O Lema do Diamante em Teoria de Anéis

Vitor de Oliveira Ferreira

DISSERTAÇÃO APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO

PARA OBTENÇÃO DO GRAU DE MESTRE
EM
MATEMÁTICA

Área de Concentração: **Álgebra**
Orientador: **Prof. Dr. Roberto Celso Fabrício Costa**

Durante a elaboração deste trabalho, o autor recebeu apoio financeiro do CNPq

O Lema do Diamante em Teoria de Anéis

Este exemplar corresponde à redação final da dissertação apresentada por Vitor de Oliveira Ferreira, devidamente corrigida e aprovada pela comissão julgadora.

São Paulo, julho de 1995.

Banca examinadora:

Prof. Dr. Roberto Celso Fabrício Costa (orientador)	IME-USP
Prof. Dr. Francisco César Polcino Milies	IME-USP
Prof. Dr. Antônio José Engler	IMECC-UNICAMP

-São Paulo, abril de 1995-

À minha querida Lu

Agradecimentos

Agradeço aos meus pais, Sonia e Eduardo, pelo incentivo dado desde meu ingresso no mestrado até os momentos mais difíceis do desenvolvimento desta dissertação.

Agradeço, também, aos meus colegas de programa, em especial a Lucia Satie Ikemoto e Marcelo Dias Passos, por suas brilhantes sugestões e por sua paciente disponibilidade para me auxiliar sempre que os procurei.

Destaco entre as pessoas que me auxiliaram a dominar os computadores — essas máquinas infernais — o Prof. Rodolfo Baeza, por suas excelentes aulas de LaTeX, e Leonardo José Borges, por ter me conduzido pelos labirintos da Internet e repartido seus vastos conhecimentos de Unix comigo.

Aos professores responsáveis pelas disciplinas que cursei, presto especial homenagem em nome do espírito de pesquisador que eles fizeram brotar em mim.

Por ter sempre acreditado em minha capacidade de concluir este trabalho e compartilhado de meus mais difíceis dias durante esse período, e pelo doce carinho de todas as horas, tenho prazer em agradecer a Luciana Pérez de Campos Pires.

Finalmente, desejo registrar meu enorme apreço pelo trabalho de orientação do Prof. (e amigo) Roberto Costa, que me tranquilizava nos momentos de nervosismo e insegurança e me desafiava, durante os inúmeros seminários que realizamos juntos, a avançar cada vez mais profundamente no trabalho de investigação do qual foi fruto esta dissertação.

Vitor de Oliveira Ferreira

Resumo

No presente trabalho apresenta-se uma exposição detalhada do **Lema do Diamante** de G. Bergman, incluindo um problema sobre ortogonalidade de idempotentes cuja soma é ainda idempotente, que motiva a introdução do principal conceito da dissertação, a saber, a **redução** de um polinômio. As técnicas de Bergman são utilizadas para fornecer uma demonstração alternativa do Teorema de Poincaré-Birkhoff-Witt e para efetuar o cálculo de uma base para uma álgebra de dimensão finita. Finalmente, introduz-se uma generalização natural dos conceitos envolvidos no Lema do Diamante para o caso não comutativo. Essa generalização mostra-se suficiente para caracterizar a estrutura de coprodutos de k-anéis especiais.

Abstract

In the present work, a detailed expansion of G. Bergman's **Diamond Lemma** is presented, including a problem on orthogonality of idempotents whose sum is still idempotent. This motivates the introduction of the main concept of the dissertation, *viz.*, the **reduction** of a polynomial. Bergman's techniques are used to give an alternative proof of the Poincaré-Birkhoff-Witt Theorem and to make calculations resulting on a basis for a finite dimensional algebra. Finally, a natural generalization for the non-commutative case of the concepts involved in The Diamond Lemma is given. This generalization turns out to be sufficient for a characterization of the structure of coproducts of special k-rings.

Conteúdo

Introdução **2**

1 Motivação **7**

2 Sistemas de Redução **12**

2.1 O Lema do Diamante 12

2.2 Observações 29

2.2.1 Ambigüidades de inclusão 29

2.2.2 Quando k é um corpo 31

2.2.3 Ordem parcial de semigrupo 34

3 Aplicações **40**

3.1 O Teorema de Poincaré-Birkhoff-Witt (PBW) 40

3.2 Identidades 47

4 Generalização para k-anéis **61**

4.1 Estrutura de bimódulos para k-anéis 61

4.2 Aplicação: coprodutos de k-anéis 78

Bibliografia **84**

Introdução

A proposta desta dissertação é fazer uma apresentação detalhada de uma técnica de abordagem de problemas em álgebra relacionados com a busca de formas normais em algumas estruturas algébricas. Essa técnica, conhecida como o "Lema do Diamante", foi introduzida no artigo [15] com o formato de um resultado genérico sobre grafos. Em 1978, G. M. Bergman adaptou os conceitos envolvidos para a linguagem de teoria de anéis no artigo [3]. Esse artigo constitui o foco central desta dissertação e todos os teoremas apresentados aqui foram enunciados naquele trabalho.

Duas das aplicações do Lema do Diamante para teoria de anéis estão cuidadosamente descritas no Capítulo 3: uma demonstração do conhecido Teorema de Poincaré-Birkhoff-Witt e o cálculo de uma base para uma álgebra presentada por geradores e relações. Seguindo a ordem proposta por Bergman, uma generalização bastante natural do principal teorema (Teorema 2.1) para k-anéis é introduzida no Capítulo 4. O Capítulo 1 ocupa-se de introduzir um problema de formas normais para anéis que, por envolver explicitamente as idéias centrais do Captítulo 2, motiva o estudo mais abrangente, auxilia o estabelecimento das hipóteses a serem verificadas e sugere maneiras de abordar dificuldades na demonstração dos principais resultados deste capítulo.

O presente trabalho não pretende contribuir com resultados originais relacionados ao assunto, mas, sim, estender-se demorada e profundamente sobre cada etapa da construção de alguns trechos do artigo de Bergman. Apesar de estarem propostas, nesse artigo, diversas formulações do Lema do Diamante aplicadas a situações em diferentes estruturas algébricas, nesta dissertação optei por apresentar apenas aquelas mais relacionadas à teoria de anéis, pretendendo, com isso, produzir um texto coeso e suficientemente compreensível

para os que estão iniciando seus estudos em teoria de anéis não comutativos.

Resta dizer que o Lema do Diamante, tal como enunciado no artigo [3], tem sido utilizado com alguma freqüência em trabalhos de algebristas das mais diversas áreas, como demonstram os artigos de Anick [2] e Makar-Limanov [12] e os mais recentes [13], [5] e [11].

No restante desta introdução, minha intenção será a de estabelecer algumas notações e fixar a terminologia utilizadas no decorrer da dissertação.

Os símbolos $\mathbb{N}$ e $\mathbb{Z}$ denotarão o conjunto dos inteiros positivos $\{1, 2, \ldots\}$ e o anel dos números inteiros, respectivamente. A referência ao conjunto $\mathbb{N} \cup \{0\}$ será feita por intermédio do símbolo $\mathbb{N}_0$.

Um conjunto dotado de uma operação binária associativa é chamado um *semigrupo*. Um semigrupo que contenha um elemento unidade recebe a designação de *monóide*. Um *grupo* é um monóide no qual todos os elementos têm um inverso. Dizemos que um grupo é um grupo *abeliano* se a operação no conjunto subjacente for comutativa.

Por um *anel*, entendemos um conjunto R dotado de duas operações binárias $+$ e $\cdot$ (esta segunda mais comumente denotada por justaposição) de maneira que $(R, +)$ seja um grupo abeliano e que estejam relacionadas por

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

quaisquer que sejam $a, b, c \in R$. Dizemos que R é um anel *associativo* se $(R, \cdot)$ for um semigrupo e *comutativo* se $ab = ba$, para todos $a, b \in R$. Um anel associativo R será dito um *anel com unidade* se existir um elemento em R, denotado por 1, tal que $(R, \cdot, 1)$ seja um monóide. Nesta dissertação trabalharemos apenas com anéis associativos com unidade. Esse fato será freqüentemente relembrado no decorrer do texto.

Um subconjunto I de um anel R é dito um *ideal à esquerda* (resp. *ideal à direita*) de R se I for um subgrupo de $(R, +)$ e se $RI \subseteq I$ (resp. $IR \subseteq I$). Um *ideal bilateral* de R é um subconjunto de R que é ao mesmo tempo um ideal à esquerda e um ideal à direita. Homomorfismos de anéis, sub-anéis e anéis quocientes são conceitos tomados como conhecidos e não serão definidos.

Seja k um anel associativo com unidade. Um *k-módulo à esquerda* é um grupo abeliano M (escrito aditivamente) sobre o qual está definida uma ação do anel k, $k \times M \longrightarrow$

M, que leva o par (r, x) no elemento rx, satisfazendo as seguintes leis para todo $r, r_i \in k$ e $x, x_i \in M$:

$$r(x_1 + x_2) = rx_1 + rx_2 \qquad (r_1 + r_2)x = r_1x + r_2x$$
$$(r_1r_2)x = r_1(r_2x) \qquad 1x = x.$$

Um *k-módulo à direita* é um grupo abeliano M sobre o qual está definida uma ação do anel k, $M \times k \longrightarrow M$, que leva o par (x, r) no elemento xr, satisfazendo as seguintes leis para todo $r, r_i \in k$ e $x, x_i \in M$:

$$(x_1 + x_2)r = x_1r + x_2r \qquad x(r_1 + r_2) = xr_1 + xr_2$$
$$x(r_1r_2) = (xr_1)r_2 \qquad x1 = x.$$

Um grupo abeliano M que é ao mesmo tempo um k-módulo à esquerda e um k-módulo à direita e satisfaz

$$r(xr') = (rx)r',$$

para todo $x \in M$ e $r, r' \in k$, é dito um *k-bimódulo.* As definições de homomorfismos de k-módulos (ou aplicações k-lineares) e de k-bimódulos, k-submódulos, sub-k-bimódulos e k-módulos e k-bimódulos quocientes são as correntes.

Um k-módulo (à esquerda) *livre* M é um k-módulo para o qual existe uma *base*, isto é, um subconjunto S de M tal que todo elemento de M tenha a forma $\sum_{s \in S} r_s s$, onde apenas uma quantidade finita dos $r_s \in k$ é diferente de zero e estão unicamente determinados. A definição de k-bimódulo livre é análoga, exigindo-se apenas que os elementos de M sejam unicamente escritos na forma $\sum_{s \in S} r_s s r'_s$.

Dada uma família de k-módulos (à esquerda) $(M_i)_{i \in I}$, indexada por um conjunto I, define-se a *soma direta* da família (M_i), denotada por $\bigoplus_{i \in I} M_i$, como sendo o k-módulo (à esquerda) M cujos elementos são famílias $(x_i)_{i \in I}$ quase nulas, com $x_i \in M_i$, e as operações são definidas coordenada a coordenada, isto é, $(x_i) + (x'_i) = (x_i + x'_i)$ e $r(x_i) = (rx_i)$. Existem injeções naturais de cada M_i em M dadas por $\alpha_i : M_i \longrightarrow M$, $\alpha_i(y) = (x_j)$, onde $x_i = y$ e $x_j = 0$ se $j \neq i$. A soma direta $\bigoplus_i M_i$ pode ainda ser caracterizada pela seguinte propriedade universal: dado um k-módulo (à esquerda) N e uma família de homomorfismos de k-módulos, $g_i : M_i \longrightarrow N$, existe um único homomorfismo de k-módulos $g : \bigoplus_i M_i \longrightarrow N$ tal que $g\alpha_i = g_i$, para todo $i \in I$. Para maiores detalhes ver [8, Sec. I.5]. A soma direta de uma família de k-bimódulos tem definição análoga.

Mais um último conceito sobre módulos precisa ser definido. Seja k um anel associativo com unidade e sejam M um k-módulo à direita e N um k-módulo à esquerda. Um par

(P, f), onde P é um grupo abeliano e $f : M \times N \longrightarrow P$ uma função que é *bilinear* (isto é, $f(x + x', y) = f(x, y) + f(x', y)$, para todos $x, x' \in M$ e $y \in N$) e *k-balanceada* (isto é $f(xr, y) = f(x, ry)$, para todos $x \in M$, $y \in N$ e $r \in k$) é dito um *produto balanceado* de M e N. Um *produto tensorial* de M e N é um produto balanceado $(M \otimes_k N, \otimes)$ que satisfaz a seguinte propriedade: dado (Q, g) um produto balanceado de M e N, existe um único homomorfismo de grupos $f : M \otimes N \longrightarrow Q$ tal que $f \circ \otimes = g$. Produtos tensoriais sempre existem [10, pp. 127–128] e são únicos a menos de isomorfismos. Além disso, tendo em vista algumas de suas propriedades, pode-se generalizar a definição de produto tensorial para uma quantidade finita qualquer de k-módulos. Produtos tensoriais de k-bimódulos podem ser dotados de uma estrutura de k-bimódulo, segundo a definição descrita em [10, pp. 133–136].

