. Para cada par $R_{2i} \oplus R_{2i}$ agrupado acima (com $1 \leq i \leq r-1$), podemos tomar um submódulo "diagonal" V_{2i} que possui projeção não nula nas duas componentes: basta olhar para o submódulo formado pelos vetores com as duas componentes iguais. Vendo cada V_{2i} como submódulo da soma direta, definimos M como sendo o quociente

$$\frac{N_1 \oplus N_3 \oplus \cdots \oplus N_{2r-1}}{V_2 \oplus \cdots \oplus V_{2r-2}}.$$

Observe que a projeção da soma direta ao quociente M leva os dois somandos do soco isomorfos a R_{2i} a uma mesma cópia de R_{2i} para todo $1 \leq i \leq r-1$. Assim, não é difícil ver que o soco da soma direta se projeta em um submódulo semissimples S isomorfo a

$$R_{2r} \oplus R_2 \oplus R_4 \oplus \cdots \oplus R_{2r-2} \oplus R_{2r}.$$

Note que R_{2r} é o único simples que aparece com multiplicidade maior do que 1.

Como $V_2 \oplus \cdots \oplus V_{2r-2}$ está contido no radical da soma $N_1 \oplus \cdots \oplus N_{2r-1}$, concluímos que o quociente radical de M é isomorfo ao quociente radical dessa segunda soma direta, ou seja,

$$\frac{M}{\operatorname{rad}(M)} \cong R_1 \oplus R_3 \oplus \cdots \oplus R_{2r-1}.$$

Mais ainda, como o soco de cada N_i está contido em seu radical, também segue que $S \subseteq \operatorname{rad}(M)$. Além disso, pelo Terceiro Teorema do Isomorfismo,

$$\frac{\operatorname{rad}(M)}{S} \cong \frac{\operatorname{rad}(N_1)}{\operatorname{soc}(N_1)} \oplus \frac{\operatorname{rad}(N_3)}{\operatorname{soc}(N_3)} \oplus \cdots \oplus \frac{\operatorname{rad}(N_{2r-1})}{\operatorname{soc}(N_{2r-1})}$$

e, consequentemente, $M/\operatorname{rad}(M)$ e $\operatorname{rad}(M)/S$ não possuem fatores de composição em comum.

Por outro lado, veja que o soco de cada N_{2i-1} intersecta trivialmente $V_2 \oplus \cdots \oplus V_{2r-2}$, então $N_{2i-1} \cap (V_2 \oplus \cdots \oplus V_{2r-2}) = 0$ e a projeção leva N_{2i-1} isomorficamente em um submódulo de M, para todo $1 \leq i \leq r$. Portanto, podemos considerar cada N_{2i-1} como um submódulo de M. Nesse caso, temos

$$M = N_1 + N_3 + \cdots + N_{2r-1}.$$

Como $N_{2i-1} \not\subseteq \operatorname{rad}(N_1 \oplus N_3 \oplus \cdots \oplus N_{2r-1})$, no quociente temos $N_{2i-1} \not\subseteq \operatorname{rad}(M)$ para todo $1 \leq i \leq r$. Por fim, não é difícil mostrar que, no quociente, $N_{2i-1} \cap N_{2i+1} \cap S$ é não nulo (e isomorfo a R_{2i}) para todo $1 \leq i \leq r-1$.

Estamos prontos para chegar em uma contradição! Como vimos acima, M e S satisfazem as condições (1) e (4) do Lema 5.6.1. Além disso, cada N_{2i-1}, visto como submódulo de M, satisfaz as condições (2) e (3) desse mesmo lema. Assim, podemos aplicar esse resultado. Se decompormos $M = M_1 \oplus M_2$ (trocando a numeração se preciso), o Lema 5.6.1 nos diz que $N_1 \cap S \subseteq M_1$ e $N_1/\operatorname{rad}(N_1) \cong R_1$ é um fator de composição de $M_1/\operatorname{rad}(M_1)$. Da mesma forma, o lema também dá um índice $i \in \{1, 2\}$ com $N_3 \cap S \subseteq M_i$ e tal que R_3 é um fator de composição de $M_i/\operatorname{rad}(M_i)$. Mas $M_1 \cap M_2 = 0$, enquanto

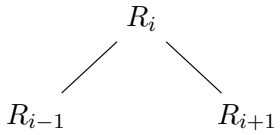
$$(N_1 \cap S) \cap (N_3 \cap S) = N_1 \cap N_3 \cap S \neq 0,$$

então deve valer $i = 1$ e $M_1/\operatorname{rad}(M_1)$ possui R_1 e R_3 como fatores de composição. Prosseguindo assim, conseguimos mostrar que $R_1, R_3, \ldots, R_{2r-1}$ são fatores de composição de $M_1/\operatorname{rad}(M_1)$ e então $R_1 \oplus R_3 \oplus \cdots \oplus R_{2r-1}$ é um somando direto de $M_1/\operatorname{rad}(M_1)$. Como

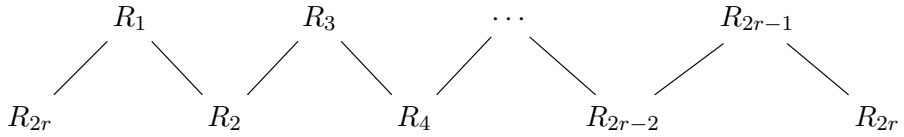
$$\frac{M_1}{\operatorname{rad}(M_1)} \oplus \frac{M_2}{\operatorname{rad}(M_2)} \cong \frac{M}{\operatorname{rad}(M)} \cong R_1 \oplus R_3 \oplus \cdots \oplus R_{2r-1},$$

necessariamente temos $M_2/\operatorname{rad}(M_2) = 0$ e, por isso, $M_2 = 0$. Como a decomposição em soma direta era qualquer, isso prova que M é indecomponível. Mas o soco de M contém S, que não é livre de multiplicidade, contrariando a Proposição 5.4.8. Desse absurdo, concluímos que o grafo de Brauer de B é de fato uma árvore!

Resta mostrarmos que há no máximo um vértice com multiplicidade maior do que 1. A estratégia será a mesma de antes. Como não iremos repetir todos os detalhes, vamos introduzir uma notação que sintetiza intuitivamente o que fizemos na parte anterior. Cada módulo N_i que definimos anteriormente possui quociente radical isomorfo a R_i. Além disso, $\operatorname{rad}(N_i)$ é a soma de dois unisseriados, um tendo R_{i-1} como soco e o outro tendo R_{i+1} como soco. Podemos representar N_i pelo seguinte desenho:

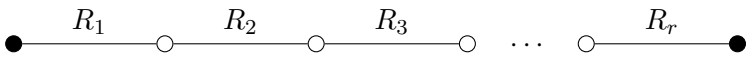


Em seguida, construímos M essencialmente "colando" $N_1, N_3, \ldots, N_{2r-1}$ ao longo dos fatores comuns dos socos. Pictorialmente, podemos representar M como



Vamos utilizar essa mesma representação esquemática para dar a ideia de como construir alguns novos módulos.

Suponha que existam dois ou mais vértices com multiplicidade maior do que 1. Dentro todos os caminhos entre dois desses vértices, escolha um que tenha comprimento mínimo. Sempre podemos encontrar tal caminho porque já sabemos que o grafo de Brauer de B é conexo. Enumere as arestas do caminho como a seguir:

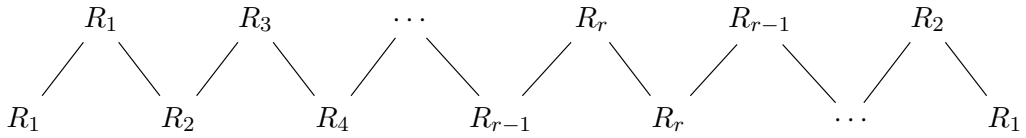


Como usualmente, os vértices preenchidos representam os vértices com multiplicidade maior do que 1. Vejamos que não é possível ter $r = 1$. Se isso acontecesse e se P_1 denota a cobertura projetiva de R_1, então o algoritmo associado a álgebras de Brauer generalizadas implicaria que $\operatorname{rad}(P_1)/\operatorname{soc}(P_1)$ seria a soma direta de dois módulos unisseriados, cada um contendo R_1 como fator de composição por conta da multiplicidade dos vértices excepcionais acima. Porém, isso contradiz o item (3) do Teorema 5.5.1. Logo, $r \geq 2$. Pela minimalidade, sabemos que todos os vértices no interior do caminho possuem multiplicidade 1. Além disso, como antes, sobre cada vértice na figura não incide nenhuma outra aresta R_j além das indicadas, porque senão poderíamos encurtar o caminho. Por isso, para cada $1 < i < r$, o mesmo argumento de antes nos permite encontrar um módulo N_i com $N_i/\operatorname{rad}(N_i) \cong R_i$, $\operatorname{soc}(N_i) \cong R_{i-1} \oplus R_{i+1}$ e tal que nenhum simples dentre $R_1, \ldots, R_r$ é um fator de composição de $\operatorname{rad}(N_i)/\operatorname{soc}(N_i)$. Para $i = 1$ e $i = r$ também conseguimos módulos com propriedades semelhantes, mas exigiremos $\operatorname{soc}(N_1) \cong R_1 \oplus R_2$ e $\operatorname{soc}(N_r) \cong R_{r-1} \oplus R_r$. Isso é possível por conta das multiplicidades maiores do que 1 nos extremos do caminho.

Para concluir, vamos "colar" esses módulos ao longo dos fatores comuns dos socos. Caímos em dois casos. Se r é ímpar, formamos a soma direta

$$N_1 \oplus N_3 \oplus \cdots \oplus N_r \oplus N_{r-1} \oplus N_{r-3} \oplus \cdots \oplus N_2$$

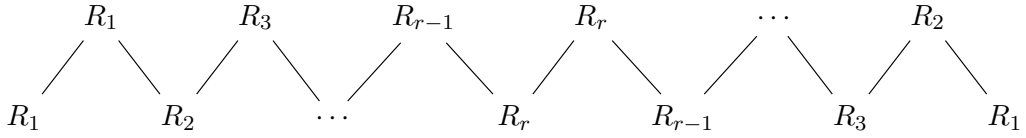
e consideramos um quociente M específico, que podemos descrever pela figura a seguir:



A construção de M é muito parecida com a construção anterior. Da mesma forma, conseguimos mostrar que M é indecomponível e que $\operatorname{soc}(M)$ não é livre de multiplicidade, o que é uma contradição. Se r é par, dessa vez consideramos a soma direta

$$N_1 \oplus N_3 \oplus \cdots \oplus N_{r-1} \oplus N_r \oplus N_{r-2} \oplus \cdots \oplus N_2$$

e o tomamos o quociente M que pode ser representado esquematicamente por



Mais uma vez, chegamos em um absurdo. Deduzimos que o grafo de Brauer de B possui no máximo um vértice excepcional, concluindo a demonstração. □

Observação 5.6.3. Durante a prova, construímos módulos indecomponíveis cujo quociente radical e cujo soco não eram simples. Indecomponíveis dessa forma não tinham aparecido antes! É claro que os indecomponíveis construídos exatamente como acima não existem, pois levam a contradições, mas podemos adaptar as duas construções. Por exemplo, seguindo um caminho de comprimento par na árvore de Brauer, conseguimos construir um indecomponível como o primeiro que aparece na demonstração. Com certos caminhos especiais, conseguimos encontrar todos os indecomponíveis de uma álgebra de Brauer utilizando essas ideias! Existem algumas sutilezas quando um dos vértices no caminho é excepcional e o argumento dado para provar a indecomponibilidade precisaria ser adaptado. A Seção 5.2 do livro [7] explica resumidamente como construir esses indecomponíveis e se baseia no artigo [15], que entra em mais detalhes.

É possível usar as informações no artigo para encontrar até mesmo a multiplicidade de B! Ele demonstra que existem $e(em+1)$ B-módulos indecomponíveis, onde m é a multiplicidade do vértice excepcional da árvore de Brauer de B. Mas sabemos que os B-módulos indecomponíveis não projetivos estão em bijeção com os b_1-módulos indecomponíveis não projetivos pelo Teorema 5.4.1. Como conhecemos os b_1-módulos indecomponíveis, concluímos que B possui $e(p^n-1)$ indecomponíveis não projetivos. Como B possui e módulos simples, existem e B-módulos indecomponíveis projetivos. Logo, temos ep^n módulos indecomponíveis no total. Concluímos que

$$e(em+1) = ep^n \implies em+1 = p^n \implies m = \frac{p^n-1}{e},$$

como enunciado no Teorema 5.1.7.

Para finalmente concluir a demonstração do Teorema 5.1.7, resta encontrarmos a multiplicidade m do vértice excepcional da árvore de Brauer de B (sem apelar para o artigo [15], como acima). Ela está escondida dentro de um objeto que definimos ao final da Seção 4.1: a matriz de Cartan! Se C_B denota a matriz de Cartan de B, então

$$\det(C_B) = em+1,$$

como veremos mais para frente.

Antes de demonstrar essa propriedade, vamos motivá-la um pouco mais. A ideia é que C_B está intimamente ligada à matriz de Cartan C_{b_1} de b_1, que sabemos calcular explicitamente: como a árvore de Brauer de b_1 é uma estrela de e arestas com multiplicidade $\mu \coloneqq (p^n-1)/e$ no centro, sabemos que os b_1-módulos projetivos indecomponíveis são unisseriados, todos com comprimento $e\mu+1=p^n$, e seus fatores de composição seguem aquela ordenação circular. Com isso, não é difícil mostrar que

$$C_{b_1} = \begin{pmatrix} \mu+1 & \mu & \mu & \cdots & \mu \\ \mu & \mu+1 & \mu & \cdots & \mu \\ \mu & \mu & \mu+1 & \cdots & \mu \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mu & \mu & \mu & \cdots & \mu+1 \end{pmatrix},$$

onde a matriz em questão é quadrada de ordem e. Agora, é intuitivamente claro que $\det(C_{b_1})$ depende de μ.

Lema 5.6.4. Com as notações acima, vale

$$\det(C_{b_1}) = e\mu + 1 = p^n.$$

Demonstração. Se I denota a matriz identidade $e \times e$ e se J é a matriz $e \times e$ cujas entradas são todas iguais a 1, então $C_{b_1} = I + \mu J$. Dessa forma,

$$C_{b_1} = I + \mu J = (-\mu)((-1/\mu)I - J) \implies \det(C_{b_1}) = (-\mu)^e \cdot \det((-1/\mu)I - J).$$

O determinante à direita é exatamente o polinômio característico de J avaliado em $-1/\mu$. Como J possui posto 1, é fácil verificar que 0 é um autovalor de J com multiplicidade $e-1$. Também é fácil checar que o vetor-coluna com entradas iguais a 1 é um autovetor de autovalor e, então concluímos que o polinômio característico de J é $p_J(x) = x^{e-1}(x-e)$. Portanto,

$$\det(C_{b_1}) = (-\mu)^e \cdot p_J(-1/\mu) = (-\mu)^e \cdot (-1/\mu)^{e-1} \cdot ((-1/\mu) - e) = e\mu + 1 = p^n,$$

como desejado. □

Assim, nosso objetivo será mostrar que $\det(C_B) = \det(C_{b_1}) = p^n$ e que $\det(C_B) = em + 1$, de onde seguirá $m = \mu = (p^n-1)/e$. Para a primeira igualdade, precisamos entender o que o determinante da matriz de Cartan representa. Iremos introduzir mais alguns conceitos.

Seja A uma k-álgebra de dimensão finita qualquer e sejam $S_1, \ldots, S_r$ representantes distintos de todas as classes de isomorfismo de A-módulos simples. Definimos o **grupo de Grothendieck** $G_0(A)$ de A como sendo o grupo abeliano livre gerado pelos símbolos $[S_1], \ldots, [S_r]$. Todo elemento de $G_0(A)$ se escreve unicamente como

$$a_1[S_1] + a_2[S_2] + \cdots + a_r[S_r]$$

para certos $a_1, a_2, \ldots, a_r \in \mathbb{Z}$. Se U é um A-módulo qualquer e se a_i denota a multiplicidade de S_i como fator de composição de U $(1 \leq i \leq r)$, então definimos

$$[U] \coloneqq a_1[S_1] + a_2[S_2] + \cdots + a_r[S_r] \in G_0(A).$$

Se U, V e W são A-módulos em uma sequência exata

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0,$$

note que os fatores de composição de V são os fatores de composição de U e de W (somando multiplicidades), então $[V] = [U] + [W]$. Uma consequência disso é que essa notação é "aditiva": se U e V são A-módulos quaisquer, então $[U \oplus V] = [U] + [V]$.

Observação 5.6.5. É possível utilizar essa última propriedade para dar uma definição mais abstrata de $G_0(A)$. Poderíamos ter definido tal grupo tomando o grupo abeliano livre gerado por todas as classes de isomorfismo de A-módulos e quocientando pelo subgrupo gerado pelos elementos da forma $[V]-[U]-[W]$ para toda sequência exata

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0.$$

Não é difícil verificar que as definições constroem o mesmo grupo a menos de isomorfismo.

Definimos $K_0(A)$ como sendo o subgrupo de $G_0(A)$ gerado por todos os elementos da forma $[P]$ onde P é um A-módulo projetivo. Como o colchete é "aditivo", $K_0(A)$ é gerado pelos elementos $[P_1],\dots,[P_r]$, onde P_i é a cobertura projetiva de S_i para todo $1 \leq i \leq r$. Agora, se $C_A = (c_{ij})$ é a matriz de Cartan de A (onde as linhas e as colunas estão indexadas seguindo a ordem $S_1,\dots,S_r$), então

$$[P_i] = c_{1i}[S_1] + c_{2i}[S_2] + \cdots + c_{ri}[S_r]$$

para todo $1 \leq i \leq r$. A matriz de Cartan reapareceu! O próximo resultado mostra que ela codifica propriedades importantes do quociente $\overline{G_0}(A) \coloneqq G_0(A)/K_0(A)$.

Lema 5.6.6. O grupo $\overline{G_0}(A)$ é finito se, e somente se, $\det(C_A) \neq 0$. Nesse caso, vale

$$\left|\overline{G_0}(A)\right| = |\det(C_A)|.$$

Demonstração. Como $K_0(A)$ é gerado pelos elementos $[P_1],\dots,[P_r]$, existe um homomorfismo sobrejetor de grupos abelianos $f : \mathbb{Z}^r \to K_0(A)$ que leva o i-ésimo vetor da base canônica de $\mathbb{Z}^r$ em $[P_i]$, para todo $1 \leq i \leq r$. Por outro lado, é imediato da definição de $G_0(A)$ a existência de um isomorfismo $g : G_0(A) \to \mathbb{Z}^r$ que leva $[S_i]$ no i-ésimo vetor da base canônica de $\mathbb{Z}^r$, para todo $1 \leq i \leq r$. Defina $\varphi : \mathbb{Z}^r \to \mathbb{Z}^r$ como sendo a composição de f com a inclusão $K_0(A) \to G_0(A)$ e com o isomorfismo g. Veja que g leva $K_0(A)$ isomorficamente na imagem de φ, então $\overline{G_0}(A)$ é isomorfo ao conúcleo de φ.

Lembre que "trocar a base" do domínio ou do contradomínio de φ equivale a compor φ com um isomorfismo $h : \mathbb{Z}^r \to \mathbb{Z}^r$ em alguma ordem. Note que o conúcleo de φ é isomorfo aos conúcleos de φh e de $h\varphi$, já que h é isomorfismo, então essa operação não altera o conúcleo. Mais ainda, podemos associar uma matriz com entradas inteiras a todo endomorfismo de $\mathbb{Z}^r$. Nesse caso, a matriz de h é inversível e, portanto, possui determinante igual a ± 1. Desse modo, o módulo do determinante da matriz associada a φh ou a $h\varphi$ ainda é igual ao módulo do determinante da matriz associada a φ. Como apontamos antes da demonstração, a matriz de φ é C_A. Por isso, concluímos que, após uma mudança de base, o conúcleo de φ ainda é isomorfo a $\overline{G_0}(A)$ e o módulo do determinante da matriz associada ainda é igual a $|\det(C_A)|$.

É um resultado clássico (veja o Teorema 3.8 na página 181 de [13], por exemplo) que, com uma mudança de base, é possível colocar a matriz de φ na *forma normal de Smith*. Isso significa, em particular, que podemos tornar a matriz de φ diagonal e de modo que os inteiros não nulos $d_1,\dots,d_s$ $(s \leq r)$ da diagonal principal sejam positivos. Segue de imediato que o conúcleo de φ é isomorfo a

$$\frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \frac{\mathbb{Z}}{d_2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_s\mathbb{Z}} \times \mathbb{Z}^{r-s}.$$

Assim, $\overline{G_0}(A)$ é finito se e só se $r = s$, ou seja, se e só se 0 não é um elemento da diagonal principal da forma normal de Smith da matriz de φ. Isso ocorre exatamente quando o determinante dessa matriz diagonal é não nulo, isto é, quando $|\det(C_A)| \neq 0$. Por fim, quando $r = s$, a ordem de $\overline{G_0}(A)$ é $d_1 d_2 \cdots d_r$, mas esse produto é o determinante da matriz diagonal em questão, que é igual a $|\det(C_A)|$. □

Vamos voltar a lidar com o Teorema 5.1.7.

Proposição 5.6.7. Com as notações anteriores, vale $\det(C_B) = \pm p^n$.

Demonstração. Pelos Lemas 5.6.4 e 5.6.6, basta provarmos que $\overline{G_0}(B) \cong \overline{G_0}(b_1)$. Vamos construir esse isomorfismo. Se U é um B-módulo qualquer, então b_1U é o somando canônico de U_{N_1} associado ao bloco b_1. Não é difícil ver que, se

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

é uma sequência exata de B-módulos, então podemos encontrar uma sequência exata

$$0 \longrightarrow b_1U \longrightarrow b_1V \longrightarrow b_1W \longrightarrow 0$$

de b_1-módulos (fizemos isso na demonstração da Proposição 5.4.11, por exemplo). Com a definição do grupo de Grothendieck dada na Observação 5.6.5, isso nos permite definir um homomorfismo de $G_0(B)$ em $G_0(b_1)$ que leva $[U]$ em $[b_1U]$ para todo B-módulo U. Se U é projetivo, então U_{N_1} também é projetivo e o mesmo deve valer para o seu somando direto b_1U. Logo, o homomorfismo em questão leva $K_0(B)$ dentro de $K_0(b_1)$, o que nos dá um homomorfismo $\varphi : \overline{G_0}(B) \to \overline{G_0}(b_1)$. Por outro lado, se V é um b_1-módulo qualquer, então BV^G é o somando canônico de V^G associado ao bloco B. Como a indução também preserva sequências exatas e módulos projetivos, um argumento análogo nos permite construir um homomorfismo $\psi : \overline{G_0}(b_1) \to \overline{G_0}(B)$ que leva a classe de $[V]$ na classe de $[BV^G]$ para todo b_1-módulo V. Mostremos que φ e ψ são inversos um do outro.

Seja S um B-módulo simples. Como S não é projetivo, o Teorema 5.4.1 nos permite tomar o seu correspondente de Green T, que é um b_1-módulo indecomponível não projetivo. Além disso, como S_{N_1} é a soma direta de T com um módulo projetivo e com módulos pertencentes a blocos diferentes de b_1, vale $b_1S \cong T \oplus P$ para algum b_1-módulo projetivo P. Assim, em $G_0(b_1)$, temos $[b_1S] = [T] + [P]$. Passando ao quociente $\overline{G_0}(b_1)$, $[P]$ é levado em 0, então φ leva a classe de $[S]$ na classe de $[T]$. Mas também sabemos do Teorema 5.4.1 que $BT^G \cong S \oplus Q$ para algum B-módulo projetivo Q. Então, em $G_0(B)$, temos $[BT^G] = [S] + [Q]$ e, passando para o quociente, concluímos que ψ leva a classe de $[T]$ na classe de $[S]$. Como as classes dos elementos da forma $[S]$, onde S varia sobre os B-módulos simples, geram $\overline{G_0}(B)$, concluímos que $\psi\varphi$ é a identidade em $\overline{G_0}(B)$. Um argumento parecido mostra que $\varphi\psi$ é a identidade em $\overline{G_0}(b_1)$, terminando a demonstração. □

Observação 5.6.8. Em breve, demonstraremos que $\det(C_B)$ é positivo e seguirá pela proposição que $\det(C_B) = p^n$, ou seja, o determinante da matriz de Cartan de qualquer bloco de kG com grupo de defeito cíclico é uma potência de p. É interessante comentar que esse resultado ainda vale se omitirmos a hipótese sobre o grupo de defeito! De fato, o determinante da matriz de Cartan de kG sempre é uma potência da característica de k. Esse resultado foi provado pelo próprio Brauer em [4], utilizando caracteres. Uma outra demonstração pode ser encontrada no Capítulo 17 do livro [20].

Como apontado, o último passo é mostrar que $\det(C_B) = em + 1$. Com isso, seguirá que $\det(C_B)$ é positivo e, juntando com a Proposição 5.6.7, teremos $em+1 = p^n$, como preciso. Assim como tivemos que encontrar C_{b_1}, devemos descrever melhor como é C_B através do algoritmo para álgebras de Brauer. Se S e T são dois B-módulos simples (que podemos ver como arestas na árvore de Brauer de B), então é fácil obter através do algoritmo que a multiplicidade de S na cobertura projetiva de T é:

- 2, se $S \cong T$ e a aresta correspondente não contém o vértice excepcional.
- $m + 1$, se $S \cong T$ e a aresta correspondente contém o vértice excepcional.
- 0, se $S \ncong T$ e as arestas correspondentes não se encontram.
- 1, se $S \ncong T$ e as arestas correspondentes se encontram em um vértice não excepcional.

- m, se $S \ncong T$ e as arestas correspondentes se encontram no vértice excepcional.

É possível compilar todos esses casos em uma descrição só: a multiplicidade de S na cobertura projetiva de T é a soma das multiplicidades dos vértices em comum entre as arestas de S e T. Observe que essa caracterização depende apenas da árvore de Brauer de B. Assim, se $\mathcal{T}$ é uma árvore de Brauer qualquer, podemos utilizar essa regra para construir uma matriz quadrada $C_{\mathcal{T}}$ cujas linhas e colunas são indexadas pelas arestas de $\mathcal{T}$. Como trocar duas arestas de ordem alterna duas linhas e duas colunas de $\mathcal{T}$ entre si, o determinante de $C_{\mathcal{T}}$ independe da ordenação das arestas na hora de construir a matriz. É nessa generalidade que vale o resultado que concluirá a prova do Teorema 5.1.7:

Proposição 5.6.9. Se $\mathcal{T}$ é uma árvore de Brauer com x arestas e vértice excepcional de multiplicidade y, então $\det(C_{\mathcal{T}}) = xy + 1$.

Antes de demonstrar a proposição, veremos um lema auxiliar sobre determinantes que nos ajudará posteriormente. Sejam $X = (x_{ij})$ e $Y = (y_{ij})$ matrizes quadradas de ordem r e s, respectivamente, e com entradas inteiras. Denote por X_0 a matriz obtida de X retirando-se a última linha e a última coluna, e denote por Y_0 a matriz obtida de Y retirando-se a primeira linha e a primeira coluna. Supondo que $x_{rr} = y_{11} = z \in \mathbb{Z}$, forme a matriz quadrada M de ordem $r + s - 1$ "juntando" X e Y nessa coordenada comum. Assim,

$$M = \begin{pmatrix} x_{11} & \cdots & x_{1,r-1} & x_{1r} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{r-1,1} & \cdots & x_{r-1,r-1} & x_{r-1,r} & 0 & \cdots & 0 \\ x_{r1} & \cdots & x_{r,r-1} & z & y_{12} & \cdots & y_{1s} \\ 0 & \cdots & 0 & y_{21} & y_{22} & \cdots & y_{2s} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & y_{s1} & y_{s2} & \cdots & y_{ss} \end{pmatrix}.$$

Temos uma fórmula para o determinante de M:

Lema 5.6.10. Nas condições acima, vale

$$\det(M) = \det(X)\det(Y_0) + \det(X_0)\det(Y) - z\det(X_0)\det(Y_0).$$

Demonstração. Se $1 \leq i, j \leq r$, denote por X_{ij} a matriz obtida de X retirando-se a i-ésima linha e a j-ésima coluna. Analogamente, se $1 \leq i, j \leq s$, podemos definir a submatriz Y_{ij} de Y e, se $1 \leq i, j \leq r + s - 1$, também podemos definir a submatriz M_{ij} de M. Note que $X_0 = X_{rr}$ e $Y_0 = Y_{11}$. Aplicando a regra de Laplace na r-ésima linha de M, obtemos

$$\det(M) = \sum_{j=1}^{r-1}(-1)^{r+j}x_{rj}\det(M_{rj}) + z\det(M_{rr}) + \sum_{j=2}^{s}(-1)^{2r+j-1}y_{1j}\det(M_{r,r+j-1}).$$

Vamos simplificar esses somatórios. Se $1 \leq j \leq r-1$, observe que M_{rj} possui a seguinte decomposição por blocos:

$$M_{rj} = \begin{pmatrix} X_{rj} & 0 \\ * & Y_0 \end{pmatrix}.$$

Logo, $\det(M_{rj}) = \det(X_{rj})\det(Y_0)$ e temos

$$\begin{aligned} \sum_{j=1}^{r-1}(-1)^{r+j}x_{rj}\det(M_{rj}) &= \left(\sum_{j=1}^{r-1}(-1)^{r+j}x_{rj}\det(X_{rj})\right)\cdot\det(Y_0) \\ &= (\det(X) - z\det(X_0))\cdot\det(Y_0), \end{aligned}$$

onde utilizamos, na última igualdade, a regra de Laplace na última linha de X. Por outro lado, se $2 \leq j \leq s$, também temos a seguinte decomposição por blocos:

$$M_{r,r+j-1} = \begin{pmatrix} X_0 & * \\ 0 & Y_{1j} \end{pmatrix}.$$

Por isso, $\det(M_{r,r+j-1}) = \det(X_0)\det(Y_{1j})$ e também temos

$$\begin{aligned} \sum_{j=2}^{s}(-1)^{2r+j-1}y_{1j}\det(M_{r,r+j-1}) &= \det(X_0)\cdot\left(\sum_{j=2}^{s}(-1)^{j+1}y_{1j}\det(Y_{1j})\right) \\ &= \det(X_0)\cdot(\det(Y) - z\det(Y_0)), \end{aligned}$$

onde usamos, na última igualdade, a regra de Laplace na primeira linha de Y. Além disso,

$$M_{rr} = \begin{pmatrix} X_0 & 0 \\ 0 & Y_0 \end{pmatrix},$$

então $\det(M_{rr}) = \det(X_0)\det(Y_0)$. Juntando as contas, obtemos o resultado desejado. □

Agora conseguimos demonstrar a Proposição 5.6.9.

Demonstração. A prova será feita por indução no número x de arestas. Se $x = 1$, o resultado é imediato da definição de $C_{\mathcal{T}}$. Suponha então que $x > 1$. Começaremos lidando com o caso em que $\mathcal{T}$ é uma estrela. Se o vértice excepcional de $\mathcal{T}$ está no centro da estrela, então $C_{\mathcal{T}}$ é igual à matriz C_{b_1} que vimos anteriormente (mas trocando e por x e μ por y), então a conta do Lema 5.6.4 nos dá $\det(C_{\mathcal{T}}) = xy+1$. Por outro lado, se o vértice excepcional de $\mathcal{T}$ não estiver no centro da estrela, então vale

$$C_{\mathcal{T}} = \begin{pmatrix} y+1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 1 & \cdots & 1 \\ 1 & 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 2 \end{pmatrix}$$

(após uma possível reordenação das arestas). Note que a submatriz de $C_{\mathcal{T}}$ obtida retirando-se a primeira linha e a primeira coluna é a matriz associada a uma estrela com $x-1$ arestas e com multiplicidade 1 no centro, então o seu determinante é $(x-1)\cdot 1 + 1 = x$, pelo que vimos logo antes. Assim, aplicando a regra de Laplace na primeira linha de $C_{\mathcal{T}}$, obtemos

$$\det(C_{\mathcal{T}}) = (y+1)x + r,$$

onde r é a soma dos cofatores de $C_{\mathcal{T}}$ associados às coordenadas $(1, j)$ para $2 \leq j \leq x$. Observe que r não depende de y. Se tivermos $y = 1$, então $C_{\mathcal{T}}$ é a matriz associada a uma estrela com x arestas e com multiplicidade 1 no centro, então já vimos que o seu determinante é $x+1$, de onde obtemos

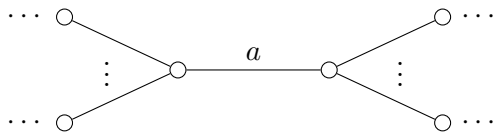
$$2x + r = x + 1 \implies r = 1 - x.$$

Portanto, para y qualquer, vale

$$\det(C_{\mathcal{T}}) = (y+1)x + (1-x) = xy + 1,$$

como preciso.

Agora, suponha que $\mathcal{T}$ não seja uma estrela. Isso significa que existe uma aresta a em $\mathcal{T}$ que, se retirada, separa a árvore em outras duas, ou seja, $\mathcal{T}$ pode ser representada como:



Seja $\mathcal{T}_L$ a subárvore de $\mathcal{T}$ formada por a mais tudo o que está à esquerda. Da mesma forma, defina $\mathcal{T}_R$ como sendo a subárvore formada por a mais o que está à direita. Ordenando as arestas de $\mathcal{T}$ de modo que primeiro apareçam as arestas de $\mathcal{T}_L$ e só depois as de $\mathcal{T}_R$, então $C_{\mathcal{T}}$ adquire a forma de M no Lema 5.6.10 com $X = C_{\mathcal{T}_L}$ e $Y = C_{\mathcal{T}_R}$, já que a única aresta que conecta $\mathcal{T}_L$ e $\mathcal{T}_R$ é a. Apagando a de $\mathcal{T}_L$, obtemos uma árvore que denotaremos por $\mathcal{T}_L^0$. Analogamente, definimos $\mathcal{T}_R^0$. Logo, o Lema 5.6.10 nos dá

$$\det(C_{\mathcal{T}}) = \det(C_{\mathcal{T}_L})\det(C_{\mathcal{T}_R^0}) + \det(C_{\mathcal{T}_L^0})\det(C_{\mathcal{T}_R}) - z\det(C_{\mathcal{T}_L^0})\det(C_{\mathcal{T}_R^0}),$$

onde z é a soma das multiplicidades dos extremos de a. Podemos utilizar a hipótese de indução para calcular os termos que apareceram! A única dificuldade é que não sabemos onde está o vértice excepcional de $\mathcal{T}$ e precisaremos separar em casos. Como todo vértice de $\mathcal{T}$ é um vértice de $\mathcal{T}_L^0$ ou um vértice de $\mathcal{T}_R^0$, podemos supor sem perda de generalidade que o vértice excepcional aparece em $\mathcal{T}_L^0$. Caímos em dois casos, a depender se o vértice excepcional é um extremo de a ou não.

Se o vértice excepcional não é um extremo de a, então $\mathcal{T}_L$ e $\mathcal{T}_L^0$ possuem multiplicidade y, enquanto $\mathcal{T}_R$ e $\mathcal{T}_R^0$ possuem multiplicidade 1. Além disso, $z = 2$. Por isso, se r é o número de arestas de $\mathcal{T}_L$ e s é o número de arestas de $\mathcal{T}_R$, então a hipótese de indução nos dá

$$\begin{aligned}
\det(C_{\mathcal{T}}) &= (ry+1)s + ((r-1)y+1)(s+1) - 2((r-1)y+1)s \\
&= (rsy+s) + (rsy + ry - sy + s - y + 1) - 2(rsy - sy + s) \\
&= ry + sy - y + 1 \\
&= (r+s-1)y + 1 \\
&= xy + 1,
\end{aligned}$$

onde utilizamos que $x = r + s - 1$. Por outro lado, se o vértice excepcional é um extremo de a, então $\mathcal{T}_L$, $\mathcal{T}_L^0$ e $\mathcal{T}_R$ possuem multiplicidade y, enquanto $\mathcal{T}_R^0$ possui multiplicidade 1. Nesse caso, $z = y + 1$. Portanto, com a mesma definição de r e s de antes, a hipótese de indução implica em

$$\begin{aligned}
\det(C_{\mathcal{T}}) &= (ry+1)s + ((r-1)y+1)(sy+1) - (y+1)((r-1)y+1)s \\
&= (rsy+s) + (rsy^2 - sy^2 + ry + sy - y + 1) - (rsy^2 - sy^2 + rsy + s) \\
&= ry + sy - y + 1 \\
&= (r+s-1)y + 1 \\
&= xy + 1.
\end{aligned}$$

Em qualquer caso, $\det(C_{\mathcal{T}})$ possui o valor desejado. □

A prova do Teorema 5.1.7 está finalizada!

Apêndice A

Exercícios e soluções

Separamos uma lista de exercícios para cada um dos capítulos do trabalho e detalhamos uma solução para cada um deles. As principais fontes foram os livros [1] e [22], mas também acrescentamos exercícios originais[1] que surgiram durante a preparação do material.

Como comentamos na Introdução, todos os exercícios de [1] se encontram resolvidos aqui. No entanto, a ordenação não é a mesma e alguns deles estão resolvidos no meio dos outros capítulos. A seguir, listamos as seções desse livro com exercícios e, para cada uma delas, indicamos pelo símbolo " $\Longrightarrow$ " a qual exercício daqui corresponde cada exercício de [1].

(1) **Semisimple modules**

- Exercício 1 $\Longrightarrow$ Exemplo 1.1.18.
- Exercício 2 $\Longrightarrow$ Exercício A.1.1.
- Exercícios 3 e 4 $\Longrightarrow$ Corolário 1.1.17.

(2) **Simple algebras**

- Exercícios de 1 a 3 $\Longrightarrow$ Exercício A.1.6.
- Exercício 4 $\Longrightarrow$ Exercício A.1.7.
- Exercício 5 $\Longrightarrow$ Exercício A.1.8.

(3) **Group algebras**

- Exercício 1 $\Longrightarrow$ Exercício A.1.13.
- Exercício 2 $\Longrightarrow$ Exercício A.1.14.
- Exercício 3 $\Longrightarrow$ Exercício A.1.22.
- Exercício 4 $\Longrightarrow$ Exercício A.1.23.
- Exercício 5 $\Longrightarrow$ Exercício A.1.17.
- Exercício 6 $\Longrightarrow$ Exercício A.1.18.
- Exercício 7 $\Longrightarrow$ Lema 1.4.1.

(4) **Indecomposable modules**

- Exercícios de 1 a 5 $\Longrightarrow$ Exercício A.2.3.

(5) **Free modules**

- Exercício 1 $\Longrightarrow$ Exercício A.2.5.

[1] Muitos deles provavelmente devem existir em algum outro lugar, então podemos pensar que são exercícios "redescobertos".

- Exercício 2 $\Longrightarrow$ Exercício A.2.8.
- Exercício 3 $\Longrightarrow$ Exercício A.2.9.
- Exercício 4 $\Longrightarrow$ Exercício A.2.2.
- Exercício 5 $\Longrightarrow$ Exercício A.1.15.

(6) **Duality**

- Exercício 1 $\Longrightarrow$ Exemplo 2.3.19.
- Exercício 2 $\Longrightarrow$ Exercício A.2.12.
- Exercício 3 $\Longrightarrow$ Exercício A.2.13.

(7) **Tensor products**

- Exercício 1 $\Longrightarrow$ Exercício A.2.6.
- Exercício 2 $\Longrightarrow$ Exercício A.1.11.
- Exercício 3 $\Longrightarrow$ Exercício A.2.19.
- Exercício 4 $\Longrightarrow$ Exercício A.2.20.
- Exercício 5 $\Longrightarrow$ Exercício A.2.21.
- Exercícios de 6 a 8 $\Longrightarrow$ Exercício A.2.22.

(8) **Induced modules**

- Exercício 1 $\Longrightarrow$ Exercício A.3.5.
- Exercício 2 $\Longrightarrow$ Exercício A.3.3.
- Exercício 3 $\Longrightarrow$ Exercício A.3.1.

(9) **Vertices and sources**

- Exercício 1 $\Longrightarrow$ Exercício A.3.6.
- Exercício 2 $\Longrightarrow$ Exercício A.3.8.
- Exercício 3 $\Longrightarrow$ Exercício A.3.12.
- Exercícios 4 e 5 $\Longrightarrow$ Exercício A.3.11.
- Exercício 6 $\Longrightarrow$ Exercício A.3.13.

(10) **Trivial intersections**

- Exercício 1 $\Longrightarrow$ Exercício A.3.14.
- Exercícios 2 e 3 $\Longrightarrow$ Exercício A.3.16.

(11) **Green correspondence**

- Exercício 1 $\Longrightarrow$ Corolário 3.4.6.
- Exercício 2 $\Longrightarrow$ Teorema 3.4.3 e Corolário 3.4.6.
- Exercício 3 $\Longrightarrow$ Exercício A.3.17.

(13) **Defect groups**

- Exercício 1 $\Longrightarrow$ Exercício A.4.4.
- Exercício 2 $\Longrightarrow$ Exemplo 4.1.20.
- Exercício 3 $\Longrightarrow$ Exercício A.4.7.

(14) **Brauer correspondence**

- Exercício 1 $\Longrightarrow$ Exemplo 4.3.11.

(15) **Canonical module**

- Exercício 1 $\Longrightarrow$ Exercício A.4.10.
- Exercício 2 $\Longrightarrow$ Exercício A.4.11.
- Exercício 3 $\Longrightarrow$ Lema 4.4.1.

(16) **Subpairs**

- Exercício 1 $\Longrightarrow$ Exemplo 4.4.10.
- Exercício 2 $\Longrightarrow$ Exercício A.4.15.
- Exercício 3 $\Longrightarrow$ Exercício A.4.16.

(17) **Brauer trees**

- Exercício 1 $\Longrightarrow$ Lema 5.1.8.
- Exercício 2 $\Longrightarrow$ Exemplo 5.1.5.
- Exercício 3 $\Longrightarrow$ Exemplo 5.1.4.
- Exercício 4 $\Longrightarrow$ Exercício A.5.2.

(18) **Nilpotent blocks**

- Exercícios 1 e 2 $\Longrightarrow$ Exercício A.5.4.
- Exercício 3 $\Longrightarrow$ Exercício A.5.5.
- Exercício 4 $\Longrightarrow$ Exercício A.5.6.
- Exercício 5 $\Longrightarrow$ Observação 5.2.4.

(19) **Local case**

- Exercício 1 $\Longrightarrow$ Exercício A.5.7.
- Exercícios de 2 a 4 $\Longrightarrow$ Exercício A.5.8.

(20) **Projective covers**

- Exercício 1 $\Longrightarrow$ Exercício A.5.9.
- Exercício 2 $\Longrightarrow$ Exercício A.5.10.
- Exercício 3 $\Longrightarrow$ Exercício A.5.11.

(21) **Simple modules**

- Exercício 1 $\Longrightarrow$ Exercício A.5.12.
- Exercício 2 $\Longrightarrow$ Exercício A.5.13.

(22) **Brauer graph**

- Exercícios 1 e 2 $\Longrightarrow$ Exercício A.5.14.
- Exercício 3 $\Longrightarrow$ Exercício A.5.15.

(23) **Trees**

- Exercício 1 $\Longrightarrow$ Exercício A.5.16.
- Exercício 2 $\Longrightarrow$ Exercício A.5.17.

Sem mais delongas, vamos aos exercícios!

A.1 Semissimplicidade

Exercício A.1.1. Descreva as camadas radicais e as camadas de soco do módulo regular da álgebra $T_n(k)$ de matrizes triangulares inferiores $n \times n$ com entradas em k.

Solução: Usaremos a notação dos Exemplos 1.1.11 e 1.1.18. Começaremos com as camadas radicais. Como N_r/N_{r+1} é semissimples, esse quociente é a soma de alguns dos módulos simples S_i. Vamos encontrar quais são esses módulos. Essencialmente, o que queremos entender é como $T_n(k)$ age na primeira diagonal não nula de N_r. Se $X = (a_{ij}) \in T_n(k)$ e $Y = (b_{ij}) \in N_r$, a entrada $(r+t, t)$ de XY é

$$\sum_{s=1}^{n} a_{r+t,s} b_{s,t} = a_{r+t,r+t} b_{r+t,t},$$

onde usamos que $a_{r+t,s} = 0$ para $s > r+t$ (já que $X \in T_n(k)$) e $b_{s,t} = 0$ para $s < r+t$ (já que $Y \in N_r$). Ou seja, quando X age em Y, a coordenada $(r+t, t)$ de Y é multiplicada por $a_{r+t,r+t}$. Mas então, no quociente N_r/N_{r+1}, a coordenada $(r+t, t)$ "vai gerar" um submódulo isomorfo a S_{r+t}! Variando t de 1 a $n-r$, segue que

$$N_r/N_{r+1} \cong S_{r+1} \oplus \cdots \oplus S_n$$

para todo $0 \leq r \leq n-1$.

Agora, vamos encontrar as camadas de soco. Queremos ver quais módulos simples compõem L_{r+1}/L_r. Analogamente ao caso anterior, queremos entender como que $T_n(k)$ age na primeira linha não nula de L_{r+1}. Se $X = (a_{ij}) \in T_n(k)$ e $Y = (b_{ij}) \in L_{r+1}$, a entrada $(n-r, t)$ de XY é

$$\sum_{s=1}^{n} a_{n-r,s} b_{s,t} = a_{n-r,n-r,} b_{n-r,t},$$

onde usamos que $a_{n-r,s} = 0$ para $s > n-r$ (já que $X \in T_n(k)$) e $b_{s,t} = 0$ para $s < n-r$ (já que $Y \in L_{r+1}$). Ou seja, quando X age em Y, a primeira linha não nula é multiplicada por $a_{n-r,n-r}$. Disso segue facilmente que, para $0 \leq r \leq n-1$,

$$L_{r+1}/L_r \cong S_{n-r} \oplus \cdots \oplus S_{n-r},$$

onde S_{n-r} aparece $n-r$ vezes. □

Exercício A.1.2. Se U e V são A-módulos, mostre que

$$\operatorname{rad}^n(U \oplus V) = \operatorname{rad}^n(U) \oplus \operatorname{rad}^n(V) \quad \text{e} \quad \operatorname{soc}^n(U \oplus V) = \operatorname{soc}^n(U) \oplus \operatorname{soc}^n(V).$$

Solução: Segue de imediato da definição de rad^n e da Proposição 1.1.15. □

Exercício A.1.3. Se $\varphi : U \to V$ é um homomorfismo de A-módulos, mostre que $\varphi(\operatorname{rad}^n(U)) = \operatorname{rad}^n(\varphi(U))$. Mostre que vale apenas uma das inclusões se trocarmos o radical pelo soco. Qual deveria ser o análogo do resultado inicial para o soco?

Solução: Para a primeira parte, temos que

$$\varphi(\operatorname{rad}^n(U)) = \varphi(\operatorname{rad}(A)^n U) = \operatorname{rad}(A)^n \varphi(U) = \operatorname{rad}^n(\varphi(U)).$$

No caso do soco, a inclusão que vale é $\varphi(\operatorname{soc}^n(U)) \subseteq \operatorname{soc}^n(\varphi(U))$. De fato, se $u \in \operatorname{soc}^n(U)$, então $\operatorname{rad}(A)^n u = 0$, de modo que

$$\operatorname{rad}(A)^n \varphi(u) = \varphi(\operatorname{rad}(A)^n u) = \varphi(0) = 0$$

e $\varphi(u) \in \operatorname{soc}^n(\varphi(U))$. Para ver que a igualdade nem sempre vale, basta tomar um módulo U que não é semissimples e $V = U/\operatorname{soc}(U)$. Nesse caso, a imagem de $\operatorname{soc}(U)$ pela projeção de U em V é 0, mas $\operatorname{soc}(V) \neq 0$ porque V é não nulo.