Dado um anel comutativo k, uma *k-álgebra* é um anel A dotado de uma ação de k, $(r, x) \longmapsto rx$, sob a qual A é também um k-módulo que satisfaz

$$r(x_1 x_2) = (rx_1)x_2 = x_1(rx_2),$$

quaisquer que sejam $r \in k$ e $x_1, x_2 \in A$. Todo anel é uma $\mathbb{Z}$-álgebra com a ação dada por $nx = x + \ldots + x$ (n parcelas), se $n \geq 1$, $0x = 0$ e $nx = -((-n)x)$, se $n < 0$. As definições de k-subálgebras e homomorfismos de k-álgebras são as usuais. Um comentário deve ser feito acerca da definição de ideal de uma k-álgebra. Naturalmente, um subconjunto I de uma k-álgebra A é definido como sendo um ideal se I for um ideal de A como anel e um k-submódulo de A como k-módulo. Nesse caso define-se da maneira usual a k-álgebra quociente A/I. No entanto, como todos os nossos anéis têm um elemento unidade 1, um ideal de uma k-álgebra A olhada apenas como um anel é automaticamente um k-submódulo de A olhada como k-módulo. Isso deve-se ao fato de termos $ra = r(1a) = (r1)a \in I$, para todo $a \in I$ e $r \in k$.

Maiores detalhes sobre as definições acima e propriedades dos objetos definidos podem ser encontrados, por exemplo, em [16].

Faremos agora alguns comentários sobre conjuntos em geral. Dado um conjunto X, uma *ordem parcial* em X é um subconjunto $\leq$ de $X \times X$ que satisfaz as três seguintes propriedades (por conveniência, ao invés de escrevermos $(x, y) \in \leq$, escreveremos $x \leq y$):

(P1) transitividade : se $x \leq y$ e $y \leq z$, então $x \leq z$;

(P2) anti-simetria : se $x \leq y$ e $y \leq x$, então $x = y$;

(P3) reflexividade : $x \leq x$, para todo $x \in X$.

Uma *ordem parcial estrita* em X é um subconjunto $<$ de $X \times X$ que satisfaz (novamente escrevendo $x < y$ no lugar de $(x, y) \in <$):

(E1) transitividade : se $x < y$ e $y < z$, então $x < z$;

(E2) anti-reflexividade : $x \not< x$ (o que quer dizer que $(x, x) \notin <$), qualquer que seja $x \in X$.

Prova-se que, dada uma ordem parcial estrita em X, se definirmos $x \leq y$ se $x = y$ ou $x < y$, então $\leq$ será uma ordem parcial em X. Reciprocamente, se $\leq$ é uma ordem parcial em X, então $x < y$ se e somente se $x \leq y$ e $x \neq y$ define uma ordem parcial estrita em X.

Uma *ordem total* em X é uma ordem parcial $\leq$ em X tal que se $x, y \in X$, então $x \leq y$ ou $y \leq x$. Uma ordem total em X é dita uma *boa ordem* se todo subconjunto não vazio Y de X tiver um elemento mínimo, isto é, se existir $y \in Y$ tal que $y \leq x$, qualquer que seja $x \in Y$. Nesta dissertação lançaremos mão de uma formulação do Axioma da Escolha que diz que todo conjunto pode ser bem ordenado, isto é, dado um conjunto X, existe uma boa ordem em X.

Capítulo 1

Motivação

Neste capítulo vamos estudar um problema que motivou a criação da linguagem e a prova do principal teorema do capítulo seguinte. Tratando-se apenas de uma motivação, a linguagem usada não será precisa e a liberdade de utilizar alguns termos não definidos será tomada. As imprecisões aqui presentes serão removidas no capítulo que se segue, onde todos os conceitos serão definidos rigorosamente.

A proposta aqui é resolver o seguinte problema :
American Mathematical Monthly ADVANCED PROBLEM 5082 [1]. *Seja R um anel (associativo) no qual se $x+x=0$ ou $x+x+x=0$ segue que $x=0$. Suponha que a, b, c e $a+b+c$ sejam idempotentes em R. É verdade que $ab=0$?*

Esse problema aparece naturalmente como extensão do mesmo problema para dois idempotentes cuja soma é também idempotente. Mais precisamente : *Seja R um anel (associativo) no qual se $x+x=0$ segue que $x=0$. Suponha que a, b e $a+b$ sejam idempotentes em R. É verdade que $ab=0$?*

A resposta neste caso é afirmativa, pois $(a+b)^2 = a+b \Rightarrow a^2+ab+ba+b^2 = a+b \Rightarrow ab = -ba$. Por outro lado, $ab = ab^2 = (ab)b = (-ba)b = -b(ab) = -b(-ba) = b^2a = ba$. Logo $ab + ab = 0$ e, portanto, $ab = 0$. No entanto, o problema anterior, com três idempotentes, tem resposta negativa. É objetivo deste primeiro capítulo apresentar uma justificativa para essa afirmação.

Podemos abordar nosso problema investigando o anel R definido por geradores a, b, c

e relações

$$
\begin{aligned}
a^2 &= a && (1.1)\\
b^2 &= b && (1.2)\\
c^2 &= c && (1.3)\\
(a+b+c)^2 &= a+b+c.
\end{aligned}
$$

O comportamento dos elementos de um quociente de um anel livre é, em geral, de difícil controle – as classes de equivalência podem, a princípio, não ter uma descrição canônica simples. Mas no caso do anel R definido acima, conseguiremos apresentar uma forma canônica de representar seus elementos, isto é, apresentar um sistema de representantes para as classes de equivalência de R.

Desenvolvendo a quarta equação, obtemos :

$$a+b+c=(a+b+c)^2=a^2+b^2+c^2+ab+ba+ac+ca+bc+cb.$$

Portanto, na presença de (1.1), (1.2) e (1.3), essa equação é equivalente a

$$ba=-ab-bc-cb-ac-ca, \tag{1.4}$$

e pode ser substituída por (1.4).

Para descrever a manipulação dos elementos de R em busca de uma forma canônica de representá-los, algumas definições serão introduzidas. Um monômio arbitrário x será dito *redutível* (segundo (1.1)–(1.4)) se contiver alguma das seqüências de letras que aparecem do lado esquerdo das identidades do sistema de equações (1.1)–(1.4). Neste caso, aplicar uma redução (associada a uma dessas identidades) a x (ou dizer que x sofre uma redução) significará substituir em x a seqüência que aparece do lado esquerdo da identidade em questão pela combinação linear de monômios que aparece do lado direito. Por exemplo, tomando $x=bba$, ao aplicar a redução associada a (1.4) a x, obtemos $x=b(-ab-bc-cb-ac-ca)=-bab-b^2c-bcb-bac-bca$. Um monômio é dito *irredutível* se não for redutível. Expressões derivadas dessas terão sentido óbvio no contexto.

No caso do anel R, existem monômios *ambíguos*, isto é, seqüências de letras que podem sofrer dois tipos diferentes de redução. São os monômios que contêm as seqüências

$$aaa,\ bbb,\ ccc;\ baa,\ bba.$$

As três primeiras são *resolúveis*, ou seja, ambas as reduções fornecem a mesma palavra, pois, por exemplo, $(aa)a = aa = a$ e $a(aa) = aa = a$. Efetuando-se as duas reduções na penúltima seqüência obtemos, por um lado,

$$baa = b(aa) = ba, \text{ usando } (1.1)$$

e, por outro lado, usando (1.4),

$$\begin{aligned} baa = (ba)a &= (-ab - bc - cb - ac - ca)a \\ &= -aba - bca - cba - aca - caa. \end{aligned}$$

Realizando-se, agora, as reduções associadas a (1.4) em aba e cba e (1.1) em caa, temos

$$\begin{aligned} baa &= -a(-ab - bc - cb - ac - ca) - bca - c(-ab - bc - cb - ac - ca) - aca - ca \\ &= ab + abc + acb + ac - bca + cab + cbc + cb + cac. \end{aligned}$$

A última igualdade é obtida por intermédio de (1.1) e (1.3). Desta maneira, igualando-se as duas formas possíveis para baa, obtemos a seguinte equação:

$$ba = ab + abc + acb + ac - bca + cab + cbc + cb + cac.$$

Por (1.4), isolando-se um termo arbitrário, temos

$$bca = abc + acb + cab + cac + cbc + 2ab + 2ac + 2cb + bc + ca. \tag{1.5}$$

Através de um processo totalmente análogo, podemos obter uma equação derivada das duas reduções possíveis de bba, que é a mesma obtida de baa, *viz.*, (1.5).

Se adicionarmos (1.5) ao nosso conjunto de relações, baa e bba reduzem-se a uma mesma expressão. Entretanto, ao adicionarmos (1.5), criamos duas novas ambigüidades : $bbca$ e $bcaa$.

Comecemos por estudar $bbca$. Por um lado, temos

$$bbca = (bb)ca = bca.$$

Por outro lado,

$$\begin{aligned} bbca &= b(bca) \\ &= b(abc + acb + cab + cac + cbc + 2ab + 2cb + bc + ca), \text{ por } 1.5 \\ &= babc + bacb + bcab + bcac + bcbc + 2bab + 2bcb + bbc + bca. \end{aligned}$$

O lado direito da identidade acima é combinação linear de monômios que ou admitem um único tipo de redução associada a uma das identidades (1.1)–(1.5) (que é o caso de $babc$, $bacb$, bab, bac, $bcab$, $bcac$, bca e bbc) ou são irredutíveis, isto é, não contêm seqüências que apareçam do lado esquerdo das identidades (1.1)–(1.5), neste caso, apenas bcb. Realizadas as reduções associadas a (1.4) em $babc$, $bacb$, bab e bac, (1.5) em $bcab$, $bcac$ e bca, e (1.2) em bbc, obtemos a equação

$$bbca = abc + acb + cab + cac + cbc + 2ab + 2ac + 2cb + bc + ca,$$

que, por (1.5), é igual a bca. Logo, $bbca$ era apenas aparentemente uma ambigüidade, uma vez que realizadas as duas possíveis reduções em $bbca$, obtemos um mesmo elemento.

Uma análise semelhante de $bcaa$ fornece-nos o mesmo resultado. Ou seja, $bcaa = bca$, quaisquer que sejam as reduções associadas a (1.1)–(1.5) realizadas em $bcaa$.

Como não há mais ambigüidades nos monômios de R, não é necessário adicionarmos novas relações ao nosso sistema.

Examinando as equações (1.1)–(1.5), notamos que se um monômio x não contiver nenhuma repetição sucessiva de uma mesma letra (que é o caso dos monômios que aparecem no lado esquerdo das identidades (1.1)–(1.3)), nem ocorrências da letra b à esquerda da letra a (o que acontece nos monômios que aparecem no lado esquerdo de (1.4) e (1.5)), então x será irredutível. Essas condições são também necessárias para a descrição dos monômios irredutíveis. De fato, se um monômio x é irredutível, então x não contém repetições sucessivas de uma mesma letra (senão seria redutível por (1.1), (1.2) ou (1.3)). Se, por outro lado, x contém alguma ocorrência de b à esquerda de a, então podemos garantir que x é redutível. Demonstraremos esse fato por indução sobre o comprimento da subpalavra de x compreendida entre um b que ocorre à esquerda de um a em x. Suponha que $x = YbZaW$, onde Y, Z e W são monômios, que eventualmente possam ser também o monômio vazio. Dado um monômio T, denotemos por $cpt(T)$ o comprimento de T, isto é, o números de letras que aparecem em T. Se $cpt(Z) = 0$, então $x = YbaW$, e portanto x é redutível. Se $cpt(Z) = 1$, então, $x = YbaaW$ ou $x = YbbaW$ ou $x = YbcaW$ e, novamente, x é redutível. Se $cpt(Z) > 1$, suponhamos, por hipótese de indução, que todo monômio $Y'bZ'aW'$ é redutível se $cpt(Z') < cpt(Z)$ e provemos que x é redutível. Como $cpt(Z) \geq 2$, podemos escrever $Z = z_1 z_2 Z'$, onde z_1 e z_2 são letras (a, b ou c) e $cpt(Z') = cpt(Z) - 2 < cpt(Z)$ (estou novamente admitindo que Z' possa ser o monômio

vazio). Analisemos todas as possibilidades para z_1 e z_2:

- se $z_1 = a$, então $x = Ybaz_2Z'aW$, portanto redutível, por (1.4),
- se $z_1 = b$, então $x = Ybbz_2Z'aW$, portanto redutível, por (1.2),
- se $z_1 = c$ e $z_2 = a$, então $x = YbcaZ'aW$, portanto redutível, por (1.5),
- se $z_1 = c$ e $z_2 = b$, então $x = YbcbZ'aW$, portanto redutível, por hipótese de indução,
- se $z_1 = c$ e $z_2 = c$, então $x = YbccZ'aW$, portanto redutível, por (1.3).

Logo, os monômios irredutíveis são exatamente aqueles nos quais não há repetição sucessiva de uma mesma letra, e seqüências com b à esquerda de a nunca ocorrem.

O processo de redução sempre termina, pois em (1.1)–(1.5) ocorre que o lado direito da identidade é combinação linear (inteira) de termos (A) de comprimento menor que o do lado esquerdo, ou (B) de mesmo comprimento que o do lado esquerdo que têm (i) menos ocorrências de b à esquerda de a e (ii) número total de ocorrências de b (resp. a) menor ou igual ao número total de ocorrências de b (resp. a) no termo do lado esquerdo.

Assim, aplicando-se as reduções (1.1)–(1.5) a um monômio qualquer, o novo elemento obtido terá as mesmas características (A) e (B) quando comparado ao monômio original.
OBS.: (B)(ii) faz-se necessário para garantirmos que o passo seguinte de redução não produzirá termos com maior ou igual número de ocorrências de b à esquerda de a. Por exemplo, se em (1.5) tivéssemos um termo aca, a redução de $bcbca$ teria um termo $bcaca$, que tem o mesmo número de ocorrências de b à esquerda de a (a saber, 2) que $bcbca$.

Logo o processo de redução de uma palavra arbitrária sempre termina em uma combinação linear (inteira) de monômios irredutíveis, e essa combinação linear é **única**, pois não há ambigüidades no sistema de reduções.

Conclui-se que o conjunto de todos os monômios irredutíveis forma uma base para R como $\mathbb{Z}$-módulo. Assim, R é um $\mathbb{Z}$-módulo livre e, portanto, é livre de torção; em particular, $2x \neq 0$ e $3x \neq 0$ se $x \neq 0$. Mas $ab \neq 0$, pois ab é um elemento irredutível e, portanto, um elemento da base de R sobre $\mathbb{Z}$.

Logo a resposta para o problema apresentado no início do capítulo é negativa.

No artigo [14], o autor apresenta uma solução alternativa para esse mesmo problema, mas que, por não envolver as idéias presentes no Capítulo 2, não será descrita aqui.

Capítulo 2

Sistemas de Redução

Neste capítulo, a fim de demonstrar um teorema motivado pelo exemplo ilustrado no capítulo anterior, introduziremos a notação a ser utilizada e uma série de definições necessárias para a formalização das idéias centrais desta dissertação, que giram em torno do conceito de redução de polinômios.

2.1 O Lema do Diamante

Seja k um anel associativo, comutativo e com unidade, e seja X um conjunto não vazio arbitrário. Chamaremos os elementos de X de *letras* e as seqüências finitas de elementos de X de *palavras* ou *monômios*. Denotaremos por $\langle X \rangle$ o semigrupo livre com unidade gerado por X (ou o monóide livre gerado por X), que é constituído pelas palavras cujas letras estão em X, isto é, $\langle X \rangle = \{A_1 \dots A_n : A_i \in X, n \in \mathbb{N}\}$, munido de uma operação binária associativa dada pela justaposição de palavras, sendo o elemento neutro a palavra vazia. Seja, agora, $k\langle X \rangle$ a k-álgebra associativa livre gerada por X:

$$k\langle X \rangle = \left\{ \sum_{W \in \langle X \rangle} \lambda_W W : W \in \langle X \rangle \right\},$$

onde as famílias $(\lambda_W)_{W \in \langle X \rangle}$ são quase nulas, isto é, existe apenas um número finito de λ_W diferentes de zero. Dois elementos a e b de $k\langle X \rangle$ são iguais se os coeficientes dos

monômios correspondentes forem iguais, isto é, se $a = \sum_{W\in\langle X\rangle} \lambda_W W$ e $b = \sum_{W\in\langle X\rangle} \mu_W W$, então $a = b$ se e somente se $(\lambda_W)_{W\in\langle X\rangle} = (\mu_W)_{W\in\langle X\rangle}$. O conjunto $k\langle X\rangle$ é um grupo aditivo abeliano, definindo-se a soma componente a componente, e também um k-módulo via

$$\begin{array}{ccc} k \times k\langle X\rangle & \longrightarrow & k\langle X\rangle \\ (\mu, \sum\limits_{W\in\langle X\rangle} \lambda_W W) & \longmapsto & \sum\limits_{W\in\langle X\rangle} (\mu\lambda_W)W. \end{array}$$

O k-módulo $k\langle X\rangle$ munido da aplicação bilinear

$$\begin{array}{ccc} k\langle X\rangle \times k\langle X\rangle & \longrightarrow & k\langle X\rangle \\ (\sum\limits_{W\in\langle X\rangle} \lambda_W W, \sum\limits_{W'\in\langle X\rangle} \mu_{W'} W') & \longmapsto & \sum\limits_{Z\in\langle X\rangle} \eta_Z Z, \end{array}$$

onde $\eta_Z = \sum\limits_{WW'=Z} \lambda_W \mu_{W'}$, é uma k-álgebra associativa que, como k-módulo, é livre de base $\langle X\rangle$. É comum denominar os elementos de $k\langle X\rangle$ de *polinômios* nas variáveis X.

OBS. 1: Os elementos de $k\langle X\rangle$ podem também ser denotados por somas finitas onde aparecem apenas aqueles termos com coeficientes não nulos. Isto é, dado $a = \sum_{W\in\langle X\rangle} \lambda_W W \in k\langle X\rangle$, a família $(\lambda_W)_{W\in\langle X\rangle}$ é quase nula. Suponha que $|\{W \in \langle X\rangle : \lambda_W \neq 0\}| = n > 0$. (No caso em que $n = 0$, denota-se, trivialmente, $a = 0$.) Se enumerarmos os elementos do conjunto acima, $W_1, W_2, \ldots, W_n$, podemos escrever $a = \sum_{W\in\langle X\rangle} \lambda_W W = \sum_{i=1}^n \lambda_{W_i} W_i$. Para simplificar a notação, escrevendo-se λ_i ao invés de λ_{W_i}, tem-se $a = \sum_{i=1}^n \lambda_i W_i$. Tomaremos a liberdade de utilizar ambas as notações, pois há contextos onde uma é mais conveniente que a outra e vice-versa.

OBS. 2: A k-álgebra associativa livre gerada por X, $k\langle X\rangle$, é mais comumente definida pela seguinte propriedade universal. Dado um anel k associativo, comutativo e com unidade e um conjunto X, dizemos que uma k-álgebra associativa F é uma *k-álgebra associativa livre gerada por X*, ou *sobre X*, se existir uma função $i : X \longrightarrow F$, tal que qualquer função $\theta : X \longrightarrow B$ de X em uma outra k-álgebra associativa B possa ser unicamente fatorada por i, isto é, dada $\theta : X \longrightarrow B$, existe um único homomorfismo (de k-álgebras associativas) $\theta' : F \longrightarrow B$ tal que o diagrama abaixo comuta.

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "\theta"'] & F \arrow[d, "\theta'"] \\ & B \end{tikzcd}$$

Pela propriedade universal de que goza, prova-se facilmente que, se existir, F é única a menos de isomorfismo. A k-álgebra associativa $k\langle X\rangle$ definida anteriormente verifica a propriedade universal acima, como é fácil de se ver, e, portanto, é uma k-álgebra associativa livre gerada por X. Pela unicidade a menos de isomorfismo, dizemos que $k\langle X\rangle$ é *a* k-álgebra associativa livre gerada por X. (Uma descrição mais detalhada de $k\langle X\rangle$ e suas propriedades encontra-se em [7, pp. 59–62].)

Seja S um conjunto (não vazio) de pares da forma $\sigma = (W_\sigma, f_\sigma)$, onde $W_\sigma \in \langle X\rangle$ e $f_\sigma \in k\langle X\rangle$, ou seja, S é apenas um subconjunto de $\langle X\rangle \times k\langle X\rangle$. Dados $\sigma \in S$ e A, $B \in \langle X\rangle$, seja $r_{A\sigma B} : k\langle X\rangle \longrightarrow k\langle X\rangle$ o endomorfismo de k-módulos definido sobre os monômios da base $\langle X\rangle$ por

$$r_{A\sigma B}(V) = \begin{cases} V & \text{se } V \neq AW_\sigma B \\ Af_\sigma B & \text{se } V = AW_\sigma B. \end{cases}$$

O endomorfismo $r_{A\sigma B}$, então, é a identidade sobre todos os monômios de $\langle X\rangle$ com excessão de $AW_\sigma B$, o qual é transformado em $Af_\sigma B$ (ou *reduzido* a $Af_\sigma B$).

O conjunto S é chamado um *sistema de redução* e os operadores lineares $r_{A\sigma B}$: $k\langle X\rangle \longrightarrow k\langle X\rangle$ definidos acima são chamados *reduções* (associadas a S). Dizemos que uma redução $r_{A\sigma B}$ *atua trivialmente* em um polinômio $a \in k\langle X\rangle$ se o coeficiente do monômio $AW_\sigma B$ em a é zero, ou, em termos menos precisos, se a "não envolve" o monômio $AW_\sigma B$; caso contrário, dizemos que $r_{A\sigma B}$ *atua não trivialmente* em a. Um elemento $a \in k\langle X\rangle$ é dito *irredutível* (segundo S) se toda redução atuar trivialmente em a, isto é, se a não envolver nenhum monômio $AW_\sigma B$, com A, $B \in \langle X\rangle$ e $\sigma \in S$. Fixado um sistema de redução S, o conjunto formado por todos os elementos irredutíveis segundo S forma um k-submódulo de $k\langle X\rangle$, que é denotado por $k\langle X\rangle_{irr}$. A prova desse fato é imediata e não será feita aqui.

Neste capítulo, S será um sistema de redução arbitrário porém fixado e todos os conceitos introduzidos serão relativos a S.

Indicaremos uma seqüência finita de reduções por $(r_1, \ldots, r_n)$, ou equivalentemente por $(r_i)_{i=1}^n$, e uma seqüência infinita de reduções será indicada por $(r_1, r_2, \ldots)$, ou $(r_i)_{i\in\mathbb{N}}$. Em ambos os casos r_i será uma abreviação para $r_{A_i\sigma_i B_i}$. Dado $a \in k\langle X\rangle$, uma seqüência finita de reduções $(r_1, \ldots, r_n)$ é dita *final* em a se $r_n \ldots r_1(a) \in k\langle X\rangle_{irr}$.

Em princípio, um elemento $a \in k\langle X\rangle$ pode sofrer a ação de reduções sucessivas

indefinidamente de maneira a modificá-lo a cada passo. Esse elemento caracteriza-se pela seguinte propriedade: existe uma seqüência infinita de reduções $(r_1, r_2, \ldots)$ tal que r_i atua não trivialmente em $r_{i-1} \ldots r_1(a)$, para todo $i \in \mathbb{N}$. A infinitude desse processo de redução confere a a a característica de ser um elemento de difícil controle dentre todos os elementos de $k\langle X\rangle$. Isso motiva a definição seguinte. Um elemento $a \in k\langle X\rangle$ é dito de *redução finita* se, para toda seqüência infinita de reduções $(r_1, r_2, \ldots)$, existir $i_0 \in \mathbb{N}$, que depende de a e da seqüência de reduções, tal que r_i atue trivialmente em $r_{i-1} \ldots r_1(a)$ para todo $i > i_0$. É claro que todo elemento irredutível é de redução finita. Segue da definição que o conjunto dos elementos de redução finita em $k\langle X\rangle$ forma um k-submódulo de $k\langle X\rangle$. Um elemento $a \in k\langle X\rangle$ que não é de redução finita tem a propriedade de, dada uma seqüência $(r_i)_{i\in\mathbb{N}}$, para cada $n \in \mathbb{N}$, existir $i = i(n) > n$ tal que r_i atue não trivialmente em $r_{i-1} \ldots r_1(a)$. Podemos, então construir a subseqüência $(r_{i_j})_{j\in\mathbb{N}}$ de $(r_i)_{i\in\mathbb{N}}$ formada apenas por aqueles r_{i_j} que atuam não trivialmente em $r_{i_j-1} \ldots r_1(a)$. E, assim, temos que existe uma seqüência infinita de reduções, $(r_{i_j})_{j\in\mathbb{N}}$, tal que r_{i_j} atua não trivialmente em $r_{i_{j-1}} \ldots r_{i_1}(a)$, para todo $j \in \mathbb{N}$. Logo, podemos caracterizar a por esta propriedade, uma vez que ela é obviamente equivalente à negação da afirmação de a ser de redução finita.