O resultado inicial é sobre imagens homomorfas e, portanto, pode ser encarado como um resultado sobre quocientes. Traduzindo para essa linguagem, se V é submódulo de U, então o que obtemos é

$$\operatorname{rad}^n\left(\frac{U}{V}\right) = \frac{\operatorname{rad}^n(U) + V}{V}.$$

Pela filosofia de que o soco é uma espécie de dual do radical, podemos tentar trocar os quocientes acima por submódulos e chegamos em

$$\operatorname{soc}^n(V) = \operatorname{soc}^n(U) \cap V$$

quando V é submódulo de U. Verifica-se facilmente que esse é o caso através da Proposição 1.1.15. □

Exercício A.1.4. Seja U um A-módulo. Nesse exercício, denotaremos o comprimento de Loewy de U por $\ell(U)$.

(a) Suponha que V é um submódulo de U. Mostre que $\ell(V) \leq \ell(U)$ e $\ell(U/V) \leq \ell(U)$. Mostre que é possível valer a igualdade mesmo quando $0 < V < U$.

(b) Suponha que $U_1, \ldots, U_n$ são submódulos de U tais que $U = U_1 + \cdots + U_n$. Mostre que $\ell(U) = \max\{\ell(U_i) \mid 1 \leq i \leq n\}$.

Solução: Para o item (a), daremos duas provas. Seja $V \leq U$. Então $\operatorname{rad}^n(V) \subseteq \operatorname{rad}^n(U)$. Tomando $n = \ell(U)$, vale que $\operatorname{rad}^n(U) = 0$ e segue o mesmo para $\operatorname{rad}^n(V)$, de modo que $\ell(V) \leq \ell(U)$. Agora, pelo Exercício A.1.3, $(\operatorname{soc}^n(U) + V)/V \subseteq \operatorname{soc}^n(U/V)$. Tomando $n = \ell(U)$, segue que $\operatorname{soc}^n(U) = U$ e, portanto, $\operatorname{soc}(U/V) = U/V$, de onde temos $\ell(U/V) \leq \ell(U)$.

Vamos para a segunda prova de (a). Usaremos alguns argumentos que aparecem quando estudamos séries de composição. Seja $V \leq U$ e tome

$$0 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n = U$$

uma cadeia de submódulos de U com quocientes semissimples e tamanho $n = \ell(U)$ (por exemplo, tal cadeia pode ser a série de socos de U). Vamos construir uma cadeia com quocientes semissimples para V e para U/V.

Considere

$$0 = U_0 \cap V \subseteq U_1 \cap V \subseteq \cdots \subseteq U_n \cap V = V.$$

Observe que a inclusão $U_{i+1} \cap V \to U_{i+1}$ seguida da projeção $U_{i+1} \to U_{i+1}/U_i$ tem núcleo $U_i \cap V$ e, por isso, podemos ver $(U_{i+1} \cap V)/(U_i \cap V)$ como submódulo de U_{i+1}/U_i. Como U_{i+1}/U_i é semissimples, o mesmo vale para $(U_{i+1} \cap V)/(U_i \cap V)$. Portanto, a cadeia acima possui quocientes semissimples e, como termina em V, devemos ter $\ell(V) \leq n = \ell(U)$.

Para o quociente, considere

$$0 = \frac{U_0 + V}{V} \subseteq \frac{U_1 + V}{V} \subseteq \cdots \subseteq \frac{U_n + V}{V} = \frac{U}{V}.$$

Pelo Terceiro e pelo Segundo Teoremas do Isomorfismo, os quocientes são

$$\frac{(U_{i+1} + V)/V}{(U_i + V)/V} \cong \frac{U_{i+1} + V}{U_i + V} = \frac{U_{i+1} + (U_i + V)}{U_i + V} \cong \frac{U_{i+1}}{U_{i+1} \cap (U_i + V)}.$$

Como $U_i \subseteq U_{i+1}$, vemos que U_i está contido em $U_{i+1} \cap (U_i + V)$. Portanto,

$$\frac{U_{i+1}}{U_{i+1} \cap (U_i + V)} \cong \frac{U_{i+1}/U_i}{(U_{i+1} \cap (U_i + V))/U_i}.$$

Isso nos diz que os quocientes da cadeia acima são quocientes dos U_{i+1}/U_i, que são semissimples. Logo, encontramos uma cadeia de tamanho n com quocientes semissimples que termina em U/V, de modo que $\ell(U/V) \leq n = \ell(U)$.

Antes de discutir a parte final do item (a), faremos o item (b). Sejam $U_1, \ldots, U_n$ submódulos de U cuja soma é U. Note que, semelhantemente ao Exercício A.1.2,

$$\begin{aligned}\operatorname{rad}^r(U) &= \operatorname{rad}(A)^r(U_1 + \cdots + U_n) \\ &= \operatorname{rad}(A)^r U_1 + \cdots + \operatorname{rad}(A)^r U_n \\ &= \operatorname{rad}^r(U_1) + \cdots \operatorname{rad}^r(U_n).\end{aligned}$$

Com isso, o menor r tal que $\operatorname{rad}^r(U) = 0$ é justamente o menor r tal que $\operatorname{rad}^r(U_i) = 0$ para todo i. Em outras palavras, $\ell(U) = \max\{\ell(U_i) \mid 1 \leq i \leq n\}$.

Agora, vamos concluir o item (a). Se U é semissimples e não simples, tome V um submódulo próprio não nulo qualquer de U. Então V também é semissimples e vale $\ell(U) = \ell(V) = 1$. Como esse exemplo não tem muita graça, vamos dar outro exemplo. Pelo item (b), escrevendo U como soma de submódulos, temos que $\ell(U)$ é o comprimento de Loewy de algum desses submódulos. Se, por exemplo, U não for cíclico (isto é, não é gerado por um único elemento), então sempre encontraremos $0 < V < U$ com $\ell(U) = \ell(V)$, pois basta tomar um conjunto gerador e escolher o gerador certo. Vamos mostrar um exemplo concreto utilizando a descrição que fizemos de $T_n(k)$. Tome $U_1 = \operatorname{soc}^{n-1}(T_n(k))$, que consiste das matrizes de $T_n(k)$ cuja primeira entrada é 0. Agora, note que o conjunto U_2 das matrizes com elementos não nulos apenas na primeira coluna é um submódulo de $T_n(k)$. É imediato que $T_n(k)$ é a soma de U_1 e U_2, que são submódulos próprios e não triviais. Mas veja que $\ell(U_1) = n - 1$ pois temos a cadeia

$$0 \subseteq \operatorname{soc}(T_n(k)) \subseteq \cdots \subseteq \operatorname{soc}^{n-1}(T_n(k)) = U_1$$

e ela não pode ser encurtada, já que $\ell(T_n(k)) = n$. Pelo item (b), necessariamente temos $\ell(U_2) = n$, como queríamos. □

Exercício A.1.5. Seja A uma k-álgebra de dimensão finita.

(a) Mostre que é possível A ser semissimples e mesmo assim possuir uma subálgebra não semissimples.

(b) Se A é um produto finito de álgebras de divisão de dimensão finita, prove que toda subálgebra de A é semissimples.

Solução: Para o item (a), basta tomar $A = M_2(k)$. Sabemos que $M_2(k)$ é uma álgebra semissimples, mas $T_2(k)$ é uma subálgebra de $M_2(k)$ que não é semissimples (veja o Exemplo 1.1.11).

Vamos para o item (b). Utilizaremos a convenção de que uma subálgebra de A possui a unidade de A. Começaremos com um resultado preliminar. Suponha que A seja uma álgebra de dimensão finita qualquer e tome B uma subálgebra de A. Se $b \in B$ é não nulo e inversível em A, afirmamos que b é inversível em B. De fato, seja $b^{-1} \in A$ o inverso de b. Como A possui dimensão finita sobre k, b^{-1} é algébrico sobre k, ou seja, existem $n \geq 1$ e $\lambda_0, \ldots, \lambda_{n-1} \in k$ tais que

$$(b^{-1})^n + \lambda_{n-1}(b^{-1})^{n-1} + \cdots + \lambda_1 b^{-1} + \lambda_0 = 0.$$

Multiplicando a expressão acima por b^{n-1}, obtemos

$$b^{-1} = -(\lambda_0 b^{n-1} + \lambda_1 b^{n-2} + \cdots + \lambda_{n-1}) \in B,$$

como preciso.

Com isso em mãos, podemos prosseguir. Suponha que $A = D_1 \times \cdots \times D_n$, onde $D_1, \ldots, D_n$ são álgebras de divisão de dimensão finita. Vamos mostrar que toda subálgebra de A também

é um produto finito de álgebras de divisão de dimensão finita e, em particular, é semissimples. Provaremos isso por indução em n. Se $n = 1$, então A é uma álgebra de divisão e, pelo parágrafo anterior, toda subálgebra de A é também uma álgebra de divisão.

Suponha que $n > 1$ e que o resultado valha para valores menores do que n. Seja B uma subálgebra de A. Se todo elemento não nulo de B é inversível, então B é uma álgebra de divisão, como preciso. Caso contrário, existe um elemento $b = (d_1, \ldots, d_n) \in B$ não nulo que não é inversível. Pelo resultado preliminar, b não pode ser inversível em A e então existe alguma coordenada de b que é igual a 0. Sem perda de generalidade, podemos supor que $d_1 = \cdots = d_i = 0$ e que $d_{i+1}, \ldots, d_n$ são não nulos, para algum $1 \leq i < n$. Para simplificar a notação, suporemos que $i = 1$. A demonstração para $i > 1$ é análoga. Como $d_2, \ldots, d_n$ são não nulos, o elemento $(d_2, \ldots, d_n)$ de $D_2 \times \cdots \times D_n$ é inversível e, pelo mesmo argumento de antes, o seu inverso $(d_2^{-1}, \ldots, d_n^{-1})$ é um polinômio em $(d_2, \ldots, d_n)$ com coeficientes em k. Assim, acrescentando a coordenada nula, vemos que $(0, d_2^{-1}, \ldots, d_n^{-1})$ é um polinômio em b com coeficientes em k e, portanto, $(0, d_2^{-1}, \ldots, d_n^{-1}) \in B$. Multiplicando b por esse elemento, chegamos em $(0, 1, \ldots, 1) \in B$. Como B é subálgebra, também vale $(1, 1, \ldots, 1) \in B$ e, subtraindo pelo elemento anterior, $(1, 0, \ldots, 0) \in B$.

Agora, sejam $\pi_1 : A \to D_1$ e $\pi_2 : A \to D_2 \times \cdots \times D_n$ as projeções canônicas, que são homomorfismos de álgebras. Assim, $\pi_1(B)$ é subálgebra de D_1 e $\pi_2(B)$ é subálgebra de $D_2 \times \cdots \times D_n$. Pela hipótese de indução, $\pi_1(B)$ e $\pi_2(B)$ são produtos de álgebras de divisão. Vamos mostrar que $B \cong \pi_1(B) \times \pi_2(B)$, o que concluirá a demonstração. A função $\varphi : B \to \pi_1(B) \times \pi_2(B)$ que leva $b \in B$ no par $(\pi_1(b), \pi_2(b))$ é certamente um homomorfismo injetor de álgebras (é praticamente a identidade). O que não é claro é que esse homomorfismo é sobrejetor. De fato, se $c \in \pi_1(B)$ e $c' \in \pi_2(B)$, então existem $x = (c_1, \ldots, c_n), y = (c_1', \ldots, c_n') \in B$ tais que $\pi_1(x) = c$ e $\pi_2(y) = c'$. Observe então que $c = c_1$ e $c' = (c_2', \ldots, c_n')$. Como $(1, 0, \ldots, 0), (0, 1, \ldots, 1) \in B$, então

$$(c_1, c_2', \ldots, c_n') = (1, 0, \ldots, 0)x + (0, 1, \ldots, 1)y \in B.$$

Dessa forma,

$$\varphi(c_1, c_2', \ldots, c_n') = (c_1, (c_2', \ldots, c_n')) = (c, c'),$$

provando a sobrejetividade de φ, como queríamos. □

Exercício A.1.6. Seja A_0 uma k-álgebra de dimensão finita sem necessariamente ter uma unidade.

(a) Prove que existe uma álgebra A com unidade 1 contendo A_0 como uma subálgebra de codimensão um.

(b) Mostre que todo ideal de A_0 é um ideal de A.

(c) Prove que se A_0 não tem ideais nilpotentes não nulos então o mesmo vale para A. Deduza que A_0 é o produto direto de álgebras de matrizes sobre álgebras de divisão (e em particular tem um elemento identidade).

Solução: A ideia para construir A é acrescentar uma coordenada em A_0 que age como uma identidade. Como k-espaço, definimos $A \coloneqq A_0 \oplus k$. Identificando A_0 e k dentro de A, todo elemento $a \in A$ se escreve unicamente na forma $a = a_0 + \lambda \cdot 1$, onde $a_0 \in A$ e $\lambda \in k$. O 1 por enquanto apenas indica que λ está na cópia de k dentro de A, mas em breve veremos que ele é a unidade de A. Dados $a = a_0 + \lambda \cdot 1$ e $b = b_0 + \mu \cdot 1$ em A, definimos o seu produto por

$$ab = (a_0 + \lambda \cdot 1)(b_0 + \mu \cdot 1) \coloneqq (a_0 b_0 + \mu \cdot a_0 + \lambda \cdot b_0) + (\lambda\mu) \cdot 1.$$

Repare que estamos forçando que o produto seja bilinear e não é difícil verificar que ele de fato o é. Também deixamos o leitor verificar que o produto acima é associativo (estamos assumindo que A_0 é associativa). É fácil constatar que a cópia de A_0 em A é subálgebra de codimensão um

isomorfa a A_0, basta tomar $\lambda = \mu = 0$ na relação acima. Por fim, o elemento $1 = 0 + 1 \cdot 1$ é o elemento neutro para o produto de A.

Para o próximo item, seja I um ideal de A_0. Se $i \in I$ e $a = a_0 + \lambda \cdot 1 \in A$ são quaisquer, então

$$ai = (a_0 + \lambda \cdot 1)(i + 0 \cdot 1) = a_0 i + \lambda \cdot i \in I$$

e

$$ia = (i + 0 \cdot 1)(a_0 + \lambda \cdot 1) = i a_0 + \lambda \cdot i \in I$$

porque I é ideal de A_0. Segue que I também é ideal de A.

Agora, vamos resolver o item (c). Seja I um ideal nilpotente de A. Provaremos que $I \subseteq A_0$ e disso seguirá que I é ideal nilpotente de A_0 e portanto $I = 0$, como queremos demonstrar. Seja $a = a_0 + \lambda \cdot 1 \in I$ qualquer. Como I é nilpotente, o mesmo vale para a. Mas, pela definição do produto, para cada n inteiro positivo existe $a_n \in A_0$ tal que

$$a^n = (a_0 + \lambda \cdot 1)^n = a_n + \lambda^n \cdot 1.$$

Tome n tal que $a^n = 0$, de onde temos $\lambda^n = 0$. Como $\lambda \in k$ e k é corpo, a única possibilidade é $\lambda = 0$. Então $a = a_0 \in A_0$ e $I \subseteq A_0$. Concluímos que A não possui ideais nilpotentes não nulos. Como A é uma álgebra com unidade, a teoria desenvolvida anteriormente funciona e, pelo que acabamos de demonstrar, $\operatorname{rad}(A) = 0$ (pois $\operatorname{rad}(A)$ é nilpotente) e A é uma álgebra semissimples. Perceba que A_0 é ideal de A pelo item (b), logo, pelo item (2) da Proposição 1.2.10, A_0 é a soma de algumas das componentes simples de A e, consequentemente, é o produto direto de álgebras de matrizes sobre álgebras de divisão. □

Exercício A.1.7. Demonstre o seguinte caso particular do Teorema de Skolem-Noether: todo automorfismo de $M_n(k)$ como álgebra é interno (ou seja, é dado por conjugação por um elemento inversível). (*Dica:* Use o fato de que $M_n(k)$ possui um único módulo simples.)

Solução: Seja $\varphi : M_n(k) \to M_n(k)$ um automorfismo de álgebra. Denote por S o espaço dos vetores-coluna de tamanho n. Pelo Lema 1.2.1, S é um $M_n(k)$-módulo através da multiplicação de matrizes e é o único módulo simples de $M_n(k)$. Veja que podemos restringir escalares de S através de φ, ou seja, podemos definir o $M_n(k)$-módulo S' que tem como espaço subjacente S mas cuja ação, denotada por $\bullet$, é dada por $X \bullet v = \varphi(X)v$ para $v \in S'$ e $X \in M_n(k)$. Como $M_n(k)$ é semissimples e tem S como único módulo simples, vemos que S' é isomorfo a uma soma direta de cópias de S. Mas, por questões de dimensão, só pode haver uma cópia de S. Assim, existe um isomorfismo de módulos $T : S \to S'$. Esquecendo a estrutura de módulo, T é um automorfismo linear do espaço dos vetores-coluna e, por álgebra linear, podemos ver T como uma matriz inversível em $M_n(k)$ e o automorfismo leva $v \in S$ para $Tv \in S'$. Como T preserva a estrutura de módulo, vale que

$$TXv = X \bullet (Tv) = \varphi(X)Tv$$

para todo $v \in S$ e $X \in M_n(k)$. Mas isso implica que

$$TX = \varphi(X)T \implies \varphi(X) = TXT^{-1}$$

para todo $X \in M_n(k)$, provando que φ é um automorfismo interno. □

Exercício A.1.8. Mostre que o número de classes de isomorfismo de módulos simples sobre A é igual ao número de componentes simples de $A/\operatorname{rad}(A)$.

Solução: A Observação 1.1.10 nos dá uma correspondência entre módulos sobre $A/\operatorname{rad}(A)$ e módulos semissimples sobre A. Um argumento análogo implica que $A/\operatorname{rad}(A)$ e A têm os mesmos módulos simples. Como $A/\operatorname{rad}(A)$ é semissimples, o Teorema de Wedderburn nos diz que o número de classes de isomorfismo de módulos simples sobre $A/\operatorname{rad}(A)$ é o número de componentes simples de $A/\operatorname{rad}(A)$. Juntando essas duas propriedades, temos o exercício. □

Exercício A.1.9. Seja U um A-módulo semissimples. Mostre que $\mathrm{End}_A(U)$ é uma álgebra de divisão se e somente se U é simples.

Solução: Uma das implicações é o Lema de Schur. Provaremos a contrapositiva da outra implicação. Suponha que U não seja simples. Como U é semissimples, podemos escrever $U = S_1 \oplus \cdots \oplus S_r$ onde cada S_i é um A-módulo simples e $r \geq 2$. Pelo Lema 1.2.5, temos um isomorfismo $\mathrm{End}_A(U) \cong M(S_1, \ldots, S_r)$. Mas $r \geq 2$, então $M(S_1, \ldots, S_r)$ não é álgebra de divisão. Por exemplo, é fácil verificar que a matriz que tem o homomorfismo identidade na coordenada $(1,1)$ e o homomorfismo nulo nas outras não é inversível. □

Exercício A.1.10. Sejam A uma álgebra semissimples e S um A-módulo simples. Prove que S pode ser visto como um módulo sobre $\mathrm{End}_A(S)$ e a multiplicidade de S como um somando de ${}_AA$ é $\dim_{\mathrm{End}_A(S)} S$. Compare com o Corolário 1.2.9.

Solução: Pelo Teorema de Wedderburn, podemos escrever

$$A \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

onde $D_1, \ldots, D_r$ são álgebras de divisão. Logo, S é obtido restringindo escalares do módulo simples de alguma dessas álgebras de matrizes. Note que um endomorfismo de S como A-módulo é exatamente a mesma coisa que um endomorfismo de S visto como módulo sobre essa álgebra de matrizes. Além disso, a multiplicidade de S como somando de A é a mesma multiplicidade de S como somando dessa álgebra de matrizes. Assim, podemos simplificar o problema e supor que $A = M_n(D)$ para alguma álgebra de divisão D. Também podemos supor que S é o espaço dos vetores-coluna de tamanho n com entradas em D e que a ação de $M_n(D)$ é por multiplicação à esquerda.

Podemos ver S como um módulo sobre $\mathrm{End}_A(S)$ do jeito canônico: dados $\varphi \in \mathrm{End}_A(S)$ e $v \in S$, definimos $\varphi \cdot v \coloneqq \varphi(v)$. Não é difícil ver que isso de fato define um $\mathrm{End}_A(S)$-módulo. Pelo item (3) do Lema 1.2.1, um endomorfismo de S corresponde à multiplicação à direita por algum elemento de D. Assim, a estrutura de S como $\mathrm{End}_A(S)$-módulo pode ser naturalmente identificada com a estrutura de S como D-espaço vetorial *à direita*. Como a dimensão de S como D-espaço é n, $\dim_{\mathrm{End}_A(S)} S = n$ também. Mas, pelo item (2) do Lema 1.2.1, n é a multiplicidade de S como somando do módulo regular de $M_n(D)$, o que prova o exercício.

O Corolário 1.2.9 é consequência desse exercício porque, para k algebricamente fechado, o Lema de Schur diz que $\mathrm{End}_A(S) \cong k$. Com a identificação do parágrafo anterior, a estrutura de $\mathrm{End}_A(S)$-módulo de S é exatamente a sua estrutura de espaço vetorial, então temos $\dim_{\mathrm{End}_A(S)} S = \dim_k S$, como aparece no enunciado do corolário. □

Exercício A.1.11. Se S é um A-módulo simples e U é um A-módulo qualquer, mostre que a multiplicidade de S como fator de composição de $U/\operatorname{rad}(U)$ é igual à dimensão de $\mathrm{Hom}_A(U, S)$ dividida pela dimensão de $\mathrm{End}_A(S)$. O que acontece quando k é algebricamente fechado? Enuncie e prove um resultado análogo para encontrar a multiplicidade de S em $\operatorname{soc}(U)$.

Solução: Se $\varphi : U \to S$ é um homomorfismo, então o Exercício A.1.3 nos diz que $\varphi(\operatorname{rad}(U)) \subseteq \operatorname{rad}(S)$. Mas S é simples, então $\operatorname{rad}(S) = 0$ e $\operatorname{rad}(U)$ está contido no núcleo de φ. Por isso, pelo Teorema do Homomorfismo, obtemos um homomorfismo induzido $\overline{\varphi} : U/\operatorname{rad}(U) \to S$. Não é difícil ver que o mapa que leva $\varphi \in \mathrm{Hom}_A(U, S)$ em $\overline{\varphi} \in \mathrm{Hom}_A(U/\operatorname{rad}(U), S)$ é um isomorfismo linear.

Agora, como $U/\operatorname{rad}(U)$ é semissimples, podemos escrever $U/\operatorname{rad}(U) = S_1 \oplus \cdots \oplus S_n$, onde $S_1, \ldots, S_n$ são A-módulos simples. Dessa forma, determinar um homomorfismo de $U/\operatorname{rad}(U)$ em S é o mesmo que determinar um homomorfismo de S_i em S para cada $1 \leq i \leq n$. Formalizando isso, conseguimos um isomorfismo linear

$$\mathrm{Hom}_A(U/\operatorname{rad}(U), S) \cong \mathrm{Hom}_A(S_1, S) \oplus \cdots \oplus \mathrm{Hom}_A(S_n, S).$$

Mas qualquer homomorfismo não nulo entre dois módulos simples é um isomorfismo, então $\mathrm{Hom}_A(S_i, S) = 0$, se $S_i \not\cong S$, e $\mathrm{Hom}_A(S_i, S) \cong \mathrm{End}_A(S)$, se $S_i \cong S$. Se m é a multiplicidade de S como fator de composição de $U/\operatorname{rad}(U)$, então

$$\dim_k \mathrm{Hom}_A(U, S) = \dim_k \mathrm{Hom}_A(U/\operatorname{rad}(U), S) = \sum_{i=1}^{n} \dim_k \mathrm{Hom}_A(S_i, S) = m \cdot \dim_k \mathrm{End}_A(S),$$

como queríamos. Se k é algebricamente fechado, o Lema de Schur implica que $\dim_k \mathrm{End}_A(S) = 1$ e, portanto, a multiplicidade procurada é exatamente $\dim_k \mathrm{Hom}_A(U, S)$.

Para encontrar a multiplicidade de S em $\operatorname{soc}(U)$, calculamos a dimensão de $\mathrm{Hom}_A(S, U)$ e dividimos pela dimensão de $\mathrm{End}_A(S)$. A demonstração é análoga. Comece notando que a imagem de qualquer homomorfismo $\varphi : S \to U$ é nula ou simples (e isomorfa a S), então a imagem sempre está dentro de $\operatorname{soc}(U)$, que é a soma de todos os submódulos simples de U. Com isso, obtemos facilmente um isomorfismo linear entre $\mathrm{Hom}_A(S, U)$ e $\mathrm{Hom}_A(S, \operatorname{soc}(U))$. Escrevendo $\operatorname{soc}(U) = S_1 \oplus \cdots \oplus S_n$, onde $S_1, \cdots, S_n$ são A-módulos simples, conseguimos encontrar um isomorfismo linear

$$\mathrm{Hom}_A(S, \operatorname{soc}(U)) \cong \mathrm{Hom}_A(S, S_1) \oplus \cdots \oplus \mathrm{Hom}_A(S, S_n)$$

e concluímos o que queríamos provar do mesmo modo que terminamos o caso anterior. □

Exercício A.1.12. Seja U um kG-módulo e suponha que $\mathrm{char}(k)$ não divide $|G|$. Mostre que o conjunto dos elementos de U fixos por G é precisamente a imagem de

$$x = \frac{1}{|G|} \sum_{g \in G} g,$$

visto como operador linear em U.

Solução: Se $u \in U$ é fixo por G, então

$$u = \frac{1}{|G|} \cdot |G| u = \frac{1}{|G|} \sum_{g \in G} gu = \left(\frac{1}{|G|} \sum_{g \in G} g \right) \cdot u = xu$$

e u está na imagem de x. Reciprocamente, se $u = xv$ para algum $v \in U$, então

$$hu = (hx)v = \left(\frac{1}{|G|} \sum_{g \in G} hg \right) \cdot v = \left(\frac{1}{|G|} \sum_{g \in G} g \right) \cdot v = xv = u$$

para todo $h \in G$, de modo que u é fixo por G.

Podemos fazer um comentário interessante: se $U = U_1 \oplus \cdots \oplus U_r$ é a decomposição de U em suas componentes simples, então x age como a projeção na componente que corresponde ao módulo trivial. Veremos mais a frente (no Capítulo 4) que quem tem esse papel é o idempotente associado à componente simples de kG que corresponde ao módulo trivial. Mas, como vimos na prova do Teorema de Maschke, essa componente é o subespaço de kG gerado por x. Como x é o único elemento não nulo dessa componente que satisfaz $x^2 = x$, ele é o idempotente em questão. □

Exercício A.1.13. Se $\mathrm{char}(k)$ divide $|G|$, mostre que o subespaço gerado pelo elemento

$$x = \sum_{g \in G} g$$

é um ideal nilpotente de kG. Use isso para dar outra prova de uma das implicações do Teorema de Maschke.

Solução: Como a multiplicação à esquerda ou à direita por um elemento em G apenas permuta os elementos do grupo, é imediato que $gx = x = xg$ para todo $g \in G$. Logo, o subespaço kx gerado por x é um ideal de kG. Além disso,

$$x^2 = \left(\sum_{g\in G} g\right) \cdot x = \sum_{g\in G} gx = \sum_{g\in G} x = |G|x$$

e, como $|G| = 0$ em k, temos $x^2 = 0$. Dessa forma, $(kx)^2 = 0$ e kx é um ideal nilpotente de kG. Pelo Teorema 1.1.8, kx está contido em $\operatorname{rad}(kG)$ e, em particular, $\operatorname{rad}(kG) \neq 0$, provando que kG não é semissimples e confirmando uma das implicações do Teorema de Maschke. □

Exercício A.1.14. Se $p = \operatorname{char}(k) > 0$ e G é um p-grupo, mostre que $\operatorname{rad}(kG)$ é o ideal de aumento IG.

Solução: Da definição de radical, $\operatorname{rad}(kG)$ é o conjunto dos elementos de kG que anulam todos os kG-módulos simples. Mas, pela Proposição 1.3.10, todos os kG-módulos simples são isomorfos ao módulo trivial. Para ficar mais claro o que se segue, denotaremos por S o módulo trivial e fixaremos $s \in S$ não nulo, que é um gerador de S como subespaço. Assim, dado um elemento $a = \sum_{g\in G} a_g g \in kG$, vemos que

$$\begin{aligned}
a \in \operatorname{rad}(kG) &\iff a \cdot S = 0 \\
&\iff a \cdot s = 0 \\
&\iff \sum_{g\in G} a_g(g \cdot s) = \left(\sum_{g\in G} a_g\right) \cdot s = 0 \\
&\iff \sum_{g\in G} a_g = 0 \\
&\iff a \in IG,
\end{aligned}$$

provando o que o exercício pede. Em um contexto mais geral, o que provamos é que IG é o anulador do módulo trivial, algo que também é fácil de ver se lembrarmos que IG é o núcleo da função de aumento. □

Exercício A.1.15. Seja $G = C_n$ o grupo cíclico de ordem $n = p^a$ com gerador x. Considere $X = x - 1 \in kG$. Mostre que $1, X, X^2, \ldots, X^{p^a-1}$ formam uma base para kG e que $X, X^2, \ldots, X^{p^a-1}$ formam um base para $\operatorname{rad}(kG)$.

Solução: Como as potências de x (indo de $1 = x^0$ até x^{p^a-1}) formam uma base para kG, segue de imediato do Teorema do Binômio de Newton que $1, X, \cdots, X^{p^a-1}$ são linearmente independentes sobre k. Como a dimensão de kG é p^a, eles formam uma base. Agora, vimos no Exercício A.1.14 que $\operatorname{rad}(kG)$ é o ideal de aumento IG. Sabendo disso, é imediato que $X \in \operatorname{rad}(kG)$ e, como $\operatorname{rad}(kG)$ é ideal, também temos $X^i \in \operatorname{rad}(kG)$ para todo $i \geq 1$. Como $\operatorname{rad}(kG)$ tem codimensão 1 em kG, concluímos que $X, X^2, \cdots, X^{p^a-1}$ formam uma base de $\operatorname{rad}(kG)$. □

Exercício A.1.16. O objetivo deste exercício é provar a forma forte do Teorema de Clifford, que é um refinamento da Proposição 1.3.13. Sejam U um kG-módulo simples e N um subgrupo normal de G. Por essa proposição, podemos escrever

$$U_N \cong S_1^{n_1} \oplus \cdots \oplus S_r^{n_r},$$

onde os S_i são kN-módulos simples não isomorfos dois a dois. Vamos provar que G permuta as componentes simples $S_i^{n_i}$ de U_N transitivamente e que $n_1 = \cdots = n_r$ e $\dim_k S_1 = \cdots = \dim_k S_r$.

(a) Se $g \in G$, mostre que gS_i é um kN-módulo simples e que $g(S_i^{n_i}) \subseteq S_j^{n_j}$ para algum $j = j(i)$.

(b) Mostre que, se $i_1 \neq i_2$, então $j(i_1) \neq j(i_2)$.

(c) Conclua que $g(S_i^{n_i}) = S_j^{n_j}$ e que G permuta as componentes simples de U_N.

(d) Construa um certo kG-submódulo de U e deduza que a ação de G nas componentes simples de U_N é transitiva.

(e) Prove as igualdades do enunciado a partir dos itens anteriores.

Solução: (a) Como vimos na demonstração da Proposição 1.3.13, gS_i é um kN-submódulo simples de U_N e, considerando fatores de composição, devemos ter $gS_i \cong S_j$ para algum j. Dessa forma, $g(S_i^{n_i})$ é soma de módulos isomorfos a S_j e, por isso, está contido na componente simples $S_j^{n_j}$. Aqui usamos que se V e V' são kN-submódulos isomorfos de U_N, então o mesmo vale para gV e gV', pois, se $\varphi : V \to V'$ é isomorfismo, então $g\varphi g^{-1} : gV \to gV'$ também é.

(b) Pelo que vimos em (a), $j(i)$ é tal que $gS_i \cong S_{j(i)}$. Assim, se $j(i_1) = j(i_2)$, temos que

$$gS_{i_1} \cong S_{j(i_1)} = S_{j(i_2)} \cong gS_{i_2} \implies S_{i_1} = g^{-1}gS_{i_1} \cong g^{-1}gS_{i_2} = S_{i_2} \implies i_1 = i_2,$$

onde usamos a observação feita ao final do item anterior na primeira implicação.

(c) Pelo item (a), vale que $\dim_k S_i^{n_i} \leq \dim_k S_j^{n_j}$. Como a função $i \mapsto j(i)$ é bijeção pelo item (b), segue que

$$\dim_k U = \sum_{i=1}^{r} \dim_k S_i^{n_i} \leq \sum_{i=1}^{r} \dim_k S_{j(i)}^{n_{j(i)}} = \dim_k U$$

e, consequentemente, é preciso valer a igualdade $\dim_k S_i^{n_i} = \dim_k S_j^{n_j}$. Por isso, $g(S_i^{n_i}) = S_j^{n_j}$ e G permuta as componentes simples de U_N.

(d) É fácil ver que

$$\sum_{g \in G} g(S_i^{n_i})$$

é um kG-submódulo não nulo de U. Como U é simples, essa soma é U e, para cada j, tem que existir $g \in G$ com $g(S_i^{n_i}) = S_j^{n_j}$. Isso prova que a ação de G nas componentes simples de U_N é transitiva.

(e) Pelo item (d), dados $1 \leq i, j \leq r$, existe $g \in G$ tal que $g(S_i^{n_i}) = S_j^{n_j}$. Como vimos no item (a), isso veio de um isomorfismo $gS_i \cong S_j$, o que mostra que S_i e S_j têm a mesma dimensão. Comparando as dimensões de $g(S_i^{n_i})$ e $S_j^{n_j}$, segue que $n_i = n_j$ também.

□

Exercício A.1.17. Se N é um subgrupo normal de G, mostre que $\operatorname{rad}(kN) = kN \cap \operatorname{rad}(kG)$.

Solução: Vamos começar provando a inclusão $kN \cap \operatorname{rad}(kG) \subseteq \operatorname{rad}(kN)$, que não usa a normalidade de N em G. Como $\operatorname{rad}(kG)$ é ideal de kG, $kN \cap \operatorname{rad}(kG)$ é um ideal de kN. Além disso, $kN \cap \operatorname{rad}(kG)$ é nilpotente, porque $\operatorname{rad}(kG)$ o é. Como $\operatorname{rad}(kN)$ é o maior ideal nilpotente de kN, devemos ter $kN \cap \operatorname{rad}(kG) \subseteq \operatorname{rad}(kN)$.

Para a outra inclusão, basta mostrar que $\operatorname{rad}(kN) \subseteq \operatorname{rad}(kG)$, pois evidentemente vale $\operatorname{rad}(kN) \subseteq kN$. Seja $x \in \operatorname{rad}(kN)$ qualquer. Se S é um kG-módulo simples, o Teorema de Clifford diz que S_N é semissimples e então, como x está no radical de kN, $xS_N = 0$ e $xS = 0$. Como x anula qualquer kG-módulo simples, vemos que $x \in \operatorname{rad}(kG)$, provando a inclusão desejada. □

Exercício A.1.18. Se N é um subgrupo normal de G e T é um kN-módulo simples, prove que existe um kG-módulo simples S tal que T é um somando direto de S_N.

Solução: Como T é simples, existe um submódulo maximal M de kN tal que $kN/M \cong T$. O próximo passo é mostrar que existe um kG-submódulo maximal M' de kG que contém M. Para isso, é suficiente mostrar que o kG-submódulo gerado por M em kG não é todo o kG. Note que o kG-submódulo gerado por M é

$$\sum_{g \in G} gM.$$

Se essa soma fosse igual a kG, existiriam $m_1, \dots, m_r \in M$ e $g_1, \dots, g_r \in G$ tais que

$$g_1 m_1 + \cdots + g_r m_r = 1.$$

Veja que $g_i m_i$ é combinação linear de elementos da classe lateral $g_i N$. Além disso, kG é a soma direta dos subespaços gerados pelas diferentes classes laterais. Como $1 \in N$, podemos supor que $g_i \in N$ para todo i. Mas então isso implica que $1 \in M$, já que M é kN-submódulo. Como 1 gera kN como kN-módulo, devemos ter $M = kN$, o que é um absurdo. Portanto, o kG-submódulo gerado por M é próprio e podemos encontrar o kG-submódulo maximal M'.

Vamos definir S como kG/M', que é simples porque M' é maximal. Compondo a inclusão $kN \to (kG)_N$ com a projeção $(kG)_N \to S_N$, temos um homomorfismo $\varphi : kN \to S_N$ de kN-módulos. Como $M \subseteq M'$, vale que $M \subseteq \ker \varphi$. Mas M é maximal em kN, logo $\ker \varphi = M$ ou $\ker \varphi = kN$. Essa segunda opção não pode ocorrer, pois implica em $1 \in M'$ e, portanto, em $M' = kG$, o que não é o caso. Pelo Teorema do Isomorfismo, S_N tem um submódulo isomorfo a $kN/M \cong T$. Como S_N é semissimples (pelo Teorema de Clifford), T é um somando direto de S_N, como queríamos. □

Exercício A.1.19. Seja G um grupo não trivial. Se todo kG-módulo simples é isomorfo ao módulo trivial, prove que $p > 0$ e que G é um p-grupo.

Solução: Se $p = 0$, sabemos do Teorema de Maschke que kG seria semissimples e, pela hipótese, seguiria que a ação de G em kG é trivial. Porém, isso não pode ser verdade, já que G não é trivial, então devemos ter $p > 0$. Agora, por hipótese, todo elemento de G age trivialmente em todos os kG-módulos simples. Assim, a Proposição 1.3.14 diz que $G = O_p(G)$ e, consequentemente, G é um p-grupo. □

Exercício A.1.20. Vamos estudar os kG-módulos de dimensão 1 e vamos generalizar a Proposição 1.3.16.

(a) Mostre que as representações unidimensionais de G sobre k são precisamente as representações unidimensionais de G/G' sobre k, vistas como representações de G através da projeção $G \to G/G'$. (Aqui, G' denota o grupo de comutadores de G.)

(b) Se k é algebricamente fechado e $p > 0$, prove que todos os kG-módulos simples são unidimensionais se e somente se $G' \subseteq O_p(G)$.

Solução: (a) Se temos uma representação $\varphi : G \to \mathrm{GL}(V)$ com V unidimensional, então $G' \subseteq \ker \varphi$, porque $\mathrm{GL}(V) \cong k^\times$ é abeliano. Por isso, φ vem de uma representação unidimensional de G/G', provando esse primeiro item.

(b) Suponha que todos os kG-módulos simples sejam unidimensionais. Pelo item (a), segue que G' está no núcleo de todas as representações irredutíveis de G, logo $G' \subseteq O_p(G)$ pela Proposição 1.3.14. Reciprocamente, se $G' \subseteq O_p(G)$ e S é um kG-módulo simples, então G' age trivialmente em S e, por isso, S pode ser visto como um $k[G/G']$-módulo simples. Mas G/G' é abeliano e k é algebricamente fechado, então a Proposição 1.3.16 diz que S tem dimensão 1, como queríamos.

□

Exercício A.1.21. Seja p um número primo. Neste exercício, que é baseado em um exercício na página 119 de [19], vamos estudar o grupo $\mathrm{SL}_2(p)$.

(a) Mostre que a ordem de $\mathrm{SL}_2(p)$ é

$$|\mathrm{SL}_2(p)| = p(p^2-1).$$

(b) Quando $p = 2$, mostre que $\mathrm{SL}_2(2) \cong S_3$. Em particular, $\mathrm{SL}_2(2)$ possui duas classes de conjugação 2-regulares.

(c) Quando $p > 2$, mostre que $\mathrm{SL}_2(p)$ possui $p+4$ classes de conjugação que são representadas pelos seguintes elementos:

(1) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$;

(2) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & \varepsilon \\ 0 & -1 \end{pmatrix}$ (onde $\varepsilon \in \mathbb{F}_p$ está fixo e não é resíduo quadrático);

(3) $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ tal que $a \in \mathbb{F}_p$ é não nulo e $a \neq \pm 1$ (a menos de troca de a por a^{-1});

(4) $\begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$ tal que o polinômio $x^2 - ax + 1 \in \mathbb{F}_p[x]$ é irredutível.

(d) No item anterior, mostre que apenas as classes de (2) não são p-regulares. Conclua que $\mathrm{SL}_2(p)$ tem exatamente p classes p-regulares.

Solução: (a) Começamos descobrindo a ordem de $\mathrm{GL}_2(p)$, o grupo das matrizes 2×2 inversíveis com entradas em $\mathbb{F}_p$. Para isso, precisamos determinar as colunas de um elemento qualquer desse grupo. A primeira coluna pode ser qualquer vetor não nulo de $\mathbb{F}_p^2$, nos dando p^2-1 possibilidades. A segunda pode ser qualquer vetor de $\mathbb{F}_p^2$ que não seja um dos p múltiplos da primeira coluna, o que dá p^2-p possibilidades. Dessa forma,

$$|\mathrm{GL}_2(p)| = (p^2-1)(p^2-p).$$

Agora, veja que a função determinante é um homomorfismo de grupos entre $\mathrm{GL}_2(p)$ e o grupo multiplicativo $\mathbb{F}_p^\times$ de $\mathbb{F}_p$. É fácil ver que esse homomorfismo é sobrejetor e que seu núcleo é $\mathrm{SL}_2(p)$, de onde segue que

$$|\mathrm{SL}_2(p)| = \frac{|\mathrm{GL}_2(p)|}{\left|\mathbb{F}_p^\times\right|} = \frac{(p^2-1)(p^2-p)}{p-1} = p(p^2-1),$$

como queríamos.

(b) Pelo item anterior, $\mathrm{SL}_2(2)$ tem 6 elementos. Note que, por exemplo,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

logo $\mathrm{SL}_2(2)$ não é abeliano. Mas o único grupo não abeliano de ordem 6 é S_3, como preciso. A segunda afirmação do item é imediata sabendo desse isomorfismo.

(c) Como matrizes conjugadas têm o mesmo polinômio característico, a ideia será separar as classes de conjugação pelos autovalores de seus elementos e se eles são diagonalizáveis ou não. Haverá uma pequena exceção quando tratarmos o caso (2).

Como os elementos de $\mathrm{SL}_2(p)$ têm determinante 1, o polinômio característico de um elemento A é da forma $x^2 - \mathrm{tr}(A)x + 1 \in \mathbb{F}_p[x]$, onde $\mathrm{tr}(A)$ é o traço de A. Calculando o traço, já conseguimos ver que os representantes da família (4) não são conjugados entre si, e, comparando autovalores, o mesmo vale para os representantes da família (3). Como as matrizes em (4) não possuem autovalores (seus polinômios característicos não têm raiz em $\mathbb{F}_p$ por hipótese), os elementos de (3) e (4) representam classes distintas. Como os autovalores que aparecem em (1) e (2) são 1 e -1 e eles não aparecem em (3) e (4), as duas primeiras famílias dão classes distintas das duas últimas. Como veremos adiante, os elementos de (1) formam o centro de $\mathrm{SL}_2(p)$ e, portanto, constituem as únicas classes de conjugação unitárias. Em breve, diferenciaremos as classes de conjugação em (2). Dessa forma, bastará mostrar que todas as classes de conjugação estão representadas. Para isso, vamos calcular a quantidade de elementos em cada uma das classes apresentadas e mostrar que sua soma é o valor encontrado no item (a).

Caso (1): Essas são as matrizes diagonalizáveis cujo polinômio característico tem uma raiz dupla. Nesse caso, uma dessas matrizes é necessariamente escalar e está no centro de $\mathrm{SL}_2(p)$. Além disso, para o determinante ser 1, as entradas na diagonal principal devem ser 1 ou -1, pois essas são as raízes de $x^2 - 1$. Aqui temos duas classes de conjugação unitárias.

Caso (2): As matrizes desse caso não são diagonalizáveis, mas têm autovalor em $\mathbb{F}_p$ com multiplicidade 2. Não iremos verificar isso diretamente, mas será uma consequência quando provarmos o exercício. Como o determinante da matriz é o produto dos autovalores, o autovalor em questão é 1 ou -1.

Vamos calcular o tamanho das classes de conjugação dos elementos listados em (2). Lembre que ε está fixo, por isso, temos apenas 4 elementos listados na família (2). Não é difícil ver que o centralizador de cada um dos elementos listados tem ordem $2p$. As contas são análogas e, por isso, faremos o caso da terceira matriz para ilustrar. Seja

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_p(2)$$

tal que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Abrindo as contas e igualando as entradas, chegamos ao sistema

$$\begin{cases} a = a + \varepsilon c \\ b + \varepsilon a = b + \varepsilon d \\ d + \varepsilon c = d \end{cases}$$

Como $\varepsilon \neq 0$, a primeira equação ou a terceira nos dá $c = 0$, enquanto a segunda implica em $a = d$. Como estamos em $\mathrm{SL}_2(p)$,

$$1 = ad - bc = a^2 \implies a = d = \pm 1.$$

Note que b pode ser qualquer. Logo, escolhendo o sinal de a e escolhendo o valor de b, totalizamos $2p$ elementos no centralizador da matriz em questão.

Como o tamanho de uma classe de conjugação é o índice do centralizador de qualquer um de seus elementos, vale que o tamanho das classes de conjugação das quatro matrizes em (2) é

$$\frac{p(p^2-1)}{2p} = \frac{p^2-1}{2}.$$

Resta diferenciarmos essas quatro classes. Comparando autovalores, basta diferenciar a primeira da terceira e a segunda da quarta. Faremos apenas esse primeiro caso, porque o outro é completamente análogo.

Vamos conjugar a primeira matriz da lista por um elemento

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_p(2)$$

qualquer. Para calcular a inversa da matriz acima, lembre que o seu determinante é 1, logo

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1-ac & a^2 \\ -c^2 & 1+ac \end{pmatrix}.$$

Na última igualdade, usamos mais uma vez que $ad - bc = 1$. Repare que a entrada $(1, 2)$ e o oposto da entrada $(2, 1)$ são quadrados. Como a ou c não são ambos nulos, algum desses quadrados é não nulo. Por outro lado, uma conta análoga mostra que os conjugados da terceira matriz de (2) são da forma

$$\begin{pmatrix} 1-\varepsilon ac & \varepsilon a^2 \\ -\varepsilon c^2 & 1+\varepsilon ac \end{pmatrix}.$$

Como ε não é resíduo quadrático, a entrada $(1, 2)$ e o oposto da entrada $(2, 1)$ só podem ser 0 ou um não quadrado. Como antes, pelo menos uma dessas duas entradas não é nula. Comparando com a conta anterior, segue que nenhum conjugado da primeira matriz de (2) pode ser conjugado à terceira matriz de (2), e vice-versa. Isso conclui o estudo da família (2).

Caso (3): As classes desse caso lidam com matrizes que possuem dois autovalores distintos e que, portanto, são diagonalizáveis. Isso implica diretamente que uma dessas matrizes é conjugada a alguma listada em (3), mas apenas em $\mathrm{GL}_2(p)$. Ao término do exercício, concluiremos que a conjugação pode ser feita sobre $\mathrm{SL}_2(p)$.

Em (3), os elementos são parametrizados pelos pares $\{a, a^{-1}\}$ com $a \neq 0$ e $a \neq a^{-1}$ (ou seja, $a \neq \pm 1$, como no enunciado). Montando um sistema assim como fizemos no caso (2), não é difícil ver que o centralizador de cada matriz de (3) é formado pelas matrizes diagonais de $\mathrm{SL}_2(p)$. Pela condição do determinante, a entrada $(1, 1)$ determina tal matriz diagonal e, além disso, essa entrada pode ser qualquer elemento não nulo de $\mathbb{F}_p$. Portanto, cada centralizador tem ordem $p - 1$ e cada classe tem tamanho

$$\frac{p(p^2-1)}{p-1} = p(p+1).$$

Note que o número de classes que aparecem no caso (3) é

$$\frac{p-3}{2},$$

porque desconsideramos 0, 1 e -1 de $\mathbb{F}_p$ e pareamos cada um dos elementos restantes com seu inverso, obtendo a quantidade acima de pares.

Caso (4): Esse caso tratará das matrizes em $\mathrm{SL}_2(p)$ que não possuem autovalores em $\mathbb{F}_p$. Ele é o mais complicado e nos basearemos nas notas [10]. Primeiro teremos que calcular os centralizadores dos elementos da família (4) em $\mathrm{GL}_2(p)$ e, para isso, precisaremos usar um pouco de teoria de Galois.

Seja $K = \mathbb{F}_{p^2}$ o corpo de p^2 elementos. Podemos supor que $\mathbb{F}_p \subseteq K$. Essa extensão é de Galois e seu grupo de Galois é cíclico de ordem 2, gerado pelo automorfismo de Frobenius

$\sigma : K \to K$ dado por $\sigma(\alpha) = \alpha^p$. Lembre que todo polinômio irredutível de grau 2 em $\mathbb{F}_p$ possui duas raízes distintas em K (existe essa fatoração essencialmente porque todo corpo de p^2 elementos é isomorfo a K e porque a extensão $\mathbb{F}_p \subseteq K$ é separável). Assim, se

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

é uma matriz da família (4), o seu polinômio característico $x^2 - ax + 1$ possui uma raiz $\alpha \in K \setminus \mathbb{F}_p$ e não é difícil ver que a outra raiz tem que ser $\sigma(\alpha)$. Com isso em mãos, vamos encontrar o centralizador de A em $\mathrm{GL}_2(p)$.

Veja K como um espaço vetorial sobre $\mathbb{F}_p$. Como $\alpha \notin \mathbb{F}_p$, uma base de K sobre $\mathbb{F}_p$ é formada por 1 e por α. Seja $L_\alpha : K \to K$ a multiplicação por α em K, que é $\mathbb{F}_p$-linear. Usando que $\alpha^2 - a\alpha + 1 = 0$, sabemos que

$$L_\alpha(1) = \alpha \cdot 1 = \alpha$$

e

$$L_\alpha(\alpha) = \alpha \cdot \alpha = \alpha^2 = -1 + a\alpha$$

e, por isso, a matriz de L na base $\{1, \alpha\}$ é precisamente A. Mais geralmente, podemos definir $L_x : K \to K$ como a multiplicação por $x \in K^\times$ e, identificando L_x com sua matriz na base $\{1, \alpha\}$, obtemos um homomorfismo de grupos injetor $\varphi : K^\times \to \mathrm{GL}_2(p)$. Como $A = \varphi(\alpha) \in \varphi(K^\times)$ e $K^\times$ é abeliano, isso mostra que o centralizador de A em $\mathrm{GL}_2(p)$ contém $\varphi(K^\times)$. Vamos mostrar que eles coincidem e, para isso, é suficiente mostrar que esse centralizador tem no máximo $|K^\times| = p^2 - 1$ elementos. Seja

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{GL}_2(p)$$

uma matriz inversível que comuta com A. Como fizemos no caso da família (2), isso nos dá a seguintes relações:

$$\begin{cases} z = -y \\ w = x - ay \end{cases}$$

Portanto, os valores de x e y determinam os valores de z e w. Por causa da inversibilidade da matriz, x e y não podem ser ambos nulos, logo, há no máximo $p^2 - 1$ elementos no centralizador de A em $\mathrm{GL}_2(p)$, como queríamos.

Finalmente, vejamos o que acontece em $\mathrm{SL}_2(p)$. O centralizador de A em $\mathrm{SL}_2(p)$ consiste exatamente dos elementos de determinante 1 do centralizador de A em $\mathrm{GL}_2(p)$. Vamos encontrá-los. Como $K^\times$ é cíclico (pois K é corpo), podemos tomar um gerador $\beta \in K^\times$. Note que $\beta \notin \mathbb{F}_p$ e que a outra raiz de seu polinômio minimal é $\sigma(\beta)$. Com o mesmo argumento que usamos para α, vale que a matriz de L_β na base $\{1, \beta\}$ é

$$\begin{pmatrix} 0 & -\beta\sigma(\beta) \\ 1 & \beta + \sigma(\beta) \end{pmatrix},$$

que tem determinante $\beta\sigma(\beta)$. Como o determinante não depende da base escolhida, vale que

$$\det(\varphi(\beta)) = \beta\sigma(\beta) = \beta \cdot \beta^p = \beta^{p+1}.$$

Assim, como o determinante é multiplicativo, um elemento $\varphi(\beta^i)$ (determinado por um único $0 \leq i < p^2 - 1$) do centralizador de A em $\mathrm{GL}_2(p)$ tem determinante 1 se e só se

$$(\beta^{p+1})^i = 1 \iff (p^2 - 1) \mid i(p+1) \iff (p-1) \mid i.$$

Como $0 \leq i < p^2 - 1$, temos $p + 1$ valores possíveis de i com essa propriedade.

Agora podemos concluir esse caso. O que acabamos de fazer prova que o centralizador de cada matriz da família (4) tem ordem $p+1$ e, por isso, cada uma de suas classes de conjugação possui

$$\frac{p(p^2-1)}{p+1} = p(p-1)$$

elementos. Para terminar, vamos contar quantas matrizes existem na família (4). O total de polinômios da forma $x^2 - ax + 1$ em $\mathbb{F}_p[x]$ é p. Dentre esses, os redutíveis são determinados por suas raízes α e α^{-1}. Tirando $\alpha = \pm 1$, qualquer outro elemento não nulo é diferente de seu inverso, de modo que o número de polinômios redutíveis da forma em questão é

$$2 + \frac{p-3}{2} = \frac{p+1}{2}.$$

Com isso, o número de matrizes na família (4) é

$$p - \frac{p+1}{2} = \frac{p-1}{2}.$$

Conclusão: Já mostramos que todas as matrizes que aparecem no enunciado são representantes de classes de conjugação distintas e contamos a quantidade de conjugados. Para concluir o item (c), basta notar que

$$2 + 4 \cdot \frac{p^2-1}{2} + \frac{p-3}{2} \cdot p(p+1) + \frac{p-1}{2} \cdot p(p-1) = p(p^2-1),$$

ou seja, as classes de conjugação que encontramos já contabilizam todos os elementos de $\mathrm{SL}_2(p)$ e, portanto, essas são todas as classes. No total, são

$$2 + 4 + \frac{p-3}{2} + \frac{p-1}{2} = p + 4$$

classes de conjugação.

(d) Vamos verificar que as classes de conjugação da família (2) são as únicas que não são p-regulares. Iremos caso a caso.

Na família (1), a identidade tem ordem 1 e o oposto da identidade tem ordem 2, logo as classes de conjugação correspondentes são p-regulares.

Na família (2), repare que

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na \\ 0 & 1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} -1 & a \\ 0 & -1 \end{pmatrix}^n = \begin{pmatrix} (-1)^n & (-1)^{n-1}na \\ 0 & (-1)^n \end{pmatrix}$$

para todo $a \in \mathbb{F}_p$ e $n \geq 1$. Disso segue que a ordem de

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix}$$

é p e, como p é ímpar, a ordem de

$$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} -1 & \varepsilon \\ 0 & -1 \end{pmatrix}$$

é $2p$. Portanto, as classes de conjugação desses elementos não são p-regulares.

Na família (3), a ordem da matriz diagonal é a ordem do elemento $a \in \mathbb{F}_p^\times$. Como essa ordem divide $\left|\mathbb{F}_p^\times\right| = p-1$, ela não pode ser divisível por p. Nesse caso, também temos classes p-regulares.

Na família (4), note que o subgrupo gerado por uma das matrizes em questão está contido no centralizador dessa matriz. Pelo item (c), esse centralizador tem ordem $p+1$. Logo, as ordens dos elementos de (4) dividem $p+1$ e as classes de conjugação correspondentes são p-regulares.

Ou seja, desconsiderando as 4 classes de conjugação em (2) dentre todas as $p+4$ classes, concluímos que há p classes de conjugação p-regulares em $\mathrm{SL}_2(p)$.

□

Exercício A.1.22. Com a notação do Exemplo 1.3.17, mostre que V_n (com $1 \leq n \leq p$) possui exatamente $n+1$ submódulos como um $k\langle g\rangle$-módulo.

Solução: Como V_1 é o módulo trivial, o resultado é imediato para $n = 1$. Assim, suponha $n > 1$. No Exemplo 1.3.17, construímos os $k\langle g\rangle$-submódulos $W_0, \ldots, W_n$ de V_n, onde $W_0 = 0$ e W_i para $i \geq 1$ é o subespaço de V_n gerado pelos monômios

$$x^{i-1}y^{n-i}, x^{i-2}y^{n-i+1}, \ldots, xy^{n-2}, y^{n-1}.$$

Vamos mostrar que esses são todos os $k\langle g\rangle$-submódulos. Se V é um submódulo de $(V_n)_{\langle g\rangle}$, seja i_0 o maior índice i tal que $V \supseteq W_i$. Mostremos que $V = W_{i_0}$. Se isso não fosse verdade, existiria $v \in V \setminus W_{i_0}$. Definimos j_0 como sendo o menor índice j tal que $v \in W_j$. Note que $j_0 > i_0$. Mas então $v \in W_{j_0} \setminus W_{j_0-1}$ e o item (3) do Lema 1.3.18 diz que o submódulo gerado por v é W_{j_0}. Isso implica que $W_{j_0} \subseteq V$, contradizendo a definição de i_0. Logo, $V = W_{i_0}$, como queríamos. Por isso, $W_0, \ldots, W_n$ são todos os $n+1$ $k\langle g\rangle$-submódulos de V_n. □

Exercício A.1.23. Seja X uma matriz $n \times n$ triangular superior com 1's na diagonal principal e com todas as entradas na diagonal imediatamente acima não nulas. Mostre que a forma canônica de Jordan de X é um único bloco de Jordan $n \times n$ de autovalor 1. Com a notação do Exemplo 1.3.17, use isso para dar outra prova da simplicidade dos módulos V_n, $1 < n \leq p$.

Solução: Como X é triangular, seus autovalores são as entradas da diagonal principal. Logo, 1 é o único autovalor de X e, para verificar a afirmação sobre a forma canônica de Jordan de X, basta mostrar que o autoespaço associado a 1 tem dimensão 1. Escreva $X = (a_{ij})$ e seja $v = (v_1, \ldots, v_n)$ um vetor-coluna não nulo tal que $Xv = v$. Seja i_0 o maior índice i tal que $v_i \neq 0$. Vamos mostrar que $i_0 = 1$, o que prova que o autoespaço é unidimensional. Se $i_0 > 1$, note que a entrada $i_0 - 1$ de Xv é

$$\sum_{j=1}^{n} a_{i_0-1,j}v_j = v_{i_0-1} + a_{i_0-1,i_0}v_{i_0},$$

onde usamos que $a_{i_0-1,j} = 0$ para $j < i_0 - 1$ (pois X é triangular superior), $a_{i_0-1,i_0-1} = 1$ e $v_j = 0$ para $j > i_0$ (pela definição de i_0). Mas $Xv = v$, logo a expressão acima é igual a v_{i_0-1} e, como $v_{i_0} \neq 0$, devemos ter $a_{i_0-1,i_0} = 0$. Isso contradiz o fato de que os elementos da diagonal imediatamente acima da principal são não nulos. Logo, $i_0 = 1$, provando a afirmação do enunciado.

No caso do Exemplo 1.3.17, isso torna mais fácil a demonstração de que x^{n-1} gera o $k\langle g\rangle$-módulo V_n e que seu soco é o subespaço gerado por y^{n-1}. Vendo V_n como $k\langle g\rangle$-módulo, seja X a matriz da ação de g em V_n na base $y^{n-1}, xy^{n-2}, \ldots, x^{n-1}$ (nessa ordem). Note que

$$gx^{i-1}y^{n-i} = x^{i-1}y^{n-i} + (i-1)x^{i-2}y^{n-i+1} + \text{termos de grau menor em } x$$

para $1 \leq i \leq n$ e, como $i - 1 \leq n - 1 < p$, X satisfaz as hipóteses do enunciado. Logo, a partir da forma canônica de Jordan, podemos encontrar uma base $v_1, \ldots, v_n$ de V_n tal que $g - 1$ leva v_i em v_{i-1} e v_1 em 0. Com isso, não é difícil ver que qualquer elemento de V_n cuja última coordenada em relação à base $v_1, \ldots, v_n$ é não nula gera V_n como $k\langle g\rangle$-módulo: aplicando $(g-1)^{n-1}$ nesse elemento vemos que $v_n \in V_n$, depois aplicando $(g-1)^{n-2}$ nesse elemento vemos que $v_{n-1} \in V_n$,

e assim em diante. Mas os elementos com essa propriedade são exatamente os elementos $v \in V_n$ com $(g-1)^{n-1}v \neq 0$. Usando a conta acima repetidas vezes, é fácil verificar que

$$(g-1)^{n-1}x^{n-1} = (n-1)! \cdot y^{n-1} \neq 0$$

e, portanto, x^{n-1} gera V_n como $k\langle g\rangle$-módulo. Agora, a Proposição 1.3.10 diz que o único módulo simples de $k\langle g\rangle$ é o trivial (já que g tem ordem p), logo o soco de V_n é o subespaço dos elementos fixos por g, ou seja, é o núcleo do operador $g-1$. Segue de imediato que o núcleo de $g-1$ é o subespaço gerado por v_1 e, por isso, é unidimensional. Mas $gy^{n-1} = y^{n-1}$ e então y^{n-1} é fixo por g, de onde concluímos que o soco de V_n como $k\langle g\rangle$-módulo tem que ser ky^{n-1}. □

A.2 Decompondo representações

Exercício A.2.1. Mostre que A é uma álgebra semissimples se e só se todo A-módulo indecomponível é simples.

Solução: Se A é semissimples, todo módulo é soma direta de módulos simples. Mas a única forma de decompor um módulo indecomponível é a trivial. Assim, há apenas um somando simples e todo módulo indecomponível é simples. Reciprocamente, podemos escrever o A-módulo regular ${}_AA$ como soma de indecomponíveis e, se todos os indecomponíveis forem simples, então ${}_AA$ é semissimples e, portanto, A é semissimples como álgebra. □

Exercício A.2.2. Se $\varphi : U \to V$ e $\psi : V \to U$ são homomorfismos de módulos satisfazendo $\varphi\psi = \mathrm{id}_V$, mostre que U é a soma direta de $\ker\varphi$ com $\operatorname{im}\psi$. Prove também a recíproca:

(a) Se φ é sobrejetor e $\ker\varphi$ é somando direto de U, então φ cinde.

(b) Se ψ é injetor e $\operatorname{im}\psi$ é somando direto de U, então ψ cinde.

Solução: Se $u \in U$, podemos escrever $u = (u - (\psi\varphi)(u)) + (\psi\varphi)(u)$. A segunda parcela está claramente em $\operatorname{im}\psi$ e a primeira está em $\ker\varphi$ porque

$$\varphi(u - (\psi\varphi)(u)) = \varphi(u) - (\varphi\psi)(\varphi(u)) = \varphi(u) - \varphi(u) = 0,$$

onde usamos que $\varphi\psi = \mathrm{id}_V$. Por isso, $U = \ker\varphi + \operatorname{im}\psi$. Agora, se $u \in \operatorname{im}\psi$, existe $v \in V$ com $u = \psi(v)$ e, se também temos $u \in \ker\varphi$, vale

$$v = (\varphi\psi)(v) = \varphi(u) = 0$$

e $u = \psi(v) = 0$. Isso mostra que $\ker\varphi \cap \operatorname{im}\psi = 0$ e a soma em questão é direta.

Vejamos a recíproca. Suponha inicialmente que φ seja sobrejetor e que $U = \ker\varphi \oplus U_1$ para algum submódulo $U_1 \leq U$. Pelo Teorema do Isomorfismo, φ induz um isomorfismo de $U/\ker\varphi$ em V. Mas esse quociente é isomorfo a U_1. Utilizando os isomorfismos canônicos, obtemos um isomorfismo $\tilde{\varphi} : U_1 \to V$ que leva u_1 em $\varphi(u_1)$. Defina $\psi : V \to U$ como a composta de $\tilde{\varphi}^{-1}$ com a inclusão $U_1 \to U$. Se $v \in V$, tome $u_1 \in U_1$ tal que $\tilde{\varphi}(u_1) = v$. Assim,

$$(\varphi\psi)(v) = \varphi(\psi(\tilde{\varphi}(u_1))) = \varphi(u_1) = \tilde{\varphi}(u_1) = v,$$

provando que $\varphi\psi = \mathrm{id}_V$. Logo, φ cinde.

Para o outro caso, suponha que ψ seja injetor e que $U = \operatorname{im}\psi \oplus U_1$ para algum submódulo $U_1 \leq U$. Como ψ é injetor, está definida a inversa $\psi^{-1} : \operatorname{im}\psi \to V$. Defina $\varphi : U \to V$ como sendo ψ^{-1} sobre $\operatorname{im}\psi$ e 0 sobre U_1. Se $v \in V$, segue que $\psi(v) \in \operatorname{im}\psi$ e, assim, $\varphi(\psi(v)) = \psi^{-1}(\psi(v)) = v$. Por isso, $\varphi\psi = \mathrm{id}_V$ e ψ cinde. □

Exercício A.2.3. Suponha que $p = \mathrm{char}(k) > 0$ e considere $G = C_p \times C_p$, o produto direto de dois grupos cíclicos de ordem p com geradores x e y.

(a) Seja V um k-espaço vetorial de dimensão 2 com base u, v. Dados $\alpha, \beta \in k$, mostre que V admite uma única estrutura de $k[C_p \times C_p]$-módulo satisfazendo

$$xu = u + \alpha v, \quad xv = v$$

e

$$yu = u + \beta v, \quad yv = v.$$

(b) Se $V_{\alpha,\beta}$ é o módulo do item (a), prove que $V_{\alpha,\beta}$ é indecomponível, exceto quando $\alpha = \beta = 0$.

(c) Verifique que todo $k[C_p \times C_p]$-módulo de dimensão 2 é isomorfo a algum $V_{\alpha,\beta}$.

(d) Mostre que $V_{\alpha,\beta}$ e $V_{\gamma,\delta}$ são isomorfos se, e somente se, $(\alpha, \beta) = \lambda(\gamma, \delta)$ para algum $\lambda \in k$ não nulo.

(e) Use o item anterior para mostrar que $k[C_p \times C_p]$ não tem tipo de representação finito se k for infinito.

(f) Prove que existem exatamente duas classes de isomorfismo de $k[C_p \times C_p]$-módulos V indecomponíveis e de dimensão 3 satisfazendo $(x-1)^2V = (y-1)^2V = 0$.

Solução: (a) Como u e v formam uma base de V, a unicidade da estrutura de módulo sobre $k[C_p \times C_p]$ seguirá automaticamente após mostrarmos que as relações do enunciado de fato definem um módulo. Sejam $X, Y : V \to V$ operadores lineares dados por

$$X(u) = u + \alpha v, \quad X(v) = v$$

e

$$Y(u) = u + \beta v, \quad Y(v) = v.$$

Para concluir o item, basta mostrar que $X^p = Y^p = I$ e $XY = YX$, onde $I = \mathrm{id}_V$, pois estas são as relações que definem o grupo $C_p \times C_p$. É fácil ver que $(X-I)^2 = (Y-I)^2 = 0$, logo,

$$(X-I)^2 = 0 \implies (X-I)^p = 0 \implies X^p - I = 0 \implies X^p = I$$

e, analogamente, $Y^p = I$. Por outro lado, é fácil ver que XY e YX levam u em $u + (\alpha + \beta)v$ e deixam v fixo, provando que $XY = YX$. Portanto, V admite a estrutura de módulo desejada.

(b) Se $V_{\alpha,\beta}$ não é indecomponível, então $V_{\alpha,\beta}$ é a soma direta de dois submódulos próprios. Por causa da dimensão, cada um desses submódulos é unidimensional e, portanto, simples. Mas $C_p \times C_p$ é p-grupo, logo, pela Proposição 1.3.10, cada um desses submódulos é trivial. Isso implica que a ação de $C_p \times C_p$ em $V_{\alpha,\beta}$ é trivial e devemos ter $\alpha = \beta = 0$. Logo, por contraposição, se $(\alpha, \beta) \neq (0, 0)$, então $V_{\alpha,\beta}$ é indecomponível.

(c) Seja V um módulo sobre $k[C_p \times C_p]$ de dimensão 2. Como $C_p \times C_p$ é p-grupo, apenas o módulo trivial é simples. Mas V contém algum $k[C_p \times C_p]$-módulo simples, logo existe $v \in V$ não nulo que é fixo por x e por y. Veja que o quociente de V pelo subespaço gerado por v é simples também por ter dimensão 1. Com isso, se $u \in V$ não é múltiplo de v, existem $\alpha, \beta \in k$ tais que $xu = u + \alpha v$ e $yu = u + \beta v$. Concluímos que $V \cong V_{\alpha,\beta}$.

(d) Sejam $\{u_1, v_1\}$ e $\{u_2, v_2\}$ as bases dadas no item (a) de $V_{\alpha,\beta}$ e $V_{\gamma,\delta}$, respectivamente. Se $(\alpha, \beta) = \lambda(\gamma, \delta)$ para algum $\lambda \in k$ não nulo, podemos definir a transformação linear $\varphi : V_{\gamma,\delta} \to V_{\alpha,\beta}$ dada por $\varphi(u_2) = u_1$ e $\varphi(v_2) = \lambda v_1$. Como $\lambda \neq 0$, φ é isomorfismo linear. Além disso,

$$\varphi(xu_2) = \varphi(u_2 + \gamma v_2) = u_1 + (\lambda\gamma)v_1 = u_1 + \alpha v_1 = xu_1 = x\varphi(u_2)$$

e, analogamente, $\varphi(yu_2) = y\varphi(u_2)$. Também é imediato que

$$\varphi(xv_2) = \varphi(yv_2) = x\varphi(v_2) = y\varphi(v_2) = \lambda v_1.$$

Logo, φ também é homomorfismo de $k[C_p \times C_p]$-módulos e temos $V_{\alpha,\beta} \cong V_{\gamma,\delta}$.

Reciprocamente, suponha que exista um isomorfismo $\varphi : V_{\alpha,\beta} \to V_{\gamma,\delta}$. Se $\alpha = \beta = 0$, então $V_{\alpha,\beta}$ é trivial e o mesmo vale para $V_{\gamma,\delta}$. Logo, nesse caso, $\gamma = \delta = 0$ e temos $(\alpha, \beta) = 1 \cdot (\gamma, \delta)$. Agora, suponha que $V_{\alpha,\beta}$ e $V_{\gamma,\delta}$ não sejam triviais. Assim, seus socos são unidimensionais, gerados por v_1 e v_2, respectivamente, e φ se restringe a um isomorfismo de $\operatorname{soc}(V_{\alpha,\beta})$ em $\operatorname{soc}(V_{\gamma,\delta})$. Em particular, φ leva v_1 em um múltiplo de v_2. Compondo com uma homotetia de $V_{\gamma,\delta}$, podemos supor que $\varphi(v_1) = v_2$. Sabemos que $\varphi(u_1) = \lambda u_2 + \mu v_2$, para certos $\lambda, \mu \in k$ e, como φ é inversível, $\lambda \neq 0$. Note que

$$\varphi(xu_1) = \varphi(u_1 + \alpha v_1) = (\lambda u_2 + \mu v_2) + \alpha v_2 = \lambda u_2 + (\mu + \alpha) v_2$$

e

$$x\varphi(u_1) = x(\lambda u_2 + \mu v_2) = (\lambda u_2 + \lambda\gamma v_2) + \mu v_2 = \lambda u_2 + (\mu + \lambda\gamma) v_2.$$

Como φ é homomorfismo, $\varphi(xu_1) = x\varphi(u_1)$ e então devemos ter $\alpha = \lambda\gamma$. Trocando x por y na conta acima, obtemos que $\beta = \lambda\delta$ e, por isso, $(\alpha, \beta) = \lambda(\gamma, \delta)$.

(e) Usando os itens (b), (c) e (d), vemos que um $k[C_p \times C_p]$-módulo indecomponível de dimensão 2 ou é isomorfo a $V_{0,1}$ ou é isomorfo a $V_{1,\beta}$ para um único $\beta \in k$. Em particular, $k[C_p \times C_p]$ possui infinitas classes de isomorfismo de módulos indecomponíveis e não pode ter tipo de representação finito.

(f) A condição $(x-1)^2 V = 0$ implica que o polinômio minimal do operador em V associado a x é $t - 1 \in k[t]$ ou $(t-1)^2 \in k[t]$. Por isso, a forma canônica de Jordan desse operador é dada por

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Analogamente, o operador associado a y tem um dessas matrizes como forma canônica de Jordan. Se x age trivialmente, então ou V é trivial, contradizendo que V é indecomponível, ou a ação de y tem a segunda matriz acima como forma canônica numa base u, v, w, o que também não é o caso, pois então poderíamos decompor V como soma direta do submódulo gerado por u e v com o submódulo gerado por w. Portanto, x não age trivialmente e, simetricamente, y também não. Em particular, vemos que o subespaço W_x de vetores fixos por x e o subespaço W_y de vetores fixos por y têm ambos dimensão 2. Como o módulo trivial é o único $k[C_p \times C_p]$-módulo simples, segue que $\operatorname{soc}(V) = W_x \cap W_y$. Vamos analisar dois casos agora, um onde o soco tem dimensão 1 e outro onde o soco tem dimensão 2. Cada um desses casos resultará em apenas uma classe de isomorfismo de módulos na qual V pode pertencer, o que provará o que é pedido no exercício.

Comecemos com o caso em que $\dim_k \operatorname{soc}(V) = 1$. Seja $w \in \operatorname{soc}(V)$ não nulo. Tome $u \in W_y$ e $v \in W_x$ linearmente independentes com w. Note que v não pode ser combinação linear de u e w porque esses vetores geram W_y e $v \notin W_y$. Logo, os vetores u, v e w formam uma base de V. Note que existem $\alpha, \beta, \gamma, \delta \in k$ tais que

$$xu = u + \alpha v + \beta w \quad \text{e} \quad yv = \gamma u + v + \delta w.$$

O coeficiente de u em xu é 1 porque V/W_x é um kC_p-módulo de dimensão 1 e, portanto, é simples e trivial. Da mesma forma, o coeficiente de v em yv também é 1. Veja que

$$(xy)v = x(\gamma u + v + \delta w) = \gamma u + (\alpha\gamma + 1)v + (\beta\gamma + \delta)w$$

e, calculando de outra forma,

$$(xy)v = (yx)v = yv = \gamma u + v + \delta w.$$

Por isso, vale $\alpha\gamma = \beta\gamma = 0$. Como $u \notin W_x$, pelo menos um dentre α e β é não nulo e devemos ter $\gamma = 0$. Agora, vamos repetir essa conta trocando v por u. Temos

$$(yx)u = y(u + \alpha v + \beta w) = u + \alpha v + (\alpha\delta + \beta)w$$

e também

$$(yx)u = (xy)u = xu = u + \alpha v + \beta w.$$

Logo, $\alpha\delta = 0$ e, como $v \notin W_y$, vale $\delta \neq 0$ e temos $\alpha = 0$. Ou seja, descobrimos que

$$xu = u + \beta w \quad \text{e} \quad yv = v + \delta w$$

para certos $\beta, \gamma \in k$ não nulos. Definindo

$$\tilde{u} = u, \quad \tilde{v} = \frac{\beta}{\delta} v \quad \text{e} \quad \tilde{w} = \beta w,$$

segue que $\tilde{u}, \tilde{v}$ e $\tilde{w}$ formam um base de V satisfazendo

$$\begin{aligned} x\tilde{u} &= \tilde{u} + \tilde{w}, & y\tilde{u} &= \tilde{u}, \\ x\tilde{v} &= \tilde{v}, & y\tilde{v} &= \tilde{v} + \tilde{w}, \\ x\tilde{w} &= \tilde{w}, & y\tilde{w} &= \tilde{w}. \end{aligned}$$

Assim, encontramos uma base na qual as ações de x e y em V são representadas pelas matrizes

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix},$$

respectivamente. Isso determina unicamente a classe de isomorfismo de V no caso de soco unidimensional. Para concluir, repare que as matrizes acima comutam e de fato têm ordem p (basta imitar o que fizemos em (a)), logo, de fato definem um $k[C_p \times C_p]$-módulo, que é indecomponível justamente porque o soco tem dimensão 1. Além disso, a condição $(x-1)^2V = (y-1)^2V = 0$ é satisfeita, como preciso.

Vejamos, agora, o que acontece quando $\dim_k \operatorname{soc}(V) = 2$. Seja $\{v, w\}$ uma base de $\operatorname{soc}(V)$ e tome $u \in V \setminus \operatorname{soc}(V)$. Note que u, v e w formam uma base de V. Como $V/\operatorname{soc}(V)$ tem dimensão 1, é um módulo simples e trivial, de onde obtemos que

$$xu = u + \alpha v + \beta w \quad \text{e} \quad yu = u + \gamma v + \delta w$$

para certos $\alpha, \beta, \gamma, \delta \in k$. Vamos provar que $\alpha v + \beta w$ e $\gamma v + \delta w$ são linearmente independentes. Primeiramente, veja que ambos os vetores são não nulos, pois u não pode estar em W_x e nem em W_y. Se os vetores em questão fossem dependentes, $\gamma v + \delta w$ seria um múltiplo de $\alpha v + \beta w$ e, com isso, o subespaço W gerado por u e $\alpha v + \beta w$ seria um submódulo de V. Mas, tomando $w' \in \operatorname{soc}(V)$ linearmente independente com $\alpha v + \beta w$, vemos que o subespaço W' gerado por w' é submódulo de V e, mais ainda, $V = W \oplus W'$, contradizendo a indecomponibilidade de V. Logo, $\alpha v + \beta w$ e $\gamma v + \delta w$ são de fato linearmente independentes e, portanto, se definirmos

$$\tilde{u} = u, \quad \tilde{v} = \gamma v + \delta w \quad \text{e} \quad \tilde{w} = \alpha v + \beta w,$$

segue que $\tilde{u}, \tilde{v}$ e $\tilde{w}$ formam uma base de V. Nessa base, as matrizes que representam as ações de x e y em V são

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

respectivamente. Como antes, isso determina unicamente a classe de isomorfismo de V no caso de soco de dimensão 2. Resta mostrarmos que as matrizes acima de fato definem um módulo satisfazendo as propriedades necessárias. Não é difícil verificar que as matrizes comutam e têm ordem p, logo, de fato podemos definir a estrutura de $k[C_p \times C_p]$-módulo num espaço vetorial V de dimensão 3. Além disso, é fácil ver que $(x-1)^2V = (y-1)^2V = 0$. Para concluir, vejamos que esse módulo é indecomponível. Se escrevermos V como uma soma direta de submódulos, um dos somandos contém um vetor u_1 da forma $u_1 = u + \lambda v + \mu w$, para $\lambda, \mu \in k$. Como $w = (x-1)u_1$ e $v = (y-1)u_1$, então o submódulo gerado por u_1 tem que ser V e, por isso, a decomposição de V como soma direta tem que ser trivial, como queríamos.

Resumindo, provamos que existem duas classes de isomorfismo de $k[C_p \times C_p]$-módulos V indecomponíveis e de dimensão 3 satisfazendo $(x-1)^2V = (y-1)^2V = 0$, como preciso. □

Exercício A.2.4. Mostre que A é uma álgebra semissimples se e somente se todo A-módulo é projetivo.

Solução: Suponha que todo A-módulo seja semissimples. Se P é um A-módulo qualquer, mostremos que P é projetivo através da caracterização (2) da Proposição 2.2.1. Se $\varphi : U \to P$ é um homomorfismo sobrejetor, então $\ker \varphi$ é submódulo de U e, portanto, um somando direto de U, já que U é semissimples. Pelo Exercício A.2.2, φ cinde. Isso prova que P é projetivo e concluímos uma das implicações.

Reciprocamente, suponha que todo A-módulo seja projetivo. Se U é um A-módulo e V é um submódulo de U qualquer, então a projeção $\pi : U \to U/V$ cinde, pois π é sobrejetora e U/V é projetivo. Como $\ker \pi = V$, segue que V é um somando direto de U. Isso prova que U é semissimples e conclui a solução do exercício. □

Exercício A.2.5. Na notação do Exemplo 1.1.11, mostre que a cobertura projetiva do $T_n(k)$-módulo simples S_i é um módulo unisseriado e que suas camadas radicais são $S_i, S_{i+1}, \ldots, S_n$.

Solução: Como a cobertura projetiva é um módulo projetivo indecomponível, podemos procurá-la dentro de $T_n(k)$. Para $1 \leq i \leq n$, denote por V_i o espaço dos vetores-coluna $n \times 1$ tais que as $i-1$ primeiras entradas são nulas. Note que $\dim_k V_i = n - i + 1$ e que V_i é naturalmente um $T_n(k)$-módulo através da multiplicação de matrizes. Mas olhando para as colunas de uma matriz triangular inferior, é evidente que

$$T_n(k) \cong V_1 \oplus V_2 \oplus \cdots \oplus V_n.$$

Assim, $V_1, \ldots, V_n$ são módulos projetivos. Vejamos que eles são unisseriados. Como $\operatorname{rad}(T_n(k))$ é o conjunto das matrizes triangulares inferiores com 0 na diagonal principal, é fácil ver que

$$\operatorname{rad}(V_i) = \operatorname{rad}(T_n(k))V_i \subseteq V_{i+1}.$$

Aqui, quando $i = n$, estamos considerando $V_{n+1} = 0$. Agora repare que a ação da matriz

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in \operatorname{rad}(T_n(k))$$

em V_i é exatamente "descer" cada entrada em uma posição, zerando a primeira não nula e sumindo com a última. Isso prova a igualdade $\operatorname{rad}(V_i) = V_{i+1}$. Com isso, concluímos que a série radical de V_i é

$$V_i \supseteq V_{i+1} \supseteq V_{i+2} \supseteq \cdots \supseteq V_n \supseteq 0.$$

Cada quociente tem dimensão 1 e portanto é simples. Pela Proposição 2.1.13, V_i é unisseriado. Em particular, V_i é indecomponível e é a cobertura projetiva de $V_i/\operatorname{rad}(V_i) = V_i/V_{i+1}$. Vamos encontrar quem é esse módulo simples. Denote por $e_i \in V_n$ o vetor-coluna que possui 1 na i-ésima entrada e 0 nas demais. Veja que $e_i \in V_i$ e que $e_i + V_{i+1}$ gera V_i/V_{i+1}, logo basta entender a ação de $T_n(k)$ nesse elemento. Se $X = (a_{ij})$ é uma matriz em $T_n(k)$, então

$$Xe_i = \sum_{l=i}^{n} a_{li} e_l,$$

onde usamos que $a_{li} = 0$ para $l < i$. Mas então

$$Xe_i \equiv a_{ii} e_i \pmod{V_{i+1}},$$

provando que a ação de X em V_i/V_{i+1} é multiplicar por a_{ii}. Disso segue facilmente que $V_i/V_{i+1} \cong S_i$. Concluímos assim que a cobertura projetiva de S_i é V_i, que é um módulo unisseriado cujas camadas radicais são $S_i, S_{i+1}, \ldots, S_n$. □

Exercício A.2.6. Generalize o Lema 2.2.5: se U é um A-módulo e P é um A-módulo projetivo com $U/\operatorname{rad}(U) \cong P/\operatorname{rad}(P)$, então U é um quociente de P.

Solução: Vamos adaptar a demonstração do Lema 2.2.5. Sejam $\pi_P : P \to P/\operatorname{rad}(P)$ e $\pi_U : U \to U/\operatorname{rad}(U)$ as projeções canônicas e seja ψ um isomorfismo entre $U/\operatorname{rad}(U)$ e $P/\operatorname{rad}(P)$. Como π_U é sobrejetor, uma das caracterizações de módulos projetivos nos dá um homomorfismo $\varphi : P \to U$ tal que $\pi_U\varphi = \psi\pi_P$. Ou seja, temos o seguinte diagrama comutativo:

$$\begin{array}{ccc} P & \xrightarrow{\varphi} & U \\ {\scriptstyle \pi_P}\downarrow & & \downarrow{\scriptstyle \pi_U} \\ \dfrac{P}{\operatorname{rad}(P)} & \xrightarrow[\psi]{} & \dfrac{U}{\operatorname{rad}(U)} \end{array}$$

Vamos mostrar que φ é sobrejetor. Suponha, por absurdo, que esse não seja o caso. Se $V = \varphi(P) \leq U$, então V é um submódulo próprio de U e existe $M \leq U$ maximal com $V \subseteq M$. Como $\operatorname{rad}(U)$ é a interseção dos submódulos maximais de U, temos $\operatorname{rad}(U) \subseteq M$ e então $V + \operatorname{rad}(U) \subseteq M$. Portanto,

$$\pi_U(V) = \frac{V + \operatorname{rad}(U)}{\operatorname{rad}(U)} \subseteq \frac{M}{\operatorname{rad}(U)} \subsetneq \frac{U}{\operatorname{rad}(U)}.$$

Mas isso é uma contradição, pois $\pi_U(V)$ é a imagem de $\pi_U\varphi = \psi\pi_P$, que é sobrejetor por ser a composta dos mapas sobrejetores ψ e π_P. Logo, φ deve ser sobrejetor e então U é um quociente de P.

Note que apenas utilizamos que ψ é sobrejetor. Além disso, o argumento final para mostrar que φ é sobrejetor se aplica em um contexto maior: é uma propriedade de *epimorfismos essenciais*. Eles serão estudados na Seção 5.3. Mais especificamente, como ψ é sobrejetor, então $\pi_U\varphi = \psi\pi_P$ também é sobrejetor e, como π_U é epimorfismo essencial (Lema 5.3.2), segue do Lema 5.3.1 que φ é sobrejetor. □

Exercício A.2.7. Mostre que um A-módulo P é projetivo se, e somente se, para toda sequência exata de A-módulos

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0,$$

a sequência correspondente

$$0 \longrightarrow \mathrm{Hom}_A(P,U) \longrightarrow \mathrm{Hom}_A(P,V) \longrightarrow \mathrm{Hom}_A(P,W) \longrightarrow 0$$

também é exata[1].

Solução: Sejam $\varphi : U \to V$ e $\psi : V \to W$ os homomorfismos não triviais que aparecem na primeira sequência. Assim, na segunda sequência, o primeiro mapa leva um homomorfismo $f \in \mathrm{Hom}_A(P,U)$ em $\varphi f \in \mathrm{Hom}_A(P,V)$. Analogamente, o segundo mapa leva um homomorfismo $g \in \mathrm{Hom}_A(P,V)$ em $\psi g \in \mathrm{Hom}_A(P,W)$. É um resultado conhecido que, para todo A-módulo P, o funtor $\mathrm{Hom}_A(P,-)$ é exato à esquerda, ou seja, para toda sequência exata

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0,$$

a sequência correspondente

$$0 \longrightarrow \mathrm{Hom}_A(P,U) \longrightarrow \mathrm{Hom}_A(P,V) \longrightarrow \mathrm{Hom}_A(P,W)$$

também é exata. Note que o último mapa da segunda sequência não é necessariamente sobrejetor. Não é complicado provar isso e deixamos a cargo do leitor.

Logo, o exercício nos pede para mostrar que P é projetivo se e somente se, dado um homomorfismo sobrejetor $\psi : V \to W$, o homomorfismo induzido $\mathrm{Hom}_A(P,V) \to \mathrm{Hom}_A(P,W)$ também é sobrejetor. Em outras palavras, queremos mostrar que P é projetivo se e somente se, dados $\psi : V \to W$ sobrejetor e $h : P \to W$ qualquer, existe $g : P \to V$ tal que $h = \psi g$. Isso é exatamente a caracterização (3) da Proposição 2.2.1! □

Exercício A.2.8. Se S é um A-módulo simples e P é a sua cobertura projetiva, mostre que a multiplicidade de S como um fator de composição de um A-módulo U é igual a[2]

$$\frac{\dim_k \mathrm{Hom}_A(P,U)}{\dim_k \mathrm{End}_A(S)}.$$

Solução: Se V é um submódulo de U, então temos uma sequência exata canônica

$$0 \longrightarrow V \longrightarrow U \longrightarrow U/V \longrightarrow 0.$$

Como P é projetivo, o Exercício A.2.7 nos diz que a sequência correspondente

$$0 \longrightarrow \mathrm{Hom}_A(P,V) \longrightarrow \mathrm{Hom}_A(P,U) \longrightarrow \mathrm{Hom}_A(P,U/V) \longrightarrow 0$$

também é exata. Em particular, vale a igualdade

$$\dim_k \mathrm{Hom}_A(P,U) = \dim_k \mathrm{Hom}_A(P,V) + \dim_k \mathrm{Hom}_A(P,U/V).$$

Assim, se

$$0 = U_0 \subseteq U_1 \subseteq U_2 \subseteq \cdots \subseteq U_{n-1} \subseteq U_n = U$$

é uma série de composição de U, repetidas aplicações da igualdade acima implicam em

$$\dim_k \mathrm{Hom}_A(P,U) = \sum_{i=1}^{n} \dim_k \mathrm{Hom}_A(P,U_i/U_{i-1}).$$

[1] Ou seja, P é projetivo se e somente se o funtor $\mathrm{Hom}_A(P,-)$ (que vai da categoria dos A-módulos para a categoria dos k-espaços vetoriais) é exato.

[2] Quando k é algebricamente fechado, o Lema de Schur diz que $\dim_k \mathrm{End}_A(S) = 1$ e então a expressão se simplifica.

Vamos encontrar a dimensão de $\mathrm{Hom}_A(P, U_i/U_{i-1})$. Como U_i/U_{i-1} é simples, vale que $\mathrm{rad}(P)$ está contido no núcleo de qualquer homomorfismo de P em U_i/U_{i-1}, de modo que o Teorema do Homomorfismo nos dá um isomorfismo linear

$$\mathrm{Hom}_A(P, U_i/U_{i-1}) \cong \mathrm{Hom}_A\left(\frac{P}{\mathrm{rad}(P)}, \frac{U_i}{U_{i-1}}\right).$$

Como $P/\mathrm{rad}(P) \cong S$, temos dois casos: ou U_i/U_{i-1} não é isomorfo a S e então não existem homomorfismos não nulos de $P/\mathrm{rad}(P)$ em U_i/U_{i-1}, ou $U_i/U_{i-1} \cong S$ e o espaço de homomorfismos acima é isomorfo a $\mathrm{End}_A(S)$. Portanto, se m é a multiplicidade de S como fator de composição de U, concluímos que

$$\dim_k \mathrm{Hom}_A(P, U) = \sum_{i=1}^{n} \dim_k \mathrm{Hom}_A(P, U_i/U_{i-1}) = m \cdot \dim_k \mathrm{End}_A(S),$$

provando o exercício. Observe que, quando k é algebricamente fechado, o Lema de Schur diz que $\dim_k \mathrm{End}_A(S) = 1$ e então temos $m = \dim_k \mathrm{Hom}_A(P, U)$. □

Exercício A.2.9. Vamos encontrar explicitamente o módulo W do Exemplo 2.2.12. Com as hipóteses e as notações desse exemplo, sabemos pelo Teorema de Schur-Zassenhaus que $G = N \rtimes H$ para algum subgrupo H. Se $h \in H$, seja $a(h)$ um inteiro tal que $hxh^{-1} = x^{a(h)}$, onde x é um gerador de N fixado. Defina $\alpha(h) = a(h) \cdot 1 \in k$.

(a) Mostre que existe um kG-módulo de dimensão 2 com uma base $\{u, v\}$ tal que

$$xu = u + v, \quad xv = v$$

e

$$hu = u, \quad hv = \alpha(h)v,$$

para todo $h \in H$.

(b) Prove que o módulo do item anterior é isomorfo a M.

(c) Encontre uma descrição explícita de W.

Solução: (a) Faremos algumas observações iniciais. Para relembrar, quando escrevemos $G = N \rtimes H$ queremos dizer que G é o produto semidireto de N e H, ou seja, que $G = NH$ e que $N \cap H = \{1\}$. O único fato que usaremos é que todo elemento de G se escreve *de modo único* como o produto de um elemento de N com um elemento de H. Se $h \in H$, como N é normal em G, hxh^{-1} está em N e de fato é uma potência de x. Veja que o inteiro $a(h)$ está definido apenas módulo a ordem de x. Como a ordem de x é uma potência de p e $\mathrm{char}(k) = p$, $\alpha(h)$ independe da escolha de $a(h)$. Agora, se $h_1, h_2 \in H$, então

$$(h_1h_2)x(h_1h_2)^{-1} = h_1(h_2xh_2^{-1})h_1^{-1} = h_1x^{a(h_2)}h_1^{-1} = (h_1xh_1^{-1})^{a(h_2)} = x^{a(h_1)a(h_2)}.$$

Como $\alpha(h)$ independe da escolha de $a(h)$, isso prova que $\alpha(h_1h_2) = \alpha(h_1)\alpha(h_2)$, ou seja, α é um homomorfismo de grupos de H em $k^\times$.

Para provar esse primeiro item, é suficiente encontrar um homomorfismo de G em $\mathrm{GL}_2(k)$ (o grupo das matrizes 2×2 inversíveis com entradas em k) que leva x em

$$X \coloneqq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

e $h \in H$ em

$$Y_h \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & \alpha(h) \end{pmatrix}.$$

Somos forçados a definir $\varphi : G \to \mathrm{GL}_2(k)$ por

$$\varphi(x^i h) = X^i Y_h$$

para todo i inteiro e $h \in H$. Aqui estamos usando que todo elemento de G é escrito de forma única como um produto entre elementos de N e H. Além disso, a princípio, o i deveria variar apenas entre 1 e a ordem de x, mas note que X tem ordem p e então φ continua bem definida se considerarmos i um inteiro qualquer. Resta verificar que φ é de fato um homomorfismo. Para isso, observe inicialmente que

$$\begin{aligned} Y_h X Y_h^{-1} &= \begin{pmatrix} 1 & 0 \\ 0 & \alpha(h) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \alpha(h)^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & \alpha(h) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & \alpha(h)^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ \alpha(h) & 1 \end{pmatrix} \\ &= X^{a(h)} \end{aligned}$$

para todo $h \in H$. Se $i, j \in \mathbb{Z}$ e $h, h' \in H$, então

$$\varphi(x^i h \cdot x^j h') = \varphi(x^i (h x^j h^{-1}) \cdot hh') = \varphi(x^{i+a(h)j} \cdot hh') = X^{i+a(h)j} Y_{hh'}.$$

Usando que α é homomorfismo e a conta da observação anterior, temos

$$\begin{aligned} X^{i+a(h)j} Y_{hh'} &= X^i (X^{a(h)})^j Y_{hh'} \\ &= X^i (Y_h X Y_h^{-1})^j Y_{hh'} \\ &= X^i Y_h \cdot X^j Y_{h^{-1}hh'} \\ &= \varphi(x^i h)\varphi(x^j h'). \end{aligned}$$

Concluímos que φ é homomorfismo, como preciso.