Proposição 2.1 *Se $a \in k\langle X\rangle$ é de redução finita, então existe uma seqüência final em a.*

Prova Suponhamos que não exista seqüência final em a. Em particular, a não é irredutível, senão, toda seqüência finita de reduções seria final em a. Vamos definir recursivamente uma seqüência infinita de reduções. Como a não é irredutível, existe uma redução r_1 que atua não trivialmente em a. Tendo definido a redução r_n para $n \geq 1$, vamos definir r_{n+1}. Sabemos que $r_n \ldots r_1(a)$ não é irredutível, pois senão $(r_i)_{i=1}^n$ seria final em a. Logo, existe redução r que atua não trivialmente em $r_n \ldots r_1(a)$. Tomamos $r_{n+1} = r$. Dessa maneira, construimos uma seqüência infinita de reduções $(r_i)_{i\in\mathbb{N}}$ tal que r_i atua não trivialmente em $r_{i-1} \ldots r_1(a)$ para todo $i \in \mathbb{N}$. Isso é uma contradição com a hipótese de a ser de redução finita. Logo, existe pelo menos uma seqüência final em a. ■

Denominamos um elemento $a \in k\langle X\rangle$ um elemento de *redução única* se a for de redução finita e se dadas duas seqüências finais arbitrárias em a, $(r_i)_{i=1}^n$ e $(s_j)_{j=1}^m$, segue $r_n \ldots r_1(a) = s_m \ldots s_1(a)$, ou seja, se a imagem de a por qualquer composição de reduções de uma seqüência final em a for sempre a mesma. Esse valor comum será denotado por $r_S(a)$.

Lema 2.1 *Sejam $a \in k\langle X\rangle$ e $(r_i)_{i=1}^n$ uma seqüência finita qualquer de reduções. Denotemos por r a composição dessas reduções, isto é, $r = r_n \dots r_1$. Valem as seguintes implicações:*

(i) se a é de redução finita, então $r(a)$ é de redução finita;

(ii) se a é de redução única, então $r(a)$ é de redução única e $r_S(r(a)) = r_S(a)$.

Prova (i) Seja $(s_i)_{i\in\mathbb{N}}$ uma seqüência infinita qualquer de reduções. Considere a seqüência $(t_i)_{i\in\mathbb{N}}$ dada por $t_i = r_i$, para $i = 1, \dots, n$ e $t_{n+j} = s_j$, para $j \in \mathbb{N}$. Como a é de redução finita, existe $k_0 \in \mathbb{N}$, que posso tomar maior que n, tal que t_k atua trivialmente em $t_{k-1} \dots t_1(a)$ para todo $k > k_0$, isto é, t_{n+j} atua trivialmente em $t_{n+j-1} \dots t_{n+1} t_n \dots t_1(a)$ para todo $j > k_0 - n$, ou seja, s_j atua trivialmente em $s_{j-1} \dots s_1(r(a))$ para todo $j > k_0 - n$. Portanto, $r(a)$ é de redução finita. (ii) Pelo item anterior, $r(a)$ é de redução finita. Seja, agora, $(s_i)_{i=1}^m$ uma seqüência final arbitrária em $r(a)$. Então, $s_m \dots s_1(r(a)) = s_m \dots s_1 r_n \dots r_1(a) \in k\langle X\rangle_{irr}$, isto é, $(r_1, \dots, r_n, s_1, \dots, s_m)$ é final em a. Como a é de redução única, $s_m \dots s_1(r(a)) = r_S(a)$. Logo, $r(a)$ é de redução única e vale a igualdade $r_S(r(a)) = r_S(a)$. ■

Os dois lemas seguintes têm como finalidade lidar com passagens mais técnicas que serão encontradas na demonstração do Teorema 2.1 que será enunciado mais adiante.

Lema 2.2 *O conjunto dos elementos de redução única de $k\langle X\rangle$ é um k-submódulo e r_S é uma aplicação k-linear desse submódulo em $k\langle X\rangle_{irr}$.*

Prova Sejam $a, b \in k\langle X\rangle$ dois elementos de redução única e seja $\alpha \in k$. Sabemos que $\alpha a + b$ é de redução finita. Seja $(r_i)_{i=1}^n$ uma seqüência final qualquer em $\alpha a + b$. Denotemos $r = r_n \dots r_1$. Pelo Lema 2.1(ii), $r(a)$ é de redução única e, portanto, existe uma composição de reduções r' tal que $r'r(a) = r_S(a)$. Analogamente, existe uma composição de reduções r'' tal que $r''r'r(b) = r_S(b)$. Como $r(\alpha a + b)$ é irredutível, temos $r(\alpha a + b) = r''r'r(\alpha a + b) = \alpha r''r'r(a) + r''r'r(b) = \alpha r_S(a) + r_S(b)$. Portanto $\alpha a + b$ é de redução única e $r_S(\alpha a + b) = \alpha r_S(a) + r_S(b)$. ■

O Lema 2.3 a ser enunciado abaixo é uma generalização do resultado apresentado no item (ii) do Lema 2.1.

Lema 2.3 *Suponha que $a, b, c \in k\langle X\rangle$ sejam polinômios não nulos tais que, para todos os monômios A, B, C ocorrendo com coeficientes não nulos em a, b, c, respectivamente, o produto ABC seja de redução única. (Em particular, isso implica que abc é de redução única.) Seja r uma composição qualquer de reduções. Então $ar(b)c$ é de redução única e $r_S(ar(b)c) = r_S(abc)$.*

Prova Comecemos por estudar o caso em que a, b, c são monômios A, B, C e r é uma redução $r_{D\sigma E}$. Nesse caso, temos $Ar_{D\sigma E}(B)C = r_{AD\sigma EC}(ABC)$. Se b for um elemento arbitrário de $k\langle X\rangle$, $b = \sum_{j=1}^{m} \mu_j B_j$, vale a igualdade $Ar_{D\sigma E}(b)C = r_{AD\sigma EC}(AbC)$, pois $Ar_{D\sigma E}(b)C = Ar_{D\sigma E}(\sum_{j=1}^{m} \mu_j B_j) = \sum_{j=1}^{m} \mu_j (Ar_{D\sigma E}(B_j)C) = \sum_{j=1}^{m} \mu_j r_{AD\sigma EC}(AB_jC) = r_{AD\sigma EC}(AbC)$. Seja, agora, $(r_i)_{i=1}^{p}$ uma seqüência qualquer de reduções, onde r_i abrevia $r_{D_i\sigma_i E_i}$. Considere a seqüência $(r'_i)_{i=1}^{p}$ dada por $r'_i = r_{AD_i\sigma_i E_i C}$. Então, se A, B, C são monômios quaisquer, $Ar_p \ldots r_1(B)C = r'_p(Ar_{p-1} \ldots r_1(B)C) = r'_p r'_{p-1}(Ar_{p-2} \ldots r_1(B)C) = \cdots = r'_p \ldots r'_1(ABC)$.

Denotando-se $r = r_p \ldots r_1$ e $r' = r'_p \ldots r'_1$, podemos concluir que se ABC é de redução única, então, pelo Lema 2.1(ii), $Ar(B)C = r'(ABC)$ é de redução única e, além disso,

$$r_S(Ar(B)C) = r_S(r'(ABC)) = r_S(ABC). \tag{2.1}$$

Nas hipótese do enunciado deste Lema, se indicarmos $a = \sum_{i=1}^{l} \lambda_i A_i$, $b = \sum_{j=1}^{m} \mu_j B_j$, $c = \sum_{k=1}^{n} \eta_k C_k$, temos

$$ar(b)c = \sum_{i,j,k} \lambda_i \mu_j \eta_k (A_i r(B_j) C_k).$$

Como, por hipótese, $A_i B_j C_k$ é de redução única para todo $i = 1, \ldots, l$, $j = 1, \ldots, m$, $k = 1, \ldots, n$, pelo que foi visto acima, podemos afirmar que $A_i r(B_j) C_k$ é de redução única. Agora, pela primeira afirmação do Lema 2.2, temos que $ar(b)c$ é também de redução única.

Vimos que o fato de $A_i B_j C_k$ ser de redução única implica também $r_S(A_i r(B_j) C_k) = r_S(A_i B_j C_k)$, como mostra a equação (2.1). A segunda afirmação do Lema 2.2 permite-nos escrever

$$r_S(ar(b)c) = \sum_{i,j,k} \lambda_i \mu_j \eta_k r_S(A_i r(B_j) C_k),$$

pois r_S é k-linear. Logo,

$$r_S(ar(b)c) \;=\; \sum_{i,j,k} \lambda_i \mu_j \eta_k r_S(A_i r(B_j) C_k)$$

$$
\begin{aligned}
&= \sum_{i,j,k} \lambda_i \mu_j \eta_k r_S(A_i B_j C_k) \\
&= r_S(abc).
\end{aligned}
$$

Isso demonstra o lema. ■

Como vimos no exemplo do capítulo anterior, um monômio pode sofrer mais de uma redução, ou seja, dado $A \in \langle X \rangle$, pode acontecer de existirem $B, C, D, E \in \langle X \rangle$ e $\sigma, \tau \in S$ tais que $r_{B\sigma C}$ e $r_{D\tau E}$ sejam distintas e atuem não trivialmente em A. Na solução do problema proposto no primeiro capítulo, denominamos esse fato de "ambigüidade". O mesmo nome será utilizado neste novo contexto. Assim, dizer que A é uma ambigüidade é dizer que ambos os monômios W_σ e W_τ ocorrem em A. Existem três possíveis posições relativas de W_σ e W_τ em A. Se W_σ e W_τ são disjuntos, posso supor, por exemplo, que W_σ é anterior a W_τ em A e, então, $A = BW_\sigma A' W_\tau E$ (neste caso, temos $C = A' W_\tau E$ e $D = BW_\sigma A'$). Se W_σ e W_τ se interceptam, mas nenhum está contido no outro, supondo W_σ anterior a W_τ, então $A = BA'B'C'E$, onde $A'B' = W_\sigma$ e $B'C' = W_\tau$ (neste caso, $C = C'E$ e $D = BA'$). Finalmente, se, por exemplo, W_σ está contido em W_τ, temos $A = DA'W_\sigma B'E$, onde $A'W_\sigma B' = W_\tau$ (e ainda, $B = DA'$ e $C = B'E$). Essa análise motiva as definições seguintes.

Diremos que uma 5-upla (σ, τ, A, B, C), com $\sigma, \tau \in S$, $A, B, C \in \langle X \rangle$ e $B \neq 1$, tal que $W_\sigma = AB$ e $W_\tau = BC$ é uma *ambigüidade de superposição* de S. Neste caso, temos $r_{1\sigma C}(ABC) = f_\sigma C$ e $r_{A\tau 1}(ABC) = Af_\tau$, onde 1 denota o elemento neutro de $\langle X \rangle$. Uma ambigüidade de superposição (σ, τ, A, B, C) será dita *resolível* se existirem composições de reduções r e r' tais que $r(f_\sigma C) = r'(Af_\tau)$.

Diremos que uma 5-upla (σ, τ, A, B, C), com $\sigma, \tau \in S, \sigma \neq \tau$ e $A, B, C \in \langle X \rangle$, tal que $W_\sigma = B$ e $W_\tau = ABC$ é uma *ambigüidade de inclusão* de S. Neste caso, temos $r_{A\sigma C}(ABC) = Af_\sigma C$ e $r_{1\tau 1}(ABC) = f_\tau$. Uma ambigüidade de inclusão (σ, τ, A, B, C) será dita *resolível* se existirem composições de reduções r e r' tais que $r(Af_\sigma C) = r'(f_\tau)$.

Não vamos fornecer uma definição rigorosa para as ambigüidades do tipo em que W_σ e W_τ são disjuntos por motivos que se tornarão evidentes no decorrer do capítulo. Deste ponto em diante, o termo *ambigüidade* vai sempre referir-se aos conceitos definidos acima de modo preciso.

Uma *ordem parcial de semigrupo* em $\langle X\rangle$ é uma ordem parcial $\leq$ em $\langle X\rangle$ com a seguinte propriedade: se $B, B' \in \langle X\rangle$ são tais que $B < B'$, então $ABC < AB'C$, para todos $A, C \in \langle X\rangle$.