(b) Seja U o módulo do item anterior. Para mostrar que $U \cong M$, vamos imitar o que fizemos no Exemplo 2.2.12. Observe primeiramente que U não é semissimples. De fato, se fosse, pelo Teorema de Clifford, U_N seria semissimples e a ação de x seria trivial, o que não é o caso. Como a dimensão de U é 2, o comprimento de Loewy de U deve ser 2 e as camadas radicais são unidimensionais e portanto simples. Logo, U é unisseriado e possui um único submódulo de dimensão 1, que é o subespaço gerado por v, como se vê facilmente. Esse submódulo é o radical de U, logo obtemos da descrição de U que $U/\operatorname{rad}(U)$ é o módulo trivial. Pelo Lema 2.2.5, U é um quociente da cobertura projetiva Q do módulo trivial. Mas $\operatorname{rad}^2(U) = 0$, então U também é quociente de $Q/\operatorname{rad}^2(Q) = M$. Como M também tem dimensão 2, concluímos que $U \cong M$.

(c) Vimos no Exemplo 2.2.12 que $W = \operatorname{rad}(M)$. Assim, W é isomorfo ao subespaço de U gerado por v. Note que um elemento $x^i h$ qualquer de G leva v em $\alpha(h)v$. Isso nos dá um descrição explícita de W em termos da estrutura de G.

□

Exercício A.2.10. Sejam U e V kG-módulos. Se $f : V^* \to U^*$ é um homomorfismo, mostre que existe um homomorfismo $\rho : U \to V$ tal que $f = \rho^*$.

Solução: Começamos provando que existe uma transformação linear $\rho : U \to V$ tal que $f = \rho^*$. Para isso, veja a transposta como uma função de $\operatorname{Hom}_k(U, V)$ em $\operatorname{Hom}_k(V^*, U^*)$. É fácil mostrar que essa função é linear e injetora. Mas o domínio e o contradomínio têm a mesma dimensão (que

é $\dim_k U \cdot \dim_k V$), logo essa transformação linear também é sobrejetora e ρ existe. Agora, pela Observação 2.3.5, vale que

$$\rho = \Psi_V^{-1}\rho^{**}\Psi_U = \Psi_V^{-1}f^*\Psi_U,$$

onde $\Psi_U : U \to U^{**}$ e $\Psi_V : V \to V^{**}$ são os isomorfismos naturais canônicos. Note que f^* é homomorfismo pois f o é. Assim, ρ é a composição de homomorfismos de kG-módulos e, por isso, também é um homomorfismo.

Um outro jeito de provar o exercício é notar que o isomorfismo linear

$$\mathrm{Hom}_k(U, V) \to \mathrm{Hom}_k(V^*, U^*)$$

é um isomorfismo de kG-módulos com a estrutura dada no Exemplo 1.3.5. De fato, sejam $\rho \in \mathrm{Hom}_k(U, V)$ e $g \in G$ quaisquer. Então

$$(g\rho)^*(\varphi) = \varphi \circ (g\rho)$$

e

$$(g\rho^*)(\varphi) = g(\rho^*(g^{-1}\varphi)) = g((g^{-1}\varphi) \circ \rho)$$

para todo $\varphi \in V^*$. Agora, dado $u \in U$ qualquer, temos

$$(\varphi \circ (g\rho))(u) = \varphi((g\rho)(u)) = \varphi(g\rho(g^{-1}u))$$

e

$$(g((g^{-1}\varphi) \circ \rho))(u) = ((g^{-1}\varphi) \circ \rho)(g^{-1}u) = (g^{-1}\varphi)(\rho(g^{-1}u)) = \varphi(g\rho(g^{-1}u)),$$

mostrando que $(g\rho)^*(\varphi) = (g\rho^*)(\varphi)$ para todo $\varphi \in V^*$, ou seja, $(g\rho)^* = g\rho^*$, como preciso. Em particular, esse isomorfismo de kG-módulos se restringe a um isomorfismo linear do subespaço de $\mathrm{Hom}_k(U, V)$ formado pelos vetores fixos por G no subespaço correspondente de $\mathrm{Hom}_k(V^*, U^*)$. Em outras palavras, a transposta nos dá um isomorfismo linear entre $\mathrm{Hom}_{kG}(U, V)$ e $\mathrm{Hom}_{kG}(V^*, U^*)$. Assim, dado $f \in \mathrm{Hom}_{kG}(V^*, U^*)$, existe um único $\rho \in \mathrm{Hom}_{kG}(U, V)$ tal que $f = \rho^*$. □

Exercício A.2.11. Mostre que um A-módulo I é injetivo se, e somente se, para toda sequência exata de A-módulos

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0,$$

a sequência correspondente

$$0 \longrightarrow \mathrm{Hom}_A(W, I) \longrightarrow \mathrm{Hom}_A(V, I) \longrightarrow \mathrm{Hom}_A(U, I) \longrightarrow 0$$

também é exata.

Solução: Esse exercício é muito semelhante ao Exercício A.2.7. Desta vez, se $\varphi : U \to V$ e $\psi : V \to W$ são os homomorfismos não triviais da primeira sequência exata, então os homomorfismos correspondentes na segunda sequência levam $f \in \mathrm{Hom}_A(W, I)$ em $f\psi \in \mathrm{Hom}_A(V, I)$ e $g \in \mathrm{Hom}_A(V, I)$ em $g\varphi \in \mathrm{Hom}_A(U, I)$. É um resultado conhecido que, para todo A-módulo I, o funtor (contravariante) $\mathrm{Hom}_A(-, I)$ é exato à esquerda, ou seja, para toda sequência exata

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0,$$

a sequência correspondente

$$0 \longrightarrow \mathrm{Hom}_A(W, I) \longrightarrow \mathrm{Hom}_A(V, I) \longrightarrow \mathrm{Hom}_A(U, I)$$

também é exata. Note que o último mapa da segunda sequência não é necessariamente sobrejetor. Não é complicado provar isso e deixamos a cargo do leitor.

Logo, o exercício nos pede para mostrar que I é injetivo se e somente se, dado um homomorfismo injetor $\varphi : U \to V$, o homomorfismo induzido $\mathrm{Hom}_A(V, I) \to \mathrm{Hom}_A(U, I)$ é sobrejetor. Em outras palavras, queremos mostrar que I é injetivo se e somente se, dados $\varphi : U \to V$ injetor e $h : U \to I$ qualquer, existe $g : V \to I$ tal que $h = g\varphi$. Isso é exatamente a caracterização (2) da Proposição 2.3.13! □

Exercício A.2.12. Se S é um A-módulo simples e I é um A-módulo injetivo com $\operatorname{soc}(I) \cong S$, mostre que a multiplicidade de S como um fator de composição de um A-módulo U é igual a

$$\frac{\dim_k \operatorname{Hom}_A(U, I)}{\dim_k \operatorname{End}_A(S)}.$$

Solução: Antes de começar a solução, faremos um comentário. O enunciado deste exercício é dual ao enunciado do Exercício A.2.8. Em particular, I atua como o conceito dual de uma cobertura projetiva de S. Nesse caso, I é uma *envolvente injetiva* de S. As envolventes injetivas serão estudadas em mais detalhes na Seção 5.3.

Voltando à solução, seja

$$0 = U_0 \subseteq U_1 \subseteq U_2 \subseteq \cdots \subseteq U_{n-1} \subseteq U_n = U$$

uma série composição de U. De modo muito análogo ao que fizemos no Exercício A.2.8, a injetividade de I juntamente com o Exercício A.2.11 implicam em

$$\dim_k \operatorname{Hom}_A(U, I) = \sum_{i=1}^{n} \dim_k \operatorname{Hom}_A(U_i/U_{i-1}, I).$$

Vamos encontrar a dimensão de $\operatorname{Hom}_A(U_i/U_{i-1}, I)$. Como U_i/U_{i-1} é simples, vale que a imagem de qualquer homomorfismo de U_i/U_{i-1} em I está contida em $\operatorname{soc}(I)$, de onde temos um isomorfismo linear

$$\operatorname{Hom}_A(U_i/U_{i-1}, I) \cong \operatorname{Hom}_A(U_i/U_{i-1}, \operatorname{soc}(I)).$$

Como $\operatorname{soc}(I) \cong S$, temos dois casos: ou U_i/U_{i-1} não é isomorfo a S e então não existem homomorfismos não nulos de U_i/U_{i-1} em $\operatorname{soc}(I)$, ou $U_i/U_{i-1} \cong S$ e o espaço de homomorfismos acima é isomorfo a $\operatorname{End}_A(S)$. Portanto, se m é a multiplicidade de S como fator de composição de U, concluímos que

$$\dim_k \operatorname{Hom}_A(U, I) = \sum_{i=1}^{n} \dim_k \operatorname{Hom}_A(U_i/U_{i-1}, I) = m \cdot \dim_k \operatorname{End}_A(S),$$

provando o exercício. Observe que, quando k é algebricamente fechado, o Lema de Schur diz que $\dim_k \operatorname{End}_A(S) = 1$ e então temos $m = \dim_k \operatorname{Hom}_A(U, I)$. □

Exercício A.2.13. Sejam S e T kG-módulos simples e sejam P_S e P_T as suas respectivas coberturas projetivas. Mostre que, se k é algebricamente fechado, então a multiplicidade de S como um fator de composição de P_T é igual à multiplicidade de T como um fator de composição de P_S. O que acontece se k não for algebricamente fechado?

Solução: Como k é algebricamente fechado, o Lema de Schur diz que $\operatorname{End}_{kG}(S)$ e $\operatorname{End}_{kG}(T)$ são isomorfos a k e, por isso, são unidimensionais. Assim, o Exercício A.2.8 diz que a multiplicidade m de S como um fator de composição de P_T é $\dim_k \operatorname{Hom}_{kG}(P_S, P_T)$. Por outro lado, sabemos que P_T é injetivo e, pelo Teorema 2.3.17, $\operatorname{soc}(P_T) \cong T$. Assim, o Exercício A.2.12 nos mostra que a multiplicidade n de T como um fator de composição de P_S também é $\dim_k \operatorname{Hom}_{kG}(P_S, P_T)$, provando o exercício. Quando k não é algebricamente fechado, não temos controle sobre as dimensões de $\operatorname{End}_{kG}(S)$ e $\operatorname{End}_{kG}(T)$, valendo apenas a igualdade

$$m \cdot \dim_k \operatorname{End}_{kG}(S) = n \cdot \dim_k \operatorname{End}_{kG}(T).$$

Mesmo assim, essa informação já é valiosa. Por exemplo, se S não aparece como fator de composição de P_T, já sabemos que T não é fator de composição de P_S, mesmo quando o corpo base não é algebricamente fechado. □

Exercício A.2.14. Sejam S um kG-módulo simples e P a sua cobertura projetiva. Se U é um kG-módulo qualquer e o decompomos como soma de indecomponíveis, mostre que a multiplicidade com a qual P aparece é igual a

$$\frac{\dim_k \operatorname{Hom}_{kG}(P,U) - \dim_k \operatorname{Hom}_{kG}(P/\operatorname{soc}(P),U)}{\dim_k \operatorname{End}_{kG}(S)}$$

e também a

$$\frac{\dim_k \operatorname{Hom}_{kG}(U,P) - \dim_k \operatorname{Hom}_{kG}(U,\operatorname{rad}(P))}{\dim_k \operatorname{End}_{kG}(S)}.$$

Solução: Note que

$$\operatorname{Hom}_{kG}(V_1 \oplus V_2, W) \cong \operatorname{Hom}_{kG}(V_1,W) \oplus \operatorname{Hom}_{kG}(V_2,W)$$

e

$$\operatorname{Hom}_{kG}(V, W_1 \oplus W_2) \cong \operatorname{Hom}_{kG}(V,W_1) \oplus \operatorname{Hom}_{kG}(V,W_2)$$

para quaisquer kG-módulos, V_1, V_2, V, W_1, W_2 e W. Por isso, as duas quantidades do enunciado são "aditivas" na "coordenada" U. Logo, podemos supor que U é indecomponível e devemos mostrar que as frações valem 1 se $U \cong P$ e 0 caso contrário.

Suponha inicialmente que $U = P$. Pelo Exercício A.2.8,

$$\frac{\dim_k \operatorname{Hom}_{kG}(P,P)}{\dim_k \operatorname{End}_{kG}(S)}$$

é a multiplicidade de S como fator de composição de P. Por outro lado, esse mesmo exercício mostra que

$$\frac{\dim_k \operatorname{Hom}_{kG}(P,\operatorname{rad}(P))}{\dim_k \operatorname{End}_{kG}(S)}$$

é a multiplicidade de S como fator de composição de $\operatorname{rad}(P)$ e, como $P/\operatorname{rad}(P) \cong S$, essa multiplicidade é um a menos do que a multiplicidade anterior. Concluímos que

$$\frac{\dim_k \operatorname{Hom}_{kG}(U,P) - \dim_k \operatorname{Hom}_{kG}(U,\operatorname{rad}(P))}{\dim_k \operatorname{End}_{kG}(S)} = 1.$$

Do mesmo modo, como P é injetivo (Teorema 2.3.14) e seu soco é isomorfo a S (Teorema 2.3.17), o Exercício A.2.12 mostra que

$$\frac{\dim_k \operatorname{Hom}_{kG}(P/\operatorname{soc}(P),P)}{\dim_k \operatorname{End}_{kG}(S)}$$

é a multiplicidade de S como fator de composição de $P/\operatorname{soc}(P)$ e, como $\operatorname{soc}(P) \cong S$, concluímos como antes que

$$\frac{\dim_k \operatorname{Hom}_{kG}(P,U) - \dim_k \operatorname{Hom}_{kG}(P/\operatorname{soc}(P),U)}{\dim_k \operatorname{End}_{kG}(S)} = 1.$$

Suponhamos agora que $U \ncong P$. Para mostrar que as duas frações do enunciado são iguais a 0, basta verificamos que

$$\operatorname{Hom}_{kG}(P,U) \cong \operatorname{Hom}_{kG}(P/\operatorname{soc}(P),U) \quad \text{e} \quad \operatorname{Hom}_{kG}(U,P) \cong \operatorname{Hom}_{kG}(U,\operatorname{rad}(P)).$$

Para o primeiro isomorfismo, basta mostrar que qualquer homomorfismo de P em U contém $\operatorname{soc}(P)$ no núcleo. Mas $\operatorname{soc}(P)$ é simples, então $\operatorname{soc}(P)$ é o único submódulo minimal de P e qualquer submódulo não nulo contém $\operatorname{soc}(P)$. Por isso, devemos mostrar que qualquer homomorfismo de P em U não é injetor. De fato, se existisse um homomorfismo injetor $P \to U$, então esse homomorfismo cindiria, porque P é injetivo, e, assim, P seria isomorfo a um somando direto de U.

Mas U é indecomponível e não isomorfo a P, então isso não pode acontecer! Analogamente, para o segundo isomorfismo, basta mostrar que qualquer homomorfismo de U em P possui imagem contida em $\operatorname{rad}(P)$. Mas $P/\operatorname{rad}(P)$ é simples, então $\operatorname{rad}(P)$ é o único submódulo maximal de P e qualquer submódulo diferente do próprio P está contido em $\operatorname{rad}(P)$. Portanto, devemos verificar que qualquer homomorfismo de U em P não é sobrejetor. Com efeito, se existisse um homomorfismo sobrejetor $U \to P$, então esse homomorfismo cindiria, porque P é projetivo, e, assim, P seria isomorfo a um somando direto de U. Como antes, isso não pode ocorrer. □

Exercício A.2.15. Prove que qualquer quociente não nulo de um A-módulo projetivo indecomponível é também indecomponível. Se $A = kG$ é uma álgebra de grupo, mostre que o mesmo vale se trocarmos "quociente" por "submódulo".

Solução: Sejam P um A-módulo projetivo indecomponível e U um quociente não nulo de P. Então temos um homomorfismo sobrejetor de P em U e, pelo Exercício A.1.3, o radical de P é levado no radical de U, o que induz um homomorfismo sobrejetor de $P/\operatorname{rad}(P)$ em $U/\operatorname{rad}(U)$. Mas $P/\operatorname{rad}(P)$ é simples pelo Teorema 2.2.4, logo esse último homomorfismo sobrejetor deve ser um isomorfismo e também temos $U/\operatorname{rad}(U)$ simples. Pelo Exemplo 2.1.11, U é indecomponível.

Se $A = kG$ e se V é um submódulo não nulo de P, então a solução do Exercício A.1.3 mostra que $\operatorname{soc}(V) \subseteq \operatorname{soc}(P)$. Mas $\operatorname{soc}(P)$ é simples pelo Corolário 2.3.16, então devemos ter $\operatorname{soc}(V) = \operatorname{soc}(P)$. Novamente pelo Exemplo 2.1.11, V é indecomponível. □

Exercício A.2.16. Prove que vale o "dual" do Lema 2.2.5 para kG-módulos: se U é um kG-módulo tal que $\operatorname{soc}(U)$ é simples, então U é um submódulo da cobertura projetiva de $\operatorname{soc}(U)$.

Solução: Vamos imitar a demonstração do Lema 2.2.5. Seja P a cobertura projetiva de $\operatorname{soc}(U)$. Pelo Teorema 2.3.17, $\operatorname{soc}(P) \cong P/\operatorname{rad}(P) \cong \operatorname{soc}(U)$. Seja $\psi : \operatorname{soc}(U) \to \operatorname{soc}(P)$ um isomorfismo e sejam $i_U : \operatorname{soc}(U) \to U$ e $i_P : \operatorname{soc}(P) \to P$ as inclusões. Pelo Teorema 2.3.14, P é injetivo e, como i_U é homomorfismo injetor, segue que existe um homomorfismo $\varphi : U \to P$ fazendo o seguinte diagrama comutar:

$$\begin{array}{ccc} U & \xrightarrow{\varphi} & P \\ {\scriptstyle i_U}\uparrow & & \uparrow{\scriptstyle i_P} \\ \operatorname{soc}(U) & \xrightarrow[\psi]{} & \operatorname{soc}(P) \end{array}$$

O exercício termina se mostrarmos que φ é injetor. De fato, se $\ker\varphi$ não fosse nulo, então ele conteria um submódulo simples. Mas $\operatorname{soc}(U)$ é simples e, portanto, é o único submódulo simples de U, de onde seguiria $\operatorname{soc}(U) \subseteq \ker\varphi$. Consequentemente, teríamos $\varphi i_U = 0$, um absurdo, porque $\varphi i_U = i_P\psi$ é a composição dos homomorfismos injetores i_P e ψ. Portanto, $\ker\varphi = 0$ e φ é injetor, como queríamos demonstrar. □

Exercício A.2.17. Suponha que $p > 0$ e que G possua um p-subgrupo de Sylow normal e cíclico. Mostre que todo kG-módulo indecomponível é um submódulo de um kG-módulo projetivo indecomponível.

Solução: Seja U um kG-módulo indecomponível. Pelo Exemplo 2.3.20, U é unisseriado. Em particular, $\operatorname{soc}(U)$ é simples e, pelo Exercício A.2.16, U é submódulo da cobertura projetiva de $\operatorname{soc}(U)$, que é um kG-módulo projetivo indecomponível. Note que tal projetivo indecomponível é unicamente determinado por U e que ele possui apenas um submódulo isomorfo a U, já que é unisseriado. □

Exercício A.2.18. Neste exercício, utilizaremos a notação do Exemplo 2.3.22.

(a) Encontre explicitamente $\operatorname{End}_{kS_3}(U)$.

(b) Use o Exercício A.1.10 para concluir que k, k_{sgn} e U são todos os kS_3-módulos simples.

(c) Encontre as multiplicidades de k, k_{sgn} e U em $kD_{15}/\operatorname{rad}(kD_{15})$.

Solução: (a) Vamos mostrar que $\operatorname{End}_{kS_3}(U)$ consiste apenas dos múltiplos da identidade. Pela definição de U, existe uma base $\{x, y\}$ de U tal que

$$(1\ 2)\cdot x = y, \quad (1\ 2)\cdot y = x$$

e

$$(1\ 2\ 3)\cdot x = y, \quad (1\ 2\ 3)\cdot y = -x - y.$$

Se $\varphi \in \operatorname{End}_{kS_3}(U)$, então existe $\lambda, \mu \in k$ tais que

$$\varphi(x) = \lambda x + \mu y,$$

já que x e y formam uma base de U. Assim,

$$\varphi(y) = \varphi((1\ 2)\cdot x) = (12)\cdot\varphi(x) = (1\ 2)\cdot(\lambda x + \mu y) = \mu x + \lambda y.$$

Também temos

$$\varphi((1\ 2\ 3)\cdot x) = \varphi(y) = \mu x + \lambda y$$

e

$$\varphi((1\ 2\ 3)\cdot x) = (1\ 2\ 3)\cdot\varphi(x) = (1\ 2\ 3)\cdot(\lambda x + \mu y) = (-\mu)x + (\lambda - \mu)y,$$

logo $\mu = 0$. Segue que $\varphi(x) = \lambda x$ e $\varphi(y) = \lambda y$, ou seja, $\varphi = \lambda \cdot \mathrm{id}_U$, provando o que queríamos.

(b) Como $\operatorname{char}(k) = 5$ não é um divisor de $|S_3| = 6$, o Teorema de Maschke nos diz que kS_3 é semissimples. Assim, podemos aplicar o Exercício A.1.10 para obter que a multiplicidade de um kG-módulo simples S como fator de composição (somando direto) de kS_3 é $\dim_{\operatorname{End}_{kS_3}(S)} S$. Aqui, a ação de $\varphi \in \operatorname{End}_{kS_3}(S)$ em $s \in S$ é dada do jeito natural: $\varphi{\cdot}s = \varphi(s)$. Mas vimos que $\operatorname{End}_{kS_3}(U)$ consiste apenas dos múltiplos da identidade, de modo que a estrutura de U como $\operatorname{End}_{kS_3}(U)$-módulo é exatamente a sua estrutura de k-espaço vetorial. Portanto, a multiplicidade de U em kS_3 é

$$\dim_{\operatorname{End}_{kS_3}(U)} U = \dim_k U = 2.$$

Como k e k_{sgn} são unidimensionais, também vemos que $\operatorname{End}_{kS_3}(k)$ e $\operatorname{End}_{kS_3}(k_{\text{sgn}})$ consistem dos múltiplos da identidade, de modo que as multiplicidades de k e k_{sgn} em kS_3 são ambas iguais a

$$\dim_k k = \dim_k k_{\text{sgn}} = 1.$$

Somando a dimensão desses fatores de composição (com as multiplicidades), obtemos $2+2+1+1=6$, que é a dimensão de kS_3. Dessa forma, estes são os únicos fatores de composição de kS_3. Consequentemente, vale que k, k_{sgn} e U são todos os kS_3-módulos simples.

(c) Como $kD_{15}/\operatorname{rad}(kD_{15})$ é semissimples, podemos prosseguir como no item anterior. Mas, se S denota qualquer um dos três módulos simples em questão, note que uma transformação linear $\varphi : S \to S$ é homomorfismo de $kD_{15}/\operatorname{rad}(kD_{15})$-módulos se e só se é um homomorfismo de kD_{15}-módulos. Isso ocorre pois passamos da estrutura de $kD_{15}/\operatorname{rad}(kD_{15})$-módulo de S para a estrutura de kD_{15}-módulo através do homomorfismo de álgebras $kD_{15} \to kD_{15}/\operatorname{rad}(kD_{15})$, que é sobrejetor. Com isso,

$$\operatorname{End}_{kD_{15}/\operatorname{rad}(kD_{15})}(S) = \operatorname{End}_{kD_{15}}(S).$$

Mas a estrutura de S como kD_{15}-módulo foi obtida por restrição da estrutura como kS_3-módulo através de um homomorfismo $kD_{15} \to kS_3$ também sobrejetor. Logo, com o mesmo argumento,

$$\operatorname{End}_{kD_{15}}(S) = \operatorname{End}_{kS_3}(S).$$

Portanto, os itens anteriores nos dizem que a multiplicidade de U em $kD_{15}/\operatorname{rad}(kD_{15})$ é 2, enquanto as multiplicidades de k e k_{sgn} são ambas iguais a 1.

□

Exercício A.2.19. Este exercício dá uma prova da Proposição 2.4.7 sem a escolha de uma base. Seja U um kG-módulo. Mostre que a multiplicidade de todo kG-módulo simples S como fator de composição de $U \otimes kG$ quocientado por seu radical é

$$\frac{\dim_k U \cdot \dim_k S}{\dim_k \operatorname{End}_{kG}(S)}.$$

Use o Exercício A.2.6 para deduzir que $U \otimes kG \cong (kG)^{\dim_k U}$.

Solução: Pelo Exercício A.1.11, basta mostrarmos que

$$\dim_k \operatorname{Hom}_{kG}(U \otimes kG, S) = \dim_k U \cdot \dim_k S.$$

Pela Proposição 2.4.6,

$$\operatorname{Hom}_{kG}(U \otimes kG, S) \cong \operatorname{Hom}_{kG}(kG \otimes U, S) \cong \operatorname{Hom}_{kG}(kG, U^* \otimes S),$$

como espaços vetoriais. Mas kG é livre, então determinar um homomorfismo de kG em $U^* \otimes S$ é o mesmo que determinar uma função da base $\{1\}$ de kG em $U^* \otimes S$. Com isso, conseguimos um isomorfismo linear

$$\operatorname{Hom}_{kG}(kG, U^* \otimes S) \cong \operatorname{Hom}_k(k, U^* \otimes S)$$

e agora é fácil calcular a dimensão:

$$\dim_k \operatorname{Hom}_k(k, U^* \otimes S) = \dim_k(U^* \otimes S) = \dim_k U \cdot \dim_k S,$$

como queríamos.

Vamos concluir a parte final do exercício. No argumento anterior, podemos trocar U pelo módulo trivial para obter que a multiplicidade de cada módulo simples S em $kG/\operatorname{rad}(kG)$ é

$$\frac{\dim_k S}{\dim_k \operatorname{End}_{kG}(S)}.$$

Consequentemente, a multiplicidade de S em $(kG)^{\dim_k U}$ quocientado por seu radical é

$$\frac{\dim_k U \cdot \dim_k S}{\dim_k \operatorname{End}_{kG}(S)}.$$

Mas dois módulos semissimples são isomorfos se e somente se cada simples tem a mesma multiplicidade nesses dois módulos. Logo, se $n = \dim_k U$,

$$\frac{(kG)^n}{\operatorname{rad}((kG)^n)} \cong \frac{U \otimes kG}{\operatorname{rad}(U \otimes kG)}.$$

Como $(kG)^n$ é projetivo, o Exercício A.2.6 diz que $U \otimes kG$ é quociente de $(kG)^n$. Mas eles têm a mesma dimensão e então são isomorfos, como desejado. □

Exercício A.2.20. Se $p > 0$ e não divide a dimensão do kG-módulo U, prove que $U \otimes U^*$ possui um somando direto isomorfo ao módulo trivial. (*Dica:* Sabendo que $U \otimes U^* \cong \operatorname{Hom}_k(U, U)$ como kG-módulos, considere os múltiplos da identidade e as transformações lineares de traço zero.)

Solução: Lembre que temos os seguintes isomorfismos de kG-módulos:

$$U \otimes U^* \cong U^* \otimes U \cong \mathrm{Hom}_k(U, U) = \mathrm{End}_k(U).$$

Sejam V e W os subespaços de $\mathrm{End}_k(U)$ formados pelos múltiplos da identidade e pelas transformações lineares de traço zero, respectivamente. Vejamos que $\mathrm{End}_k(U)$ é a soma direta de V e W. Se $\varphi \in V \cap W$, então existe $\lambda \in k$ tal que $\varphi = \lambda \cdot \mathrm{id}_U$ e

$$0 = \mathrm{tr}(\varphi) = \mathrm{tr}(\lambda \cdot \mathrm{id}_U) = \lambda \cdot \mathrm{tr}(\mathrm{id}_U) = \lambda \cdot \dim_k U.$$

Como p não divide a dimensão de U, então $\dim_k U$ é inversível (se visto como elemento de k), de onde obtemos $\lambda = 0$ e $\varphi = 0$. Por isso, a interseção de V e W é trivial. Como a soma de suas dimensões é a dimensão de $\mathrm{End}_k(U)$, devemos ter $\mathrm{End}_k(U) = V \oplus W$. Vamos concluir provando que V e W são submódulos de $\mathrm{End}_k(U)$ e que V é trivial. Se $g \in G$, então temos uma transformação linear induzida $\rho_g \in \mathrm{End}_k(U)$. Pela definição da estrutura de kG-módulo de $\mathrm{End}_k(U)$, temos

$$g \cdot \varphi = \rho_g \circ \varphi \circ \rho_{g^{-1}} = \rho_g \circ \varphi \circ \rho_g^{-1}$$

para todos $g \in G$ e $\varphi \in \mathrm{End}_k(U)$. Como V está contido no centro da álgebra $\mathrm{End}_k(U)$, vale $g \cdot \varphi = \varphi$ para todos $g \in G$ e $\varphi \in V$, o que mostra que V é um submódulo de $\mathrm{End}_k(U)$ isomorfo ao trivial. Além disso, como o traço é invariante por conjugação, vale $g \cdot \varphi \in W$ para todos $g \in G$ e $\varphi \in W$, provando que W também é submódulo de $\mathrm{End}_k(U)$. Isso termina o exercício. □

Exercício A.2.21. Seja k um corpo algebricamente fechado de característica $p > 0$ e seja $G = \mathrm{SL}_2(p)$. Se U é um kG-módulo tal que $U \cong U^*$ e $\mathrm{End}_{kG}(U) \cong k$, mostre que U é simples.

Solução: Como utilizamos algumas vezes no Exemplo 2.4.14, todo kG-módulo simples S é isomorfo ao seu dual. Isso acontece porque S^* é simples e possui a mesma dimensão que S, mas, como vimos no Exemplo 1.3.17, há somente um módulo simples com a dimensão de S: o próprio S. Dessa forma, o Lema 2.3.3 nos dá que todo kG-módulo semissimples é isomorfo ao seu dual. Como $U/\operatorname{rad}(U)$ é semissimples, temos

$$\frac{U}{\operatorname{rad}(U)} \cong \left(\frac{U}{\operatorname{rad}(U)}\right)^*.$$

Usando a Proposição 2.3.9 e que $U \cong U^*$, vale

$$\left(\frac{U}{\operatorname{rad}(U)}\right)^* \cong \operatorname{soc}(U^*) \cong \operatorname{soc}(U).$$

Logo, temos um isomorfismo $\varphi : U/\operatorname{rad}(U) \to \operatorname{soc}(U)$. Se $\pi : U \to U/\operatorname{rad}(U)$ é a projeção canônica, então a composição $\varphi\pi$ é um homomorfismo sobrejetor de U em $\operatorname{soc}(U)$. Compondo com a inclusão $i : \operatorname{soc}(U) \to U$, obtemos um homomorfismo ψ de U em U cuja imagem é $\operatorname{soc}(U)$. Por hipótese, $\mathrm{End}_{kG}(U) \cong k$, ou seja, os homomorfismos de U em U são dados pelos múltiplos da identidade. Assim, existe $\lambda \in k$ tal que $\psi(u) = \lambda u$ para todo $u \in U$. Mas $\lambda \neq 0$, já que a imagem $\operatorname{soc}(U)$ não é nula, então λ é um escalar inversível e ψ é um isomorfismo. Portanto, devemos ter $U = \operatorname{soc}(U)$, logo U é semissimples. Como $\mathrm{End}_{kG}(U) \cong k$, concluímos que U é simples através do Exercício A.1.9. □

Exercício A.2.22. Seja k um corpo algebricamente fechado de característica $p > 0$ e seja $G = \mathrm{SL}_2(p)$. Neste exercício, utilizaremos as notações introduzidas no Exemplo 2.4.14.

(a) Se um kG-módulo indecomponível U é um somando direto de um produto tensorial de kG-módulos simples, prove que U é um somando direto de $V_2^{\otimes n}$ para algum inteiro $n \geq 0$.

(b) Mostre que podemos tomar $n \leq 2p - 2$ no item anterior.

(c) Mostre que P_1 é um somando direto de $V_2^{\otimes 2p-2}$ e que ele não é um somando direto de $V_2^{\otimes n}$ para $0 \leq n < 2p-2$.

Solução: (a) Basta mostrar que todo produto tensorial de kG-módulos simples é um somando direto de $V_2^{\otimes n}$ para algum inteiro $n \geq 0$. Na notação do Exemplo 2.4.14, seja

$$V_{i_1} \otimes V_{i_2} \otimes \cdots \otimes V_{i_r}$$

um produto tensorial de kG-módulos simples, onde $1 \leq i_j \leq p$ para todo $1 \leq j \leq r$. Podemos supor que todos os índices i_j são maiores do que 1, pois, como V_1 é o módulo trivial, podemos omitir toda aparição de V_{i_j} com $i_j = 1$ e, se todos os índices forem iguais a 1, então o produto tensorial é trivial e podemos tomar $n = 0$. Se $p = 2$, então vale

$$V_{i_1} \otimes V_{i_2} \otimes \cdots \otimes V_{i_r} = V_2^{\otimes r}$$

e a prova termina tomando $n = r$. Se $p > 2$, com o Lema 2.4.15 não é difícil ver que V_{i_j} é um somando direto de $V_2^{\otimes i_j - 1}$. Logo, aplicando o item (3) da Proposição 2.4.4 repetidas vezes, vemos que o produto tensorial de módulos simples em questão é um somando direto de

$$V_2^{\otimes i_1 - 1} \otimes V_2^{\otimes i_2 - 1} \otimes \cdots \otimes V_2^{\otimes i_r - 1} = V_2^{\otimes n},$$

onde $n = i_1 + i_2 + \cdots + i_r - r$.

(b) Inicialmente, vamos mostrar por indução que $V_2^{\otimes n}$ é a soma direta de um módulo semissimples com um módulo projetivo para todo $n \geq 0$. Se $n = 0$, então $V_2^{\otimes n} \cong V_1$ é simples. Agora, suponha que $n \geq 0$ e que $V_2^{\otimes n}$ seja a soma de um módulo semissimples S com um projetivo P. Então

$$V_2^{\otimes n+1} \cong V_2 \otimes (S \oplus P) \cong (V_2 \otimes S) \oplus (V_2 \otimes P).$$

Como P é projetivo, $V_2 \otimes P$ é projetivo pelo Corolário 2.4.8. Resta mostrar que $V_2 \otimes S$ é soma de semissimples com projetivo e, como o produto tensorial distribui pela soma, podemos supor que S é simples. Se $S \cong V_1$, então $V_2 \otimes V_1 \cong V_2$ é simples. Por outro lado, se $S = V_p$, então S é projetivo e $V_2 \otimes S$ é projetivo. Por fim, se $p > 2$ e $S = V_n$ com $2 \leq n < p$, então, pelo Lema 2.4.15, $V_2 \otimes V_n \cong V_{n-1} \oplus V_{n+1}$ é semissimples. Dessa forma, vemos que $V_2^{\otimes n+1}$ é a soma direta de um módulo semissimples com um projetivo, como preciso.

Se U é um somando direto indecomponível de $V_2^{\otimes n}$, então o Teorema de Krull-Schmidt e o que acabamos de provar mostram que U é simples ou U é projetivo indecomponível. Assim, basta descobrir em quais potências tensoriais de V_2 os simples $V_1, \ldots, V_p$ e os projetivos indecomponíveis $P_1, \ldots, P_{p-1}, P_p = V_p$ aparecem.

Começamos com o caso $p = 2$. Então V_1 aparece em $V_2^{\otimes 0}$ e V_2 aparece em $V_2^{\otimes 1}$. Como V_2 é projetivo, então $V_2 \otimes V_2$ também o é. Logo, seus somandos indecomponíveis são isomorfos a V_2 ou a P_1. Mas se apenas houvessem somandos isomorfos a V_2, então $V_2^{\otimes n}$ seria a soma direta de cópias de V_2 para todo $n \geq 1$ e P_1 nunca apareceria numa potência tensorial de V_2, o que contradiz o Teorema 2.4.12. Portanto, P_1 aparece em $V_2^{\otimes 2}$. Consequentemente, o valor de n no item (a) pode ser tomado com $n \leq 2 = 2p - 2$. Observe também que o menor valor de n para o qual P_1 é um somando direto de $V_2^{\otimes n}$ também é $n = 2 = 2p - 2$.

Vamos para o caso $p = 3$. Como vimos no Exemplo 2.4.14, temos os seguintes isomorfismos:

$$\begin{aligned} V_2 \otimes V_2 &\cong V_1 \oplus V_3, \\ V_2 \otimes V_3 &\cong P_2, \\ V_2 \otimes P_2 &\cong P_1 \oplus V_3 \oplus V_3 \oplus V_3. \end{aligned}$$

Com isso, é fácil ver que todos os simples e todos os projetivos indecomponíveis aparecem em $V_2^{\otimes n}$ quando variamos n de 0 a $4 = 2p-2$. Além disso, o menor valor de n tal que P_1 é um somando direto de $V_2^{\otimes n}$ é $n = 4 = 2p-2$.

Por fim, suponha $p > 3$. Como vimos no Exemplo 2.4.14, temos os seguintes isomorfismos:

$$\begin{aligned} V_2 \otimes V_n &\cong V_{n-1} \oplus V_{n+1} \quad (2 \leq n < p), \\ V_2 \otimes V_p &\cong P_{p-1}, \\ V_2 \otimes P_{p-1} &\cong P_{p-2} \oplus V_p \oplus V_p, \\ V_2 \otimes P_n &\cong P_{n-1} \oplus P_{n+1} \quad (2 < n \leq p-2), \\ V_2 \otimes P_2 &\cong P_1 \oplus P_3 \oplus V_p. \end{aligned}$$

Assim, não é difícil ver que todos os simples e todos os projetivos indecomponíveis aparecem em $V_2^{\otimes n}$ quando variamos n de 0 a $2p-2$. Além disso, o menor valor de n tal que P_1 é um somando direto de $V_2^{\otimes n}$ é $n = 2p-2$.

(c) Já fizemos no item anterior.

□

A.3 Módulos e subgrupos

Exercício A.3.1. Sejam U um kG-módulo e V um kH-módulo.

(a) Se $\gamma \in \mathrm{Hom}_{kH}(U_H, V)$, mostre que a função γ' que leva $u \in U$ em

$$\sum_{s \in [G/H]} s \otimes \gamma(s^{-1}u) \in V^G$$

é um homomorfismo de kG-módulos.

(b) Prove que a função que leva γ em γ' é um isomorfismo linear de $\mathrm{Hom}_{kH}(U_H, V)$ em $\mathrm{Hom}_{kG}(U, V^G)$.

(c) Seja $\pi : V^G \to V$ o homomorfismo de kH-módulos que leva $1 \otimes v$ em v e $s \otimes v$ em 0, para $v \in V$, $s \in G$, $s \notin H$. Se $\gamma \in \mathrm{Hom}_{kH}(U_H, V)$, verifique que $\pi\gamma' = \gamma$.

Solução: (a) É imediato que γ' é uma transformação linear. Vejamos que ela preserva a estrutura de kG-módulo. Sejam $u \in U$ e $g \in G$. Então

$$\gamma'(gu) = \sum_{s \in [G/H]} s \otimes \gamma(s^{-1}gu) = g \cdot \sum_{s \in [G/H]} (g^{-1}s) \otimes \gamma((g^{-1}s)^{-1}u).$$

Para cada $s \in [G/H]$, existem $t_s \in [G/H]$ e $h_s \in H$ tais que $g^{-1}s = t_s h_s$. Por isso[1],

$$\begin{aligned} \gamma'(gu) &= g \cdot \sum_{s \in [G/H]} (t_s h_s) \otimes \gamma(h_s^{-1} t_s^{-1} u) \\ &= g \cdot \sum_{s \in [G/H]} t_s \otimes h_s h_s^{-1} \gamma(t_s^{-1} u) \\ &= g \cdot \sum_{s \in [G/H]} t_s \otimes \gamma(t_s^{-1} u), \end{aligned}$$

[1]Note que podemos usar um argumento parecido para mostrar que γ' independe da escolha do conjunto de representantes $[G/H]$!

onde usamos na penúltima igualdade que γ é homomorfismo de kH-módulos. Mas, se $s_1, s_2 \in [G/H]$, veja que

$$t_{s_1}H = t_{s_2}H \iff g^{-1}s_1H = g^{-1}s_2H \iff s_1H = s_2H \iff s_1 = s_2,$$

então t_s percorre todo o conjunto de representantes $[G/H]$ quando variamos $s \in [G/H]$. Consequentemente,

$$\gamma'(gu) = g \cdot \sum_{s\in[G/H]} t_s \otimes \gamma(t_s^{-1}u) = g \cdot \sum_{s\in[G/H]} s \otimes \gamma(s^{-1}u) = g\gamma'(u),$$

como queríamos demonstrar.

(b) É fácil ver que a função que leva γ em γ' é linear. Agora, pela Reciprocidade de Frobenius, já sabemos que

$$\mathrm{Hom}_{kH}(U_H, V) \cong \mathrm{Hom}_{kG}(U, V^G)$$

e então esses espaços possuem a mesma dimensão. Logo, para mostrar que a transformação linear que temos é um isomorfismo, basta mostrar que ela é injetora. De fato, usando a Proposição 3.1.7, se $\gamma'(u) = 0$ para todo $u \in U$, então devemos ter $\gamma(s^{-1}u) = 0$ para todos $s \in [G/H]$ e $u \in U$. Mas isso implica que $\gamma(u) = 0$ para todo $u \in U$, ou seja, $\gamma = 0$. Por isso, o núcleo da transformação linear em questão é trivial, como preciso.

(c) Como vimos no item (a), γ' independe da escolha de $[G/H]$ e podemos então supor que $1 \in [G/H]$. Assim, se $u \in U$, então

$$\pi(\gamma'(u)) = \pi\left(\sum_{s\in[G/H]} s \otimes \gamma(s^{-1}u)\right) = \pi(1 \otimes \gamma(1^{-1}u)) = \gamma(u).$$

Por isso, $\pi\gamma' = \gamma$. Como π é homomorfismo de kH-módulos, observe que a composição com π define uma transformação linear de $\mathrm{Hom}_{kG}(U, V^G)$ em $\mathrm{Hom}_{kH}(U_H, V)$. Pelo que acabamos de ver, essa transformação linear é a inversa do isomorfismo do item (b).

□

Exercício A.3.2. Sejam V, V_1 e V_2 kH-módulos e U, U_1 e U_2 kG-módulos.

(a) Se $V_1 \to V_2$ e $U_1 \to U_2$ são homomorfismos de kH-módulos e de kG-módulos, respectivamente, prove que os diagramas induzidos

$$\begin{array}{ccc} \mathrm{Hom}_{kG}(V_1^G, U) & \xrightarrow{\sim} & \mathrm{Hom}_{kH}(V_1, U_H) \\ \uparrow & & \uparrow \\ \mathrm{Hom}_{kG}(V_2^G, U) & \xrightarrow{\sim} & \mathrm{Hom}_{kH}(V_2, U_H) \end{array}$$

e

$$\begin{array}{ccc} \mathrm{Hom}_{kG}(V^G, U_1) & \xrightarrow{\sim} & \mathrm{Hom}_{kH}(V, (U_1)_H) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{kG}(V^G, U_2) & \xrightarrow{\sim} & \mathrm{Hom}_{kH}(V, (U_2)_H) \end{array}$$

são comutativos, onde os mapas horizontais são os isomorfismos descritos na demonstração do Lema 3.1.11.

(b) Use o isomorfismo do Exercício A.3.1 para provar um resultado análogo, no qual a indução e a restrição trocam de posição.

Solução: (a) Em ambos os diagramas, o isomorfismo

$$\mathrm{Hom}_{kG}(V^G, U) \xrightarrow{\sim} \mathrm{Hom}_{kH}(V, U_H)$$

é dado pela restrição a V, como visto na demonstração da Reciprocidade de Frobenius. Mais especificamente, seja $i_V : V \to V^G$ a inclusão dada por

$$i_V(v) = 1 \otimes v$$

para todo $v \in V$. Então i_V é homomorfismo de kH-módulos e o isomorfismo em questão leva $\varphi : V^G \to U$ em $\varphi i_V : V \to U_H$.

Comecemos com o primeiro diagrama. Seja $\alpha : V_1 \to V_2$ o homomorfismo em questão. Assim, a transformação linear induzida de $\mathrm{Hom}_{kG}(V_2^G, U)$ em $\mathrm{Hom}_{kG}(V_1^G, U)$ leva um homomorfismo $\varphi : V_2^G \to U$ em $\varphi\alpha^G : V_1^G \to U$. Por outro lado, a transformação linear induzida de $\mathrm{Hom}_{kG}(V_2, U_H)$ em $\mathrm{Hom}_{kG}(V_1, U_H)$ leva um homomorfismo $\psi : V_2 \to U_H$ em $\psi\alpha : V_1 \to U_H$. Dessa forma, para mostrar que o diagrama é comutativo, devemos mostrar que

$$\varphi i_{V_2}\alpha = \varphi\alpha^G i_{V_1}$$

para todo $\varphi \in \mathrm{Hom}_{kG}(V_2^G, U)$. É suficiente mostrar que $i_{V_2}\alpha = \alpha^G i_{V_1}$ e, de fato, se $v_1 \in V_1$, então

$$i_{V_2}(\alpha(v_1)) = 1 \otimes \alpha(v_1) = \alpha^G(1 \otimes v_1) = \alpha^G(i_{V_1}(v_1)),$$

como desejado. Repare que nessa última igualdade estamos dizendo que α^G estende α se identificarmos V_1 dentro de V_1^G, o que já sabíamos que acontece pelo Lema 3.1.11.

Para o segundo diagrama, seja $\beta : U_1 \to U_2$ o homomorfismo do enunciado. Denotaremos por $\beta_H : (U_1)_H \to (U_2)_H$ a restrição de β a um homomorfismo de kH-módulos (que é essencialmente β). Dessa vez, o mapa vertical da esquerda leva um homomorfismo $\varphi : V^G \to U_1$ em $\beta\varphi : V^G \to U_2$, enquanto o mapa vertical da direita leva um homomorfismo $\psi : V \to (U_1)_H$ em $\beta_H\psi : V \to (U_2)_H$. O que queremos mostrar é que

$$(\beta\varphi)i_V = \beta_H(\varphi i_V)$$

para todo $\varphi \in \mathrm{Hom}_{kG}(V^G, U_1)$. Mas isso é imediato, porque β e β_H representam a mesma função entre os conjuntos $U_1 = (U_1)_H$ e $U_2 = (U_2)_H$.

(b) Neste item, queremos usar o isomorfismo

$$\mathrm{Hom}_{kG}(U, V^G) \xrightarrow{\sim} \mathrm{Hom}_{kH}(U_H, V)$$

construído no Exercício A.3.1. Explicitamente, se $\pi_V : V^G \to V$ é a projeção descrita no item (c) desse exercício, então o isomorfismo em questão leva $\varphi : U \to V^G$ em $\pi_V\varphi : U_H \to V$.

Seja $\alpha : V_1 \to V_2$ um homomorfismo de kH-módulos. O análogo do primeiro diagrama do item (a) é:

$$\begin{array}{ccc} \mathrm{Hom}_{kG}(U, V_1^G) & \xrightarrow{\sim} & \mathrm{Hom}_{kH}(U_H, V_1) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{kG}(U, V_2^G) & \xrightarrow{\sim} & \mathrm{Hom}_{kH}(U_H, V_2) \end{array}$$

O mapa vertical da esquerda leva um homomorfismo $\varphi : U \to V_1^G$ em $\alpha^G\varphi : U \to V_2^G$, enquanto o da direita leva um homomorfismo $\psi : U_H \to V_1$ em $\alpha\psi : U_H \to V_2$. Para mostrar que esse diagrama é comutativo, temos que verificar que

$$\pi_{V_2}\alpha^G\varphi = \alpha\pi_{V_1}\varphi$$

para todo $\varphi \in \mathrm{Hom}_{kG}(U, V_1^G)$. Como antes, basta mostrar que $\pi_{V_2}\alpha^G = \alpha\pi_{V_1}$. Seja $[G/H] \subseteq G$ um conjunto de representantes das classes laterais à esquerda de H em G que contém 1. Podemos escrever um elemento qualquer de V_1^G como

$$\sum_{s\in[G/H]} s \otimes v_s$$

para certos $v_s \in V_1$. Com isso,

$$\pi_{V_2}\left(\alpha^G\left(\sum_{s\in[G/H]} s\otimes v_s\right)\right) = \pi_{V_2}\left(\sum_{s\in[G/H]} s\otimes\alpha(v_s)\right) = \alpha(v_1)$$

e

$$\alpha\left(\pi_{V_1}\left(\sum_{s\in[G/H]} s\otimes v_s\right)\right) = \alpha(v_1),$$

de onde concluímos a igualdade restante.

Agora, seja $\beta : U_1 \to U_2$ um homomorfismo de kG-módulos. O análogo do segundo diagrama do item (b) é:

$$\begin{array}{ccc} \mathrm{Hom}_{kG}(U_1, V^G) & \xrightarrow{\sim} & \mathrm{Hom}_{kH}((U_1)_H, V) \\ \uparrow & & \uparrow \\ \mathrm{Hom}_{kG}(U_2, V^G) & \xrightarrow{\sim} & \mathrm{Hom}_{kH}((U_2)_H, V) \end{array}$$

O mapa vertical da esquerda leva um homomorfismo $\varphi : U_2 \to V^G$ em $\varphi\beta : U_1 \to V^G$, enquanto o da direita leva um homomorfismo $\psi : (U_2)_H \to V$ em $\psi\beta_H : (U_1)_H \to V$. Para mostrar que esse diagrama é comutativo, devemos verificar que

$$(\pi_V\varphi)\beta_H = \pi_V(\varphi\beta)$$

para todo $\varphi \in \mathrm{Hom}_{kG}(U_2, V^G)$. Mas, como no item anterior, isso é verdade, porque β e β_H representam a mesma função entre os conjuntos $U_1 = (U_1)_H$ e $U_2 = (U_2)_H$.

□

Exercício A.3.3. Sejam H e L dois subgrupos de G, seja U um kH-módulo e seja V um kL-módulo. Prove que

$$U^G \otimes V^G \cong \bigoplus_{g\in[L\backslash G/H]} ({}^gU)_{L\cap gHg^{-1}} \otimes V_{L\cap gHg^{-1}})^G.$$

Este é o Teorema do Produto Tensorial de Mackey.

Solução: Pelo item (5) do Lema 3.1.10, vale

$$U^G \otimes V^G \cong ((U^G)_L \otimes V)^G.$$

Pela Fórmula de Decomposição de Mackey, temos

$$(U^G)_L \cong \bigoplus_{g\in[L\backslash G/H]} ({}^gU)_{L\cap gHg^{-1}})^L,$$

então

$$((U^G)_L \otimes V)^G \cong \bigoplus_{g\in[L\backslash G/H]} (({}^gU)_{L\cap gHg^{-1}})^L \otimes V)^G,$$

onde usamos o item (3) da Proposição 2.4.4 e o item (1) do Lema 3.1.10. Agora, novamente pelo item (5) do Lema 3.1.10,

$$({}^gU)_{L\cap gHg^{-1}})^L \otimes V \cong ({}^gU)_{L\cap gHg^{-1}} \otimes V_{L\cap gHg^{-1}})^L.$$

Por fim, juntando o que temos e usando o item (3) do Lema 3.1.10, concluímos que

$$\begin{aligned} U^G \otimes V^G &\cong \bigoplus_{g\in[L\backslash G/H]} ((({}^gU)_{L\cap gHg^{-1}} \otimes V_{L\cap gHg^{-1}})^L)^G \\ &\cong \bigoplus_{g\in[L\backslash G/H]} (({}^gU)_{L\cap gHg^{-1}} \otimes V_{L\cap gHg^{-1}})^G, \end{aligned}$$

como queríamos. □

Exercício A.3.4. Sejam H um subgrupo de G e V um kH-módulo.

(a) Se $g_1, g_2 \in G$, prove que ${}^{g_1}({}^{g_2}V) = {}^{g_1g_2}V$.

(b) Se $g \in G$ e W é submódulo de V, mostre que ${}^gW$ é submódulo de ${}^gV$. Deduza que V é simples, semissimples ou indecomponível se, e somente se, ${}^gV$ satisfaz a propriedade correspondente.

(c) Se $g_1, g_2 \in G$ são tais que $g_1H = g_2H$, prove que $g_1Hg_1^{-1} = g_2Hg_2^{-1}$ e que ${}^{g_1}V \cong {}^{g_2}V$.

(d) Se L é um subgrupo de H, verifique que $({}^gV)_{gLg^{-1}} = {}^g(V_L)$.

Solução: (a) Como espaços vetoriais, ${}^{g_1}({}^{g_2}V)$ e ${}^{g_1g_2}V$ são iguais. Como

$$g_1(g_2Hg_2^{-1})g_1^{-1} = (g_1g_2)H(g_1g_2)^{-1},$$

eles são representações do mesmo grupo. É imediato verificar que esse grupo age do mesmo modo nos dois módulos.

(b) Como espaços vetoriais, W e ${}^gW$ são iguais. Além disso, se $ghg^{-1} \in gHg^{-1}$, então

$$ghg^{-1} \cdot {}^gW = h \cdot W = W = {}^gW,$$

provando que ${}^gW$ é submódulo de ${}^gV$. Pelo item (a), temos $V = {}^{g^{-1}}({}^gV)$ e, com isso, vemos que a função que leva $W \leq V$ em ${}^gW \leq {}^gV$ é uma bijeção entre os conjuntos de submódulos de cada um desses módulos. Como a conjugação de representações preserva somas diretas (já que o espaço vetorial subjacente não é alterado), a segunda parte do item segue.

(c) Seja $h \in H$ tal que $g_1 = g_2h$. Note que

$$g_1Hg_1^{-1} = (g_2h)H(g_2h)^{-1} = g_2(hHh^{-1})g_2^{-1} = g_2Hg_2^{-1},$$

de modo que ${}^{g_1}V$ e ${}^{g_2}V$ são representações do mesmo grupo. Assim, defina a função $\varphi : {}^{g_1}V \to {}^{g_2}V$ que leva $v \in {}^{g_1}V$ para $hv \in {}^{g_2}V$. Aqui, h age de acordo com a estrutura de kH-módulo de V. Como h induz um operador linear inversível em V, vemos que φ é isomorfismo linear. Além disso, se $g_1h'g_1^{-1} \in g_1Hg_1^{-1}$ e $v \in {}^{g_1}V$, então

$$\varphi(g_1h'g_1^{-1} \cdot v) = \varphi(h'v) = hh'v = (hh'h^{-1})(hv) = g_2hh'h^{-1}g_2^{-1} \cdot hv = g_1h'g_1^{-1} \cdot \varphi(v).$$

A primeira aparição de $\cdot$ representa a ação em ${}^{g_1}V$, a segundo e a terceira aparições representam a ação em ${}^{g_2}V$ e, onde os elementos estão justapostos, temos a ação em V. Concluímos assim que φ é um isomorfismo de $k[g_1Hg_1^{-1}]$-módulos.

(d) Como L é subgrupo de H, então gLg^{-1} é subgrupo de gHg^{-1}. Assim, os módulos em destaque estão definidos sobre o mesmo grupo. Por construção, eles possuem o mesmo espaço vetorial subjacente e é imediato verificar que gLg^{-1} age do mesmo modo em ambos os módulos.

□

Exercício A.3.5. Neste exercício, você verificará algumas das afirmações feitas ao final da prova do Critério de Indecomponibilidade de Green. Usaremos a notação introduzida na demonstração.

(a) Através das relações

$$\overline{e}_{11}M = M\overline{e}_{pp} \quad \text{e} \quad \overline{e}_{i+1,i+1}M = M\overline{e}_{ii},$$

para $1 \leq i < p$, verifique que M é como descrita na demonstração.

(b) Com uma mudança de base, prove que M é semelhante à matriz

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & \mu^p \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Como esta é a matriz companheira do polinômio $x^p - \mu^p$, conclua que a forma canônica de Jordan de M é J.

(c) Seja $Y \in M_p(k)$ inversível tal que $J = YMY^{-1}$. Mostre que a conjugação por Y induz um isomorfismo de álgebras entre a subálgebra de $M_p(k)$ formada pelas matrizes que comutam com M e a subálgebra formada pelas matrizes que comutam com J.

Solução: (a) Por simplicidade, interpretaremos os índices módulo p, de modo que a relação no enunciado valha para todo $1 \leq i \leq p$. Escrevendo $M = (m_{ij})$, veja que

$$\overline{e}_{ii}M\overline{e}_{jj}$$

é a matriz que possui zero em todas as entradas exceto na entrada (i, j), onde vale m_{ij}. Mas, se $i \neq j + 1$, então

$$\overline{e}_{ii}M\overline{e}_{jj} = \overline{e}_{ii}\overline{e}_{j+1,j+1}M = 0,$$

provando que $m_{ij} = 0$. Logo, M é da forma

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & \lambda_p \\ \lambda_1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_{p-1} & 0 \end{pmatrix}$$

para certos escalares $\lambda_1, \lambda_2, \ldots, \lambda_p \in k$. Como M é inversível, nenhuma de suas colunas pode ser nula, então os escalares $\lambda_1, \ldots, \lambda_p$ são não nulos.

(b) Basta conjugar M pela matriz diagonal D cuja entrada $(1, 1)$ é $d_1 = 1$ e cuja entrada (i, i) é

$$d_i = \frac{1}{\lambda_1 \cdots \lambda_{i-1}}$$

para $1 < i \leq p$. De fato, temos

$$DMD^{-1} = \begin{pmatrix} 0 & 0 & \cdots & 0 & d_1\lambda_p d_p^{-1} \\ d_2\lambda_1 d_1^{-1} & 0 & \cdots & 0 & 0 \\ 0 & d_3\lambda_2 d_2^{-1} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & d_p\lambda_{p-1}d_{p-1}^{-1} & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 & \cdots & 0 & \mu^p \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

onde relembramos que $\mu^p = \lambda_1 \cdots \lambda_p$. Mas esta é a matriz companheira do polinômio $x^p - \mu^p = (x - \mu)^p$. Logo, o polinômio minimal dessa matriz também é $(x - \mu)^p$, de onde concluímos que sua forma canônica de Jordan é o bloco J.

(c) Se $X \in M_p(k)$ é uma matriz que comuta com M, então

$$\begin{aligned}(YXY^{-1})J &= (YXY^{-1})(YMY^{-1}) \\ &= Y(XM)Y^{-1} \\ &= Y(MX)Y^{-1} \\ &= (YMY^{-1})(YXY^{-1}) \\ &= J(YXY^{-1}).\end{aligned}$$

Por isso, o automorfismo de $M_p(k)$ dado por conjugação por Y leva a subálgebra das matrizes que comutam com M para dentro da subálgebra das matrizes que comutam com J. Mas um argumento análogo mostra que a inversa desse automorfismo leva matrizes que comutam com J em matrizes que comutam com M. Concluímos que esse automorfismo de $M_p(k)$ se restringe a um isomorfismo entre as subálgebras indicadas.

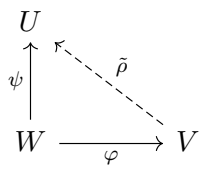
□

Exercício A.3.6. Defina o que seriam módulos relativamente injetivos e demonstre um resultado análogo à Proposição 3.2.1.

Solução: Seja U um kG-módulo e seja H um subgrupo de G. Diremos que U é relativamente H-injetivo se U satisfizer as seguintes propriedades:

(1) Se $\varphi : U \to V$ é um homomorfismo injetor de kG-módulos cuja restrição φ_H cinde como homomorfismo de kH-módulos, então φ cinde.

(2) Sejam $\varphi : W \to V$ e $\psi : W \to U$ homomorfismos de kG-módulos. Se existe um homomorfismo de kH-módulos $\tilde{\rho} : V_H \to U_H$ que faz o seguinte diagrama comutar



então existe um homomorfismo de kG-módulos $\rho : V \to U$ que também faz o diagrama comutar.

Como ocorre na Proposição 3.2.1, vamos mostrar que as duas afirmações acima são equivalentes. Para facilitar, vamos provar que ambas são equivalentes a:

(3) U é relativamente H-projetivo.

Ou seja, no fim de tudo, teremos um resultado análogo ao Teorema 2.3.14: a definição de módulo relativamente H-injetivo é equivalente à definição de módulo relativamente H-projetivo!

A observação mais importante é que U é relativamente H-projetivo se, e somente se, U^* o é. De fato, se U é relativamente H-projetivo, existe um kH-módulo V tal que U é somando direto de V^G. Pelo Lema 2.3.3, U^* é somando direto de $(V^G)^*$. Mas $(V^G)^* \cong (V^*)^G$ pelo Lema 3.1.10, de onde concluímos que U^* é relativamente H-projetivo. Reciprocamente, se U^* é relativamente H-projetivo, o mesmo argumento prova que $U^{**} \cong U$ é relativamente H-projetivo.

Estamos prontos para mostrar as equivalências:

(1) $\implies$ (3). Pela observação anterior, é suficiente mostrar que U^* é relativamente H-projetivo. Para isso, vamos usar a caracterização (3) da Proposição 3.2.1. Seja $\varphi : V \to U^*$ um homomorfismo sobrejetor de kG-módulos que cinde como homomorfismo de kH-módulos, ou seja, existe um homomorfismo de kH-módulos $f : U^* \to V$ tal que $\varphi f = \mathrm{id}_{U^*}$. Tomando a transposta, vemos que $f^*\varphi^* = \mathrm{id}_{U^{**}}$, logo, $\varphi^* : U^{**} \to V^*$ é um homomorfismo injetor de kG-módulos que cinde como homomorfismo de kH-módulos. Mas $U^{**} \cong U$ satisfaz (1) por hipótese, então existe um homomorfismo de kG-módulos $g : V^* \to U^{**}$ tal que $g\varphi^* = \mathrm{id}_{U^{**}}$. Pelo Exercício A.2.10, existe um homomorfismo de kG-módulos $\psi : U^* \to V$ tal que $g = \psi^*$. Aplicando a Observação 2.3.5, segue de $\psi^*\varphi^* = \mathrm{id}_{U^{**}}$ que $\varphi\psi = \mathrm{id}_{U^*}$. Isso mostra que φ cinde como homomorfismo de kG-módulos, como queríamos. Logo, U^* é relativamente H-projetivo e o mesmo vale para U.

(3) $\implies$ (2). Suponha que U seja relativamente H-projetivo. Como já vimos, U^* é relativamente H-projetivo. Mostremos que vale (2). Sejam $\varphi : W \to V$ e $\psi : W \to U$ homomorfismos de kG-módulos e suponha que exista um homomorfismo de kH-módulos $\tilde{\rho} : V_H \to U_H$ tal que $\tilde{\rho}\varphi = \psi$. Tomando a transposta, obtemos os homomorfismos de kG-módulos $\varphi^* : V^* \to W^*$ e $\psi^* : U^* \to W^*$ e o homomorfismo de kH-módulos $(\tilde{\rho})^* : (U^*)_H \to (V^*)_H$, que satisfazem $\varphi^*(\tilde{\rho})^* = \psi^*$. Usando a caracterização (4) da Proposição 3.2.1 para U^*, encontramos um homomorfismo de kG-módulos $f : U^* \to V^*$ tal que $\varphi^* f = \psi^*$. Pelo Exercício A.2.10, existe um homomorfismo de kG-módulos $\rho : V \to U$ tal que $f = \rho^*$. Aplicando a Observação 2.3.5, segue de $\varphi^*\rho^* = \psi^*$ que $\rho\varphi = \psi$. Isso demonstra a validade de (2).

(2) $\implies$ (1). Seja $\varphi : U \to V$ um homomorfismo injetor que cinde como homomorfismo de kH-módulos. Logo, existe $\tilde{\rho} : V_H \to U_H$ tal que $\tilde{\rho}\varphi = \mathrm{id}_U$. Assim, tomando $W = U$ e $\psi = \mathrm{id}_U$, a propriedade (2) nos dá um homomorfismo de kG-módulos $\rho : V \to U$ tal que $\rho\varphi = \psi = \mathrm{id}_U$. Isso prova que φ também cinde como homomorfismo de kG-módulos. □

Exercício A.3.7. Seja G um p-grupo finito não trivial, onde p é um número primo. Defina o **subgrupo de Frattini** $\Phi(G)$ como sendo a interseção de todos os subgrupos maximais de G.

(a) Mostre que $\Phi(G)$ consiste dos elementos "não geradores" de G, isto é, dos elementos $g \in G$ tais que, se X é subconjunto de G e $X \cup \{g\}$ gera G, então X já gera G.

(b) Como G é um p-grupo finito, lembre que todo subgrupo próprio $H \leq G$ é subgrupo normal de um $K \leq G$ com $[K : H] = p$. Use isto para mostrar que $\Phi(G)$ contém todas as potências p-ésimas e todos os comutadores de G.

(c) Prove que $\Phi(G)$ é um subgrupo normal de G e que

$$\frac{G}{\Phi(G)} \cong (C_p)^r$$

para algum $r \geq 1$.

(d) Mostre que r é o tamanho mínimo de um conjunto gerador de G.

(e) Conclua que, se G não é cíclico, então $C_p \times C_p$ é quociente de G.

Solução: (a) Seja $g \in \Phi(G)$. Para mostrar que g tem a propriedade desejada, considere um subconjunto $X \subseteq G$ que não é gerador. Vamos mostrar que $X \cup \{g\}$ não gera G. De fato, como o subgrupo gerado por X é próprio, ele está contido em algum subgrupo maximal M de G. Mas $g \in \Phi(G) \subseteq M$, então o subgrupo gerado por X e g também está contido em M e é diferente de G.

Reciprocamente, tome $g \in G$ com a propriedade do enunciado. Seja $M \leq G$ um subgrupo maximal. Como $M \neq G$, então M não gera G e, pela propriedade de g, $M \cup \{g\}$ também não gera G. Como $M \cup \{g\}$ contém o subgrupo maximal M, o subgrupo gerado por M e g deve ser M. Logo, $g \in M$. Como M era um subgrupo maximal qualquer, concluímos que $g \in \Phi(G)$.

(b) Seja M um subgrupo maximal de G. Como G é p-grupo, então M tem índice p em G e é normal. Logo, podemos formar o quociente G/M, que é cíclico de ordem p. Como esse quociente é abeliano e todos os seus elementos têm ordem p, isso quer dizer que qualquer comutador e qualquer potência p-ésima de G está em M. Como M era subgrupo maximal qualquer de G, obtemos que $\Phi(G)$ contém todas as potências p-ésimas e todos os comutadores de G.

(c) Seja M um subgrupo maximal de G. Se $g \in G$, então gMg^{-1} também é subgrupo maximal. De fato, se $gMg^{-1} \leq M' \leq G$, então $M \leq g^{-1}M'g \leq G$ e, pela maximalidade de M, obtemos $M' = gMg^{-1}$ ou $M' = G$. Portanto, a interseção de todos os subgrupos maximais é normal em G. Podemos adaptar um pouco o argumento para mostrar que, na verdade, $\Phi(G)$ é um subgrupo *característico* de G, ou seja, invariante por todos os automorfismos de G.

Agora, pelo item (b), $\Phi(G)$ contém todas as potências p-ésimas e todos os comutadores, de modo que o quociente $G/\Phi(G)$ é abeliano e todo elemento possui ordem p. Tome $X = \{\alpha_1, \ldots, \alpha_r\} \subseteq G/\Phi(G)$ como sendo um conjunto minimal de geradores desse quociente. Como $G/\Phi(G)$ é abeliano e $\alpha_1, \ldots, \alpha_r$ têm ordem p, todo elemento se escreve na forma

$$\alpha_1^{i_1} \cdots \alpha_r^{i_r},$$

onde cada expoente i_j varia de 0 a $p-1$. Além disso, a representação acima é única. De fato, caso contrário, não é difícil ver que encontraríamos uma potência α_i^j com $1 \leq j \leq p-1$ no subgrupo gerado por $X \setminus \{\alpha_i\}$. Como α_i tem ordem p e p não divide j, então α_i é uma potência de α_i^j e poderíamos descartar α_i do conjunto gerador minimal X, um absurdo. Com essa unicidade na representação, é fácil obter um isomorfismo entre $G/\Phi(G)$ e $(C_p)^r$.

(d) Se $g_1, \ldots, g_s \in G$ formam um conjunto gerador de G, então as classes laterais desses elementos certamente geram $G/\Phi(G)$. Mas o número mínimo de elementos de um conjunto gerador de $G/\Phi(G) \cong (C_p)^r$ é r, então temos $s \geq r$. Vamos mostrar que G possui um conjunto gerador com exatamente r elementos. Sejam $g_1, \ldots, g_r \in G$ tais que suas projeções no quociente gerem $G/\Phi(G)$. Isso quer dizer que $\{g_1, \ldots, g_r\} \cup \Phi(G)$ gera G. Aplicando o item (a) repetidas vezes, podemos desconsiderar desse conjunto gerador os elementos de $\Phi(G)$, de onde concluímos que $g_1, \ldots, g_r$ geram G, como preciso.

Como indicado no livro [12], este item e o anterior acabaram de demonstrar o Teorema da Base de Burnside!

(e) Se G não é gerado por um elemento, então os itens (c) e (d) dizem que $G/\Phi(G) \cong (C_p)^r$ para algum $r \geq 2$. Assim, como $C_p \times C_p$ é um quociente de $(C_p)^r$, esse grupo também é um quociente de G.

□

Exercício A.3.8. Se U e V são kG-módulos e U é relativamente H-projetivo, mostre que $U \otimes V$ também o é.

Solução: Como U é relativamente H-projetivo, existe um kH-módulo W satisfazendo $U \mid W^G$. Pela Proposição 2.4.4, temos $U \otimes V \mid W^G \otimes V$. Pelo item (5) do Lema 3.1.10,

$$W^G \otimes V \cong (W \otimes V_H)^G$$

é relativamente H-livre, de onde concluímos que $U \otimes V$ é relativamente H-projetivo. □

Exercício A.3.9. Seja V um kH-módulo indecomponível. Se V possui vértice Q e se $g \in G$, mostre que gQg^{-1} é um vértice de ${}^gV$.

Solução: Inicialmente, vamos destacar uma propriedade. Se L é um subgrupo de H e se W é um kL-módulo, então ${}^g(W^H) \cong ({}^gW)^{gHg^{-1}}$. De fato, sabemos que W^H possui W como kL-submódulo e é gerado por ele como kH-módulo. Assim, ${}^gW$ é um submódulo de ${}^g((W^H)_L) = ({}^g(W^H))_{gLg^{-1}}$ e também gera ${}^g(W^H)$ como $k[gHg^{-1}]$-módulo. Comparando as dimensões, segue do Corolário 3.1.6 que ${}^g(W^H)$ é relativamente gLg^{-1}-livre com respeito a ${}^gW$, ou seja, ${}^g(W^H) \cong ({}^gW)^{gHg^{-1}}$.

Voltemos ao exercício. Note inicialmente que ${}^gV$ é indecomponível pelo Exercício A.3.4. Seja S uma fonte de V com respeito a Q. Como $V \mid S^H$, então ${}^gV \mid {}^g(S^H) \cong ({}^gS)^{gHg^{-1}}$. Logo, existe um vértice R de ${}^gV$ contido em gQg^{-1} e temos $|R| \leq |Q|$. Por outro lado, se T é uma fonte de ${}^gV$ com respeito a R, então ${}^gV \mid T^{gHg^{-1}}$ nos dá $V \mid {}^{g^{-1}}(T^{gHg^{-1}}) \cong ({}^{g^{-1}}T)^H$. Logo, algum conjugado de Q está contido em $g^{-1}Rg$ e vale $|Q| \leq |R|$. Concluímos que $|Q| = |R|$ e, como $R \subseteq gQg^{-1}$, devemos ter $R = gQg^{-1}$, como preciso. □

Exercício A.3.10. Seja Q um subgrupo de G. Suponha que U seja um kG-módulo indecomponível que é relativamente Q-projetivo e tal que U_Q possui um somando indecomponível que não é relativamente projetivo com relação a nenhum subgrupo próprio de Q. Mostre que Q é um vértice de U.

Solução: Como U é relativamente Q-projetivo, podemos encontrar um vértice R de U contido em Q. Seja S uma fonte de U com relação a R. Assim, $U \mid S^G$ e, pela Fórmula de Decomposição de Mackey,

$$U_Q \mid (S^G)_Q \cong \bigoplus_{g \in [Q \backslash G / R]} (({}^gS)_{Q \cap gRg^{-1}})^Q.$$

Se W é o somando indecomponível de U_Q com a propriedade do enunciado, segue do Teorema de Krull-Schmidt que

$$W \mid (({}^gS)_{Q \cap gRg^{-1}})^Q$$

para algum $g \in G$. Consequentemente, W é relativamente projetivo com relação a $Q \cap gRg^{-1}$ e devemos ter $Q = Q \cap gRg^{-1}$, ou seja, $Q \subseteq gRg^{-1}$. Isso diz que $|Q| \leq |R|$. Mas $R \subseteq Q$, então devemos ter $R = Q$, provando que Q é um vértice de U. □

Exercício A.3.11. Seja Q um p-subgrupo de G.

(a) Se V é um kQ-módulo indecomponível de vértice Q, prove que V^G possui um somando indecomponível com vértice Q.

(b) Deduza que todo p-subgrupo de G é um vértice de um kG-módulo indecomponível.

(c) Deduza também que todo p-subgrupo de G está contido em algum p-subgrupo de Sylow de G.

Solução: (a) Como V é indecomponível e $V \mid (V^G)_Q$, existe um kG-módulo indecomponível U tal que $U \mid V^G$ e $V \mid U_Q$. Note que U é relativamente Q-projetivo e, como V é um somando direto de U_Q com vértice Q, o Exercício A.3.10 nos dá que U tem vértice Q, como desejado.

(b) Se Q é um p-subgrupo de G, então, pelo Exemplo 3.2.14, existe um kQ-módulo indecomponível V e de vértice Q: basta tomar V como sendo o kQ-módulo trivial. Logo, pelo item anterior, existe um kG-módulo indecomponível com vértice Q.

(c) Se Q é um p-subgrupo de G, o item anterior garante a existência de um kG-módulo indecomponível U com vértice Q. Se P é um p-subgrupo de Sylow de G, então, pelo Teorema 3.2.3, U é relativamente P-projetivo e P deve conter gQg^{-1} para algum $g \in G$. Segue que $Q \subseteq g^{-1}Pg$ e, como $g^{-1}Pg$ também é um p-subgrupo de Sylow, o item está concluído.

□

Exercício A.3.12. Seja k um corpo algebricamente fechado de característica $p > 0$.

(a) Seja Q um p-subgrupo de G e seja V um kQ-módulo indecomponível. Se R é um vértice de V, mostre que $[Q : R]$ divide a dimensão de V.

(b) Com as notações do item anterior, conclua que, se a dimensão de V não é divisível por p, então Q é um vértice de V.

(c) Se U é um kG-módulo indecomponível, prove que a dimensão de U é divisível pelo índice de um de seus vértices em um p-subgrupo de Sylow de G.

Solução: (a) Seja S uma fonte de V com relação a R. Como S é indecomponível e Q é p-grupo, o Corolário 3.1.16 diz que S^Q é indecomponível. Mas $V \mid S^Q$, então vale $V \cong S^Q$. Logo,

$$\dim_k V = \dim_k S^Q = [Q : R] \cdot \dim_k S$$

e este primeiro item está provado.

(b) Se a dimensão de V não é divisível por p, então $[Q : R] = 1$, ou seja, $R = Q$ e Q é um vértice de V.

(c) Sejam Q um vértice de U, S uma fonte de U com relação a Q e P um p-subgrupo de Sylow de G contendo Q. Como $U \mid S^G$, a Fórmula de Decomposição de Mackey nos dá

$$U_P \mid (S^G)_P \cong \bigoplus_{g \in [P\backslash G/Q]} ({}^gS)_{P \cap gQg^{-1}})^P.$$

Se V é um somando indecomponível de U_P, então existe $g \in G$ com

$$V \mid ({}^gS)_{P \cap gQg^{-1}})^P$$

e então V possui um vértice Q_V contido em $P \cap gQg^{-1}$. Dessa forma,

$$\begin{aligned} |Q| = \left|gQg^{-1}\right| = [gQg^{-1} : Q_V]|Q_V| &\implies \frac{|P|}{|Q_V|} = \frac{|P|}{|Q|}[gQg^{-1} : Q_V] \\ &\implies [P : Q_V] = [P : Q][gQg^{-1} : Q_V]. \end{aligned}$$

Pelo item (a), $[P : Q_V]$ divide a dimensão de V. Logo, pela conta acima, $[P : Q]$ também divide essa dimensão. Mas a dimensão de U_P é a soma das dimensões de seus somandos indecomponíveis, de onde concluímos que $[P : Q]$ divide $\dim_k U_P = \dim_k U$.

□

Exercício A.3.13. Sejam H um subgrupo de G e U um kG-módulo indecomponível com $U \mid (k_H)^G$, onde k denota o kG-módulo trivial. Prove que U tem fonte trivial. (*Dica:* Tome Q um vértice de U e aplique a Fórmula de Decomposição de Mackey para $((k_H)^G)_Q$.)

Solução: Seja Q um vértice de U e seja S uma fonte de U com relação a Q. Vamos mostrar que $S \cong k_Q$. Pelo Teorema 3.2.12, S é um somando direto de U_Q e, como $U \mid (k_H)^G$, temos

$$S \mid ((k_H)^G)_Q \cong \bigoplus_{g \in [Q\backslash G/H]} (({}^g(k_H))_{Q \cap gHg^{-1}})^Q,$$

onde utilizamos a Fórmula de Decomposição de Mackey. Note que ${}^g(k_H) \cong k_{gHg^{-1}}$, então cada somando acima é da forma $(k_{Q \cap gHg^{-1}})^Q$. Como S é indecomponível, encontramos $g \in G$ tal que

$$S \mid (k_{Q \cap gHg^{-1}})^Q.$$

Pelo Teorema 3.2.12, Q é um vértice de S, então devemos ter $Q \cap gHg^{-1} = Q$ e a expressão acima se simplifica para $S \mid k_Q$. Mas k_Q é indecomponível, então $S \cong k_Q$, como queríamos. □

Exercício A.3.14. Seja φ um homomorfismo sobrejetor de um kG-módulo projetivo Q em um kG-módulo V. Se U é um kG-módulo, mostre que um homomorfismo $\psi : U \to V$ se fatora através de um projetivo se, e somente se, existe um homomorfismo $\alpha : U \to Q$ tal que $\varphi\alpha = \psi$.

Solução: Se existe α como acima, certamente ψ se fatora através do projetivo Q. Reciprocamente, suponha que ψ se fatore através de algum projetivo P. Logo, existem homomorfismos $\beta : U \to P$ e $\gamma : P \to V$ tais que $\gamma\beta = \psi$. Assim, temos o seguinte diagrama:

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle \gamma} & & \\ Q & \xrightarrow{\varphi} & V & \longrightarrow & 0 \end{array}$$

Como φ é sobrejetor e P é projetivo, existe um homomorfismo $\rho : P \to Q$ tal que $\varphi\rho = \gamma$. Definindo $\alpha : U \to Q$ por $\alpha = \rho\beta$, temos

$$\varphi\alpha = \varphi(\rho\beta) = (\varphi\rho)\beta = \gamma\beta = \psi,$$

como queríamos. □

Exercício A.3.15. Sejam U, U_1 e U_2 kG-módulos.

(a) Prove que

$$\overline{\mathrm{Hom}}_{kG}(U_1 \oplus U_2, U) \cong \overline{\mathrm{Hom}}_{kG}(U_1, U) \oplus \overline{\mathrm{Hom}}_{kG}(U_2, U)$$

e

$$\overline{\mathrm{Hom}}_{kG}(U, U_1 \oplus U_2) \cong \overline{\mathrm{Hom}}_{kG}(U, U_1) \oplus \overline{\mathrm{Hom}}_{kG}(U, U_2).$$

(b) Se U_1 ou U_2 é projetivo, mostre que $\overline{\mathrm{Hom}}_{kG}(U_1, U_2) = 0$.

Solução: (a) Sejam $i_1 : U_1 \to U_1 \oplus U_2$ e $i_2 : U_2 \to U_1 \oplus U_2$ as inclusões. É rotineiro verificar que temos um isomorfismo linear

$$\mathrm{Hom}_{kG}(U_1 \oplus U_2, U) \cong \mathrm{Hom}_{kG}(U_1, U) \oplus \mathrm{Hom}_{kG}(U_2, U)$$

que leva um homomorfismo $\varphi : U_1 \oplus U_2 \to U$ no par $(\varphi i_1, \varphi i_2)$. Para provar o primeiro isomorfismo do exercício, basta mostrar que φ se fatora através de um projetivo se, e somente se, o mesmo vale para φi_1 e φi_2. Se φ se fatora através de um projetivo, podemos compor os mapas em questão com i_1 e i_2 e vemos facilmente que φi_1 e φi_2 se fatoram pelo mesmo projetivo. Reciprocamente, suponha que exista um kG-módulo projetivo P_j e homomorfismos $\alpha_j : U_j \to P_j$ e $\beta_j : P_j \to U$ tais que $\varphi i_j = \beta_j\alpha_j$, para $j = 1, 2$. Defina $\alpha : U_1 \oplus U_2 \to P_1 \oplus P_2$ por

$$\alpha(u_1, u_2) = (\alpha_1(u_1), \alpha_2(u_2))$$

para todos $u_1 \in U_1$ e $u_2 \in U_2$, e $\beta : P_1 \oplus P_2 \to U$ por

$$\beta(p_1, p_2) = \beta_1(p_1) + \beta_2(p_2)$$

para todos $p_1 \in P_1$ e $p_2 \in P_2$. Então α e β são homomorfismos de kG-módulos e

$$\begin{aligned}(\beta\alpha)(u_1, u_2) &= \beta_1(\alpha_1(u_1)) + \beta_2(\alpha_2(u_2)) \\ &= \varphi(i_1(u_1)) + \varphi(i_2(u_2)) \\ &= \varphi((u_1, 0) + (0, u_2)) \\ &= \varphi(u_1, u_2)\end{aligned}$$

para todos $u_1 \in U_1$ e $u_2 \in U_2$, provando a igualdade $\beta\alpha = \varphi$. Dessa forma, φ se fatora através de $P_1 \oplus P_2$, que é projetivo.

Para demonstrar o outro isomorfismo, considere as projeções $\pi_1 : U_1 \oplus U_2 \to U_1$ e $\pi_2 : U_1 \oplus U_2 \to U_2$. Temos um isomorfismo linear

$$\mathrm{Hom}_{kG}(U, U_1 \oplus U_2) \cong \mathrm{Hom}_{kG}(U, U_1) \oplus \mathrm{Hom}_{kG}(U, U_2)$$

que leva um homomorfismo $\varphi : U \to U_1 \oplus U_2$ no par $(\pi_1\varphi, \pi_2\varphi)$. Basta mostrar que φ se fatora através de um projetivo se, e só se, o mesmo vale para $\pi_1\varphi$ e $\pi_2\varphi$. Como anteriormente, uma das implicações é fácil. Reciprocamente, suponha que exista um kG-módulo projetivo P_j e homomorfismos $\alpha_j : U \to P_j$ e $\beta_j : P_j \to U_j$ tais que $\pi_j\varphi = \beta_j\alpha_j$, para $j = 1, 2$. Defina $\alpha : U \to P_1 \oplus P_2$ por

$$\alpha(u) = (\alpha_1(u), \alpha_2(u))$$

para todo $u \in U$, e $\beta : P_1 \oplus P_2 \to U_1 \oplus U_2$ por

$$\beta(p_1, p_2) = (\beta_1(p_1), \beta_2(p_2))$$

para todos $p_1 \in P_1$ e $p_2 \in P_2$. Então α e β são homomorfismos de kG-módulos e

$$(\beta\alpha)(u) = (\beta_1(\alpha_1(u)), \beta_2(\alpha_2(u))) = (\pi_1(\varphi(u)), \pi_2(\varphi(u))) = \varphi(u)$$

para todo $u \in U$, provando a igualdade $\beta\alpha = \varphi$. Concluímos que φ se fatora através de $P_1 \oplus P_2$, que é projetivo. Isso termina o primeiro item.

(b) Seja $\varphi : U_1 \to U_2$ um homomorfismo. Se U_1 é projetivo, então podemos escrever $\varphi = \varphi\,\mathrm{id}_{U_1}$ e segue que φ se fatora através de um projetivo. Analogamente, se U_2 é projetivo, vale $\varphi = \mathrm{id}_{U_2}\,\varphi$ e, novamente, φ se fatora através de um projetivo. Logo, em qualquer caso, concluímos que todo elemento de $\mathrm{Hom}_{kG}(U_1, U_2)$ se fatora através de um projetivo, mostrando que $\overline{\mathrm{Hom}}_{kG}(U_1, U_2) = 0$.

□

Exercício A.3.16. Usaremos as notações do Corolário 3.3.4.

(a) Se $\varphi \in \mathrm{Hom}_{kG}(U_1, U_2)$, mostre que φ se fatora através de um projetivo se e só se o mesmo vale para a restrição $\varphi_L \in \mathrm{Hom}_{kL}((U_1)_L, (U_2)_L)$.

(b) Pelo Teorema 3.3.1, podemos supor que

$$(U_1)_L = V_1 \oplus X_1 \quad \text{e} \quad (U_2)_L = V_2 \oplus X_2,$$

onde X_1 e X_2 são kL-módulos projetivos. De acordo com essas decomposições, sejam $i : V_1 \to (U_1)_L$ a inclusão e $\pi : (U_2)_L \to V_2$ a projeção. Prove que o mapa que leva $\varphi \in \mathrm{Hom}_{kG}(U_1, U_2)$ em $\pi\varphi i \in \mathrm{Hom}_{kL}(V_1, V_2)$ induz um isomorfismo

$$\overline{\mathrm{Hom}}_{kG}(U_1, U_2) \cong \overline{\mathrm{Hom}}_{kL}(V_1, V_2).$$

Solução: (a) Seja $\varphi \in \mathrm{Hom}_{kG}(U_1, U_2)$. Se φ se fatora através de um projetivo P, então podemos restringir os mapas envolvidos para concluir que φ_L se fatora através de P_L, que é projetivo pela Proposição 2.2.7. Reciprocamente, suponha que φ_L se fatore através de um kL-módulo projetivo Q. Assim, existem homomorfismos $\alpha : (U_1)_L \to Q$ e $\beta : Q \to (U_2)_L$ tais que $\varphi_L = \beta\alpha$. Provaremos que φ se fatora através de Q^G, que é um kG-módulo projetivo pelo Lema 3.1.10. Pelo Exercício A.3.1, temos um homomorfismo de kG-módulos $\alpha' : U_1 \to Q^G$ dado por

$$\alpha'(u_1) = \sum_{s \in [G/L]} s \otimes \alpha(s^{-1}u_1)$$

para todo $u_1 \in U_1$. Por outro lado, pela propriedade universal de Q^G, existe um homomorfismo de kG-módulos $\beta' : Q^G \to U_2$ que estende β. Dessa forma, se

$$\sum_{s \in [G/L]} s \otimes x_s$$

é um elemento de Q^G (onde $x_s \in Q$), então

$$\beta'\left(\sum_{s \in [G/L]} s \otimes x_s\right) = \sum_{s \in [G/L]} s \cdot \beta(x_s).$$

Com isso, veja que

$$\begin{aligned}\beta'(\alpha'(u_1)) &= \sum_{s \in [G/L]} s \cdot \beta(\alpha(s^{-1}u_1)) \\ &= \sum_{s \in [G/L]} s \cdot \varphi(s^{-1}u_1) \\ &= \sum_{s \in [G/L]} \varphi(u_1) = [G : L] \cdot \varphi(u_1)\end{aligned}$$

para todo $u_1 \in U_1$, onde usamos que φ é homomorfismo de kG-módulos na terceira igualdade. Mas L contém um p-subgrupo de Sylow de G, então p não divide $[G : L]$ e podemos definir um homomorfismo $\beta'' : Q^G \to U_2$ por

$$\beta'' = \frac{1}{[G : L]} \cdot \beta'.$$

Concluímos que $\varphi = \beta''\alpha'$ e, portanto, φ se fatora através de Q^G, como queríamos.

(b) Para não confundir, denote $i = i_{V_1}$ e $\pi = \pi_{V_2}$. Defina também $i_{X_1} : X_1 \to (U_1)_L$ como sendo a outra inclusão e $\pi_{X_2} : (U_2)_L \to X_2$ como sendo a outra projeção. Como vimos na solução do Exercício A.3.15, temos um isomorfismo linear

$$\mathrm{Hom}_{kL}((U_1)_L, (U_2)_L) \to \mathrm{Hom}_{kL}(V_1, (U_2)_L) \oplus \mathrm{Hom}_{kL}(X_1, (U_2)_L)$$

que leva $\varphi : (U_1)_L \to (U_2)_L$ no par $(\varphi i_{V_1}, \varphi i_{X_1})$. Também vimos nessa solução que φ se fatora através de um projetivo se, e somente se, o mesmo vale para φi_{V_1} e φi_{X_1}. Mas, como φi_{X_1} sempre se fatora através de X_1, que é projetivo, então temos:

$$\varphi \text{ se fatora através de projetivo} \iff \varphi i_{V_1} \text{ se fatora através de projetivo.}$$

Agora, também temos um isomorfismo linear

$$\mathrm{Hom}_{kL}(V_1, (U_2)_L) \to \mathrm{Hom}_{kL}(V_1, V_2) \oplus \mathrm{Hom}_{kL}(V_1, X_2)$$

que leva $\psi : V_1 \to (U_2)_L$ no par $(\pi_{V_2}\psi, \pi_{X_2}\psi)$. Como antes, ψ se fatora através de um projetivo se, e só se, o mesmo vale para $\pi_{V_2}\psi$ e $\pi_{X_2}\psi$. Como X_2 é projetivo, podemos "desconsiderar" $\pi_{X_2}\psi$ e temos:

$$\psi \text{ se fatora através de projetivo} \iff \pi_{V_2}\psi \text{ se fatora através de projetivo.}$$

Estamos prontos para concluir o exercício. Note inicialmente que a função que leva $\varphi \in \mathrm{Hom}_{kG}(U_1, U_2)$ em $\pi\varphi i \in \mathrm{Hom}_{kL}(V_1, V_2)$ é linear. Além disso, pelo item (a) e pelo parágrafo anterior, se $\varphi : U_1 \to U_2$ é um homomorfismo de kG-módulos, então:

$$\begin{aligned}\varphi \text{ se fatora através de um projetivo} &\iff \varphi_L \text{ se fatora através de um projetivo} \\ &\iff \pi\varphi i \text{ se fatora através de um projetivo.}\end{aligned}$$

Dessa forma, a transformação linear de $\mathrm{Hom}_{kG}(U_1, U_2)$ em $\mathrm{Hom}_{kL}(V_1, V_2)$ induz uma transformação linear injetora

$$\overline{\mathrm{Hom}}_{kG}(U_1, U_2) \to \overline{\mathrm{Hom}}_{kL}(V_1, V_2)$$

entre os quocientes. Mas o Corolário 3.3.4 diz que os espaços acima possuem a mesma dimensão, então essa transformação linear injetora é um isomorfismo, como queríamos demonstrar.

□

Exercício A.3.17. Se U é um kG-módulo qualquer, mostre que existem kG-módulos projetivos P_1 e P_2 e também kG-módulos W_1 e W_2, cada um sendo uma soma direta de módulos induzidos de normalizadores de p-subgrupos de G diferentes de $\{1\}$, tais que

$$U \oplus P_1 \oplus W_1 \cong P_2 \oplus W_2.$$

Solução: Seja $\mathscr{N}$ a família de subgrupos de G dada por

$$\mathscr{N} := \{N_G(Q) \mid Q \neq \{1\} \text{ é um } p\text{-subgrupo de } G\}.$$

Apenas neste exercício, diremos que um kG-módulo W é relativamente $\mathscr{N}$-livre se W for a soma direta de módulos relativamente L-livres com $L \in \mathscr{N}$. Assim, queremos encontrar módulos projetivos P_1 e P_2 e módulos relativamente $\mathscr{N}$-livres W_1 e W_2 tais que

$$U \oplus P_1 \oplus W_1 \cong P_2 \oplus W_2.$$

Como soma direta de módulos projetivos é um módulo projetivo e como soma direta de módulos relativamente $\mathscr{N}$-livres é um módulo relativamente $\mathscr{N}$-livre, basta mostrar o exercício para U indecomponível. Para isso, faremos indução no tamanho de um vértice Q de U.

Primeiramente, suponha que $|Q| = 1$, ou seja, que $Q = \{1\}$. Nesse caso, sendo U relativamente 1-projetivo, temos que U é projetivo. Dessa forma, podemos tomar $P_1 = W_1 = W_2 = 0$ e $P_2 = U$ para satisfazer as condições desejadas. Agora, suponha que $|Q| > 1$ e que o resultado valha para todo kG-módulo indecomponível com vértice de tamanho menor do que $|Q|$. Definindo $L = N_G(Q)$, a Correspondência de Green garante a existência de um kL-módulo V e de um kG-módulo X relativamente $\mathfrak{X}$-projetivo tais que

$$U \oplus X \cong V^G,$$

onde $\mathfrak{X}$ denota a família

$$\mathfrak{X} = \{Q \cap gQg^{-1} \mid g \in G, g \notin L\}.$$

Como L é o normalizador de Q em G, todo subgrupo em $\mathfrak{X}$ é um subgrupo próprio de Q. Mas todo somando indecomponível de X é relativamente projetivo com relação a um subgrupo em $\mathfrak{X}$, logo,

todo somando indecomponível de X possui um vértice de tamanho estritamente menor do que $|Q|$. Aplicando a hipótese de indução e usando que a propriedade do enunciado é preservada por somas diretas, conseguimos encontrar kG-módulos projetivos P_1' e P_2' e kG-módulos relativamente $\mathscr{N}$-livres W_1' e W_2' tais que

$$X \oplus P_1' \oplus W_1' \cong P_2' \oplus W_2'.$$

Defina

$$P_1 \coloneqq P_2' \quad \text{e} \quad P_2 \coloneqq P_1',$$

que são projetivos, e

$$W_1 \coloneqq W_2' \quad \text{e} \quad W_2 \coloneqq V^G \oplus W_1',$$

que são relativamente $\mathscr{N}$-livres, já que $L \in \mathscr{N}$ e então V^G é relativamente $\mathscr{N}$-livre. Por fim, note que

$$\begin{aligned} U \oplus P_1 \oplus W_1 &= U \oplus P_2' \oplus W_2' \\ &\cong U \oplus X \oplus P_1' \oplus W_1' \\ &\cong V^G \oplus P_1' \oplus W_1' \\ &\cong P_2 \oplus W_2. \end{aligned}$$

Isso conclui a prova por indução e o exercício está resolvido. □

A.4 Teoria dos blocos

Exercício A.4.1. Seja U um A-módulo e sejam $A_1, \ldots, A_r$ os blocos de A com idempotentes associados $e_1, \ldots, e_r$. Se $1 \leq i \leq r$, mostre que são equivalentes:

(1) U pertence a A_i.