Seja, agora, S um sistema de redução fixado. O semigrupo $\langle X\rangle$ pode, em princípio, ser ordenado de muitas maneiras distintas; no entanto, queremos trabalhar com ordens parciais de semigrupo em $\langle X\rangle$ que estejam relacionadas com S.

Uma ordem parcial de semigrupo em $\langle X\rangle$, $\leq$, e o sistema de redução S serão ditos *compatíveis* se, para todo $\sigma = (W_\sigma, f_\sigma) \in S$, f_σ for zero ou uma combinação linear não nula de monômios $< W_\sigma$.

Pode-se associar a S o ideal bilateral de $k\langle X\rangle$ gerado pelos elementos $W_\sigma - f_\sigma$, onde $\sigma = (W_\sigma, f_\sigma)$ percorre o conjunto S. Esse ideal será denotado por $I(S)$, ou, quando o sistema de redução em questão estiver claro, simplesmente por I.

Seja $\leq$ uma ordem parcial de semigrupo em $\langle X\rangle$. Se $\leq$ e S são compatíveis e se M é um elemento arbitrário de $\langle X\rangle$, denotaremos por I_M o submódulo de $k\langle X\rangle$ gerado por todos os elementos $B(W_\sigma - f_\sigma)C$, onde B e C são monômios de $\langle X\rangle$ tais que $BW_\sigma C < M$ e $\sigma = (W_\sigma, f_\sigma) \in S$.

Fixada uma ordem parcial de semigrupo em $\langle X\rangle$, $\leq$, de modo que $\leq$ e S sejam compatíveis, dizemos que uma ambigüidade de superposição (σ, τ, A, B, C) é *resolível com respeito a* $\leq$ se $f_\sigma C - Af_\tau \in I_{ABC}$. Analogamente, dizemos que uma ambigüidade de inclusão (σ, τ, A, B, C) é *resolível com respeito a* $\leq$ se $Af_\sigma C - f_\tau \in I_{ABC}$.

Seja $\leq$ uma ordem parcial de semigrupo em $\langle X\rangle$ fixada, de modo que $\leq$ e S sejam compatíveis. Vejamos como se comportam um elemento $a \in k\langle X\rangle$ e sua imagem por uma composição de reduções em relação ao ideal I e aos submódulos I_A.

Lema 2.4 *Sejam $a \in k\langle X\rangle$ um polinômio arbitrário e $r = r_n \ldots r_1$ uma composição qualquer de reduções. Então $a - r(a) \in I$.*

Prova Suponha que $a = \sum_{A\in\langle X\rangle} \lambda_A A$. Demonstraremos inicialmente o resultado quando r é uma redução $r_{D\sigma E}$. Temos

$$\begin{aligned} r_{D\sigma E}(a) &= r_{D\sigma E}(\sum_{A\in\langle X\rangle} \lambda_A A) \\ &= \sum_{A\in\langle X\rangle} \lambda_A r_{D\sigma E}(A) \\ &= \sum_{A\neq DW_\sigma E} \lambda_A A + \lambda_{DW_\sigma E} D f_\sigma E. \end{aligned}$$

Assim,

$$a - r_{D\sigma E}(a) = \lambda_{D\sigma E} D(W_\sigma - f_\sigma)E.$$

Logo, $a - r_{D\sigma E}(a) \in I$

Agora, se $r_1, \ldots, r_n$ é uma seqüência de reduções, pelo que foi feito acima, sabemos que $r_i \ldots r_1(a) - r_{i+1} r_i \ldots r_1(a) \in I$, para todo $i = 1, \ldots, n-1$. Logo, $a - r(a) = a - r_n \ldots r_1(a) = (a - r_1(a)) + (r_1(a) - r_2 r_1(a)) + \cdots + (r_{n-1} \ldots r_1(a) - r_n r_{n-1} \ldots r_1(a)) \in I$, pois I é um ideal. ■

Observe que, em vista do Lema 2.4 e do fato de que $W_\sigma - f_\sigma = W_\sigma - r_{1\sigma 1}(W_\sigma)$, para todo $\sigma \in S$, pode-se afirmar que I nada mais é do que o ideal bilateral de $k\langle X\rangle$ gerado pelos elementos da forma $a - r(a)$, onde a percorre $k\langle X\rangle$ e r percorre o conjunto de todas as reduções determinadas por S.

Lema 2.5 *Sejam $r_{D\sigma E}$ uma redução qualquer, $C \in \langle X\rangle$ um monômio arbitrário e $a \in k\langle X\rangle$ um elemento que é combinação linear de monômios $< C$. Então valem:*

(i) se $r_{D\sigma E}(a) \neq 0$, então $r_{D\sigma E}(a)$ também é combinação linear de monômios $< C$;

(ii) $a - r_{D\sigma E}(a) \in I_C$.

Prova Se $a = \sum_{A \in \langle X\rangle} \lambda_A A$, temos

$$r_{D\sigma E}(a) = \sum_{A \neq DW_\sigma E} \lambda_A A + \lambda_{DW_\sigma E} D f_\sigma E.$$

(i) Se $\lambda_{DW_\sigma E} = 0$, então $r_{D\sigma E}(a) = a$ e, portanto, é combinação linear de monômios $< C$. Se $f_\sigma = 0$, $r_{D\sigma E}(a)$ também é combinação linear de monômios $< C$. Quando $\lambda_{DW_\sigma E} \neq 0$ e $f_\sigma \neq 0$, podemos escrever $f_\sigma = \sum_{B \in \langle X\rangle} \mu_B B$, com $B < W_\sigma$ para todo B tal que $\mu_B \neq 0$ e, assim,

$$\begin{aligned} \lambda_{DW_\sigma E} D f_\sigma E &= \lambda_{DW_\sigma E} D(\sum_{B \in \langle X\rangle} \mu_B B)E \\ &= \lambda_{DW_\sigma E} \sum_{B \in \langle X\rangle} \mu_B (DBE). \end{aligned}$$

Como para $\mu_B \neq 0$ temos $B < W_\sigma$, segue que $DBE < DW_\sigma E$ se $\mu_B \neq 0$. Mas, por hipótese, $DW_\sigma E < C$. Daí segue o resultado. (ii) Pela demonstração do Lema 2.4, temos que $a - r_{D\sigma E}(a) = \lambda_{DW_\sigma E} D(W_\sigma - f_\sigma)E$. Logo, $a - r_{D\sigma E}(a) \in I_C$. ■

Corolário 2.1 *Se $r = r_n \dots r_1$ é uma composição qualquer de reduções, $C \in \langle X \rangle$ e $a \in k\langle X \rangle$ um elemento que é combinação linear de monômios $< C$, então $a - r(a) \in I_C$.*

Prova Se $r_1(a) = 0$, então $a - r(a) = a - r_1(a)$, que, pelo Lema 2.5(ii), pertence a I_C. Se $r_1(a) \neq 0$ e $r(a) = 0$, seja i_0 o menor i tal que $r_i \dots r_1(a) = 0$, se $r(a) \neq 0$, tome $i_0 = n$. Assim, para todo $i < i_0$, temos $r_i \dots r_1(a) \neq 0$. Portanto, pelo Lema 2.5(i), segue que $r_i \dots r_1(a)$ é combinação linear de monômios $< C$, para todo $i < i_0$. Pela parte (ii) do mesmo lema, segue que $r_i \dots r_1(a) - r_{i+1} r_i \dots r_1(a) \in I_C$, para $i = 1, \dots, i_0 - 1$. Logo, $a - r(a) = a - r_{i_0} \dots r_1(a) = (a - r_1(a)) + (r_1(a) - r_2 r_1(a)) + \dots + (r_{i_0-1} \dots r_1(a) - r_{i_0} r_{i_0-1} \dots r_1(a)) \in I_C$, pois I_C é um submódulo. ■

O Corolário 2.1 tem uma aplicação imediata de grande utilidade na verificação da resolubilidade de ambigüidades com respeito a $\leq$.

Lema 2.6 *Sejam $\leq$ uma ordem parcial de semigrupo em $\langle X \rangle$, tal que $\leq$ e S sejam compatíveis, $C \in \langle X \rangle$ e $a, b \in k\langle X \rangle$ polinômios que são combinações lineares de monômios $< C$. Se $r = r_1 \dots r_n$ e $r' = r'_1 \dots r'_m$ são composições arbitrárias de reduções, temos a seguinte equivalência:*

$$a - b \in I_C \Longleftrightarrow r(a) - r'(b) \in I_C.$$

Em particular, se (σ, τ, A, B, C) é uma ambigüidade de superposição (resp. inclusão), então ela é resolúvel com respeito a $\leq$ se e somente se $r(f_\sigma C) - r'(A f_\tau) \in I_{ABC}$ (resp. $r(A f_\sigma C) - r'(f_\tau) \in I_{ABC}$), onde r e r' indicam composições quaisquer de reduções.

Prova Em vista do Corolário 2.1, sabemos que $a - r(a) \in I_C$ e que $r'(b) - b \in I_C$. Logo $(a - b) - (r(a) - r'(b)) \in I_C$. ■

Vamos enunciar agora uma proposição que relaciona resolubilidade de ambigüidades com resolubilidade com respeito a $\leq$.

Proposição 2.2 *Dada uma ordem parcial de semigrupo $\leq$ em $\langle X \rangle$ tal que $\leq$ e S sejam compatíveis, toda ambigüidade resolúvel de S é resolúvel com respeito a $\leq$.*

Prova Seja (σ, τ, A, B, C) uma ambigüidade de superposição. Suponhamos que (σ, τ, A, B, C) seja resolúvel, então existem composições de reduções r e r' tais que $r(f_\sigma C) -$

$r'(Af_\tau) = 0$. Logo, $r(f_\sigma C) - r'(Af_\tau) \in I_{ABC}$. Pelo Lema 2.6, (σ, τ, A, B, C) é resolúvel com respeito a $\leq$. A demonstração para ambigüidades de inclusão é análoga. ■

Mais um lema trivial será enunciado com vistas a suprimir da demonstração do Teorema 2.1 uma passagem muito recorrente e de característica mais técnica.

Lema 2.7 *Sejam $\leq$ uma ordem parcial de semigrupo em $\langle X \rangle$, tal que $\leq$ e S sejam compatíveis e A um monômio qualquer de $\langle X \rangle$. Se $a \in k\langle X \rangle$ é tal que $a \in I_A$, então $LaM \in I_{LAM}$, para todo L e todo M em $\langle X \rangle$.* ■

Neste ponto faremos uma pausa no estudo das reduções de um polinômio para introduzir um resultado geral sobre conjuntos parcialmente ordenados que nos será útil mais adiante.

Dado um conjunto $\mathcal{X}$ dotado de uma ordem parcial $\preceq$, dizemos que $\preceq$ tem *condição de cadeia descendente* (c.c.d.) se, para toda cadeia descendente

$$\cdots \preceq x_m \preceq \cdots \preceq x_3 \preceq x_2 \preceq x_1,$$

com $x_i \in \mathcal{X}$ ($i \in \mathbb{N}$), existir $n \in \mathbb{N}$ tal que $x_n = x_{n+j}$, para todo $j \in \mathbb{N}$. É bem conhecido que essa condição é equivalente à existência de elemento minimal em qualquer subconjunto não-vazio de $\mathcal{X}$.

Se $\mathcal{X}$ é um conjunto parcialmente ordenado por $\preceq$ com c.c.d. (e, portanto, $\mathcal{X}$ tem elemento minimal), podemos enunciar um *princípio de indução* em $\mathcal{X}$ inspirado no princípio de indução finita do conjunto dos inteiros positivos.

Proposição 2.3 (Princípio de indução) *Suponha que uma determinada propriedade P seja satisfeita por todo elemento minimal de $\mathcal{X}$ e que, dado $d \in \mathcal{X}$ não minimal, se P é satisfeita por todo $a \in \mathcal{X}$ tal que $a \prec d$, então P é satisfeita por d. Nestas condições, P é satisfeita por todo $a \in \mathcal{X}$.*

Prova Seja $\mathcal{Y}$ o subconjunto de $\mathcal{X}$ formado por aqueles elementos que não satisfazem P. Suponha que $\mathcal{Y}$ é não-vazio. Como $\preceq$ tem c.c.d., existe d elemento minimal de $\mathcal{Y}$. Existe, também, pelo menos um elemento $a \in \mathcal{X}$ tal que $a \prec d$, pois, caso contrário, d seria minimal em $\mathcal{X}$ e, portanto, P seria satisfeita por d, ou seja, $d \notin \mathcal{Y}$, o que é absurdo.