(2) $A_i U = U$.

(3) e_i age trivialmente em U.

(4) $A_j U = 0$ para todo $j \neq i$.

(5) $e_j U = 0$ para todo $j \neq i$.

Solução: Pelo Lema 4.1.13, (1) é equivalente às afirmações (3) e (5) juntas. Como visto na prova desse lema, (2) é equivalente a (3), e (4) é equivalente a (5). Assim, é suficiente mostrar que (3) e (5) são equivalentes.

(3) $\implies$ (5). Suponha que e_i aja trivialmente em U. Assim, se $u \in U$ e j é um índice diferente de i, vale

$$e_j u = e_j(e_i u) = (e_j e_i)u = 0 \cdot u = 0.$$

Logo, $e_j U = 0$ para todo índice $j \neq i$.

(5) $\implies$ (3). Suponha que $e_j U = 0$ para todo índice $j \neq i$. Logo, se $u \in U$, então $e_j u = 0$ para $j \neq i$ e temos

$$u = 1 \cdot u = (e_1 + \cdots + e_r)u = e_i u.$$

Isso mostra que e_i age trivialmente em U. □

Exercício A.4.2. Sejam U e V A-módulos. Se U e V pertencem a blocos distintos, demonstre que $\mathrm{Hom}_A(U, V) = 0$ e que toda sequência exata

$$0 \longrightarrow U \longrightarrow W \longrightarrow V \longrightarrow 0$$

cinde.

Solução: Pelo Lema 4.1.14, os fatores de composição de U pertencem ao mesmo bloco ao qual U pertence. Da mesma forma, a afirmação análoga vale para V, então vemos que U e V não possuem fatores de composição em comum. Consequentemente, qualquer homomorfismo de U em V deve ser nulo.

Note que utilizamos que U e V possuem comprimento finito. É possível dar uma demonstração simples que vale num contexto mais geral. Para isso, seja e_U o idempotente associado ao bloco de U. Assim, e_U age trivialmente em U e $e_U V = 0$. Se $\varphi : U \to V$ é um homomorfismo, então

$$\varphi(u) = \varphi(e_U u) = e_U \varphi(u) = 0,$$

para todo $u \in U$, onde utilizamos que $\varphi(u)$ é um elemento de V e, portanto, é anulado por e_U. Isso mostra que $\mathrm{Hom}_A(U, V) = 0$.

Para a segunda afirmação, podemos utilizar o Lema 4.1.18 e mais alguma argumentação, mas optamos por realizar uma provar mais geral e mais simples também. Como fizemos no Lema 4.1.14, W é anulado por qualquer bloco de A diferente dos blocos que "contêm" U e V. Assim, pela Proposição 4.1.15, vale $W = e_U W \oplus e_V W$, onde e_U e e_V são os idempotentes associados aos blocos de U e de V, respectivamente. Se U' é a cópia de U dentro de W, vale

$$U' = e_U U' \subseteq e_U W.$$

Agora, como $W/U' \cong V$ e $e_U V = 0$, temos $e_U W \subseteq U'$. Por isso, $e_U W = U'$ e então U' é um somando direto de W. Concluímos que a sequência exata cinde. □

Exercício A.4.3. Sejam A uma k-álgebra de dimensão finita e B um de seus blocos. Sabemos que existe uma correspondência natural entre os B-módulos e os A-módulos que pertencem a B. Prove que essa correspondência preserva módulos simples, módulos indecomponíveis, módulos projetivos e módulos injetivos.

Solução: Vamos relembrar rapidamente como é a correspondência natural do enunciado. Decompondo A como soma direta de seus blocos, obtemos uma projeção canônica $\pi : A \to B$, que é um homomorfismo de álgebras. Assim, dado um B-módulo U, podemos restringir escalares através de π e ver U como um A-módulo. É fácil ver que $BU = U$ e que qualquer outro bloco de A anula U, mostrando que U pertence ao bloco B. Reciprocamente, podemos considerar a inclusão canônica $i : B \to A$. Ela é quase um homomorfismo de álgebras, só não preserva a unidade. Porém, se U é um A-módulo pertencente a B, então a identidade de B fixa os elementos de U e ainda funciona restringir escalares através de i, tornando U um B-módulo. Não é difícil verificar que essas duas construções são uma a inversa da outra.

Para mostrar que a correspondência preserva simplicidade e indecomponibilidade, é suficiente provar que ela preserva submódulos, já que os espaços vetoriais subjacentes dos módulos são os mesmos. Isso é imediato: se U é um B-módulo e $V \leq U$, então a restrição ainda preserva o fato de que $V \leq U$ como A-módulos. A outra direção também segue diretamente das definições, bastando lembrar que submódulo de um módulo pertencente a B ainda pertence a B.

Para provar que módulos projetivos são preservados, vamos utilizar a caracterização (2) da Proposição 2.2.1. De forma análoga, prova-se que a correspondência preserva módulos injetivos a partir da caracterização (1) da Proposição 2.3.13. Seja P um A-módulo projetivo pertencente a B. Se $\varphi : U \to P$ é um homomorfismo sobrejetor de B-módulos, vejamos que φ cinde. Como U é um B-módulo, podemos ver U como um A-módulo pertencente a B e é fácil ver que φ é também um homomorfismo sobrejetor de A-módulos. Sendo P um A-módulo projetivo, então φ cinde como homomorfismo de A-módulos e existe um homomorfismo de A-módulos $\psi : P \to U$ tal que $\varphi\psi = \mathrm{id}_P$. Novamente, não é difícil verificar que ψ também é homomorfismo de B-módulos, de onde segue que φ cinde como homomorfismo de B-módulos. Concluímos que P é um B-módulo projetivo.

Reciprocamente, seja P um B-módulo projetivo. Para mostrar que P é projetivo como A-módulo, considere $\varphi : U \to P$ um homomorfismo sobrejetor de A-módulos qualquer. Mostremos

que φ cinde. Pela Proposição 4.1.15, podemos escrever $U = U_B \oplus V$, onde U_B é um submódulo pertencente a B e V é a soma direta de submódulos pertencentes aos outros blocos de V. Como P pertence a B, o Exercício A.4.2 implica que a restrição de φ a V é o homomorfismo nulo. Segue então que a outra restrição $\varphi' : U_B \to P$ é homomorfismo sobrejetor. Como U_B pertence a B, agora podemos ver φ' como um homomorfismo sobrejetor de B-módulos. Mas P é um B-módulo projetivo, o que nos dá um homomorfismo de B-módulos $\psi' : P \to U_B$ tal que $\varphi'\psi' = \mathrm{id}_P$. Compondo ψ' com a inclusão $U_B \to U$, obtemos um homomorfismo de A-módulos $\psi : P \to U$ que satisfaz $\varphi\psi = \mathrm{id}_P$, provando que φ cinde, como queríamos. □

Exercício A.4.4. Se S e T são A-módulos simples, prove que S e T pertencem ao mesmo bloco se, e somente se, existe uma sequência

$$S = S_1, S_2, \ldots, S_n = T$$

de módulos simples tais que

$$\mathrm{Hom}_A(P_i, P_{i+1}) \neq 0 \quad \text{ou} \quad \mathrm{Hom}_A(P_{i+1}, P_i) \neq 0$$

para todo $1 \leq i < n$, onde P_j denota a cobertura projetiva de S_j para $1 \leq j \leq n$.

Solução: Pelo Exercício A.2.8, a condição $\mathrm{Hom}_A(P_i, P_{i+1}) \neq 0$ equivale a pedir que S_i seja fator de composição da cobertura projetiva de S_{i+1}. Assim, se está satisfeita a afirmação do enunciado, então também está satisfeito o item (2) do Teorema 4.1.17 e, por isso, S e T pertencem ao mesmo bloco.

Reciprocamente, se S e T pertencem ao mesmo bloco, o item (3) do Teorema 4.1.17 nos dá uma sequência

$$S = S_1, S_2, \cdots, S_n = T$$

de módulos simples tais que S_i e S_{i+1} são isomorfos ou então existe uma extensão de um deles pelo outro que não cinde. Mas, como vimos na demonstração da implicação (3) $\implies$ (2) desse teorema, conseguimos mostrar que S_i é fator de composição da cobertura projetiva de S_{i+1} ou vice-versa, concluindo o exercício. □

Exercício A.4.5. Seja U um kG-módulo.

(a) Mostre que, se U e U^* pertencem a um bloco B de kG, então, para todo kG-módulo V pertencente a B, V^* também pertence a B.

(b) Encontre um exemplo de uma álgebra de grupo kG em característica positiva com um módulo U de modo que U e U^* pertençam a blocos distintos.

Solução: (a) Inicialmente, note que os fatores de composição de U^* são isomorfos aos duais dos fatores de composição de U. De fato, se

$$0 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n = U$$

é uma série de composição de U, então podemos formar a série

$$0 = U^\perp = U_n^\perp \subseteq U_{n-1}^\perp \subseteq \cdots \subseteq U_0^\perp = 0^\perp = U^*.$$

Pelo Lema 2.3.6 e pela Proposição 2.3.8, a série acima é de composição e seus quocientes são isomorfos aos duais dos quocientes da série inicial, como queríamos.

Pelo Lema 4.1.14, um módulo pertence ao bloco B se, e somente se, os seus fatores de composição pertencem ao bloco B. Portanto, juntando com a nossa observação inicial, podemos supor que U e V são simples. Mais ainda, pelo item (2) do Teorema 4.1.17, podemos supor que U e V são fatores de composição de um mesmo módulo projetivo indecomponível

P. Pela Proposição 2.3.8 e pelo Corolário 2.3.12, P^* é projetivo indecomponível e, pela observação inicial, contém U^* e V^* como fatores de composição. Dessa forma, U^* e V^* pertencem ao mesmo bloco. Mas, por hipótese, U^* pertence a B, então o mesmo vale para V^*, como queríamos.

(b) Seja k um corpo algebricamente fechado de característica $p > 0$ e considere $G = C_{pq}$ como sendo o grupo cíclico de ordem pq, onde q é um número primo diferente de p e de 2. Pelo Exemplo 2.2.10, a cobertura projetiva de um kG-módulo simples S apenas contém S como fator de composição. Por isso, pelo Teorema 4.1.17, kG-módulos simples não isomorfos pertencem a blocos diferentes. Agora, seja $\lambda \in k$ satisfazendo $\lambda^q = 1$ e $\lambda \neq 1$. Pelo Exemplo 2.3.19, podemos construir o módulo simples $U \coloneqq S_\lambda$ e ele satisfaz $U^* \cong S_{\lambda^{-1}}$. Como $\lambda \neq 1$ e q é um primo diferente de 2, temos $\lambda^2 \neq 1$ e, assim, $\lambda \neq \lambda^{-1}$. Concluímos que $U \ncong U^*$ e esses módulos pertencem a blocos distintos.

□

Exercício A.4.6. Se U e V pertencem a algum bloco de kG, é verdade que $U \otimes V$ também pertence a esse bloco?

Solução: Não! Por exemplo, tome k algebricamente fechado de característica $p > 2$ e considere $G = \mathrm{SL}_2(p)$. Pelo Exemplo 4.1.20, V_2 pertence a um bloco diferente de V_1 e de V_3. Mas, pelo Lema 2.4.15, $V_2 \otimes V_2 \cong V_1 \oplus V_3$.

Outro exemplo pode ser obtido considerando-se os grupos cíclicos. Se k é algebricamente fechado, o Exemplo 2.2.10 mostra que a cobertura projetiva de um kG-módulo simples S apenas contém S como fator de composição. Pelo Teorema 4.1.17, módulos simples não isomorfos pertencem a blocos diferentes. Assim, se S é um kG-módulo simples diferente do trivial, $S \otimes S$ é simples e pertence a um bloco diferente de S (lembre que as classes de isomorfismo de módulos simples de dimensão 1 formam um grupo com o produto tensorial). □

Exercício A.4.7. Suponha que G possua um p-subgrupo de Sylow normal e cíclico. Usando a notação do Exemplo 2.2.12, mostre que dois kG-módulos simples S e T pertencem ao mesmo bloco se, e somente se,

$$T \cong S \otimes W^{\otimes n}$$

para algum $n \geq 0$. (*Dica:* Mostre que $W^{\otimes n} \cong k$ para algum $n \geq 1$.)

Solução: Começaremos com a dica. Como observamos na Seção 2.4, o conjunto das classes de isomorfismo de kG-módulos de dimensão 1 é um grupo abeliano no qual a multiplicação é dada pelo produto tensorial e a identidade é o módulo trivial k. Esse grupo (chamado de *grupo dual* de G) é finito e, portanto, todo elemento possui ordem finita. Assim, conseguimos encontrar um inteiro $n \geq 1$ tal que $W^{\otimes n} \cong k$.

Uma outra forma de encontrar tal n é utilizando o próprio Exemplo 2.2.12. Como feito nesse exemplo, se a ordem do p-subgrupo de Sylow de G é p^a, então o soco da cobertura projetiva do módulo trivial é isomorfo a $W^{\otimes p^a - 1}$. Mas, pelo Teorema 2.3.17, esse soco é isomorfo a k, como preciso.

Agora, vamos provar a equivalência que o exercício pede.

($\Longrightarrow$) Suponha que S e T pertençam ao mesmo bloco. Pelo item (2) do Teorema 4.1.17, existe uma sequência de módulos simples

$$S = S_1, S_2, \ldots, S_l = T$$

de modo que, para todo $1 \leq i < l$, S_i e S_{i+1} são fatores de composição de um mesmo módulo projetivo indecomponível P_i. Pelo Exemplo 2.2.12, P_i é unisseriado e temos uma descrição precisa de seus fatores de composição: se o fator S_{i+1} aparece "depois" do fator S_i, então existe $n_i \geq 0$ tal que

$$S_{i+1} \cong S_i \otimes W^{\otimes n_i}$$

e, caso contrário, existe $n_i \geq 0$ com

$$S_i \cong S_{i+1} \otimes W^{\otimes n_i}.$$

Mas W possui ordem finita no grupo dual de G, então, nesse segundo caso, podemos achar $n_i' > n_i$ com $W^{\otimes n_i'} \cong k$ e temos

$$S_{i+1} \cong S_{i+1} \otimes W^{\otimes n_i'} \cong (S_{i+1} \otimes W^{\otimes n_i}) \otimes W^{\otimes n_i' - n_i} \cong S_i \otimes W^{\otimes n_i' - n_i}.$$

Logo, para todo $1 \leq i < l$, existe um inteiro $n_i \geq 0$ com $S_{i+1} \cong S_i \otimes W^{\otimes n_i}$. Dessa forma, se $n \coloneqq n_1 + \cdots + n_{l-1}$, então

$$T = S_l \cong S_1 \otimes W^{\otimes n} = S \otimes W^{\otimes n},$$

como queríamos demonstrar.

($\Longleftarrow$) Suponha que exista um inteiro $n \geq 0$ com $T \cong S \otimes W^{\otimes n}$. Como vimos, W possui ordem finita no grupo dual de G e, mais ainda, sabemos que a sua ordem é no máximo $p^a - 1$, onde p^a denota a ordem do p-subgrupo de Sylow de G. Por isso, podemos supor que $n \leq p^a - 1$. Mas então a descrição dada no Exemplo 2.2.12 implica que T é fator de composição da cobertura projetiva de S. Pelo item (2) do Teorema 4.1.17, S e T pertencem ao mesmo bloco. □

Exercício A.4.8. Suponha que k seja algebricamente fechado e de característica $p > 0$. Suponha também que a ordem de um p-subgrupo de Sylow de G seja p^a, com $a \geq 1$. Se B é um bloco de kG de defeito d, mostre que a dimensão de todo kG-módulo pertencente a B é divisível por p^{a-d}.

Solução: Seja U um kG-módulo pertencente a B. Para mostrar que p^{a-d} divide a dimensão de U, é suficiente demonstrar que isso vale quando U é indecomponível. Se D é um grupo de defeito de B, então o Teorema 4.2.2 diz que U possui um vértice Q contido em D. Se P é um p-subgrupo de Sylow de G contendo Q, então o Exercício A.3.12 diz que $[P : Q]$ divide a dimensão de U. Se $|Q| = p^b$ com $b \geq 0$, então $b \leq d \leq a$ e $a - b \geq a - d$, de onde segue que $[P : Q] = p^{a-b}$ é divisível por p^{a-d}. Isso conclui o exercício. □

Exercício A.4.9. Se N é um subgrupo normal de G, mostre que o bloco principal de kG cobre apenas o bloco principal de kN. Conclua que o bloco principal de kN não possui conjugados além dele mesmo, ou seja, seu estabilizador é G.

Solução: Seja b um bloco de kN coberto pelo bloco principal B_0 de kG. Sabemos do item (1) do Teorema 4.4.4 que os blocos cobertos por B_0 são os conjugados de b. Agora, pelo item (3) da Proposição 4.4.2, segue que um bloco b' de kN é coberto por B_0 precisamente quando $b'U \neq 0$, onde U é um kG-módulo não nulo pertencente a B_0. Podemos tomar U como sendo o kG-módulo trivial k e, como k_N é o kN-módulo trivial, ele pertence apenas ao bloco principal de kN. Assim, $b'k \neq 0$ se e só se b' é o bloco principal de kN, de onde concluímos que B_0 apenas cobre o bloco principal b_0 de kN. Novamente pelo item (1) do Teorema 4.4.4, concluímos que $gb_0g^{-1} = b_0$ para todo $g \in G$. □

Exercício A.4.10. Seja k um corpo algebricamente fechado de característica $p > 0$. Se $N \neq \{1\}$ é um subgrupo normal de G cuja ordem não é divisível por p, prove que kG possui mais de um bloco.

Solução: Como p não divide a ordem de N, o Teorema de Maschke diz que kN é semissimples e então seus blocos são todos de defeito zero e cada um deles corresponde a uma classe de isomorfismo de kN-módulos simples. Além disso, como k é algebricamente fechado, o Teorema de Brauer diz que o número de classes de isomorfismo de kN-módulos simples é igual ao número de classes de conjugação de N. Como $N \neq \{1\}$, esse número é maior do que 1 e obtemos que kN possui ao menos dois blocos. Pelo Exercício A.4.9, o bloco principal de kG cobre apenas o bloco principal de kN. Mas kN possui pelo menos um bloco não principal, que deve ser coberto necessariamente por um bloco não principal de kG. Concluímos que kG possui pelo menos dois blocos. □

Exercício A.4.11. Se Q é um p-subgrupo normal de G e $Q \supseteq C_G(Q)$, mostre que kG possui exatamente um bloco. Tomando o grupo simétrico $G = S_4$, use esse resultado para concluir que kS_4 possui exatamente um bloco quando $p = 2$.

Solução: Como Q é um p-grupo, sabemos que o único bloco de kQ é o principal, já que existe apenas uma classe de isomorfismo de kQ-módulos simples. Um grupo de defeito desse bloco principal é um p-subgrupo de Sylow de Q e, por isso, é o próprio Q. Como $C_G(Q) \subseteq Q$, o item (2) do Teorema 4.4.4 nos diz que o bloco principal de kQ é coberto por exatamente um bloco de kG. Ou seja, existe um único bloco de kG cobrindo o único bloco de kQ. Como todo bloco de kG cobre algum bloco de kQ, concluímos que kG possui apenas um único bloco.

Agora, considere $G = S_4$ e $p = 2$. Lembre que

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

é um subgrupo normal de S_4. Pelo parágrafo anterior, para mostrar que kS_4 possui exatamente um bloco, basta mostrar que $C_{S_4}(Q) \subseteq Q$. Vamos mostrar que vale a igualdade. Como Q é abeliano, certamente vale $Q \subseteq C_{S_4}(Q)$. Por outro lado, $C_{S_4}(Q)$ está contido no centralizador do elemento $(1\ 2)(3\ 4)$. Como a classe de conjugação de $(1\ 2)(3\ 4)$ possui três elementos (são os elementos de Q diferentes de 1), concluímos que seu centralizador possui $24/3 = 8$ elementos. Note que $(1\ 2)$ comuta com $(1\ 2)(3\ 4)$, mas

$$(1\ 2) \cdot (1\ 3)(2\ 4) = (1\ 3\ 2\ 4) \neq (1\ 4\ 2\ 3) = (1\ 3)(2\ 4) \cdot (1\ 2).$$

Isso mostra que $(1\ 2) \in C_{S_4}((1\ 2)(3\ 4))$, mas $(1\ 2) \notin C_{S_4}(Q)$. Como $C_{S_4}(Q)$ está contido propriamente em $C_{S_4}((1\ 2)(3\ 4))$, que possui ordem 8, segue do Teorema de Lagrange que $C_{S_4}(Q)$ possui no máximo 4 elementos. Mas $Q \subseteq C_{S_4}(Q)$ e $|Q| = 4$, então devemos ter $C_{S_4}(Q) = Q$, como preciso. □

Exercício A.4.12. Se D e D' são subgrupos conjugados de G, mostre que $N_G(D)$ e $N_G(D')$ também são conjugados. Verifique que essa conjugação pode ser tomada de modo a levar D em D' e $DC_G(D)$ em $D'C_G(D')$. Conclua que $DC_G(D)/D \cong D'C_G(D')/D'$.

Solução: Seja $g \in G$ tal que $D' = gDg^{-1}$. Afirmamos que $N_G(D') = gN_G(D)g^{-1}$ e $C_G(D') = gC_G(D)g^{-1}$. Isso pode ser verificado diretamente, mas vamos provar isso utilizando algo mais geral e ilustrativo.

Suponha que G aja (à esquerda) num conjunto X. Se $x \in X$, mostremos que $\operatorname{Stab}(gx) = g \operatorname{Stab}(x) g^{-1}$, onde $\operatorname{Stab}(x)$ e $\operatorname{Stab}(gx)$ denotam os estabilizadores de x e gx, respectivamente. Se $ghg^{-1} \in g \operatorname{Stab}(x) g^{-1}$, onde $h \in \operatorname{Stab}(x)$, então temos

$$(ghg^{-1}) \cdot gx = (ghg^{-1}g)x = (gh)x = g \cdot hx = g \cdot x = gx,$$

mostrando que $ghg^{-1} \in \operatorname{Stab}(gx)$. Logo, $g \operatorname{Stab}(x) g^{-1} \subseteq \operatorname{Stab}(gx)$. Mas o mesmo argumento nos dá

$$g^{-1} \operatorname{Stab}(gx) g \subseteq \operatorname{Stab}(g^{-1}(gx)) = \operatorname{Stab}(x) \implies \operatorname{Stab}(gx) \subseteq g \operatorname{Stab}(x) g^{-1}$$

e está provado o que queríamos mostrar.

Agora, G age no conjunto dos seus subgrupos por conjugação e o estabilizador de um subgrupo é, por definição, o seu normalizador. Por isso,

$$N_G(D') = \operatorname{Stab}(gDg^{-1}) = g \operatorname{Stab}(D) g^{-1} = gN_G(D)g^{-1}.$$

Mas G também age em seus elementos por conjugação e o estabilizador de um elemento é, por definição, o seu centralizador. Logo, o mesmo argumento mostra que $C_G(gdg^{-1}) = gC_G(d)g^{-1}$ para todo $d \in D$ e temos

$$C_G(D') = \bigcap_{d \in D} C_G(gdg^{-1}) = \bigcap_{d \in D} gC_G(d)g^{-1} = g \left(\bigcap_{d \in D} C_G(d) \right) g^{-1} = gC_G(D)g^{-1},$$

como preciso.

Vamos concluir o exercício. A conjugação por g leva D em D' e $N_G(D)$ em $N_G(D')$. Também vale

$$g(DC_G(D))g^{-1} = gDg^{-1} \cdot gC_G(D)g^{-1} = D'C_G(D')$$

e então $DC_G(D)$ é levado em $D'C_G(D')$. Como a conjugação por g nos dá um isomorfismo de $DC_G(D)$ em $D'C_G(D')$ que leva D em D', obtemos $DC_G(D)/D \cong D'C_G(D')/D'$. □

Exercício A.4.13. Seja $H \leq G$. Seja b um bloco de kH com grupo de defeito D. Se $g \in G$, mostre que gbg^{-1} é um bloco de $k[gHg^{-1}]$ com grupo de defeito gDg^{-1}.

Solução: Logo após o enunciado do Teorema 4.5.4, foi explicado o porquê de gbg^{-1} ser um bloco de $k[gHg^{-1}]$. Precisamos verificar apenas que gDg^{-1} é de fato um grupo de defeito de gbg^{-1}. Pelo Corolário 4.3.6, existe um kH-módulo indecomponível V pertencente a b que possui D como vértice. Desse modo, ${}^gV$ é um $k[gHg^{-1}]$-módulo indecomponível e possui gDg^{-1} como vértice (Exercício A.3.9). Agora, imitando o argumento dado no último parágrafo da demonstração do Lema 4.4.9, obtemos que ${}^gV$ pertence a gbg^{-1} e, pelo Teorema 4.2.2, gDg^{-1} está contido em um grupo de defeito D' de gbg^{-1}. Por outro lado, podemos desfazer a conjugação e utilizar esse mesmo raciocínio para mostrar que $g^{-1}D'g$ está contido em um grupo de defeito de b. Isso implica que D e D' possuem a mesma ordem, de onde concluímos que $D' = gDg^{-1}$. □

Exercício A.4.14. Seja $H \leq G$. Seja b um bloco de kH e tome um bloco B de kG tal que $b \mid B_{H\times H}$. Se $g \in G$, então sabemos que gbg^{-1} é um bloco de $k[gHg^{-1}]$.

(a) Prove que ${}^{(g,g)}b \cong gbg^{-1}$ como $k[gHg^{-1} \times gHg^{-1}]$-módulos.

(b) Conclua que gbg^{-1} é um somando direto de $B_{gHg^{-1}\times gHg^{-1}}$.

(c) Use o item anterior para mostrar que conjugados de B-subgrupos de G também são B-subgrupos. Verifique que a conjugação também preserva B-subgrupos de Sylow.

Solução: Logo após o enunciado do Teorema 4.5.4, foi explicado o porquê de gbg^{-1} ser um bloco de $k[gHg^{-1}]$.

(a) Note que ${}^{(g,g)}b$ é de fato um $k[gHg^{-1}\times gHg^{-1}]$-módulo. Seja $\varphi : {}^{(g,g)}b \to gbg^{-1}$ o isomorfismo linear dado pela conjugação. Se $(gh_1g^{-1}, gh_2g^{-1}) \in gHg^{-1} \times gHg^{-1}$ e se $x \in {}^{(g,g)}b$, então

$$\begin{aligned}\varphi((gh_1g^{-1}, gh_2g^{-1}) \cdot x) &= \varphi(h_1xh_2^{-1}) \\ &= gh_1xh_2^{-1}g^{-1} \\ &= (gh_1g^{-1})(gxg^{-1})(gh_2g^{-1})^{-1} \\ &= (gh_1g^{-1}, gh_2g^{-1}) \cdot \varphi(x).\end{aligned}$$

Portanto, φ é também um homomorfismo de $k[gHg^{-1} \times gHg^{-1}]$-módulos e o isomorfismo desejado está estabelecido.

(b) Como $b \mid B_{H\times H}$, podemos conjugar ambos os módulos por (g, g) para obter

$${}^{(g,g)}b \mid {}^{(g,g)}(B_{H\times H}) = \left({}^{(g,g)}B\right)_{(g,g)(H\times H)(g,g)^{-1}} \cong B_{gHg^{-1}\times gHg^{-1}}.$$

O último isomorfismo vale porque ${}^{(g,g)}B \cong B$, já que B é um $k[G \times G]$-módulo (veja o item (c) do Exercício A.3.4). Pelo item anterior, ${}^{(g,g)}b \cong gbg^{-1}$ e concluímos que gbg^{-1} é um somando direto de $B_{gHg^{-1}\times gHg^{-1}}$.

(c) Seja (Q, b) um B-subgrupo de G. Assim, $b^G = B$ e, em particular, $b \mid B_{QC_G(Q)\times QC_G(Q)}$. Se $g \in G$, então sabemos que o conjugado (gQg^{-1}, gbg^{-1}) é um subpar. Como $(gbg^{-1})^G$ está definido, segue do item anterior que $(gbg^{-1})^G = B$, mostrando que (gQg^{-1}, gbg^{-1}) também é um B-subgrupo de G. Por fim, se (Q, b) é um B-subgrupo de Sylow, então Q é um grupo de defeito de B, logo o conjugado gQg^{-1} também é um grupo de defeito de B e concluímos que (gQg^{-1}, gbg^{-1}) também é um B-subgrupo de Sylow.

□

Exercício A.4.15. Generalize o Exercício A.3.11: se Q é um subgrupo do grupo de defeito D do bloco B de kG, mostre que existe um kG-módulo indecomponível pertencente a B com vértice Q.

Solução: Pela Observação 4.4.8, existe um bloco b_D de $kDC_G(D)$ tal que $b_D^G = B$. Assim, (D, b_D) é um B-subgrupo (de Sylow) de G. Pelo Teorema 4.5.5, existe um bloco b_Q de $kQC_G(Q)$ tal que $(Q, b_Q) \subseteq (D, b_D)$ e, consequentemente, (Q, b_Q) é um B-subgrupo de G. Observe que $b \coloneqq b_Q^{N_G(Q)}$ é um bloco de $kN_G(Q)$ e que, pelo Lema 4.3.1, $b^G = b_Q^G = B$. Procedendo como na demonstração do Corolário 4.3.6, conseguimos construir um $kN_G(Q)$-módulo indecomponível V pertencente a b e com vértice Q. Estamos nas condições de aplicar a Correspondência de Green e podemos tomar o kG-módulo U que é o correspondente de Green de V. Dessa forma, U é indecomponível, possui vértice Q e, pelo Corolário 4.3.5, U pertence a $b^G = B$, como desejado. □

Exercício A.4.16. Suponha que k seja algebricamente fechado. Se (Q, b_Q) é um subpar de G, podemos olhar para o subgrupo $S \coloneqq \mathrm{Stab}(b_Q)$ de $N_G(Q)$. Prove que (Q, b_Q) é um b_Q^S-subgrupo de Sylow de S se, e somente se, (Q, b_Q) é um b_Q^G-subgrupo de Sylow de G.

Solução: ($\Longleftarrow$) Suponha que (Q, b_Q) seja um b_Q^G-subgrupo de Sylow de G, isto é, suponha que Q seja um grupo de defeito de b_Q^G. Como todo grupo de defeito de b_Q contém Q (porque Q é normal em $QC_G(Q)$), o Lema 4.3.1 mostra que b_Q^S possui um grupo de defeito contendo Q. Por outro lado, como $b_Q^G = (b_Q^S)^G$, todo grupo de defeito de b_Q^S está contido em um grupo de defeito de b_Q^G, que é conjugado a Q e então tem cardinalidade $|Q|$. Assim, por questões de ordem, concluímos que Q é um grupo de defeito de b_Q^S, mostrando que (Q, b_Q) é um b_Q^S-subgrupo de Sylow de S.

($\Longrightarrow$) Suponha que (Q, b_Q) seja um b_Q^S-subgrupo de Sylow de S, isto é, suponha que Q seja um grupo de defeito de b_Q^S. Como todo grupo de defeito de b_Q contém Q e está contido em um grupo de defeito de b_Q^S, obtemos que b_Q possui Q como grupo de defeito. Agora, observe que $QC_G(Q)$ é normal em S e que o estabilizador de b_Q em S é o próprio S. Assim, como k é algebricamente fechado e como b_Q^S é o único bloco de kS cobrindo b_Q, segue do item (5) do Teorema 4.4.4 que

$$[S : QC_G(Q)]_p = [Q : Q \cap QC_G(Q)] = [Q : Q] = 1.$$

Isso mostra que b_Q é um bloco de $kQC_G(Q)$ com grupo de defeito Q e tal que $[\mathrm{Stab}(b_Q) : QC_G(Q)]$ não é divisível por p. Pelo Lema 4.4.6 (e por sua demonstração), concluímos que b_Q^G possui grupo de defeito Q, ou seja, (Q, b_Q) é um b_Q^G-subgrupo de Sylow de G.

Este exercício é uma generalização de uma propriedade de p-subgrupos para B-subgrupos! De fato, como estamos considerando $S \subseteq N_G(Q)$, segue que S é exatamente o estabilizador do subpar (Q, b_Q) na ação de G por conjugação. No caso de subgrupos, o estabilizador de Q na ação por conjugação é o normalizador $N_G(Q)$ e sabemos que Q é um p-subgrupo de Sylow de $N_G(Q)$ se e só se Q é um p-subgrupo de Sylow de G. Imitando a prova feita para o caso de grupos, conseguimos obter uma outra demonstração para a implicação ($\Longrightarrow$)!

Para a demonstração alternativa, suponha que (Q, b_Q) seja um b_Q^S-subgrupo de Sylow de S mas não um b_Q^G-subgrupo de Sylow de G. Pelo Teorema 4.5.4, podemos encontrar um b_Q^G-subgrupo de Sylow (D, b_D) contendo (Q, b_Q) e deve valer $Q \subsetneq D$. Mas Q é subnormal em D, então conseguimos encontrar um subgrupo R com $Q \subsetneq R \subseteq D$ e Q normal em R. Pelo Teorema 4.5.5, existe um

subpar (R, b_R) contido em (D, b_D) e outro subpar (Q, b'_Q) normal em (R, b_R). Como (Q, b_Q) e (Q, b'_Q) estão ambos contidos em (D, b_D), o Teorema 4.5.5 também nos dá $b_Q = b'_Q$. Assim, (Q, b_Q) é normal em (R, b_R), implicando que R estabiliza Q e b_Q, ou seja, $R \subseteq S$. Por outro lado, também temos $C_G(R) \subseteq C_G(Q) \subseteq S$, então $RC_G(R) \subseteq S$ e podemos ver (R, b_R) como um b-subgrupo para algum bloco b de kS. Mas então a continência $(Q, b_Q) \subsetneq (R, b_R)$ diz que $b = b_Q^S$, o que contradiz o fato de (Q, b_Q) ser um b_Q^S-subgrupo de Sylow de S. □

A.5 Blocos com grupo de defeito cíclico

Exercício A.5.1. Se A é uma álgebra de Brauer, descreva como são os submódulos dos A-módulos projetivos indecomponíveis a partir da árvore de Brauer.

Solução: Seja P um A-módulo projetivo indecomponível. Ele é a cobertura projetiva de um módulo simples S que corresponde a uma aresta da árvore de Brauer. Se v e w são os extremos desta aresta, a definição de álgebra de Brauer nos fornece dois módulos unisseriados P_v e P_w tais que $\operatorname{rad}(P)/\operatorname{soc}(P) \cong P_v \oplus P_w$. É importante observar que P_v e P_w não possuem fatores de composição em comum. De fato, o único possível fator de composição em comum seria S, que é o único módulo simples incidindo sobre v e sobre w ao mesmo tempo. Porém, a única forma de S aparecer como fator de composição de P_v e de P_w é se v e w forem ambos excepcionais, o que não acontece já que há apenas um único vértice excepcional.

Seja U um submódulo de P. Se U é não nulo e próprio, então $\operatorname{soc}(P) \subseteq U \subseteq \operatorname{rad}(P)$, já que $\operatorname{soc}(P)$ e $P/\operatorname{rad}(P)$ são simples e, por isso, $\operatorname{soc}(P)$ é o único submódulo minimal e $\operatorname{rad}(P)$ é o único submódulo maximal. Dessa forma, U corresponde a um submódulo de $\operatorname{rad}(P)/\operatorname{soc}(P) \cong P_v \oplus P_w$. Logo, basta determinar os submódulos de $P_v \oplus P_w$.

Suponha agora que U denote um submódulo de $P_v \oplus P_w$. Vamos provar que $U = U_v \oplus U_w$ para certos submódulos $U_v \leq P_v$ e $U_w \leq P_w$. Sejam U_v e U_w os maiores submódulos de P_v e de P_w, respectivamente, tais que $U_v, U_w \subseteq U$. Esses submódulos existem, porque P_v e P_w são unisseriados, e podem ser nulos. Dessa maneira, $U_v \oplus U_w \subseteq U$. Afirmamos que vale a igualdade. De fato, se isso não acontece, então U corresponde a um submódulo não nulo $\overline{U}$ de

$$\frac{P_v \oplus P_w}{U_v \oplus U_w} \cong \frac{P_v}{U_v} \oplus \frac{P_w}{U_w}.$$

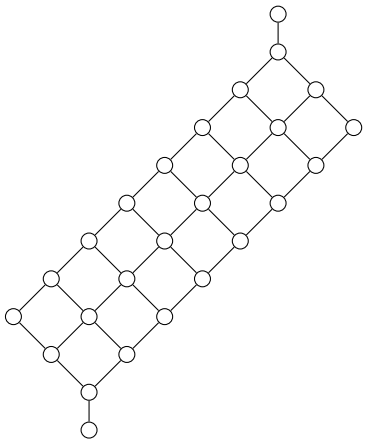
Em particular, $\operatorname{soc}(\overline{U}) \neq 0$ e este é um submódulo de

$$\operatorname{soc}\left(\frac{P_v}{U_v} \oplus \frac{P_w}{U_w}\right) = \operatorname{soc}\left(\frac{P_v}{U_v}\right) \oplus \operatorname{soc}\left(\frac{P_w}{U_w}\right).$$

Pelo menos um dentre $\operatorname{soc}(P_v/U_v)$ e $\operatorname{soc}(P_w/U_w)$ é não nulo, então se mostrarmos que $\operatorname{soc}(\overline{U})$ contém um deles, seguirá que U contém um submódulo de P_v maior do que U_v ou um submódulo de P_w maior do que U_w, chegando numa contradição. Como P_v e P_w são unisseriados e não possuem fatores de composição em comum, $\operatorname{soc}(P_v/U_v)$ e $\operatorname{soc}(P_w/U_w)$ são nulos ou são módulos simples não isomorfos. Portanto, basta mostrar que, se S_1 e S_2 são módulos simples não isomorfos, então os únicos submódulos próprios e não nulos de $S_1 \oplus S_2$ são as cópias canônicas de S_1 e de S_2 na soma direta. Com efeito, um submódulo $V \leq S_1 \oplus S_2$ próprio e não nulo é isomorfo a algum S_i, digamos S_1. Então a composição da inclusão de V em $S_1 \oplus S_2$ junto com a projeção de $S_1 \oplus S_2$ em S_2 deve ser nula, já que $V \cong S_1$ e S_2 são simples não isomorfos. Isso implica que V está contido na cópia canônica de S_1 dentro de $S_1 \oplus S_2$ e, como ela é simples, V é igual a essa cópia canônica, como queríamos demonstrar.

Concluímos que os submódulos de $P_v \oplus P_w$ são da forma $U_v \oplus U_w$ com $U_v \leq P_v$ e $U_w \leq P_w$. Por sua vez, como P_v e P_w são unisseriados, os seus submódulos são dados por suas séries radicais. Por fim, os fatores de composição são determinados pela árvore de Brauer. Desse modo, conseguimos deduzir quais são os submódulos de P e como são as suas estruturas.

Com essa descrição, podemos desenhar facilmente o reticulado de submódulos de P! Vamos dar um exemplo concreto: suponha que P_v possua comprimento 2 e P_w possua comprimento 7. Então o reticulado de submódulos de P é:



No grafo acima, cada vértice representa um submódulo de P e dois vértices estão conectados se o submódulo de cima contém o submódulo debaixo e o quociente de um pelo outro é simples, ou seja, não há outro submódulo entre eles. Observe que temos um único submódulo maximal e um único submódulo minimal, que são $\mathrm{rad}(P)$ e $\mathrm{soc}(P)$, respectivamente. Entre eles, temos um quadriculado 2×7 que forma o reticulado de submódulos de $\mathrm{rad}(P)/\mathrm{soc}(P)$. No caso geral, se P_v possui comprimento m e P_w possui comprimento n, trocamos esse quadriculado por um quadriculado $m \times n$. □

Exercício A.5.2. Seja A uma álgebra de Brauer e sejam $T_1, \ldots, T_t$ os A-módulos simples que incidem sobre um vértice v da árvore de Brauer. Suponha que a ordenação circular desses módulos seja a ordenação dada pela numeração. Se v possui multiplicidade m (tomando $m = 1$ se v não é excepcional) e se q é um inteiro positivo menor ou igual a mt, mostre que, a menos de isomorfismo, existe um único A-módulo unisseriado de comprimento q cujo primeiro fator de composição é T_1, cujo próximo fator de composição é T_2, e assim em diante, usando a ordenação circular dos T_i's.

Solução: Vamos analisar a cobertura projetiva P do simples T_1. Sabemos que $\mathrm{rad}(P)/\mathrm{soc}(P)$ é a soma direta de dois módulos unisseriados P_v e P_w, onde w denota o extremo da aresta correspondente a T_1 diferente de v. Pelo algoritmo dado na definição de álgebra de Brauer, sabemos que o comprimento de P_v é $mt - 1$ e seus fatores de composição são $T_2, T_3, \ldots$, nessa ordem. Seja V o submódulo de P_v tal que P_v/V possui comprimento $q-1$. Como $q \leq mt$, podemos encontrar tal submódulo V e observe que P_v/V é unisseriado e seus fatores de composição ainda seguem a ordenação circular, começando de T_2. Assim, $V \oplus P_w$ é um submódulo de $P_v \oplus P_w \cong \mathrm{rad}(P)/\mathrm{soc}(P)$ e, voltando pelo quociente, esse submódulo corresponde a um submódulo U de $\mathrm{rad}(P)$ contendo $\mathrm{soc}(P)$.

Mostremos que P/U é o A-módulo procurado, isto é, provemos que P/U é unisseriado de comprimento q cujo primeiro fator de composição é T_1, depois T_2, e assim em diante. Como $U \subseteq \mathrm{rad}(P)$, vale

$$\mathrm{rad}\left(\frac{P}{U}\right) = \mathrm{rad}(A) \cdot \frac{P}{U} = \frac{\mathrm{rad}(A) \cdot P}{U} = \frac{\mathrm{rad}(P)}{U}.$$

Dessa forma,

$$\frac{P/U}{\mathrm{rad}(P/U)} = \frac{P/U}{\mathrm{rad}(P)/U} \cong \frac{P}{\mathrm{rad}(P)} \cong T_1.$$

Logo, basta mostrar que $\mathrm{rad}(P/U)$ é unisseriado de comprimento $q-1$ e seus fatores de composição seguem a ordenação cíclica, começando de T_2. Mas temos

$$\mathrm{rad}\left(\frac{P}{U}\right) = \frac{\mathrm{rad}(P)}{U} \cong \frac{\mathrm{rad}(P)/\mathrm{soc}(P)}{U/\mathrm{soc}(P)} \cong \frac{P_v \oplus P_w}{V \oplus P_w} \cong P_v/V$$

e já sabemos que P_v/V satisfaz a propriedade desejada. Isso prova a existência do módulo requerido no exercício.

Resta garantir que há somente um módulo com a propriedade em questão. Seja W um A-módulo como no enunciado. Como $W/\operatorname{rad}(W) \cong T_1$, o Lema 2.2.5 mostra que $W \cong P/U'$ para algum submódulo U' de P. Como $W \neq 0$, vale $U' \neq P$ e temos $U' \subseteq \operatorname{rad}(P)$. Por outro lado, o comprimento de P é pelo menos $mt + 1 > q$, então $W \ncong P$ e devemos ter $U' \neq 0$, implicando $\operatorname{soc}(P) \subseteq U'$. A partir disso, vamos mostrar que $U' = U$. Como U' está contido no radical de P, sabemos que $\operatorname{rad}(W) \cong \operatorname{rad}(P)/U'$. Assim, como U' contém o soco de P, U' corresponde a um submódulo V' de $P_v \oplus P_w$ e este satisfaz

$$\frac{P_v \oplus P_w}{V'} \cong \frac{\operatorname{rad}(P)/\operatorname{soc}(P)}{U'/\operatorname{soc}(P)} \cong \frac{\operatorname{rad}(P)}{U'} \cong \operatorname{rad}(W).$$

Basta provar que $V' = V \oplus P_w$. Pelo Exercício A.5.1, $V' = V_v \oplus V_w$ para certos submódulos $V_v \leq P_v$ e $V_w \leq P_w$. Como $\operatorname{rad}(W)$ é unisseriado, devemos ter $V_v = P_v$ ou $V_w = P_w$. No primeiro caso, temos

$$\frac{P_w}{V_w} \cong \frac{P_v \oplus P_w}{P_v \oplus V_w} = \frac{P_v \oplus P_w}{V'} \cong \operatorname{rad}(W),$$

mas P_w e $\operatorname{rad}(W)$ não possuem fatores de composição em comum (por um argumento análogo ao dado no Exercício A.5.1), então deve valer $\operatorname{rad}(W) = 0$ e segue $V_w = P_w$. Em resumo, em qualquer caso vale $V_w = P_w$ e, consequentemente,

$$\frac{P_v}{V_v} \cong \frac{P_v \oplus P_w}{V_v \oplus P_w} = \frac{P_v \oplus P_w}{V'} \cong \operatorname{rad}(W).$$

Como P_v é unisseriado, P_v possui um único submódulo cujo quociente possui comprimento $q-1$, que é V. Concluímos que $V_v = V$ e, assim, $V' = V \oplus P_w$. Logo, $U = U'$ e temos $W \cong P/U$, provando a unicidade desejada. □

Exercício A.5.3. Seja D um grupo cíclico de ordem p^n, com $n \geq 1$. Se D_1 é o subgrupo de D de ordem p, prove que o subgrupo de $\operatorname{Aut}(D)$ formado pelos elementos que agem trivialmente em D_1 possui ordem p^{n-1}.

Solução: Se x é um gerador de D, então

$$D_1 = \langle x^{p^{n-1}} \rangle = \{1, x^{p^{n-1}}, \ldots, x^{(p-1)p^{n-1}}\}.$$

Se $\varphi : D \to D$ é um automorfismo, então $\varphi(x) = x^d$ para algum d coprimo com p^n, ou seja, não divisível por p. Logo, φ fixa D_1 se e só se

$$x^{d \cdot i \cdot p^{n-1}} = x^{i \cdot p^{n-1}}$$

para todo $0 \leq i \leq p-1$. Mas isso acontece exatamente quando

$$d \cdot p^{n-1} \equiv p^{n-1} \pmod{p^n} \iff d \equiv 1 \pmod{p}.$$

Como número de elementos entre 1 e p^n que são congruentes a 1 modulo p é p^{n-1}, concluímos que o subgrupo de $\operatorname{Aut}(D)$ que age trivialmente em D_1 tem a ordem desejada. □

Exercício A.5.4. Para este exercício, utilizaremos as notações do final da demonstração da Proposição 5.2.3, a única diferença é que E denotará uma álgebra qualquer agora.

(a) Se U e V são E-módulos, mostre que

$$\operatorname{Hom}_E(U, V) \cong \operatorname{Hom}_{M_d(E)}(U_d, V_d).$$

(b) Se W é um $M_d(E)$-módulo, encontre um E-módulo V tal que $W \cong V_d$.

Solução: (a) Ao final da demonstração da Proposição 5.2.3, verificamos que

$$\mathrm{End}_E(U) \cong \mathrm{End}_{M_d(E)}(U_d).$$

A prova deste item será semelhante, mas não utilizaremos o Corolário 1.2.7 como anteriormente.

Se $\varphi : U \to V$ é um homomorfismo de E-módulos, então podemos definir a função $\varphi_d : U_d \to V_d$ por

$$\varphi_d(u_1, \ldots, u_d) = (\varphi(u_1), \ldots, \varphi(u_d))$$

para todos $u_1, \ldots, u_d \in U$. Não é difícil verificar que $\varphi_d \in \mathrm{Hom}_{M_d(E)}(U_d, V_d)$. Isso define uma transformação linear de $\mathrm{Hom}_E(U, V)$ em $\mathrm{Hom}_{M_d(E)}(U_d, V_d)$ que é injetora. A maior dificuldade será verificar que essa transformação linear é sobrejetora.

Seja $\psi : U_d \to V_d$ um homomorfismo de $M_d(E)$-módulos. Vamos encontrar $\varphi \in \mathrm{Hom}_E(U, V)$ tal que $\varphi_d = \psi$. O primeiro passo é demonstrar que ψ é uma transformação "diagonal", como já veremos. Sejam $\mu_U^i : U \to U_d$ e $\mu_V^i : V \to V_d$ as i-ésimas inclusões canônicas e sejam $\pi_U^i : U_d \to U$ e $\pi_V^i : V_d \to V$ as i-ésimas projeções canônicas. Defina

$$\psi_{ij} \coloneqq \pi_V^j \psi \mu_U^i$$

para todos $1 \leq i, j \leq d$. Vamos mostrar que $\psi_{ij} = 0$ se $i \neq j$. Primeiramente, note que

$$\psi = \mathrm{id}_{V_d} \circ \psi \circ \mathrm{id}_{U_d} = \left(\sum_{j=1}^{d} \mu_V^j \pi_V^j \right) \psi \left(\sum_{i=1}^{d} \mu_U^i \pi_U^i \right) = \sum_{i,j=1}^{d} \mu_V^j \psi_{ij} \pi_U^i.$$

Se $e_{ij} \in M_d(E)$ denota a matriz elementar cuja (i, j)-ésima entrada é 1, temos

$$\begin{aligned} \psi(e_{ij} \cdot (u_1, \ldots, u_d)) &= \psi(0, \ldots, u_j, \ldots, 0) \\ &= \sum_{r,s=1}^{d} \mu_V^s \psi_{rs} \pi_U^r (0, \ldots, u_j, \ldots, 0) \\ &= \sum_{s=1}^{d} \mu_V^s \psi_{is}(u_j) \end{aligned}$$

para todos $u_1, \ldots, u_d \in U$. Acima, $(0, \ldots, u_j, \ldots, 0)$ denota o vetor-coluna cuja i-ésima coordenada vale u_j e cujas outras coordenadas são nulas. Mas ψ é um homomorfismo de $M_d(E)$-módulos, então isso é igual a

$$e_{ij} \cdot \psi(u_1, \ldots, u_d) = e_{ij} \cdot \sum_{r,s=1}^{d} \mu_V^s \psi_{rs} \pi_U^r (u_1, \ldots, u_d) = \sum_{r=1}^{d} \mu_V^i \psi_{rj}(u_r).$$

Como a imagem de inclusões μ_V^s distintas estão em coordenadas distintas de V_d, concluímos que, se $s \neq i$,

$$\mu_V^s \psi_{is}(u_j) = 0 \implies \psi_{is}(u_j) = 0$$

para todo $u_j \in U$ e então $\psi_{is} = 0$, e, tomando $s = i$,

$$\psi_{ii}(u_j) = \sum_{r=1}^{d} \psi_{rj}(u_r)$$

para todos $u_1, \ldots, u_d \in U$. Como $\psi_{is} = 0$ para todo $s \neq i$ e como i era qualquer, vemos que $\psi_{ij} = 0$ sempre que $i \neq j$. Usando essa informação na última igualdade em destaque acima, obtemos $\psi_{ii}(u_j) = \psi_{jj}(u_j)$ para todo $u_j \in U$, ou seja, $\psi_{ii} = \psi_{jj}$. Desse modo, se denotarmos $\varphi \coloneqq \psi_{11}$, vemos que

$$\psi(u_1, \ldots, u_d) = \sum_{i,j}^{d} \mu_V^j \psi_{ij} \pi_U^i(u_1, \ldots, u_d) = \sum_{i=1}^{d} \mu_V^i \varphi(u_i) = (\varphi(u_1), \ldots, \varphi(u_d))$$

para todos $u_1, \ldots, u_d \in U$. Como ψ comuta com matrizes escalares de $M_d(E)$, é imediato que $\varphi \in \operatorname{Hom}_E(U, V)$ e então concluímos que $\psi = \varphi_d$, como queríamos. Isso mostra o isomorfismo pedido no exercício.

(b) Denote por V o subespaço $e_{11}W$ de W (como no item anterior, e_{ij} denotará a matriz elementar com entrada 1 na coordenada (i, j)). Vendo E como a subálgebra de $M_d(E)$ formada pelas matrizes escalares, é imediato que V é um E-submódulo de W, já que as matrizes escalares comutam com e_{11}. Vamos mostrar que $W \cong V_d$. Defina a transformação linear $\psi : V_d \to W$ por

$$\psi(v_1, \ldots, v_d) = \sum_{i=1}^{d} e_{i1} v_i$$

para todos $v_1, \ldots, v_d \in V$. Note que ψ é injetora: se $\psi(v_1, \ldots, v_d) = 0$, então

$$v_j = e_{11} v_j = e_{1j} e_{j1} v_j = e_{1j} \cdot \sum_{i=1}^{d} e_{i1} v_i = e_{1j} \cdot \psi(v_1, \ldots, v_d) = e_{1j} \cdot 0 = 0$$

para todo $1 \leq j \leq d$. Aqui utilizamos que $v_j = e_{11} v_j$, porque $v_j \in V = e_{11}W$ e $e_{11}^2 = e_{11}$. A transformação ψ também é sobrejetora: se $w \in W$, então

$$w = 1 \cdot w = \sum_{i=1}^{d} e_{ii} w = \sum_{i=1}^{d} e_{i1}(e_{1i} w) = \psi(e_{11} w, e_{12} w, \ldots, e_{1d} w),$$

observando que $e_{1i} w = e_{11}(e_{1i} w) \in e_{11}W = V$ para todo $1 \leq i \leq d$. Resta mostrar que ψ é um homomorfismo de $M_d(E)$-módulos e, para isso, basta mostrar que ψ comuta com a ação de cada matriz escalar de $M_d(E)$, o que é tranquilo, e com a ação de cada e_{ij}. Para provar essa última parte, veja que, se $v_1, \ldots, v_d \in V$, então

$$\begin{aligned} \psi(e_{ij} \cdot (v_1, \ldots, v_d)) &= \psi(0, \ldots, v_j, \ldots, 0) \\ &= e_{i1} v_j \\ &= e_{ij} \cdot e_{j1} v_j \\ &= e_{ij} \cdot \sum_{r=1}^{d} e_{r1} v_r = e_{ij} \cdot \psi(v_1, \ldots, v_d), \end{aligned}$$

onde $(0, \ldots, v_j, \ldots, 0)$ denota o vetor-coluna cuja i-ésima coordenada vale v_j e cujas outras coordenadas são nulas. Assim, concluímos que $W \cong V_d$.

□

Exercício A.5.5. O livro [1] contém o seguinte exercício: com as notações da Proposição 5.2.5, prove que, se S e T são kG-módulos simples, então

$$\dim_k \operatorname{Hom}_{kG}(P_S, P_T) = |N| \cdot \dim_k \operatorname{Hom}_{k\overline{G}}(\overline{P_S}, \overline{P_T}).$$

Dê um contraexemplo para mostrar que esse exercício está errado.

Solução: Suponha que N seja um p-subgrupo de Sylow normal em G. Como p não divide a ordem de $\overline{G} = G/N$, então $k\overline{G}$ é semissimples pelo Teorema de Maschke e todo $k\overline{G}$-módulo é projetivo. Por isso, devemos ter isomorfismos $\overline{P_S} \cong S$ e $\overline{P_T} \cong T$ como $k\overline{G}$-módulos. Agora, se S e T não são isomorfos e se o exercício estivesse certo, então valeria

$$\dim_k \operatorname{Hom}_{kG}(P_S, P_T) = |N| \cdot \dim_k \operatorname{Hom}_{k\overline{G}}(S, T) = |N| \cdot 0 = 0,$$

porque $\operatorname{Hom}_{k\overline{G}}(S, T) = 0$. Pelo Exercício A.2.8, S não é fator de composição de P_T. Variando S sobre todos os módulos simples não isomorfos a T, concluímos que P_T possui apenas T como fator de composição. Mas T também é qualquer, de onde obtemos que toda cobertura projetiva de um módulo simples possui um único fator de composição (a menos de multiplicidade). Entretanto, isso não é verdade! Por exemplo, se N é um p-subgrupo de Sylow normal e cíclico, encontramos a estrutura dos projetivos indecomponíveis no Exemplo 2.2.12 e vimos que os fatores de composição podem ser os mais variados. Como caso concreto, temos o Exemplo 2.3.22: se $p = 5$, mostramos que o 5-subgrupo de Sylow do grupo diedral D_{15} é normal e cíclico, e verificamos, por exemplo, que a cobertura projetiva do módulo trivial possui um fator de composição diferente do módulo trivial. □

Exercício A.5.6. Use a Proposição 5.2.5 para dar uma prova alternativa da descrição obtida no Exemplo 2.2.12 dos projetivos indecomponíveis de um grupo com um p-subgrupo de Sylow normal e cíclico.

Solução: Seja G um grupo que possui um p-subgrupo de Sylow N que é normal, cíclico e de ordem p^a. Sejam S um kG-módulo simples e P_S a sua cobertura projetiva. Como a ordem de $\overline{G} := G/N$ não é divisível por p, o Teorema de Maschke mostra que $k\overline{G}$ é semissimples e, por isso, todo $k\overline{G}$-módulo é projetivo. Logo, seguindo as notações da Proposição 5.2.5, devemos ter $\overline{P_S} \cong S$ como $k\overline{G}$-módulos (e como kG-módulos). Agora, pela primeira afirmação do Lema 2.2.11, a série radical de P_S é igual à sua série radical como kN-módulo. Pela prova da Proposição 5.2.5, a série do enunciado da proposição é a série radical de P_S como kN-módulo e, portanto, como kG-módulo também! Assim, essa proposição mostra que o comprimento radical de P_S é o comprimento radical da álgebra kN e as camadas radicais são

$$\frac{\operatorname{rad}^i(P_S)}{\operatorname{rad}^{i+1}(P_S)} \cong \overline{P_S} \otimes \frac{\operatorname{rad}^i(kN)}{\operatorname{rad}^{i+1}(kN)} \cong S \otimes \frac{\operatorname{rad}^i(kN)}{\operatorname{rad}^{i+1}(kN)}$$

para $i \geq 0$, onde estamos vendo kN e seus subquocientes como kG-módulos através da conjugação. Desse modo, para obter a mesma descrição do Exemplo 2.2.12, devemos mostrar que o comprimento radical de kN é p^a e que existe um kG-módulo unidimensional W tal que

$$\frac{\operatorname{rad}^i(kN)}{\operatorname{rad}^{i+1}(kN)} \cong W^{\otimes i}$$

como kG-módulos para todo $0 \leq i < p^a$. Sendo W unidimensional, obteremos que $S \otimes W^{\otimes i}$ também é simples e, assim, as camadas radicais de P_S são simples. Disso seguirá que P_S é unisseriado de comprimento p^a e seus fatores de composição são, em ordem,

$$S,\ S \otimes W,\ S \otimes W \otimes W,\ S \otimes W \otimes W \otimes W,\ \ldots$$

Tomando S como sendo o módulo trivial, veja que W deverá ser a segunda camada radical de P_S, como descrito no Exemplo 2.2.12.

Vamos estudar a série radical de kN. Como N é cíclico, podemos tomar um gerador $x \in N$. Pelo Exercício A.1.15, uma base de $R := \operatorname{rad}(kN)$ é dada por

$$(x-1),\ (x-1)^2,\ (x-1)^3,\ \ldots,\ (x-1)^{p^a-1}.$$

Com isso, usando que $(x-1)^{p^a} = x^{p^a} - 1 = 0$, é fácil ver que uma base para $\mathrm{rad}^i(kN) = R^i$ é

$$(x-1)^i,\ (x-1)^{i+1},\ (x-1)^{i+2},\ \ldots,\ (x-1)^{p^a-1}.$$

Logo, o comprimento radical de kN é p^a.

Iremos construir o módulo W como no Exercício A.2.9. Como N é normal em G, para cada $g \in G$ existe um inteiro positivo $a(g)$ tal que $gxg^{-1} = x^{a(g)}$. Definindo $\alpha(g) = a(g) \cdot 1 \in k$, note que $\alpha(g)$ não depende de uma escolha particular do inteiro $a(g)$, já que a ordem de x é uma potência de p e $\mathrm{char}(k) = p$. Com isso, não é difícil verificar que α é um homomorfismo de G no grupo multiplicativo $k^\times$. Isso dá origem a um kG-módulo unidimensional W onde a ação de um elemento $g \in G$ é a multiplicação pelo escalar $\alpha(g) \in k^\times$. Para todo $i \geq 0$, $W^{\otimes i}$ também é unidimensional e um elemento $g \in G$ atua por multiplicação por $\alpha(g)^i \in k^\times$.

Vejamos que as camadas radicais de kN são isomorfas, como kG-módulos, às potências tensoriais de W. Se $0 \leq i < p^a$, pela descrição anterior, é fácil ver que R^i/R^{i+1} é unidimensional e gerado pela classe do elemento $(x-1)^i$. Quando $i = 0$, vemos que kN/R é gerado pela classe de 1 e, como 1 está no centro de kG, a ação de G em kN/R é trivial, de onde obtemos

$$\frac{R^0}{R^1} = \frac{kN}{R} \cong k \cong W^{\otimes 0}.$$

Quando $i = 1$, R/R^2 é gerado pela classe de $x-1$. Se $g \in G$, então

$$g \cdot (x-1) = g(x-1)g^{-1} = gxg^{-1} - 1 = x^{a(g)} - 1 = (x-1)(x^{a(g)-1} + \cdots + x + 1)$$

e, módulo R^2, temos

$$\begin{aligned}(x-1)(x^{a(g)-1} + \cdots + x + 1) &= (x-1)(x^{a(g)-1} + \cdots + x - (\alpha(g)-1)) + \alpha(g)(x-1) \\ &\equiv \alpha(g)(x-1) \pmod{R^2}.\end{aligned}$$

Acima, utilizamos que $x-1$ e $x^{a(g)-1} + \cdots + x - (\alpha(g)-1)$ estão em R, porque R é o ideal de aumento de kN (veja o Exercício A.1.14). Isso mostra que R/R^2 é unidimensional e um elemento $g \in G$ age por multiplicação por $\alpha(g)$. Logo, $R/R^2 \cong W$. A prova dos outros isomorfismos segue do que acabamos de fazer. De fato, considerando agora $1 < i < p^a$, sabemos que R^i/R^{i+1} é unidimensional e gerado pela classe de $(x-1)^i$. A conta anterior mostra que

$$g(x-1)g^{-1} = \alpha(g)(x-1) + y(g)$$

para algum elemento $y(g) \in R^2$, então

$$g \cdot (x-1)^i = g(x-1)^i g^{-1} = (g(x-1)g^{-1})^i = (\alpha(g)(x-1) + y(g))^i.$$

Olhando módulo R^{i+1}, temos

$$\begin{aligned}g \cdot (x-1)^i &= (\alpha(g)(x-1) + y(g))^i \\ &= \alpha(g)^i(x-1)^i + i\alpha(g)^{i-1}(x-1)^{i-1}y(g) + \cdots \\ &\equiv \alpha(g)^i(x-1)^i \pmod{R^{i+1}}.\end{aligned}$$

Na segunda igualdade acima, utilizamos o Teorema do Binômio de Newton, já que kN é uma álgebra comutativa, e, para a congruência, note que

$$(x-1)^{i-j}y(g)^j \in R^{i-j} \cdot R^{2j} = R^{i+j} \subseteq R^{i+1}$$

se $1 \leq j \leq i$. Dessa forma, R^i/R^{i+1} é unidimensional e um elemento $g \in G$ age por multiplicação por $\alpha(g)^i$, de onde concluímos que $R^i/R^{i+1} \cong W^{\otimes i}$. Isso termina o exercício. □

Exercício A.5.7. Seja N um subgrupo normal de G e S um kN-módulo simples estável sob conjugação por G (isto é, ${}^gS \cong S$ para todo $g \in G$).

(a) Se G/N é cíclico de ordem $p^a m$, onde $p \nmid m$, prove que S possui exatamente m extensões para G (no mesmo sentido do Lema 5.2.8).

(b) Se G/N é um p-grupo, mostre que S possui uma única extensão para G.

Solução: (a) Como S é simples e estável por conjugação e como G/N é cíclico, podemos imitar o argumento dado no início da demonstração do Lema 5.2.8 para encontrar uma extensão de S para G. Sabendo dessa existência, vamos nos basear na próxima parte da prova desse lema para mostrar que S possui exatamente m extensões.

Mostraremos que as extensões de S para G são os fatores de composição de S^G. Seja T uma extensão de S para G, que sabemos que existe. Como $T_N \cong S$ é simples, T também o é. Note que

$$S^G \cong (T_N)^G \cong (T_N \otimes k_N)^G \cong T \otimes (k_N)^G,$$

onde k denota o kG-módulo trivial.

Pelo Exemplo 3.1.8, $(k_N)^G \cong k[G/N]$, onde $k[G/N]$ está sendo considerado como um kG-módulo por restrição de escalares através da projeção canônica. Como G é cíclico de ordem $p^a m$, concluímos do Exemplo 2.2.10 que

$$k[G/N] \cong J_1 \oplus \cdots \oplus J_m,$$

onde $J_1, \ldots, J_m$ são as coberturas projetivas dos m $k[G/N]$-módulos simples $V_1, \ldots, V_m$. Vimos nos Exemplos 1.3.15 e 2.1.12 que $V_1, \ldots, V_m$ são unidimensionais, cada J_i é unisseriado de comprimento p^a e o único fator de J_i é V_i. Utilizando o Corolário 2.4.2, vemos que $T \otimes J_i$ possui uma cadeia de submódulos onde cada quociente é isomorfo a $T \otimes V_i$. Mas $T \otimes V_i$ é simples, já que T é simples e V_i é unidimensional! Concluímos que $T \otimes V_i$ é o único fator de composição de $T \otimes J_i$.

Agora, vale

$$S^G \cong T \otimes (k_N)^G \cong T \otimes k[G/N] \cong \bigoplus_{i=1}^{m} (T \otimes J_i),$$

então os fatores de composição de S^G são

$$T \otimes V_1, T \otimes V_2, \cdots, T \otimes V_m,$$

onde não estamos considerando a multiplicidade e possivelmente estamos repetindo algum módulo simples. Observe que algum dos módulos listados acima é isomorfo a T, porque um dos V_i deve ser isomorfo ao módulo trivial. Isso mostra que toda extensão de S para G é um fator de composição de S^G. Reciprocamente, observe que

$$(T \otimes V_i)_N = T_N \otimes (V_i)_N \cong S \otimes k_N \cong S,$$

então todo fator de composição de S^G é uma extensão de S para G.

Para concluir que S possui exatamente m extensões para G, resta mostrar que $T \otimes V_i \ncong T \otimes V_j$ se $i \neq j$. Pela Reciprocidade de Frobenius e pelo Lema de Schur, vale[1]

$$\mathrm{Hom}_{kG}(T \otimes V_i, S^G) \cong \mathrm{Hom}_{kN}((T \otimes V_i)_N, S) \cong \mathrm{Hom}_{kN}(S, S) = \mathrm{End}_{kN}(S) \cong k.$$

[1] Lembre que k é algebricamente fechado ao longo do Capítulo 5.

Por outro lado,

$$\mathrm{Hom}_{kG}(T\otimes V_i, S^G) \cong \mathrm{Hom}_{kG}\left(T\otimes V_i, \bigoplus_{j=1}^{m}(T\otimes J_j)\right) \cong \bigoplus_{j=1}^{m}\mathrm{Hom}_{kG}(T\otimes V_i, T\otimes J_j).$$

Como $T\otimes V_i$ é simples, a dimensão de $\mathrm{Hom}_{kG}(T\otimes V_i, T\otimes J_j)$ é a multiplicidade de $T\otimes V_i$ como fator de composição do soco de $T\otimes J_j$, que por sua vez é uma soma de cópias de $T\otimes V_j$ (porque o único fator de composição de $T\otimes J_j$ é $T\otimes V_j$). Em particular, $\mathrm{Hom}_{kG}(T\otimes V_i, T\otimes J_i)\neq 0$. Mas como $\mathrm{Hom}_{kG}(T\otimes V_i, S^G)$ possui dimensão 1, a única possibilidade é

$$\dim_k \mathrm{Hom}_{kG}(T\otimes V_i, T\otimes J_i) = 1$$

e

$$\dim_k \mathrm{Hom}_{kG}(T\otimes V_i, T\otimes J_j) = 0$$

se $j\neq i$. Concluímos que, se $j\neq i$, então $T\otimes V_i$ não é fator de composição do soco de $T\otimes J_j$, ou seja, $T\otimes V_i \ncong T\otimes V_j$, como desejado.

(b) Como G/N é um p-grupo, $[G:N]=p^a$ para algum $a\geq 0$. Vamos demonstrar o exercício por indução em a. Se $a=0$, é imediato. Se $a=1$, G/N possui ordem p e, portanto, é cíclico, então o resultado segue do item (a).

Suponha agora que o resultado valha para um certo inteiro não negativo a e mostremos que ele vale para $a+1$. Com alguns resultados sobre p-grupos (mais especificamente, o resultado de que todo subgrupo de um p-grupo é *subnormal*), conseguimos encontrar um subgrupo normal N' de G contendo N tal que N' possui índice p em G. Ou seja, temos uma cadeia de subgrupos

$$N\leq N'\leq G$$

onde N é normal em N', N' é normal em G, $[N':N]=p^a$ e $[G:N']=p$. Por hipótese de indução, S possui uma única extensão T para N'. Como $T_N\cong S$ e S é simples, T é um kN'-módulo simples. Vamos mostrar que T admite uma única extensão para G. Para isso, basta aplicar o item (a), mas primeiro devemos mostrar que T é estável sob conjugação por G. Seja $g\in G$. Pela unicidade de T dada pela hipótese de indução, para mostrar que ${}^gT\cong T$, é suficiente provar que $({}^gT)_N\cong S$. De fato, como S é estável sob conjugação por G, temos

$$({}^gT)_N = {}^g(T_N)\cong {}^gS\cong S,$$

como desejado. Logo, T admite uma única extensão U para G. Como $U_{N'}\cong T$ e $T_N\cong S$, vale $U_N\cong S$ e U é uma extensão de S para G. Por fim, se U' é uma outra extensão de S para G, então $U'_{N'}$ é uma extensão de S para N', então a unicidade nos dá $U'_{N'}\cong T$ e, como T admite uma única extensão para G, $U'\cong U$. Isso prova que S admite uma única extensão para G.

□

Exercício A.5.8. Este exercício dá uma ideia de como provar os itens (1), (2) e (4) do Lema 5.2.12 de modo mais "funtorial". Utilizaremos as notações introduzidas nesse lema.

(a) Prove que $\varphi=\mathrm{id}_V$ se, e somente se, para todo homomorfismo $\alpha: M\to V$ vale $\varphi\alpha=\alpha$. Use isso para dar outra demonstração do item (1) do Lema 5.2.12.

(b) Mostre que ψ é injetor se, e somente se, para todo homomorfismo não nulo $\alpha: M\to V_1$ vale $\psi\alpha\neq 0$. Obtenha uma propriedade análoga para a sobrejetividade e use essas equivalências para dar outra prova do item (2) do Lema 5.2.12.

(c) Caracterize sequências exatas curtas em termos de homomorfismos e dê uma demonstração alternativa do item (4) do Lema 5.2.12.

Solução: (a) Se $\varphi = \mathrm{id}_V$, é imediato que $\varphi\alpha = \alpha$ para todo homomorfismo $\alpha : M \to V$. Por outro lado, se φ satisfaz a propriedade descrita, então podemos tomar $M = V$ e $\alpha = \mathrm{id}_V$ para concluir que $\varphi \circ \mathrm{id}_V = \mathrm{id}_V$. Mas compor com a identidade não altera a entrada inicial, logo $\varphi \circ \mathrm{id}_V$ também é igual a φ, de onde obtemos $\varphi = \mathrm{id}_V$. Isso prova a primeira parte o item. Note também que podemos assumir que o módulo M é sempre um kI_1-módulo pertencente a $\beta_1^{I_1}$.

Vamos demonstrar o item (1) do Lema 5.2.12. Suponha que $\varphi^{N_1} = \mathrm{id}_{V^{N_1}}$. Para mostrar que $\varphi = \mathrm{id}_V$, basta mostrar que φ possui a propriedade do parágrafo anterior. De fato, se $\alpha : M \to V$ é um homomorfismo onde M é um $\beta_1^{I_1}$-módulo, então vale

$$\varphi^{N_1}\alpha^{N_1} = \alpha^{N_1} \implies (\varphi\alpha)^{N_1} = \alpha^{N_1}.$$

O Lema 5.2.11 nos dá uma bijeção entre $\mathrm{Hom}_{kI_1}(M, V)$ e $\mathrm{Hom}_{kN_1}(M^{N_1}, V^{N_1})$ através da indução, então a igualdade acima nos permite concluir que $\varphi\alpha = \alpha$, como desejado.

A recíproca é imediata: se $\varphi = \mathrm{id}_V$, então $\varphi^{N_1} = \mathrm{id}_{V^{N_1}}$ (já que a indução é funtorial). Também é possível demonstrar isso através da propriedade do primeiro parágrafo, utilizando que todo b_1-módulo é a indução de um $\beta_1^{I_1}$-módulo e também que todo homomorfismo $\alpha' : M^{N_1} \to V^{N_1}$ é da forma $\alpha' = \alpha^{N_1}$ para algum $\alpha : M \to V$ (Lema 5.2.11).

(b) Se ψ é injetor, então $\psi(v) \neq 0$ para todo $v \in V_1$ não nulo. Logo, se $\alpha : M \to V_1$ é não nulo, então existe um elemento não nulo na imagem de α e obtemos $\psi\alpha \neq 0$. Reciprocamente, suponha que ψ não seja injetor. Desse modo, $\ker\psi$ é um submódulo não nulo de V_1 e, por isso, a inclusão $\alpha : \ker\psi \to V_1$ é um homomorfismo não nulo. Como $\psi\alpha = 0$, ψ não pode satisfazer a propriedade desejada neste caso. Mais uma vez, observe que podemos assumir que o módulo M é sempre um kI_1-módulo pertencente a $\beta_1^{I_1}$, porque, na demonstração anterior, $\ker\psi$ pertence a $\beta_1^{I_1}$ por ser submódulo de V_1.

Para a sobrejetividade, temos a seguinte caracterização: ψ é sobrejetor se, e somente se, para todo homomorfismo não nulo $\alpha : V_2 \to M$ vale $\alpha\psi \neq 0$. De fato, se ψ é sobrejetor e se $\alpha : V_2 \to M$ é não nulo, então existe $w \in V_2$ tal que $\alpha(w) \neq 0$ e podemos encontrar $v \in V_1$ tal que $\psi(v) = w$, logo $(\alpha\psi)(v) = \alpha(w) \neq 0$ e temos $\alpha\psi \neq 0$. Reciprocamente, suponha que ψ não seja sobrejetor. Desse modo, o quociente $V_2/\operatorname{im}\psi$ é não nulo e, assim, a projeção $\alpha : V_2 \to V_2/\operatorname{im}\psi$ é um homomorfismo não nulo. Como $\alpha\psi = 0$, ψ não pode satisfazer a propriedade em questão neste caso. Novamente, como $V_2/\operatorname{im}\psi$ é quociente do $\beta_1^{I_1}$-módulo V_2, podemos assumir que M sempre é um kI_1-módulo pertencente a $\beta_1^{I_1}$.

Vamos provar o item (2) do Lema 5.2.12. Inicialmente, suponha que ψ^{N_1} seja injetor. Para mostrar que ψ também é injetor, basta provar que ψ satisfaz a propriedade do enunciado. De fato, se $\alpha : M \to V_1$ é um homomorfismo não nulo onde M é um $\beta_1^{I_1}$-módulo, então α^{N_1} é não nulo (pelo isomorfismo do Lema 5.2.11) e vale

$$(\psi\alpha)^{N_1} = \psi^{N_1}\alpha^{N_1} \neq 0,$$

já que ψ^{N_1} é injetor e α^{N_1} é não nulo. Utilizando mais uma vez o isomorfismo do Lema 5.2.11, temos $\psi\alpha \neq 0$, como preciso.

Para a recíproca, suponha que ψ seja injetor. Note que a propriedade provada no primeiro parágrafo pode ser facilmente adaptada trocando-se ψ por ψ^{N_1} e $\beta_1^{I_1}$-módulos por b_1-módulos. Logo, para mostrar que ψ^{N_1} é injetor, basta verificar essa propriedade. Com efeito, se $\alpha' : M' \to V_1^{N_1}$ é um homomorfismo não nulo onde M' é um b_1-módulo, então, pelo Lema 5.2.11, podemos supor que $M' = M^{N_1}$ para algum $\beta_1^{I_1}$-módulo M e que $\alpha' = \alpha^{N_1}$

para algum homomorfismo $\alpha : M \to V_1$. Como $\alpha^{N_1} \neq 0$, o isomorfismo do Lema 5.2.11 diz que $\alpha \neq 0$ e, como ψ é injetor, $\psi\alpha \neq 0$. Induzindo para N_1, obtemos

$$\psi^{N_1}\alpha^{N_1} = (\psi\alpha)^{N_1} \neq 0,$$

como queríamos.

A prova do item (2) do Lema 5.2.12 para o caso da sobrejetividade é quase idêntica à do caso da injetividade por conta da caracterização que demos acima no segundo parágrafo.

(c) Seja

$$0 \longrightarrow U \xrightarrow{\alpha} V \xrightarrow{\lambda} W \longrightarrow 0 \qquad (*)$$

uma sequência de $\beta_1^{I_1}$-módulos e considere a sequência correspondente de b_1-módulos:

$$0 \longrightarrow U^{N_1} \xrightarrow{\alpha^{N_1}} V^{N_1} \xrightarrow{\lambda^{N_1}} W^{N_1} \longrightarrow 0 \qquad (**)$$

Para provar o item (4) do Lema 5.2.12, queremos mostrar que $(*)$ é exata se e só se $(**)$ o é. Assim, precisamos caracterizar uma sequência exata curta através de morfismos. Como já fizemos isso para a injetividade e para a sobrejetividade, usaremos esses termos na nossa nova caracterização.

Provaremos que $(*)$ é exata se, e somente se, α é injetor, λ é sobrejetor, $\lambda\alpha = 0$ e, para todo homomorfismo $\gamma : M \to V$ tal que $\lambda\gamma = 0$, existe um homomorfismo $\gamma' : M \to U$ tal que $\gamma = \alpha\gamma'$.

($\Longrightarrow$) Suponha que $(*)$ seja exata. Nesse caso, é imediato que α é injetor e que λ é sobrejetor. Além disso, como $\operatorname{im}\alpha = \ker\lambda$, vale $\lambda\alpha = 0$. Vamos mostrar a propriedade que resta. Seja $\gamma : M \to V$ um homomorfismo tal que $\lambda\gamma = 0$. Isso está dizendo que $\operatorname{im}\gamma$ está contido em $\ker\lambda = \operatorname{im}\alpha$. Como α é injetor, ele é isomorfismo com a sua imagem, então podemos encontrar uma inversa $\alpha' : \operatorname{im}\alpha \to U$. Assim, podemos tomar $\gamma' \coloneqq \alpha'\gamma$, que é homomorfismo de M em U satisfazendo

$$\alpha\gamma' = \alpha\alpha'\gamma = \mathrm{id}_{\operatorname{im}\alpha}\,\gamma = \gamma,$$

como desejado.

($\Longleftarrow$) Suponha que $(*)$ satisfaça as propriedades listadas. Como α é injetor e λ é sobrejetor, basta mostrar que $(*)$ é exata em V. A condição $\lambda\alpha = 0$ diz precisamente que $\operatorname{im}\alpha \subseteq \ker\lambda$, então mostremos a outra inclusão. Seja $\gamma : \ker\lambda \to V$ a inclusão canônica. É imediato que $\lambda\gamma = 0$, então existe um homomorfismo $\gamma' : \ker\lambda \to U$ tal que $\gamma = \alpha\gamma'$. Mas a imagem de γ é $\ker\lambda$, então concluímos que $\ker\lambda \subseteq \operatorname{im}\alpha$, como preciso.

Como sempre, podemos assumir que M é um kI_1-módulo pertencente a $\beta_1^{I_1}$, já que na demonstração acima apenas precisamos tomar $M = \ker\lambda$, que é um submódulo de V. Outra observação importante é que podemos adaptar o argumento acima para dar uma caracterização análoga da exatidão de $(**)$.

Vamos demonstrar o item (4) do Lema 5.2.12. Já vimos no item (b) que α é injetor se e só se α^{N_1} é injetor, e que λ é sobrejetor se e só se λ^{N_1} é sobrejetor. Utilizando o isomorfismo do Lema 5.2.11, também concluímos que $\lambda\alpha = 0$ se e só se $\lambda^{N_1}\alpha^{N_1} = (\lambda\alpha)^{N_1} = 0$. Portanto, basta mostrar que vale a propriedade

$$\text{Se } \gamma : M \to V \text{ satisfaz } \lambda\gamma = 0, \text{ então existe } \gamma' : M \to U \text{ com } \gamma = \alpha\gamma'$$

onde M é um $\beta_1^{I_1}$-módulo, se e somente se vale a propriedade

$$\text{Se } \gamma_1 : M' \to V^{N_1} \text{ satisfaz } \lambda^{N_1}\gamma_1 = 0, \text{ então existe } \gamma_1' : M' \to U^{N_1} \text{ com } \gamma_1 = \alpha^{N_1}\gamma_1'$$

onde M' é um b_1-módulo. Chame a primeira propriedade de (i) e a segunda de (ii).

(i) $\implies$ (ii). Seja $\gamma_1 : M' \to V^{N_1}$ um homomorfismo satisfazendo $\lambda^{N_1}\gamma_1 = 0$, onde M' é um b_1-módulo. Pelo Lema 5.2.11, podemos supor que $M' = M^{N_1}$ para algum $\beta_1^{I_1}$-módulo M e que $\gamma_1 = \gamma^{N_1}$ para algum homomorfismo $\gamma : M \to V$. Como

$$(\lambda\gamma)^{N_1} = \lambda^{N_1}\gamma^{N_1} = \lambda^{N_1}\gamma_1 = 0,$$

o isomorfismo do Lema 5.2.11 implica que $\lambda\gamma = 0$. Por (i), existe $\gamma' : M \to U$ com $\gamma = \alpha\gamma'$. Tomando $\gamma_1' \coloneqq (\gamma')^{N_1}$, concluímos que

$$\gamma_1 = \gamma^{N_1} = (\alpha\gamma')^{N_1} = \alpha^{N_1}(\gamma')^{N_1} = \alpha^{N_1}\gamma_1',$$

como preciso.

(ii) $\implies$ (i). Seja $\gamma : M \to V$ um homomorfismo satisfazendo $\lambda\gamma = 0$, onde M é um $\beta_1^{I_1}$-módulo. Desse modo,

$$\lambda^{N_1}\gamma^{N_1} = (\lambda\gamma)^{N_1} = 0^{N_1} = 0$$

e podemos aplicar (ii). Assim, existe $\gamma_1' : M^{N_1} \to U^{N_1}$ tal que $\gamma^{N_1} = \alpha^{N_1}\gamma_1'$. Pelo Lema 5.2.11, existe um homomorfismo $\gamma' : M \to U$ tal que $\gamma_1' = (\gamma')^{N_1}$. Logo,

$$\gamma^{N_1} = \alpha^{N_1}\gamma_1' = \alpha^{N_1}(\gamma')^{N_1} = (\alpha\gamma')^{N_1}$$

e, mais uma vez pelo Lema 5.2.11, $\gamma = \alpha\gamma'$.

Isso conclui o exercício!

Algo interessante é que podemos caracterizar a exatidão de uma sequência em um ponto utilizando homomorfismos também, então equivalências como a do Lema 5.2.11 preservam sequências exatas de tamanho arbitrário. Optamos por mostrar a caracterização apenas para sequências curtas para simplificar a prova.

□

Exercício A.5.9. Sejam U e V kG-módulos. Prove as seguintes identidades:

(a) $\Omega(U \oplus V) \cong \Omega U \oplus \Omega V$ e $\Omega^{-1}(U \oplus V) \cong \Omega^{-1}U \oplus \Omega^{-1}V$.

(b) $\Omega^{-1}(U^*) \cong (\Omega U)^*$.

(c) $\Omega(U \otimes V) \cong \Omega^0(\Omega U \otimes V) \cong \Omega^0(U \otimes \Omega V)$ e $\Omega^{-1}(U \otimes V) \cong \Omega^0(\Omega^{-1}U \otimes V) \cong \Omega^0(U \otimes \Omega^{-1}V)$.

(d) $IG \otimes U \cong \Omega U \oplus Q$ para algum kG-módulo projetivo Q, onde IG denota o ideal de aumento de kG.

(e) Se n é um inteiro positivo, defina $\Omega^n U \coloneqq \Omega \cdots \Omega U$ (n vezes) e $\Omega^{-n}U \coloneqq \Omega^{-1} \cdots \Omega^{-1}U$ (n vezes). Para quaisquer inteiros r e s, vale

$$\Omega^r\Omega^s U \cong \Omega^{r+s}U.$$

Solução: (a) Pelo item (3) da Proposição 5.3.3, a soma $\pi_U \oplus \pi_V : PU \oplus PV \to U \oplus V$ é um epimorfismo essencial e, como soma direta de projetivos é projetiva, essa é uma cobertura projetiva de $U \oplus V$. Logo, o núcleo desse homomorfismo, que é $\Omega U \oplus \Omega V$, é isomorfo a $\Omega(U \oplus V)$. Analogamente, através do item (3) da Proposição 5.3.11, $\lambda_U \oplus \lambda_V : U \oplus V \to IU \oplus IV$ é uma envolvente injetiva de $U \oplus V$, de onde obtemos $\Omega^{-1}(U \oplus V) \cong \Omega^{-1}U \oplus \Omega^{-1}V$.

(b) Como $\pi_U : PU \to U$ é uma cobertura projetiva, a Proposição 5.3.16 mostra que a transposta $\pi_U^* : U^* \to (PU)^*$ é uma envolvente injetiva. É um resultado usual de álgebra linear que $\operatorname{im}(\pi_U^*) = (\ker \pi_U)^\perp$, logo, pelo Lema 2.3.6, vale

$$\Omega^{-1}(U^*) \cong \frac{(PU)^*}{\operatorname{im}(\pi_U^*)} = \frac{0^\perp}{(\ker \pi_U)^\perp} \cong (\ker \pi_U)^* = (\Omega U)^*,$$

como desejado.

(c) Podemos fazer o produto tensorial entre o homomorfismo $\pi_U : PU \to U$ e a identidade $\mathrm{id}_V : V \to V$, obtendo, pela Proposição 2.4.1, um homomorfismo

$$\pi_U \otimes \mathrm{id}_V : PU \otimes V \to U \otimes V.$$

A partir da definição do produto tensorial de transformações lineares, não é difícil verificar que $\pi_U \otimes \mathrm{id}_V$ é um homomorfismo sobrejetor, pois π_U e id_V o são. Além disso, é imediato que $\Omega U \otimes V$ está contido no núcleo de $\pi_U \otimes \mathrm{id}_V$ e, por questões de dimensão, essa inclusão deve ser uma igualdade. Como PU é projetivo, $PU \otimes V$ também o é pelo Corolário 2.4.8, então o Corolário 5.3.9 mostra que

$$\Omega U \otimes V = \ker(\pi_U \otimes \mathrm{id}_V) \cong \Omega(U \otimes V) \oplus K$$

para algum kG-módulo projetivo K. Segue que

$$\Omega^0(\Omega U \otimes V) \cong \Omega^0\Omega(U \otimes V) \oplus \Omega^0 K \cong \Omega(U \otimes V).$$

Repetindo o mesmo argumento mas trocando as posições de U e V, obtemos o outro isomorfismo $\Omega^0(U \otimes \Omega V) \cong \Omega(U \otimes V)$.

De modo análogo, podemos fazer o produto tensorial entre o homomorfismo $\lambda_U : U \to IU$ e a identidade $\mathrm{id}_V : V \to V$ para obter um homomorfismo

$$\lambda_U \otimes \mathrm{id}_V : U \otimes V \to IU \otimes V.$$

Dessa vez, é mais delicado verificar que este homomorfismo é injetor. Como o produto tensorial está sendo tomado sobre um corpo, sabemos que uma base de $U \otimes V$ pode ser formada através do "produto tensorial" de uma base de U com uma base de V. Como λ_U e id_V são injetores, essas bases são levadas em conjuntos linearmente independentes de IU e de V, respectivamente, então ainda continuamos com um conjunto linearmente independente ao formarmos o "produto tensorial" desses dois conjuntos. Por isso, $\lambda_U \otimes \mathrm{id}_V$ leva uma base em um conjunto linearmente independente, o que garante a injetividade desse homomorfismo. Agora, é imediato que a imagem de $\lambda_U \otimes \mathrm{id}_V$ está contida em $\operatorname{im}\lambda_U \otimes V$ e, novamente por questões de dimensão, essa inclusão deve ser uma igualdade. Como IU é injetivo, $IU \otimes V$ também o é pelo Corolário 2.4.8 e pelo Teorema 2.3.14, então o Corolário 5.3.18 (juntamente com o Corolário 2.4.2) mostra que

$$\Omega^{-1}U \otimes V \cong \frac{IU \otimes V}{\operatorname{im}\lambda_U \otimes V} \cong \Omega^{-1}(U \otimes V) \oplus K$$

para algum kG-módulo projetivo K. Segue que

$$\Omega^0(\Omega^{-1}U \otimes V) \cong \Omega^0\Omega^{-1}(U \otimes V) \oplus \Omega^0 K \cong \Omega^{-1}(U \otimes V).$$

Repetindo o mesmo argumento mas trocando as posições de U e V, obtemos o outro isomorfismo $\Omega^0(U \otimes \Omega^{-1}V) \cong \Omega^{-1}(U \otimes V)$.

(d) É suficiente mostrar que $\Omega^0(IG \otimes U) \cong \Omega U$. Se $\epsilon : kG \to k$ é a função de aumento, então ϵ é um homomorfismo sobrejetor de kG-módulos. Como kG é projetivo, o Corolário 5.3.9 nos diz que

$$IG = \ker \epsilon \cong \Omega k \oplus R$$

para algum kG-módulo projetivo R. Pelo Corolário 2.4.8, $R \otimes U$ é projetivo, então

$$\Omega^0(IG \otimes U) \cong \Omega^0(\Omega k \otimes U) \oplus \Omega^0(R \otimes U) \cong \Omega(k \otimes U) \oplus 0 \cong \Omega U,$$

como queríamos.

(e) Isso é bem imediato a partir dos isomorfismos do Lema 5.3.20. Formalmente, é preciso lidar como cada escolha de sinais para r e s e prosseguir por indução dupla, aplicando o Lema 5.3.20 no passo de indução. É fácil se convencer disso, mas escrever isso é mais complicado e não o faremos.

□

Exercício A.5.10. Se U e V são kG-módulos, mostre que o espaço $\overline{\mathrm{Hom}}_{kG}(U, V)$ é isomorfo ao subespaço de $\Omega^0(U^* \otimes V)$ formado pelos vetores fixos pela ação de G. Use isso para dar uma demonstração alternativa da Proposição 5.3.23.

Solução: Vamos começar com uma observação interessante. Sabemos que $\mathrm{Hom}_k(U, V)$ é naturalmente um kG-módulo (isomorfo a $U^* \otimes V$) e que o seu subespaço formado pelos vetores fixos por G é precisamente $\mathrm{Hom}_{kG}(U, V)$. Neste exercício, queremos "limpar" a parte projetiva. Temos duas formas de fazer isso: a primeira delas é tomando esse subespaço de vetores fixos $\mathrm{Hom}_{kG}(U, V)$ e quocientando pelo subespaço dos homomorfismos que se fatoram através de um projetivo. Isso nos dá $\overline{\mathrm{Hom}}_{kG}(U, V)$. Por outro lado, podemos primeiramente retirar a parte projetiva de $\mathrm{Hom}_k(U, V) \cong U^* \otimes V$ formando $\Omega^0(U^* \otimes V)$ e depois disso consideramos os vetores fixos. O exercício mostra que essas duas construções dão o mesmo resultado!

Para mostrar que os espaços vetoriais em questão são isomorfos, vamos mostrar que ambos possuem dimensão igual a

$$\dim_k \mathrm{Hom}_{kG}(U, V) + \dim_k \mathrm{Hom}_{kG}(\Omega^{-1}U, V) - \dim_k \mathrm{Hom}_{kG}(IU, V).$$

Vamos começar calculando a dimensão do subespaço de $\Omega^0(U^* \otimes V)$ formado pelos vetores fixos pela ação de G. Esse subespaço é na verdade um kG-submódulo de $\Omega^0(U^* \otimes V)$ isomorfo a uma soma de cópias do módulo trivial. Além disso, qualquer homomorfismo do módulo trivial k em $\Omega^0(U^* \otimes V)$ possui imagem contida nesse submódulo. Logo, a dimensão desse subespaço é

$$\dim_k \mathrm{Hom}_{kG}(k, \Omega^0(U^* \otimes V)).$$

Agora, podemos escrever $U^* \otimes V = \Omega^0(U^* \otimes V) \oplus R$, onde R é um kG-módulo projetivo. Desse modo, a dimensão procurada é também igual a

$$\dim_k \mathrm{Hom}_{kG}(k, U^* \otimes V) - \dim_k \mathrm{Hom}_{kG}(k, R).$$

Pela Proposição 2.4.6,

$$\mathrm{Hom}_{kG}(k, U^* \otimes V) \cong \mathrm{Hom}_{kG}(k \otimes U, V) \cong \mathrm{Hom}_{kG}(U, V).$$

Vamos mostrar que a igualdade

$$\dim_k \mathrm{Hom}_{kG}(k, R) = \dim_k \mathrm{Hom}_{kG}(IU, V) - \dim_k \mathrm{Hom}_{kG}(\Omega^{-1}U, V)$$

é válida, o que comprovará que a dimensão do subespaço fixo de $\Omega^0(U^* \otimes V)$ é o valor indicado no início da solução.