Além disso, se $a \in \mathcal{X}$ é tal que $a \prec d$, então $a \notin \mathcal{Y}$, pois d é minimal de $\mathcal{Y}$. Logo P é satisfeita para todo $a \prec d$. Por hipótese P é satisfeita por d e, então, d não pode pertencer a $\mathcal{Y}$, o que é uma contradição. Essa contradição decorre do fato de termos suposto que $\mathcal{Y}$ era não-vazio. Logo $\mathcal{Y}$ é vazio e, assim, P é satisfeita por todo $a \in \mathcal{X}$. ■

Voltemos ao nosso estudo de reduções de polinômios.

Sejam S um sistema de redução fixado e $\leq$ uma ordem parcial de semigrupo em $\langle X \rangle$ com c.c.d. de modo que $\leq$ e S sejam compatíveis. Nessas condições, $\langle X \rangle$ tem elemento minimal. Afirmo que todo elemento minimal de $\langle X \rangle$ é de redução única. De fato, seja A um elemento minimal de $\langle X \rangle$. Se A for irredutível, A é de redução única trivialmente; senão, existe uma redução r que atua não trivialmente em A. Como $\leq$ e S são compatíveis, $r(A)$ é zero ou é uma combinação linear de monômios $< A$. Como A é minimal em $\langle X \rangle$, $r(A) = 0$. Nesse caso, A é de redução única, uma vez que 0 é irredutível.

Fixado um sistema de redução S, o lema seguinte fornece-nos condições suficientes para que todo elemento de $k\langle X \rangle$ seja de redução finita.

Lema 2.8 *Se $\leq$ é uma ordem parcial de semigrupo em $\langle X \rangle$ com c.c.d. tal que $\leq$ e S sejam compatíveis, então todo elemento de $k\langle X \rangle$ é de redução finita.*

Prova Mostraremos inicialmente, por indução, que todo elemento de $\langle X \rangle$ é de redução finita. Já vimos que os elementos minimais de $\langle X \rangle$ são de redução única; em particular, são de redução finita. Seja $D \in \langle X \rangle$ um elemento não minimal. Suponhamos que todo $A \in \langle X \rangle$ tal que $A < D$ seja de redução finita e mostremos que D é de redução finita. Seja $(r_i)_{i \in \mathbb{N}}$ uma seqüência infinita qualquer de reduções. É preciso encontrar $i_0 \in \mathbb{N}$ tal que r_i atue trivialmente em $r_{i-1} \ldots r_1(D)$, para todo $i > i_0$. Se r_i atua trivialmente em $r_{i-1} \ldots r_1(D)$, para todo $i \in \mathbb{N}$, então tomo $i_0 = 1$; senão, existe $j \in \mathbb{N}$ tal que r_j atua não trivialmente em $r_{j-1} \ldots r_1(D)$. Se esse é o caso, tomamos j_0 como o menor j com essa propriedade. Como j_0 é mímino, $r_{j_0-1} \ldots r_1(D) = D$. Se $r_{j_0} \ldots r_1(D) = r_{j_0}(D) = 0$, tomamos $i_0 = j_0$; senão, $r_{j_0} r_{j_0-1} \ldots r_1(D) = r_{j_0}(D) = \sum_{k=1}^{n} \lambda_k C_k$, com $C_k < D$ $(k = 1, \ldots, n)$, pois $\leq$ e S são compatíveis. Considere, agora, a seqüência $(s_i)_{i \in \mathbb{N}}$ dada por $s_i = r_{j_0+i}$. Como, por hipótese de indução, cada C_k $(k = 1, \ldots, n)$ é de redução finita, existem $i(k) \in \mathbb{N}$, tais que, para cada $k = 1, \ldots, n$, a redução s_i atua trivialmente em $s_{i-1} \ldots s_1(C_k)$, para todo $i > i(k)$. Seja $i' = max\{i(k) : k = 1, \ldots, n\}$. Dessa forma, s_i atua trivialmente

em $s_{i-1}\dots s_1(C_k)$, para todo $i > i'$ e todo $k = 1,\dots,n$, ou seja, r_{j_0+i} atua trivialmente em $r_{j_0+i-1}\dots r_{j_0+1}(C_k)$, para todo $i > i'$ e todo $k = 1,\dots,n$. Portanto, para todo $i > i'$, r_{j_0+i} atua trivialmente em $\sum_{k=i}^{n} \lambda_k r_{j_0+i-1}\dots r_{j_0+1}(C_k) = r_{j_0+i-1}\dots r_{j_0+1}(\sum_{k=1}^{n} \lambda_k C_k) = r_{j_0+i-1}\dots r_{j_0+1}(r_{j_0}(D)) = r_{j_0+i-1}\dots r_{j_0+1} r_{j_0}\dots r_1(D)$. Basta, portanto, tomar $i_0 = j_0 + i'$. Mostramos que todo monômio de $\langle X\rangle$ é de redução finita. Como o conjunto dos elementos de redução finita forma um k-submódulo de $k\langle X\rangle$ e $k\langle X\rangle$ é gerado por $\langle X\rangle$ como k-módulo, segue que todos os elementos de $k\langle X\rangle$ são de redução finita. ■

Agora já temos condições de enunciar e demonstrar o teorema central deste capítulo.

Teorema 2.1 (Lema do Diamante) *Seja S um sistema de redução para a k-álgebra associativa livre $k\langle X\rangle$ e $\leq$ uma ordem parcial de semigrupo em $\langle X\rangle$ com condição de cadeia descendente, de modo que $\leq$ e S sejam compatíveis. Então as condições abaixo são equivalentes.*

(a) Todas as ambigüidades de S são resolúveis.

(a') Todas as ambigüidades de S são resolúveis com respeito a $\leq$.

(b) Todos os elementos de $k\langle X\rangle$ são de redução única (segundo S).

(c) Um sistema de representantes em $k\langle X\rangle$ para os elementos da k-álgebra quociente $R = k\langle X\rangle/I$, que é determinada pelos geradores X e relações $W_\sigma = f_\sigma$ ($\sigma \in S$), é dado pelo k-submódulo $k\langle X\rangle_{irr}$ de $k\langle X\rangle$ gerado pelos monômios de $\langle X\rangle$ que são irredutíveis segundo S.

Quando valem essas condições, R pode ser identificada com o k-módulo $k\langle X\rangle_{irr}$ que, por sua vez, pode ser visto como k-álgebra com a multiplicação dada por $a \cdot b = r_S(ab)$.

Como os monômios irredutíveis de $k\langle X\rangle$ formam uma base para $k\langle X\rangle_{irr}$ como k-módulo, quando vale alguma condição acima (e, portanto todas elas), as imagens dos monômios irredutíveis no k-módulo quociente $k\langle X\rangle/I$ formam uma base para R como k-módulo. Quando vale a condição (b) do teorema acima, se $a \in k\langle X\rangle$ é um polinômio qualquer, costuma-se denominar o elemento $r_S(a)$ de *forma normal* de a.

Prova Provemos, primeiramente, que a condição (c) é equivalente a

(c') $k\langle X\rangle = k\langle X\rangle_{irr} \oplus I$.

De fato, por um lado, se $a \in k\langle X\rangle$, então $a + I \in k\langle X\rangle/I$. Por (c), segue que existe um único $u \in k\langle X\rangle_{irr}$ tal que $a + I = u + I$. Portanto, $a - u \in I$. Logo $a = u + (a - u)$ e a

decomposição é única, pois u é único. Por outro lado, se $a + I \in k\langle X\rangle/I$, então, por (c'), existe um único $u \in k\langle X\rangle_{irr}$ tal que $a - u \in I$. Assim, $a + I = u + I$. Logo $k\langle X\rangle_{irr}$ é um sistema de representantes para R.

A demonstração deste teorema seguirá o seguinte esquema:

$$\begin{array}{ccccc} (a) & \Rightarrow & (a') & & \\ & & \Downarrow & & \\ (a) & \Leftarrow & (b) & \Leftrightarrow & (c'). \end{array}$$

Pelo Lema 2.8, podemos afirmar que todos os elementos $a \in k\langle X\rangle$ são de redução finita. Assim, nas implicações $(c') \Rightarrow (b)$ e $(a') \Rightarrow (b)$ será suficiente mostrarmos que duas seqüências finais em um elemento arbitrário $a \in k\langle X\rangle$ fornecem um mesmo elemento irredutível quando suas composições forem calculadas em a.

$(b) \Rightarrow (c')$: Por hipótese, o submódulo dos elementos de redução única é igual a $k\langle X\rangle$. O operador linear $r_S : k\langle X\rangle \to k\langle X\rangle$ é uma projeção, pois, dado $a \in k\langle X\rangle$, $r_S(a) \in k\langle X\rangle_{irr}$. Portanto, $r_S(r_S(a)) = r_S(a)$, para todo $a \in k\langle X\rangle$, ou seja, $(r_S)^2 = r_S$. Temos que $Im(r_S) = k\langle X\rangle_{irr}$, pois $Im(r_S) \subseteq k\langle X\rangle_{irr}$, por definição de r_S, e $k\langle X\rangle_{irr} \subseteq Im(r_S)$, uma vez que, se $u \in k\langle X\rangle_{irr}$, então $r_S(u) = u$. Além disso, $ker(r_S) = I$. De fato, se $a \in ker(r_S)$, então $r_S(a) = 0$ e, pelo Lema 2.4, se $r_1, \ldots, r_n$ é uma seqüência final em a, $a = a - r_S(a) = a - r_n \ldots r_1(a) \in I$. Logo, $ker(r_S) \subseteq I$. Por outro lado, se $A, B \in \langle X\rangle$ e $\sigma = (W_\sigma, f_\sigma) \in S$, então $r_S(A(W_\sigma - f_\sigma)B) = r_S(AW_\sigma B) - r_S(Af_\sigma B)$. Pelo Lema 2.3, temos $r_S(AW_\sigma B) = r_S(Ar_{1\sigma 1}(W_\sigma)B) = r_S(Af_\sigma B)$. Assim, $r_S(A(W_\sigma - f_\sigma)B) = 0$ e, portanto, $I \subseteq ker(r_S)$. Logo $k\langle X\rangle = k\langle X\rangle_{irr} \oplus I$.

$(c') \Rightarrow (b)$: Seja $a \in k\langle X\rangle$. Mostremos que a é de redução única. Sejam $r_1, \ldots, r_n$ e $s_1, \ldots, s_m$ duas seqüências finais em a. Denotemos $b = r_n \ldots r_1(a) \in k\langle X\rangle_{irr}$ e $b' = s_m \ldots s_1(a) \in k\langle X\rangle_{irr}$. Sabemos, pelo Lema 2.4, que $a - b \in I$ e $b' - a \in I$. Assim, $b' - b = (b' - a) + (a - b) \in I$ e, como $k\langle X\rangle_{irr}$ é submódulo, $b' - b \in k\langle X\rangle_{irr}$, ou seja, $b' - b \in k\langle X\rangle_{irr} \cap I = \{0\}$. Logo, $b = b'$ e, portanto, a é de redução única.

$(a) \Rightarrow (a')$: É a Proposição 2.2.

$(b) \Rightarrow (a)$: Seja (σ, τ, A, B, C) uma ambigüidade de superposição em S. Pelo Lema 2.1 (ou Lema 2.3), temos, por um lado, $r_S(ABC) = r_S(r_{1\sigma C}(ABC)) = r_S(f_\sigma C)$ e, por outro lado, $r_S(ABC) = r_S(r_{A\tau 1}(ABC)) = r_S(Af_\tau)$. Logo, existem composições de reduções r e r' tais que $r(f_\sigma C) = r_S(ABC) = r'(Af_\tau)$ e, portanto, a ambigüidade é resolúvel. A demonstração para o caso de ambigüidades de inclusão é análoga.

$(a') \Rightarrow (b)$: É suficiente mostrar que os monômios $D \in \langle X \rangle$ são de redução única, pois os elementos de redução única formam um k-submódulo de $k\langle X \rangle$ (Lema 2.2) e os monômios de $\langle X \rangle$ geram $k\langle X \rangle$ como k-módulo. A demonstração será feita por indução. Já vimos que os monômios minimais de $\langle X \rangle$ são de redução única. Seja, agora, $D \in \langle X \rangle$ um monômio não minimal e assuma que todos os monômios $A \in \langle X \rangle$ tais que $A < D$ sejam de redução única. Mostremos que D é de redução única. O domínio da aplicação linear r_S é o submódulo dos elementos de redução única e, assim, estamos supondo que o submódulo gerado pelos monômios $< D$ está contido no domínio de r_S, o que implica que I_D está contido no domínio de r_S. Nessas condições, temos que $ker(r_S) \supseteq I_D$. De fato, sejam $A, B \in \langle X \rangle$ e $\sigma = (W_\sigma, f_\sigma) \in S$, tais que $AW_\sigma B < D$. Então $AW_\sigma B$ é de redução única. Pelo Lema 2.3, $Af_\sigma B = Ar_{1\sigma 1}(W_\sigma)B$ é de redução única e $r_S(AW_\sigma B) = r_S(Af_\sigma B)$. Portanto, $r_S(A(W_\sigma - f_\sigma)B) = 0$, o que implica que $A(W_\sigma - f_\sigma)B \in ker(r_S)$. Como esses elementos geram I_D, segue que $I_D \subseteq ker(r_S)$.

Suponhamos que D não é irredutível, pois se D for irredutível, D é de redução única trivialmente. Sejam, agora $r_1, \ldots, r_n$ e $s_1, \ldots, s_m$ duas seqüências finais em D. Sejam i_0 o menor i $(i = 1, \ldots, n)$ tal que r_i atue não trivialmente em $r_{i-1} \ldots r_1(D)$ e j_0 o menor j $(j = 1, \ldots, m)$ tal que s_j atue não trivialmente em $s_{j-1} \ldots s_1(D)$. Temos, então, $r_{i_0-1} \ldots r_1(D) = D$ e $s_{j_0-1} \ldots s_1(D) = D$. Logo, $r_n \ldots r_1(D) = r_n \ldots r_{i_0+1} r_{i_0} r_{i_0-1} \ldots r_1(D)$ $= r_n \ldots r_{i_0+1}(r_{i_0}(D))$. Analogamente, $s_m \ldots s_1(D) = s_m \ldots s_{j_0+1}(s_{j_0}(D))$. Vejamos como se comportam $r_{i_0}(D)$ e $s_{j_0}(D)$. Se $r_{i_0}(D) = 0$, então $r_{i_0}(D)$ é de redução única trivialmente; senão, $r_{i_0}(D) = \sum_{k=1}^{p} \lambda_k C_k$, com $C_k < D$ $(k = 1, \ldots, p)$, pois $\leq$ e S são compatíveis. Neste caso, temos que, para todo $k = 1, \ldots, p$, C_k é de redução única por hipótese de indução. Portanto $r_{i_0}(D)$ é um polinômio de redução única. Fazendo um raciocínio análogo, podemos concluir que $s_{j_0}(D)$ também é de redução única. Como $r_n \ldots r_{i_0+1}(r_{i_0}(D)) = r_n \ldots r_1(D) \in k\langle X \rangle_{irr}$ e $s_m \ldots s_{j_0+1}(s_{j_0}(D)) = s_m \ldots s_1(D)$ $\in k\langle X \rangle_{irr}$, pois $(r_i)_{i=1}^n$ e $(s_j)_{j=1}^m$ são finais em D, segue $r_S(r_{i_0}(D)) = r_n \ldots r_1(D)$ e $r_S(s_{j_0}(D)) = s_m \ldots s_1(D)$. Sendo as seqüências finais escolhidas arbitrárias, para mostrar que D é de redução única, é suficiente mostrar que $r_S(r_{L\sigma M'}(D)) = r_S(r_{L'\tau M}(D))$, onde $r_{L\sigma M'}$ e $r_{L'\tau M}$ são reduções que atuam não trivialmente em D.

Dividiremos a questão colocada acima em três casos de acordo com as posições relativas de W_σ e W_τ em D. Vamos supor, sem perda de generalidade, que o comprimento de L é menor ou igual ao comprimento de L'. Em termos mais precisos, estamos supondo que

o número de letras que compõem L é menor ou igual ao número de letras que compõem L'.

1o. caso: W_σ e W_τ interceptam-se, mas nenhum contém o outro. Isto quer dizer que $D = LABCM$, onde (σ, τ, A, B, C) é uma ambigüidade de superposição de S e, neste caso, tem-se $L' = LA$ e $M' = CM$. Efetuando-se o cálculo

$$r_{L\sigma M'}(D) - r_{L'\tau M}(D) = Lf_\sigma CM - LAf_\tau M = L(f_\sigma C - Af_\tau)M,$$

temos $r_{L\sigma M'}(D) - r_{L'\tau M}(D) \in I_{LABCM} = I_D$, pois, por (a'), (σ, τ, A, B, C) é resolúvel com respeito a $\leq$ e, assim, $f_\sigma C - Af_\tau \in I_{ABC}$, o que, pelo Lema 2.7, implica a afirmação. Como $I_D \subseteq ker(r_S)$, segue que $r_S(r_{L\sigma M'}(D) - r_{L'\tau M}(D)) = 0$.

2o. caso: W_τ está contido em W_σ. Neste caso temos $D = LABCM'$, onde (τ, σ, A, B, C) é uma ambigüidade de inclusão de S, $L' = LA$ e $M = CM'$. Temos, assim,

$$r_{L\sigma M'}(D) - r_{L'\tau M}(D) = Lf_\sigma M' - LAf_\tau CM' = L(f_\sigma - Af_\tau C)M'.$$

Por (a'), $f_\sigma - Af_\tau C \in I_{ABC}$. Logo, $L(f_\sigma - Af_\tau C)M' \in I_{LABCM'} = I_D$. Como $I_D \subseteq ker(r_S)$, segue que $r_S(r_{L\sigma M'}(D) - r_{L'\tau M}(D)) = 0$.

3o. caso: W_σ e W_τ são disjuntos, isto é, $D = LW_\sigma NW_\tau M$, $L' = LW_\sigma N$ e $M' = NW_\tau M$. Então, $r_{L\sigma M'}(D) = Lf_\sigma NW_\tau M$ e $r_{L'\tau M}(D) = LW_\sigma Nf_\tau M$. Tratemos, inicialmente, o caso em que $f_\sigma \neq 0$ e $f_\tau \neq 0$. Como $\leq$ e S são compatíveis, $f_\sigma = \sum_{i=1}^n \lambda_i C_i$, com $C_i < W_\sigma$. Nas hipóteses do Lema 2.3, coloquemos $a = Lf_\sigma N = \sum_{i=1}^n \lambda_i LC_i N$, $b = W_\tau$ e $c = M$. Então $LC_i NW_\tau M < LW_\sigma NW_\tau M = D$ $(i = 1, \ldots, n)$, pois $\leq$ é uma ordem parcial de semigrupo em $\langle X \rangle$. Por hipótese de indução, os monômios $LC_i NW_\tau M$ $(i = 1, \ldots, n)$ são de redução única. Nessas condições, o Lema 2.3 diz que $Lf_\sigma Nf_\tau M = Lf_\sigma Nr_{1\tau 1}(W_\tau)M$ é de redução única e que $r_S(Lf_\sigma Nf_\tau M) = r_S(Lf_\sigma Nr_{1\tau 1}(W_\tau)M) = r_S(Lf_\sigma NW_\tau M) = r_S(r_{L\sigma M'}(D))$. Se fizermos, agora, $a = L, b = W_\sigma$ e $c = Nf_\tau M$ no Lema 2.3, concluiremos, de modo análogo, que $r_S(Lf_\sigma Nf_\tau M) = r_S(Lr_{1\sigma 1}(W_\sigma)Nf_\tau M) = r_S(LW_\sigma Nf_\tau M) = r_S(r_{L'\tau M}(D))$. Logo, $r_S(r_{L\sigma M'}(D)) = r_S(r_{L'\tau M}(D))$. E o resultado está provado neste caso. Suponhamos, agora, que $f_\sigma = 0$. Por um lado, $r_S(r_{L\sigma M'}(D)) = 0$. Por outro lado, $r_S(r_{L'\tau M}(D)) = r_S(LW_\sigma Nf_\tau M)$. Se $f_\tau = 0$, então $r_S(r_{L'\tau M}(D)) = 0$ e se $f_\tau \neq 0$, usamos o raciocínio acima (e o Lema 2.3) para concluir que $r_S(r_{L'\tau M}(D)) = r_S(LW_\sigma Nf_\tau M) = r_S(Lf_\sigma Nf_\tau M) = 0$. E, novamente, obtemos o resultado desejado.

Aqui cabe uma observação. Fica claro que, nas hipóteses do Teorema 2.1, aquele

tipo de ambigüidade causada pela ocorrência em uma palavra de dois monômios distintos e **disjuntos** é automaticamente resolúvel, o que pode notar-se pelo fato de não ter sido necessária na demonstração deste caso outra hipótese senão aquelas sobre a ordem $\leq$. Justifica-se, assim, a atitude tomada anteriormente de não incluir dentre as definições de ambigüidade uma para a do tipo em questão.

Nas condições acima, o homomorfismo de k-módulos $\varphi : k\langle X\rangle \to k\langle X\rangle_{irr}$, dado por $\varphi(a) = r_S(a)$, para todo $a \in k\langle X\rangle$, é sobrejetor. Sabemos também que $ker(\varphi) = ker(r_S) = I$. Desta maneira, temos que $k\langle X\rangle/I$ e $k\langle X\rangle_{irr}$ são isomorfos como k-módulos. Como $k\langle X\rangle/I$ tem uma estrutura de k-álgebra, podemos transportá-la a $k\langle X\rangle_{irr}$ via o isomorfismo $\psi : k\langle X\rangle/I \to k\langle X\rangle_{irr}$, definido por $\psi(a+I) = \varphi(a)$, para todo $a + I \in k\langle X\rangle/I$. Basta, para isso, definir $a \cdot b = \psi(\psi^{-1}(a)\psi^{-1}(b))$, para todos $a, b \in k\langle X\rangle_{irr}$. Como $a, b \in k\langle X\rangle_{irr}$, temos $\psi(a+I) = \varphi(a) = r_S(a) = a$ e $\psi(b+I) = \varphi(b) = r_S(b) = b$. Logo, $\psi^{-1}(a) = a+I$ e $\psi^{-1}(b) = b+I$. Assim, $k\langle X\rangle_{irr}$ é uma k-álgebra com a multiplicação $a \cdot b = \psi((a+I)(b+I)) = \psi(ab+I) = \varphi(ab) = r_S(ab)$. ■

Dados um sistema de redução S para a k-álgebra $k\langle X\rangle$ e $\leq$ uma ordem parcial de semigrupo em $\langle X\rangle$ com c.c.d., tais que $\leq$ e S sejam compatíveis, associado a cada elemento $a \in k\langle X\rangle$, podemos definir um grafo orientado cujo conjunto de vértices é composto pelo elemento a e por polinômios $r_i \ldots r_1(a)$, onde $(r_1, \ldots, r_n)$ é uma seqüência final em a. Dados dois vértices v, w, existe uma aresta de v para w se existir uma seqüência final em a, $(r_1, \ldots, r_n)$, tal que $r_i \ldots r_1(a) = v$ e $r_{i+1}r_i \ldots r_1(a) = r_{i+1}(v) = w$. Em princípio, os vértices correspondentes aos elementos irredutíveis associados a cada seqüência final em a não precisam coincidir. Todavia, quando vale alguma das condições $(a), (a'), (b), (c)$ do Teorema 2.1, isto é, quando os elementos de $k\langle X\rangle$ são de redução única, todos esses elementos irredutíveis coincidem com $r_S(a)$, a forma normal de a, fornecendo assim, ao grafo construído o aspecto de um diamante. Essa construção sugere o nome dado ao Teorema 2.1 (Lema do Diamante).

O Teorema 2.1 tem um corolário imediato:

Corolário 2.2 *Seja $k\langle X\rangle$ a álgebra associativa livre sobre X e $\leq$ uma ordem parcial de semigrupo em $\langle X\rangle$ com condição de cadeia descendente. Se S é um sistema de redução sem ambigüidades e tal que $\leq$ e S são compatíveis, então o conjunto de relações $W_\sigma = f_\sigma$ $(\sigma \in S)$ é independente. Mais precisamente, se $S_1 \subseteq S_2$ são dois sistemas de redução*

tais que $\leq$ e S_1 são compatíveis e $\leq$ e S_2 também o são, se todas as ambigüidades são resolúveis segundo S_1 e S_2, e se S_2 contém algum σ tal que W_σ é irredutível com respeito a S_1, então a inclusão $I_1 \subseteq I_2$ é estrita, onde I_1 é o ideal associado a S_1 e I_2 o ideal associado a S_2.

Prova Sejam $k\langle X\rangle^1_{irr}$ e $k\langle X\rangle^2_{irr}$ os submódulos de $k\langle X\rangle$ formados pelos elementos irredutíveis segundo S_1 e S_2 respectivamente. Pelo Teorema 2.1, temos $k\langle X\rangle = k\langle X\rangle^1_{irr} \oplus I_1 = k\langle X\rangle^2_{irr} \oplus I_2$. Por definição, temos $k\langle X\rangle^2_{irr} \subseteq k\langle X\rangle^1_{irr}$ e $I_1 \subseteq I_2$ e, por hipótese, $k\langle X\rangle^2_{irr} \neq k\langle X\rangle^1_{irr}$. Logo, $I_1 \neq I_2$. ■

2.2 Observações

Esta seção será divida em três subseções que devem abranger questões qualitativas acerca da existência dos objetos estudados na seção anterior.