Lembre que cada kG-módulo projetivo indecomponível possui soco simples e isomorfo ao kG-módulo simples correspondente. Logo, escrevendo R como soma de projetivos indecomponíveis, segue que $\dim_k \operatorname{Hom}_{kG}(k, R)$ é exatamente o número de vezes que a cobertura projetiva Pk do módulo trivial k aparece como somando indecomponível de R! Como $\Omega^0(U^* \otimes V)$ não possui somandos diretos projetivos, essa multiplicidade é a mesma multiplicidade de Pk como somando de $U^* \otimes V$, que, pelo Exercício A.2.14, é igual a

$$\frac{\dim_k \operatorname{Hom}_{kG}(Pk, U^* \otimes V) - \dim_k \operatorname{Hom}_{kG}(Pk/\operatorname{soc}(Pk), U^* \otimes V)}{\dim_k \operatorname{End}_{kG}(k)}.$$

O denominador é igual a 1, então o ignoraremos a partir de agora. Nesse caso, é mais conveniente pensar em Pk como sendo a envolvente injetiva de k e, consequentemente, o denotaremos por Ik. Note que $Ik/\operatorname{soc}(Ik)$ nada mais é do que $\Omega^{-1}k$. Aplicando a Proposição 2.4.6, podemos escrever o número em questão como

$$\dim_k \operatorname{Hom}_{kG}(Ik \otimes U, V) - \dim_k \operatorname{Hom}_{kG}(\Omega^{-1}k \otimes U, V).$$

Vamos encontrar um módulo projetivo R' tal que $Ik \otimes U \cong IU \oplus R'$ e $\Omega^{-1}k \otimes U \cong \Omega^{-1}U \oplus R'$. Isso concluirá o que queremos mostrar, porque então teremos

$$\dim_k \operatorname{Hom} kG(Ik \otimes U, V) = \dim_k \operatorname{Hom}_{kG}(IU, V) + \dim_k \operatorname{Hom}_{kG}(R', V)$$

e

$$\dim_k \operatorname{Hom}_{kG}(\Omega^{-1}k \otimes U, V) = \dim_k \operatorname{Hom}_{kG}(\Omega^{-1}U, V) + \dim_k \operatorname{Hom}_{kG}(R', V)$$

e, subtraindo essas equações, chegamos que $\dim_k \operatorname{Hom}_{kG}(k, R)$ é de fato igual a

$$\dim_k \operatorname{Hom}_{kG}(IU, V) - \dim_k \operatorname{Hom}_{kG}(\Omega^{-1}U, V).$$

Com efeito, sabemos que a inclusão $k \cong \operatorname{soc}(Ik) \to Ik$ é uma envolvente injetiva. Fazendo o produto tensorial dessa inclusão com a identidade em U, obtemos um homomorfismo $\psi : U \to Ik \otimes U$. Argumentando como fizemos na solução do item (c) do Exercício A.5.9, não é difícil mostrar que ψ é injetor. Pelo Corolário 2.4.8, $Ik \otimes U$ é injetivo, então a Proposição 5.3.17 nos dá um homomorfismo injetor $\rho : IU \to Ik \otimes U$ tal que $\rho\lambda_U = \psi$. Ademais, podemos decompor $Ik \otimes U = \operatorname{im}\rho \oplus R'$, onde R' é projetivo por ser somando direto de um projetivo. Observe que $\operatorname{im}\rho \cong IU$ porque ρ é injetor. Mais do que isso, como $\rho\lambda_U = \psi$, temos $\operatorname{im}\psi \subseteq \operatorname{im}\rho$ e $\operatorname{im}\rho/\operatorname{im}\psi \cong IU/\operatorname{im}\lambda_U = \Omega^{-1}U$. Desse modo,

$$\Omega^{-1}k \otimes U = \frac{Ik}{\operatorname{soc}(Ik)} \otimes U \cong \frac{Ik \otimes U}{\operatorname{soc}(Ik) \otimes U} = \frac{\operatorname{im}\rho \oplus R'}{\operatorname{im}\psi} \cong \Omega^{-1}U \oplus R',$$

como queríamos. A dimensão do subespaço fixo de $\Omega^0(U^* \otimes V)$ está finalmente calculada!

Agora é a hora de calcular a dimensão de $\overline{\operatorname{Hom}}_{kG}(U, V)$. Esse é o quociente do espaço $\operatorname{Hom}_{kG}(U, V)$ pelo subespaço X formado pelos homomorfismos que se fatoram através de um projetivo. Dessa forma, para chegar no resultado desejado, devemos mostrar que

$$\dim_k X = \dim_k \operatorname{Hom}_{kG}(IU, V) - \dim_k \operatorname{Hom}_{kG}(\Omega^{-1}U, V).$$

Considere a sequência exata

$$0 \longrightarrow U \longrightarrow IU \longrightarrow \Omega^{-1}U \longrightarrow 0$$

Aplicando o funtor $\operatorname{Hom}_k(-, V)$, que é contravariante, obtemos a sequência exata

$$0 \longrightarrow \operatorname{Hom}_k(\Omega^{-1}U, V) \xrightarrow{f} \operatorname{Hom}_k(IU, V) \xrightarrow{g} \operatorname{Hom}_k(U, V)$$

Não demonstraremos que a sequência acima é realmente exata (isso é um resultado geral que utilizamos até mesmo no Exercício A.2.11). Iremos aplicar o "funtor de pontos fixos" na sequência acima para obter

$$0 \longrightarrow \mathrm{Hom}_{kG}(\Omega^{-1}U, V) \xrightarrow{f'} \mathrm{Hom}_{kG}(IU, V) \xrightarrow{g'} \mathrm{Hom}_{kG}(U, V)$$

Aqui, f' e g' são as restrições de f e g, respectivamente. Não é difícil verificar que f' e g' de fato levam um homomorfismo de kG-módulos em um homomorfismo de kG-módulos. Afirmamos que a nova sequência é exata. Como f é injetor, isso também vale para a restrição f'. Por outro lado, como $gf = 0$, também temos $g'f' = 0$. A única parte mais complicada é verificar que $\ker g' \subseteq \mathrm{im}\, f'$. Com efeito, se $\psi \in \mathrm{Hom}_{kG}(IU, V)$ satisfaz $g'(\psi) = 0$, então ψ está no núcleo de g e existe $\varphi \in \mathrm{Hom}_k(\Omega^{-1}U, V)$ tal que $\psi = f(\varphi)$. Como ψ é homomorfismo de kG-módulos, ψ é fixo pela ação de G e obtemos que $f(x\varphi) = f(\varphi)$ para todo $x \in G$. Mas f é injetora, então $x\varphi = \varphi$ para todo $x \in G$ e $\varphi \in \mathrm{Hom}_{kG}(\Omega^{-1}U, V)$, mostrando que $\psi = f'(\varphi)$ está na imagem de f'. Sabendo dessa exatidão, obtemos que a dimensão da imagem de g' é

$$\dim_k \mathrm{Hom}_{kG}(IU, V) - \dim_k \mathrm{Hom}_{kG}(\Omega^{-1}U, V).$$

Concluiremos a solução mostrando que a imagem de g' é exatamente X. Seja $\varphi : U \to V$ um homomorfismo. Se φ está na imagem de g', então φ é a composição de $\lambda_U : U \to IU$ com um homomorfismo de IU em V, logo φ se fatora pelo projetivo IU. Reciprocamente, se φ se fatora através de um projetivo, então o Teorema 2.3.14 garante que φ se fatora através de um injetivo e, pelo Lema 5.3.13, φ é a composição de λ_U com um homomorfismo $IU \to V$, ou seja, φ está na imagem de g'.

Antes de prosseguir para a última afirmação do exercício, é interessante fazer um comentário sobre esse "funtor de pontos fixos". Se U é um kG-módulo, podemos associar o seu subespaço $\mathrm{Fix}(U)$ de pontos fixos. Dado um homomorfismo $U \to V$, é imediato que a restrição nos dá uma transformação linear $\mathrm{Fix}(U) \to \mathrm{Fix}(V)$. Na verdade, não é difícil verificar que $\mathrm{Fix}(-)$ é um funtor! A conta anterior pode ser adaptada para mostrar que esse funtor é exato à esquerda. Outra maneira de mostrar essa exatidão à esquerda é notar que $\mathrm{Fix}(-)$ é o adjunto à direita do funtor que leva um espaço vetorial no kG-módulo com a ação trivial!

Vamos terminar dando uma prova alternativa da Proposição 5.3.23. Se U e V são kG-módulos, então acabamos de verificar que

$$\overline{\mathrm{Hom}}_{kG}(\Omega U, \Omega V) \cong \mathrm{Fix}(\Omega^0((\Omega U)^* \otimes \Omega V)).$$

Pelo Exercício A.5.9,

$$\Omega^0((\Omega U)^* \otimes \Omega V) \cong \Omega^0(\Omega^{-1}(U^*) \otimes \Omega V) \cong \Omega^{-1}(U^* \otimes \Omega V).$$

Utilizando também o Lema 5.3.20, chegamos em

$$\Omega^{-1}(U^* \otimes \Omega V) \cong \Omega^{-1}\Omega^0(U^* \otimes \Omega V) \cong \Omega^{-1}\Omega(U^* \otimes V) \cong \Omega^0(U^* \otimes V).$$

Por isso,

$$\mathrm{Fix}(\Omega^0((\Omega U)^* \otimes \Omega V)) \cong \mathrm{Fix}(\Omega^0(U^* \otimes V)).$$

Mas provamos neste exercício que

$$\mathrm{Fix}(\Omega^0(U^* \otimes V)) \cong \overline{\mathrm{Hom}}_{kG}(U, V),$$

então concluímos que

$$\overline{\mathrm{Hom}}_{kG}(\Omega U, \Omega V) \cong \overline{\mathrm{Hom}}_{kG}(U, V),$$

como desejado. □

Exercício A.5.11. Se U é um kG-módulo indecomponível e não projetivo e S é uma fonte de U, mostre que ΩS é uma fonte de ΩU.

Solução: Seja Q um vértice de U e S um kQ-módulo indecomponível que é uma fonte para U. Como a indução de um módulo projetivo ainda é projetivo (item (2) do Lema 3.1.10) e como $U \mid S^G$, então S não pode ser projetivo. Assim, pelo Teorema 5.3.22, ΩS é indecomponível. Pela Proposição 5.3.24, Q também é um vértice de ΩU, então resta mostrar que $\Omega U \mid (\Omega S)^G$ para concluir que ΩS é uma fonte de ΩU. Isso pode ser feito imitando o primeiro parágrafo da demonstração da Proposição 5.3.24. □

Exercício A.5.12. Com as notações da Seção 5.4, sejam U e V b_1-módulos satisfazendo

$$\dim_k U + \dim_k V \leq q.$$

Prove que $\mathrm{Hom}_{kN_1}(U,V) \cong \overline{\mathrm{Hom}}_{kN_1}(U,V)$.

Solução: Como Hom e $\overline{\mathrm{Hom}}$ respeitam somas diretas (veja o Exercício A.3.15), podemos supor que U e V são indecomponíveis. Como $l(U) \leq \dim_k U$ e $l(V) \leq \dim_k V$, segue que

$$l(U) + l(V) - q \leq 0.$$

Pelo Lema 5.4.5, o único homomorfismo de U em V que se fatora através de um projetivo é o homomorfismo nulo. Concluímos que $\mathrm{Hom}_{kN_1}(U,V) \cong \overline{\mathrm{Hom}}_{kN_1}(U,V)$. □

Exercício A.5.13. Sejam M um A-módulo e N um submódulo que é a soma direta de submódulos V_1 e V_2, ambos isomorfos a um mesmo A-módulo V. Se a extensão de M/N por $N/V_1 \cong V$ é isomorfa à extensão de M/N por $N/V_2 \cong V$ (no sentido da Proposição 5.4.10), prove que M possui um quociente isomorfo a V.

Solução: Temos uma extensão canônica de M/N por N/V_1, que é o quociente M/V_1. Analogamente, a extensão de M/N por N/V_2 que consideraremos é o quociente M/V_2. Por hipótese, temos um diagrama comutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N/V_1 & \longrightarrow & M/V_1 & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \mathrm{id}_{M/N}} & & \\ 0 & \longrightarrow & N/V_2 & \longrightarrow & M/V_2 & \longrightarrow & M/N & \longrightarrow & 0 \end{array}$$

Os mapas φ e ψ são isomorfismos. As duas linhas são exatas e os mapas são, respectivamente, a inclusão de N/V_i em M/V_i e a projeção de M/V_i em M/N que leva $m + V_i \in M/V_i$ em $m + N \in M/N$ (para $i = 1, 2$). Para encontrar um quociente de M isomorfo a V, vamos construir um homomorfismo sobrejetor de M em V_1.

Seja $m \in M$. Escreva $\psi(m + V_1) = m' + V_2$ para algum $m' \in M$. Partindo do elemento $m + V_1 \in M/V_1$, temos dois caminhos possíveis para percorrer pelo diagrama. Começando com ψ e depois aplicando a projeção em M/N, obtemos $m' + N$. Por outro lado, começando com a projeção em M/N e depois aplicando a identidade, chegamos em $m + N$. Da comutatividade do diagrama, deve valer $m' + N = m + N$, ou seja, $m' = m + n$ para algum $n \in N$. Como N é a soma de V_1 e V_2, podemos escrever $n = v_1 + v_2$ com $v_1 \in V_1$ e $v_2 \in V_2$. Assim,

$$\psi(m + V_1) = m' + V_2 = (m + n) + V_2 = (m + v_1 + v_2) + V_2 = (m + v_1) + V_2.$$

Note que v_1 é único: se $v_1' \in V_1$ é outro elemento satisfazendo $\psi(m + V_1) = (m + v_1') + V_2$, então

$$(m + v_1) + V_2 = (m + v_1') + V_2 \implies v_1 - v_1' \in V_2.$$

Mas $v_1, v_1' \in V_1$ e $V_1 \cap V_2 = 0$, logo $v_1 - v_1' = 0$, isto é, $v_1 = v_1'$. Portanto, conseguimos definir a função $f : M \to V_1$ que leva $m \in M$ no único elemento $v_1 \in V_1$ satisfazendo $\psi(m + V_1) = (m + v_1) + V_2$. Se $m_1, m_2 \in M$, observe que

$$\begin{aligned}\psi((m_1 + m_2) + V_1) &= \psi(m_1 + V_1) + \psi(m_2 + V_1) \\ &= ((m_1 + f(m_1)) + V_2) + ((m_2 + f(m_2)) + V_2) \\ &= (m_1 + m_2 + f(m_1) + f(m_2)) + V_2,\end{aligned}$$

logo, da definição de $f(m_1 + m_2)$, deve valer $f(m_1 + m_2) = f(m_1) + f(m_2)$. De modo análogo, conseguimos mostrar que $f(am) = af(m)$ para todos $a \in A$ e $m \in M$. Portanto, $f : M \to V_1$ é um homomorfismo de A-módulos!

Resta mostrar que f é sobrejetor. Seja $v_1 \in V_1$ qualquer. Como $V_1 \subseteq N$, podemos formar o elemento $v_1 + V_2 \in N/V_2$. Lembre que φ é inversível, então está definido $\varphi^{-1}(v_1 + V_2)$ e, como $N = V_1 + V_2$, este elemento é da forma $v_2 + V_1$ para algum $v_2 \in V_2$. Assim,

$$\psi(v_2 + V_1) = \psi(\varphi^{-1}(v_1 + V_2)) = v_1 + V_2,$$

onde usamos a comutatividade do diagrama e identificamos N/V_1 dentro de M/V_1 e N/V_2 dentro de M/V_2. Mas, pela definição de f, sabemos que

$$\psi(v_2 + V_1) = (v_2 + f(v_2)) + V_2 = f(v_2) + V_2.$$

Desse modo, $v_1 + V_2 = f(v_2) + V_2$. Como $v_1, f(v_2) \in V_1$ e $V_1 \cap V_2 = 0$, concluímos que $f(v_2) = v_1$. Isso garante a sobrejetividade de f, como preciso. □

Exercício A.5.14. Sejam $U_1, \ldots, U_r$ os B-módulos indecomponíveis não projetivos, um de cada classe de isomorfismo, e sejam $W_1, \ldots, W_r$ os respectivos b_1-módulos indecomponíveis não projetivos associados através da Correspondência de Green (vide o Teorema 5.4.1). Sabemos que

$$\overline{\mathrm{Hom}}_{kG}(U_i, U_j) \cong \overline{\mathrm{Hom}}_{kN_1}(W_i, W_j)$$

para todos $1 \leq i, j \leq r$ (Corolário 5.4.2) e que o correspondente de ΩU_i é ΩW_i para todo $1 \leq i \leq r$ (Proposição 5.3.24).

(a) Definindo $X_i \coloneqq \Omega W_i$ para todo $1 \leq i \leq r$, verifique que a correspondência que associa U_i a X_i possui as mesmas propriedades descritas acima.

(b) Mostre que, se trocarmos a Correspondência de Green por essa nova correspondência, então, em algum sentido, o que fizemos nas Seções 5.4 e 5.5 ainda funciona.

(c) Dê um sentido à seguinte afirmação: "com a nova correspondência, os papéis das permutações ρ e σ se alternam".

Solução: (a) Inicialmente, observe que a nova correspondência ainda estabelece uma bijeção entre B-módulos indecomponíveis não projetivos e b_1-módulos indecomponíveis não projetivos pelo Teorema 5.3.22. A primeira propriedade do enunciado segue de imediato do que temos e da Proposição 5.3.23:

$$\overline{\mathrm{Hom}}_{kG}(U_i, U_j) \cong \overline{\mathrm{Hom}}_{kN_1}(W_i, W_j) \cong \overline{\mathrm{Hom}}_{kN_1}(\Omega W_i, \Omega W_j) = \overline{\mathrm{Hom}}_{kN_1}(X_i, X_j),$$

para todos $1 \leq i, j \leq r$. A segunda também é tranquila: como a Correspondência de Green leva ΩU_i em ΩW_i, essa nova correspondência leva ΩU_i em $\Omega(\Omega W_i) = \Omega X_i$, para todo $1 \leq i \leq r$.

(b) No início da Seção 5.4, estabelecemos a correspondência entre B-módulos e b_1-módulos a partir da Correspondência de Green. Para demonstrar os resultados seguintes, utilizamos essencialmente apenas as duas propriedades enunciadas neste exercício. Por isso, como a nova correspondência do item (a) também possui essas propriedades, podemos empregar os mesmos argumentos. O problema é tudo aquilo que envolve o Teorema 5.4.12, pois, nesse ponto, precisamos de outras propriedades da Correspondência de Green, especialmente para demonstrar a Proposição 5.4.11. Temos de verificar como esse resultado fica com a nova correspondência.

Primeiro, devemos destacar um aspecto fundamental que aparece no início da Seção 5.4. Através do Teorema 5.4.3, ordenamos os B-módulos simples $S_0, \dots, S_{e-1}$ de modo que o quociente radical do correspondente de Green T_i de S_i seja isomorfo a V_i para todo $0 \leq i < e$. Essa ordenação foi fundamental para construir a permutação π utilizada na hora de estudar extensões de B-módulos simples. Desta vez, teremos uma outra ordenação. Por simplicidade, na notação do enunciado, diremos que X_i é o "Ω-correspondente" de U_i e vice-versa, para todo $1 \leq i \leq r$. Como o Teorema 5.4.3 também funciona se trocarmos a Correspondência de Green por essa "Ω-correspondência", podemos ordenar os B-módulos simples como $S_0^\Omega, S_1^\Omega, \dots, S_{e-1}^\Omega$ de modo que $T_i^\Omega/\operatorname{rad}(T_i^\Omega) \cong V_i$ para todo $0 \leq i < e$, onde T_i^Ω é o Ω-correspondente de S_i^Ω. Isso nos fornece uma permutação π_Ω do conjunto $\{0, 1, \dots, e-1\}$ caracterizada por $\operatorname{soc}(T_i^\Omega) \cong V_{\pi_\Omega(i)}$ para todo $0 \leq i < e$.

Vejamos qual é a relação entre π e π_Ω. Como a cobertura projetiva de T_i é V_{iq}, sabemos que ΩT_i é o submódulo de V_{iq} satisfazendo $V_{iq}/\Omega T_i \cong T_i$. Como o soco do unisseriado V_{iq} é V_i, temos $\operatorname{soc}(\Omega T_i) \cong V_i$. Seguindo a ordenação circular dos fatores de composição de V_{iq}, obtemos de $\operatorname{soc}(T_i) \cong V_{\pi(i)}$ que $\Omega T_i/\operatorname{rad}(\Omega T_i) \cong V_{\pi(i)+1}$. Ou seja, quando o Ω-correspondente de um B-módulo simples possui soco V_i, o seu quociente radical é $V_{\pi(i)+1}$. Em outras palavras, se o Ω-correspondente de um B-módulo simples possui quociente radical V_i, o seu soco deve ser $V_{\pi^{-1}(i-1)}$. Portanto,

$$\pi_\Omega(i) = \pi^{-1}(i-1)$$

para todo $0 \leq i < e$ (onde lemos os índices módulo e). Essa discussão também mostra que

$$S_i^\Omega \cong S_{\pi^{-1}(i-1)} = S_{\pi_\Omega(i)}$$

e que

$$T_i^\Omega \cong \Omega T_{\pi^{-1}(i-1)} = \Omega T_{\pi_\Omega(i)}$$

para todo $0 \leq i < e$.

Agora, vamos analisar o Teorema 5.4.12. No nosso novo contexto, devemos ter as seguintes hipóteses: seja U um B-módulo indecomponível não projetivo com $U/\operatorname{rad}(U)$ simples e com Ω-correspondente isomorfo a V_{is}. Se $0 \leq j < e$, vamos descobrir quando existe uma sequência exata

$$0 \longrightarrow S_j^\Omega \longrightarrow M \longrightarrow U \longrightarrow 0$$

que não cinde. Na linguagem usual da Seção 5.4, o correspondente de Green de U é $\Omega^{-1}V_{is} \cong V_{i+s-1,q-s}$ (o isomorfismo segue porque o quociente radical de $\Omega^{-1}V_{is}$ é isomorfo ao soco de V_{is}), e estamos tentando estender U por $S_{\pi_\Omega(j)}$. Pelo enunciado original do Teorema 5.4.12, a extensão desejada existe se vale

$$(q-s) + l(T_{\pi_\Omega(j)}) > q \quad \text{e} \quad i + s - 1 \equiv \pi(\pi_\Omega(j)) \pmod{e}$$

ou

$$(q-s) + l(T_{\pi_\Omega(j)}) \leq q \quad \text{e} \quad (i+s-1) + (q-s) \equiv \pi_\Omega(j) \pmod{e}.$$

Agora, como

$$l(T_{\pi_\Omega(j)}) = q - l(\Omega T_{\pi_\Omega(j)}) = q - l(T_j^\Omega),$$

a primeira desigualdade é equivalente a $s + l(T_j^\Omega) < q$, enquanto a segunda é equivalente a $s + l(T_j^\Omega) \geq q$. Além disso, pela relação entre π e π_Ω, a primeira congruência se torna:

$$i + s - 1 \equiv \pi(\pi_\Omega(j)) = j - 1 \pmod{e} \iff i + s \equiv j \pmod{e}.$$

Por fim, como $q \equiv 1 \pmod{e}$, a segunda congruência é equivalente à igualdade $i = \pi_\Omega(j)$ (a congruência desaparece porque os elementos estão entre 0 e $e-1$).

Desse modo, demonstramos que, se U é como anteriormente, então existe aquela sequência exata que não cinde exatamente quando ocorre

$$s + l(T_j^\Omega) < q \quad \text{e} \quad i + s \equiv j \pmod{e}$$

ou

$$s + l(T_j^\Omega) \geq q \quad \text{e} \quad i = \pi_\Omega(j).$$

Essas são essencialmente as condições do Teorema 5.4.12, apenas o caso da igualdade trocou de posição. Além disso, caso exista, a extensão M é indecomponível, satisfaz $M/\operatorname{rad}(M) \cong U/\operatorname{rad}(U)$ e é projetiva exatamente quando há igualdade na desigualdade acima. Como também temos $\pi_\Omega(i) + 1 \equiv i + l(T_i^\Omega) \pmod{e}$ (porque $V_{\pi_\Omega(i)}$ é o soco de T_i^Ω), também conseguimos enunciar o análogo do Corolário 5.4.13 com a Ω-correspondência.

Estamos quase lá! Todas as construções e demonstrações da Seção 5.5 funcionam quase perfeitamente para a Ω-correspondência pelo que já vimos, só resta garantirmos uma última propriedade. Nas provas dessa seção, precisamos várias vezes conhecer quem é o correspondente de Green da extensão indecomponível dada pelo Teorema 5.4.12 (quando ela não é projetiva). Temos que verificar que, com a Ω-correspondência, os Ω-correspondentes possuem o mesmo formato. Ou seja, se U e j são como anteriormente, devemos mostrar que o Ω-correspondente da extensão é $V_{i,s+l(T_j^\Omega)}$, quando

$$s + l(T_j^\Omega) < q \quad \text{e} \quad i + s \equiv j \pmod{e},$$

ou $V_{j,s+l(T_j^\Omega)-q}$, quando

$$s + l(T_j^\Omega) > q \quad \text{e} \quad i = \pi_\Omega(j).$$

Vimos que o correspondente de Green de U é $V_{i+s-1,q-s}$ e que $S_j^\Omega \cong S_{\pi_\Omega(j)}$. Também notamos que o primeiro caso acima corresponde ao primeiro caso do Teorema 5.4.12, enquanto o segundo caso acima corresponde ao segundo caso do teorema. Pela observação no final da Seção 5.4, se estamos no primeiro caso acima, então o correspondente de Green da extensão é

$$V_{\pi_\Omega(j),(q-s)+l(T_{\pi_\Omega}(j))-q} = V_{\pi_\Omega(j),l(T_{\pi_\Omega(j)})-s}.$$

Aplicando o operador de Heller, concluímos que o Ω-correspondente da extensão é

$$V_{\pi_\Omega(j)+l(T_{\pi_\Omega(j)})-s,s+q-l(T_{\pi_\Omega(j)})}.$$

Como $q - l(T_{\pi_\Omega(j)}) = l(\Omega T_{\pi_\Omega(j)}) = l(T_j^\Omega)$, o comprimento do módulo acima é $s + l(T_j^\Omega)$. Agora, como $t + l(T_t) \equiv \pi(t) + 1 \pmod{e}$ para todo $0 \leq t < e$, note que

$$\pi_\Omega(j) + l(T_{\pi_\Omega(j)}) - s \equiv \pi(\pi_\Omega(j)) + 1 - s \equiv j - s \equiv i \pmod{e},$$

onde utilizamos ao final que $i + s \equiv j \pmod{e}$. Portanto, essa conta mostra que, no primeiro caso, o Ω-correspondente de fato é $V_{i,s+l(T_j^\Omega)}$. Por outro lado, se estamos no segundo caso, o final da Seção 5.4 mostra que o correspondente de Green da extensão é

$$V_{i+s-1,(q-s)+l(T_{\pi_\Omega(j)})}.$$

Aplicando o operador de Heller, obtemos que o Ω-correspondente da extensão é

$$V_{i+l(T_{\pi_\Omega(j)})+(q-1),s-l(T_{\pi_\Omega(j)})} = V_{i+l(T_{\pi_\Omega(j)}),s-l(T_{\pi_\Omega(j)})},$$

onde usamos que e divide $q-1$. Como $l(T_{\pi_\Omega(j)}) = q - l(T_j^\Omega)$, o comprimento do módulo acima é $s + l(T_j^\Omega) - q$. Agora, como $i = \pi_\Omega(j)$, vale

$$i + l(T_{\pi_\Omega(j)}) = i + l(T_i) \equiv \pi(i) + 1 = \pi(\pi_\Omega(j)) + 1 \equiv j \pmod{e}.$$

Por isso, essa outra conta nos dá que, no segundo caso, o Ω-correspondente é $V_{j,s+l(T_j^\Omega)-q}$, como afirmamos.

Isso já conclui este item do exercício. Porém, queremos esclarecer mais um detalhe. Acabamos de ver que tudo das Seções 5.4 e 5.5 que vale para a Correspondência de Green também vale para a Ω-correspondência, exceto uma coisa: a posição da igualdade no Teorema 5.4.12. Isso poderia influenciar alguns argumentos, como o final da demonstração do Teorema 5.5.1. Mas a verdade é que, quando vale $s + l(T_j^\Omega) = q$, são equivalentes $i = \pi_\Omega(j)$ e $i + s \equiv j \pmod{e}$, então não temos com o que nos preocupar! De fato, como $j + l(T_j^\Omega) \equiv \pi_\Omega(j) + 1 \pmod{e}$, com essa igualdade temos

$$j \equiv \pi_\Omega(j) - l(T_j^\Omega) + 1 \equiv \pi_\Omega(j) + (q - l(T_j^\Omega)) = \pi_\Omega(j) + s \pmod{e},$$

de onde segue a equivalência desejada. Portanto, não importa em qual caso colocamos a igualdade. Esse comentário poderia ter sido feito já no Teorema 5.4.12.

(c) De certa forma, como observamos na Seção 5.5, ρ e σ representam os casos do Teorema 5.4.12. Como vimos no item (b), a troca de correspondência alterna os casos desse teorema. Nesse sentido, os papéis de ρ e σ se alternam, mas vamos dar um sentido mais interessante à afirmação do enunciado. Seja $\mathcal{G}$ o grafo de Brauer de B, como construímos na Seção 5.5. A partir de $\mathcal{G}$, conseguimos recuperar ρ e σ (a menos de renomeação dos simples) por conta do modo que esse grafo foi construído. Porém, não é possível descobrir qual dentre essas duas permutações é ρ e qual é σ. E há um motivo para existir essa ambiguidade. Executando a Seção 5.5 com a Ω-correspondência, encontramos um grafo $\mathcal{G}_\Omega$. Ele deve ser necessariamente isomorfo a $\mathcal{G}$. A seguir, construiremos um isomorfismo de $\mathcal{G}_\Omega$ em $\mathcal{G}$ que troca os tipos dos vértices: os vértices de tipo ρ viram vértices de tipo σ, e vice-versa. Isso dá um sentido muito mais legal para a frase do enunciado!

Vamos entrar em mais detalhes agora. A partir da permutação π_Ω, definimos as permutações ρ_Ω e σ_Ω de $\{0, 1, \ldots, e-1\}$ que satisfazem $\rho_\Omega = \pi_\Omega^{-1}$ e $\sigma_\Omega(i) \equiv \pi_\Omega(i) + 1 \pmod{e}$ para todo $0 \leq i < e$. Para auxiliar, seja τ a permutação cíclica usual, que satisfaz $\tau(i) \equiv i+1 \pmod{e}$ para $0 \leq i < e$. Assim, $\sigma_\Omega = \tau\pi_\Omega$. Como fizemos para construir o grafo de Brauer $\mathcal{G}$ de B, também conseguimos construir um grafo $\mathcal{G}_\Omega$ a partir de ρ_Ω e σ_Ω, que é bipartido entre vértices de tipo ρ_Ω (cada um deles sendo uma órbita da permutação ρ_Ω) e vértices de tipo σ_Ω (cada um deles sendo uma órbita da permutação σ_Ω). Para relacionar $\mathcal{G}_\Omega$ a $\mathcal{G}$, devemos relacionar ρ_Ω e σ_Ω com ρ e σ. Observando que $\pi_\Omega = \pi^{-1}\tau^{-1}$, temos

$$\rho_\Omega = \pi_\Omega^{-1} = (\pi^{-1}\tau^{-1})^{-1} = \tau\pi = \sigma$$

e

$$\sigma_\Omega = \tau\pi_\Omega = \tau\pi^{-1}\tau^{-1} = \tau\rho\tau^{-1}.$$

Como π comuta com ρ e π_Ω comuta com ρ_Ω, podemos rescrever essas relações das seguintes formas:

$$\sigma = \rho_\Omega = \pi_\Omega\rho_\Omega\pi_\Omega^{-1}$$

e

$$\sigma_\Omega = \tau\rho\tau^{-1} = (\tau\pi)\rho(\pi^{-1}\tau^{-1}) = \pi_\Omega^{-1}\rho\pi_\Omega \implies \rho = \pi_\Omega\sigma_\Omega\pi_\Omega^{-1}.$$

Desse modo, σ e ρ_Ω são conjugados, então possuem a mesma estrutura cíclica. A afirmação análoga também vale para ρ e σ_Ω. Mas, mais do que isso, ambas as conjugações podem ser realizadas através de π_Ω. Ou seja, renomeando o conjunto $\{0, 1, \ldots, e-1\}$ através da permutação π_Ω, levamos σ_Ω em ρ e ρ_Ω em σ, e órbitas são levadas em órbitas bijetivamente. Isso define uma função bijetora do conjunto dos vértices de $\mathcal{G}_\Omega$ no conjunto dos vértices de $\mathcal{G}$. Repare que um vértice de tipo σ_Ω é levado em um vértice de ρ e um vértice de tipo ρ_Ω é levado em um vértice de tipo σ. Por fim, é imediato que dois vértices de $\mathcal{G}_\Omega$ estão conectados por uma aresta se e só se os vértices correspondentes de $\mathcal{G}$ também estão. Nesse caso, temos uma bijeção natural entre as arestas levando a aresta S_i^Ω na aresta $S_{\pi_\Omega(i)}$ para todo $0 \leq i < e$. Assim, temos um isomorfismo entre os grafos $\mathcal{G}_\Omega$ e $\mathcal{G}$ que alterna os tipos dos vértices!

Vamos concluir com um exemplo concreto (mas hipotético) para ilustrar o que acabamos de fazer. Tome $e = 5$ e considere a permutação $\pi = (0\ 1)(2\ 3)$ de $\{0, 1, 2, 3, 4\}$ (com $\pi(4) = 4$). Nesse caso, temos $\rho = \pi$,

$$\sigma = \rho_\Omega = (0\ 2\ 4), \quad \pi_\Omega = (0\ 4\ 2) \quad \text{e} \quad \sigma_\Omega = (1\ 2)(3\ 4).$$

Vamos listar as órbitas:

$$\begin{aligned}
\text{Órbitas de } \rho &= \{0,1\}, \{2,3\} \text{ e } \{4\} \\
\text{Órbitas de } \sigma &= \{0,2,4\}, \{1\} \text{ e } \{3\} \\
\text{Órbitas de } \rho_\Omega &= \{0,2,4\}, \{1\} \text{ e } \{3\} \\
\text{Órbitas de } \sigma_\Omega &= \{0\}, \{1,2\} \text{ e } \{3,4\}
\end{aligned}$$

Renomeando através de π_Ω (ou seja, trocando 0 por 4, 1 por 1, 2 por 0, 3 por 3 e 4 por 2), veja que as órbitas de ρ_Ω são levadas nas órbitas de σ (na verdade não há alteração) e as órbitas de σ_Ω são levadas nas órbitas de ρ. Além disso, é fácil verificar que uma órbita de ρ_Ω intersecta uma órbita de σ_Ω no elemento i (representando a aresta S_i^Ω de $\mathcal{G}_\Omega$) se e só se as órbitas correspondentes de σ e ρ se intersectam no elemento $\pi_\Omega(i)$ (representando a aresta $S_{\pi_\Omega(i)}$ de $\mathcal{G}$), para todo $0 \leq i < 5$.

□

Exercício A.5.15. Com as notações da Seção 5.5, mostre que todo B-módulo não projetivo obtido de S_i através de sucessivas extensões de "tipo σ" (ou seja, extensões que caem no segundo caso do Teorema 5.4.12) é um quociente de U_i^σ. Trocando σ por ρ, prove um resultado análogo.

Solução: Uma extensão de S_i de tipo σ é feita, por definição, acrescentando-se uma cópia de $S_{\sigma(i)}$ "embaixo" de S_i. Pelo Teorema 5.4.12, essa extensão existe exatamente quando $l(T_i)+l(T_{\sigma(i)}) \leq q$ e, pela Proposição 5.4.10, ela é única. Além disso, essa extensão é não projetiva exatamente quando a desigualdade é estrita. Supondo que valha a desigualdade estrita, seja M_1 essa extensão. Já nos deparamos com ela quando estávamos construindo U_i^σ. Nesse momento, vimos que, para fazer uma extensão de M_1 de tipo σ, devemos acrescentar uma cópia de $S_{\sigma^2(i)}$ e deve valer a condição $l(T_i) + l(T_{\sigma(i)}) + l(T_{\sigma^2(i)}) \leq q$. Quando estamos sob essas condições, garantimos a existência de uma única extensão M_2 de tipo σ e, com a desigualdade estrita, M_2 não é projetivo. Mais uma vez, esse módulo é o mesmo M_2 que apareceu na construção de U_i^σ. Note que M_1 é um quociente de M_2 pela definição da extensão. Podemos proceder assim: a cada passo, só há no máximo uma extensão a se fazer e, no j-ésimo passo, existe uma extensão M_j se e somente se está definido M_{j-1} e

$$l(T_i) + l(T_{\sigma(i)}) + \cdots + l(T_{\sigma^j(i)}) \leq q.$$

Nesse caso, M_{j-1} é um quociente de M_j e M_j não é projetivo exatamente quando a desigualdade é estrita. Agora, por construção, $M_b = U_i^\sigma$ é a última extensão que não é projetiva, já que b é o maior inteiro não negativo com

$$l(T_i) + l(T_{\sigma(i)}) + \cdots + l(T_{\sigma^b(i)}) < q.$$

Assim, um B-módulo não projetivo obtido de S_i através de sucessivas extensões de tipo σ é S_i ou então algum M_j $(1 \leq j \leq b)$ e, portanto, é um quociente de $M_b = U_i^\sigma$, como desejado. É interessante observar que talvez ainda seja possível realizar uma extensão de tipo σ a partir de U_i^σ, mas ela será necessariamente projetiva. Depois disso, não faz mais sentido fazer extensões de tipo σ (e na verdade, qualquer extensão desse projetivo necessariamente cindirá e não poderá mais ser indecomponível). Estudando a construção de U_i^ρ, obtemos de modo similar o resultado análogo onde trocamos σ por ρ. □

Exercício A.5.16. Mostre que o Lema 5.6.1 também funciona para uma decomposição de M em mais de dois somandos diretos.

Solução: Vamos adaptar a demonstração dada para esse lema. Sejam M, N e S módulos como no enunciado. Seja

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_r$$

uma decomposição de M como soma direta de submódulos $M_1, M_2, \ldots, M_r$ $(r \geq 2)$. Devemos encontrar um índice $i \in \{1, 2, \ldots, r\}$ tal que $N \cap S \subseteq M_i$ e $M_i/\operatorname{rad}(M_i)$ possui um quociente isomorfo a $N/\operatorname{rad}(N)$.

Para cada $1 \leq i \leq r$, seja N_i a projeção de N no somando M_i. Se valesse $N_i \subseteq \operatorname{rad}(M_i)$ para todo $1 \leq i \leq r$, então

$$N \subseteq N_1 \oplus \cdots \oplus N_r \subseteq \operatorname{rad}(M_1) \oplus \cdots \oplus \operatorname{rad}(M_r) = \operatorname{rad}(M),$$

contradizendo a condição (3) do enunciado. Por isso, uma daquelas inclusões não pode valer. Sem perda de generalidade, suporemos que $N_1 \not\subseteq \operatorname{rad}(M_1)$. Em particular, $N_1 \neq 0$ e então, como N_1 é um quociente não nulo de N, que possui quociente radical simples, devemos ter $N_1/\operatorname{rad}(N_1) \cong N/\operatorname{rad}(N)$. Agora, a inclusão de N_1 em M_1 induz um homomorfismo de $N_1/\operatorname{rad}(N_1)$ em $M_1/\operatorname{rad}(M_1)$. Como $N_1 \not\subseteq \operatorname{rad}(M_1)$, esse homomorfismo é não nulo e, como $N_1/\operatorname{rad}(N_1)$ é simples, ele deve ser injetor. Portanto, $N/\operatorname{rad}(N) \cong N_1/\operatorname{rad}(N_1)$ é um fator de composição do módulo semissimples $M_1/\operatorname{rad}(M_1)$. Consequentemente, $M_1/\operatorname{rad}(M_1)$ possui um quociente isomorfo a $N/\operatorname{rad}(N)$.

Basta mostramos que $N \cap S \subseteq M_1$ para concluir a demonstração. Para isso, teremos que verificar primeiramente que $N_i \subseteq S$ para $2 \leq i \leq r$. Fixe $2 \leq i \leq r$. Se $N_i \not\subseteq \operatorname{rad}(M_i)$, poderíamos argumentar como antes para concluir que $N/\operatorname{rad}(N)$ também é fator de composição de $M_i/\operatorname{rad}(M_i)$. Como $M_1/\operatorname{rad}(M_1)$ e $M_i/\operatorname{rad}(M_i)$ são somandos distintos de $M/\operatorname{rad}(M)$, isso implicaria que $M/\operatorname{rad}(M)$ não é livre de multiplicidade, um absurdo. Portanto, $N_i \subseteq \operatorname{rad}(M_i)$ e então $N_i \subseteq \operatorname{rad}(M)$. Agora, pelo Segundo Teorema do Isomorfismo, temos

$$\frac{N_i}{N_i \cap S} \cong \frac{N_i + S}{S} \leq \frac{\operatorname{rad}(M)}{S},$$

onde a inclusão segue do fato de N_i e S serem submódulos de $\operatorname{rad}(M)$. Se $N_i \cap S \subsetneq N_i$, então deve valer $N_i \neq 0$ e, como antes, $N_i/\operatorname{rad}(N_i) \cong N/\operatorname{rad}(N)$. Logo, $N_i/\operatorname{rad}(N_i)$ é simples e $\operatorname{rad}(N_i)$ é o único submódulo maximal de N_i. Segue que $N_i \cap S \subseteq \operatorname{rad}(N_i)$ e então $N/\operatorname{rad}(N) \cong N_i/\operatorname{rad}(N_i)$ é um quociente e $N_i/(N_i \cap S)$. Pelo isomorfismo em destaque acima, $N/\operatorname{rad}(N)$ é um fator de composição de $\operatorname{rad}(M)/S$. Mas $N/\operatorname{rad}(N)$ já é fator de composição de $M/\operatorname{rad}(M)$, o que contradiz a condição (4) do enunciado. Desse modo, deve valer $N_i \cap S = N_i$, isto é, $N_i \subseteq S$, como afirmamos. Como S é semissimples, isso implica que N_i também é semissimples, ou seja, $\operatorname{rad}(N_i) = 0$.

Por fim, observe que $N \cap S \subsetneq N$, porque, caso contrário, teríamos $N = N \cap S \subseteq S \subseteq \operatorname{rad}(M)$, o que não é verdade. Como $N/\operatorname{rad}(N)$ é simples, segue que $N \cap S \subseteq \operatorname{rad}(N)$. Assim,

$$N \cap S \subseteq \operatorname{rad}(N) \subseteq \operatorname{rad}(N_1) + \operatorname{rad}(N_2) + \cdots + \operatorname{rad}(N_r) = \operatorname{rad}(N_1) + 0 + \cdots + 0 \subseteq N_1 \subseteq M_1,$$

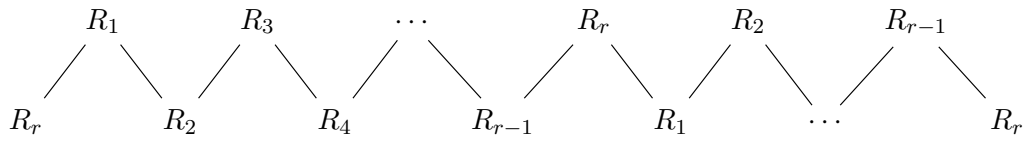
concluindo a solução. □

Exercício A.5.17. Na demonstração do Teorema 5.6.2, quando mostramos que não havia ciclos no grafo de Brauer do bloco B, utilizamos que esse grafo é bipartido em vértices de tipo ρ e de tipo σ. Isso garantia que um certo ciclo possuía comprimento par. Desta vez, analisando ciclos de comprimento ímpar, dê uma prova alternativa para essa parte sem usar essa propriedade.

Solução: Com as notações do Teorema 5.6.2, vamos mostrar que o grafo de Brauer de B é acíclico. Suponha, por absurdo, que haja um ciclo nesse grafo e considere um ciclo de tamanho mínimo. Liste as suas arestas como $R_1, R_2, \ldots, R_r$ ($r \geq 2$), na ordem em que são percorridas. Se r é par, já vimos na demonstração do Teorema 5.6.2 como chegar em uma contradição. Suponha, então, que r seja ímpar. Como nessa demonstração, para cada $1 \leq i \leq r$, podemos encontrar um B-módulo indecomponível N_i satisfazendo $N_i/\operatorname{rad}(N_i) \cong R_i$, $\operatorname{soc}(N_i) \cong R_{i-1} \oplus R_{i+1}$ (esses índices são lidos módulo r, como de costume) e nenhum simples dentre $R_1, \ldots, R_r$ é um fator de composição de $\operatorname{rad}(N_i)/\operatorname{soc}(N_i)$. Agora, vamos utilizar aquele mesmo argumento de "colagem": podemos tomar um quociente M da soma direta

$$N_1 \oplus N_3 \oplus \cdots \oplus N_r \oplus N_2 \oplus N_4 \oplus \cdots \oplus N_{r-1}$$

que identifica fatores "consecutivos" no soco, obtendo um módulo que pode ser descrito pela figura a seguir:



Como fizemos no Teorema 5.6.2, conseguimos mostrar que M é indecomponível. Porém, o soco de M contém duas cópias de R_r e então não é livre de multiplicidade, contradizendo a Proposição 5.4.8! Isso finaliza o exercício. □

Referências Bibliográficas

[1] **Alperin, J. L.** Local representation theory. Modular representations as an introduction to the local representation theory of finite groups. *Cambridge University Press, Cambridge,* 1986.

[2] **Assem, I.; Coelho, F. U.** Basic representation theory of algebras. Graduate Texts in Mathematics, 283. *Springer, Cham,* 2020.

[3] **Benson, D. J.** Representations and cohomology. I. Basic representation theory of finite groups and associative algebras. Second edition. Cambridge Studies in Advanced Mathematics, 30. *Cambridge University Press, Cambridge,* 1998.

[4] **Brauer, R.** On the Cartan invariants of groups of finite order. *Ann. of Math. (2)* 42 (1941), 53–61.

[5] **Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A.** ATLAS of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray. *Oxford University Press, Eynsham,* 1985.

[6] **Cooperman, G.; Hiss, G.; Lux, K.; Müller, J.** The Brauer tree of the principal 19-block of the sporadic simple Thompson group. *Experiment. Math.* **6** (1997), no. 4, 293–300.

[7] **Craven, D. A.** Representation theory of finite groups: a guidebook. *Springer, Cham,* 2019.

[8] **Curtis, C. W.** Representation theory of finite groups: from Frobenius to Brauer. *Math. Intelligencer* **14** (1992), no. 4, 48–57.

[9] **Curtis, C. W.; Jans, J. P.** On algebras with a finite number of indecomposable modules. *Trans. Amer. Math. Soc.* 114 (1965), 122–132.

[10] **Evens, S.** Conjugacy classes in $\mathrm{GL}(2, \mathbb{F}_q)$. Notas. https://www3.nd.edu/~sevens/gl2f.pdf. (Último acesso: 06/12/2021.)

[11] **Feit, W.** Possible Brauer trees. *Illinois J. Math.* **28** (1984), no. 1, 43–56.

[12] **Hall, M., Jr.** The theory of groups. *The Macmillan Company, New York,* 1959.

[13] **Jacobson, N.** Basic algebra. I. Second edition. *W. H. Freeman and Company, New York,* 1985.

[14] ———. Basic algebra. II. Second edition. *W. H. Freeman and Company, New York,* 1989.

[15] **Janusz, G. J.** Indecomposable modules for finite groups. *Ann. of Math. (2)* 89 (1969), 209–241.

[16] **Lam, T. Y.** Lectures on modules and rings. Graduate Texts in Mathematics, 189. *Springer-Verlag, New York,* 1999.

[17] ———**.** A first course in noncommutative rings. Second edition. Graduate Texts in Mathematics, 131. *Springer-Verlag, New York,* 2001.

[18] **Peacock, R. M.** Blocks with a cyclic defect group. *J. Algebra* 34 (1975), 232–259.

[19] **Schneider, P.** Modular representation theory of finite groups. *Springer, Dordrecht,* 2013.

[20] **Serre, J.-P.** Linear representations of finite groups. *Springer-Verlag, New York-Heidelberg,* 1977.

[21] **Steinberg, B.** On the Burnside-Brauer-Steinberg theorem (2014). arXiv (Preprint). https://arxiv.org/pdf/1409.7632. (Último acesso: 06/12/2021.)

[22] **Webb, P.** A course in finite group representation theory. *Cambridge University Press, Cambridge,* 2016.

[23] **Zimmermann, A.** Representation theory. A homological algebra point of view. Algebra and Applications, 19. *Springer, Cham,* 2014.

Índice Remissivo