2.2.1 Ambigüidades de inclusão

Nas aplicações que serão apresentadas no capítulo seguinte pode-se notar que não há ambigüidades de inclusão. Isto se deve ao fato de que é sempre possível evitá-las de maneira a obter-se um novo sistema de redução que origina o mesmo anel quociente, mas que não contém ambigüidades de inclusão, desde que se saiba que todos os elementos de $k\langle X\rangle$ sejam de redução única. Essa construção será descrita a seguir.

Seja $S \subseteq \langle X\rangle \times k\langle X\rangle$ um sistema de redução. Vamos construir um subconjunto S' de S da seguinte maneira:

1. retiramos de S todo σ tal que W_σ contenha algum W_τ, para $\tau \in S$, como subpalavra própria;

2. sempre que existir mais do que um elemento $\sigma_1, \sigma_2, \ldots \in S$ de modo que $W_{\sigma_1} = W_{\sigma_2} = \ldots$, retiramos de S todos os σ_i em tal situação a menos de um deles escolhido arbitrariamente.

Obtemos, assim, um novo sistema de redução S' para $k\langle X\rangle$ que, por construção, não contém ambigüidades de inclusão. (Todas as que existiam em S foram retiradas nos passos 1 e 2.)

A maneira como S' foi construído permite-nos fazer uma observação preliminar. Se tomarmos um elemento $\sigma \in S$, então podemos afirmar que existe $\sigma' \in S'$ tal que $W_{\sigma'}$ é subpalavra (própria ou não) de W_σ. Esse fato será demonstrado por indução em $cpt(W_\sigma)$. Seja $n_0 = min\{cpt(W_\sigma) : \sigma \in S\} \geq 0$ e seja $\sigma \in S$ tal que $cpt(W_\sigma) = n_0$. Neste caso não existe $\tau \in S$ tal que W_τ seja subpalavra própria de W_σ, pois, se existisse tal τ, teríamos $cpt(W_\tau) < cpt(W_\sigma)$. Então, ou $\sigma \in S'$ ou existe $\sigma' \in S'$ tal que $W_{\sigma'} = W_\sigma$. Seja $\sigma \in S$ tal que $cpt(W_\sigma) = n > n_0$ e suponha que, para todo $\tau \in S$ tal que $n_0 \leq cpt(W_\tau) < n$, exista $\tau' \in S'$ tal que $W_{\tau'}$ seja subpalavra própria de W_τ. Se $\sigma \in S'$ não há o que provar. Caso contrário, temos dois casos a considerar. No primeiro, existe $\tau \in S$ e $A, B \in \langle X \rangle$, com $A \neq 1$ ou $B \neq 1$ tais que $W_\sigma = AW_\tau B$, implicando $cpt(W_\tau) < cpt(W_\sigma) = n$, portanto, por hipótese de indução, existem $\tau' \in S'$ e $A', B' \in \langle X \rangle$ tais que $W_\tau = A'W_{\tau'}B'$, o que implica que $W_\sigma = AA'W_{\tau'}B'B$ e, neste caso, $W_{\tau'}$ é subpalavra própria de W_σ. No segundo, existe $\sigma' \in S'$ tal que $W_\sigma = W_{\sigma'}$.

O sistema S' goza de algumas propriedades que serão listadas abaixo em forma de lemas. Seja $a \in k\langle X \rangle$ um elemento arbitrário.

Lema 2.9 *a é redutível segundo S se e somente se a é redutível segundo S'.*

Prova A demonstração será feita somente para os monômios de $k\langle X \rangle$, uma vez que o conjunto dos elementos irredutíveis segundo qualquer sistema de redução é um k-submódulo de $k\langle X \rangle$ e, além disso, os monômios geram $k\langle X \rangle$ como k-módulo. Como $S' \subseteq S$, uma das implicações acima é óbvia. Suponha, agora, que A é um monômio redutível segundo S. Como anteriormente, existem $C, D \in \langle X \rangle$ e $\sigma \in S$ tais que $A = CW_\sigma D$. Então existe $\sigma' \in S'$ tal que $W_{\sigma'}$ seja subpalavra de W_σ, isto é, existem $C', D' \in \langle X \rangle$ tais que $W_\sigma = C'W_{\sigma'}D'$ e, neste caso, $A = CW_\sigma D = CC'W_{\sigma'}D'D$, o que implica que A é redutível segundo S'. ■

Na demonstração do próximo lema, utilizaremos a notação $k\langle X \rangle_{irrS}$ para indicar o submódulo dos elementos irredutíveis segundo S e $k\langle X \rangle_{irrS'}$ para o submódulo dos elementos irredutíveis segundo S'. Pelo Lema 2.9, temos $k\langle X \rangle_{irrS} = k\langle X \rangle_{irrS'}$.

Lema 2.10 *Se a é de redução única segundo S, então a é de redução única segundo S' e vale $r_{S'}(a) = r_S(a)$.*

Prova Primeiramente mostremos que se a é de redução finita segundo S, então

a é de redução finita segundo S'. De fato, seja $(r_1, r_2, \ldots)$ uma seqüência infinita de reduções em S'. Em particular, $(r_1, r_2, \ldots)$ é uma seqüência infinita de reduções em S (pois $S' \subseteq S$). Assim, existe $i_0 \in \mathbb{N}$ tal que r_i atua trivialmente em $r_{i-1} \ldots r_1(a)$, para todo $i > i_0$. Logo a é de redução finita segundo S'. Seja agora $(r_1, \ldots, r_n)$ uma seqüência final em a segundo S'. Então $r_n \ldots r_1(a) \in k\langle X\rangle_{irrS'} = k\langle X\rangle_{irrS}$. Assim, $(r_1, \ldots, r_n)$ é final em a segundo S e, portanto, $r_n \ldots r_1(a) = r_S(a)$. Logo, a é de redução única segundo S' e vale $r_{S'}(a) = r_S(a)$. ■

Tendo em vista o resultado dos Lema 2.10, podemos concluir que se todo elemento de $k\langle X\rangle$ for de redução única segundo S, então todo elemento de $k\langle X\rangle$ será de redução única segundo S' e, além disso, valerá $r_{S'} = r_S$.

Se indicarmos por $I(S)$ o ideal de $k\langle X\rangle$ definido a partir de S, isto é, o ideal bilateral de $k\langle X\rangle$ gerado pelas diferenças $W_\sigma - f_\sigma$, com σ percorrendo o sistema de redução S, e $I(S')$ o correspondente ideal segundo S', podemos concluir, pelo Teorema 2.1, que se todo elemento de $k\langle X\rangle$ for de redução única segundo S, então $k\langle X\rangle = I(S) \oplus k\langle X\rangle_{irrS}$ como k-módulos. Temos também que todo elemento de $k\langle X\rangle$ será de redução única segundo S' e, assim, $k\langle X\rangle = I(S') \oplus k\langle X\rangle_{irrS'}$. Pelo Lema 2.9, temos $k\langle X\rangle_{irrS} = k\langle X\rangle_{irrS'}$. Como $I(S') \subseteq I(S)$, segue $I(S) = I(S')$. Logo $R = k\langle X\rangle/I(S)$ e $R' = k\langle X\rangle/I(S')$ são o mesmo anel. O fato de termos $r_S = r_{S'}$ permite-nos afirmar ainda que as formas normais dos elementos de R e R', dadas pelos isormofismos entre esses k-módulos e $k\langle X\rangle_{irrS} = k\langle X\rangle_{irrS'}$, induzidos pelas aplicações r_S e $r_{S'}$, respectivamente, são as mesmas.

As considerações acima justificam a afirmação que diz que, quando todos os elementos de $k\langle X\rangle$ são de redução única, as ambigüidades de inclusão são sempre evitáveis e, portanto, não precisamos estudá-las em separado. É evidente que, em termos práticos, pode ocorrer de não conseguirmos fazer a eliminação de todas as ambigüidades de inclusão. (Nos casos em que S é infinito, freqüentemente é impossível realizar um algoritmo de eliminação de ambigüidades de inclusão sobre o qual se tenha certeza da finitude.) Assim a discussão acima em alguns casos só tem valor teórico.

2.2.2 Quando k é um corpo

A pergunta "Uma k-álgebra R gerada por um conjunto X sempre tem uma forma normal do tipo apresentado no Teorema 2.1?" tem resposta afirmativa no caso em que k

é um corpo.

Começemos o estudo da situação descrita na seção anterior quando o anel k é um corpo fazendo algumas considerações sobre a ordem parcial de semigrupo em $\langle X \rangle$. Vamos definir uma *boa ordem de semigrupo* em $\langle X \rangle$ como sendo uma boa ordem em $\langle X \rangle$ que preserva a operação de semigrupo, isto é, uma ordem total $\leq$ em $\langle X \rangle$ com condição de cadeia descendente tal que se B e B' são monômios em $\langle X \rangle$ que satisfazem $B < B'$, então temos $ABC < AB'C$, para quaisquer $A, C \in \langle X \rangle$.

Dado um conjunto X, sempre existe uma boa ordem de semigrupo em $\langle X \rangle$. Para tanto basta tomarmos uma boa ordem em X e, para $A, B \in \langle X \rangle$ definimos: $A < B$ se e somente se $cpt(A) < cpt(B)$ ou $cpt(A) = cpt(B)$ e A precede B lexicograficamente. Essa é trivialmente uma ordem total em $\langle X \rangle$ que respeita a operação de semigrupo. Além disso, $\leq$ tem condição de cadeia descendente. Mostraremos esse fato provando que todo subconjunto não vazio de $\langle X \rangle$ tem elemento minimal. Seja $\Sigma \subseteq \langle X \rangle$ um subconjunto não vazio de $\langle X \rangle$ e seja $n = min\{cpt(A) : A \in \Sigma\}$. Vamos definir ainda o subconjunto Σ' de Σ dado por $\Sigma' = \{A \in \Sigma : cpt(A) = n\}$. Vamos demonstrar por indução em n que Σ' tem elemento minimal. Se $n = 0$, então $\Sigma' = \{1\}$ e, portanto, 1 é minimal de Σ'. Se $n > 0$, suponha, por hipótese de indução, que todo subconjunto de $\langle X \rangle$ formado por palavras com comprimento igual a $n - 1$ tenha (pelo menos) um elemento minimal. Mostremos que Σ' tem um elemento minimal. Seja $Y \subseteq X$ o subconjunto de X dado por $Y = \{x_1 \in X : x_1 \ldots x_n \in \Sigma' \text{ e } x_i \in X\}$. Como X é bem ordenado, existe elemento minimal x_0 em Y. Seja, agora, $\Sigma'' = \{x_2 \ldots x_n \in \langle X \rangle : x_1 x_2 \ldots x_n \in \Sigma' \text{ e } x_i \in X\}$. Todas as palavras de Σ'' têm comprimento $n - 1$, portanto, por hipótese de indução, existe elemento minimal A_0 em Σ''. Como $\leq$ é ordem parcial de semigrupo, $x_0 A_0$ é minimal em Σ'. Afirma-se, então, que um elemento minimal de Σ' é também um elemento minimal de Σ, uma vez que todos os elementos que pertencem a Σ e não pertencem a Σ' têm comprimento estritamente maior do que o do elemento minimal de Σ'.

Seja R uma k-álgebra (k corpo) gerada por um conjunto X. Construímos o monóide livre $\langle X \rangle$ gerado por X e dotamo-lo de uma boa ordem de semigrupo, denotada por $\leq$; por exemplo, aquela introduzida acima. Construímos em seguida a k-álgebra livre $k\langle X \rangle$ gerada por X.

Seja $\varphi : k\langle X \rangle \longrightarrow R$ o homomorfismo (sobrejetor) de k-álgebras definido nos geradores de $k\langle X \rangle$ por $\varphi(x) = x$, para todo $x \in X$. Como os elementos $x \in X$ geram R, temos

que $R \cong k\langle X\rangle / ker(\varphi)$. Vamos denotar $\varphi(a) = \overline{a}$. Com essa notação temos $\overline{ab} = \overline{a}\overline{b}$ e se $a = \sum_A \lambda_A A$, então $\overline{a} = \sum_A \lambda_A \overline{A}$.

Dado $a \in k\langle X\rangle$, se escrevermos $a = \sum_A \lambda_A A$, defino o **suporte** de a por $supp(a) = \{A \in \langle X\rangle : \lambda_A \neq 0\}$. Como $k\langle X\rangle$ é livre, temos que $supp(a)$ é um conjunto finito bem definido para todo $a \in k\langle X\rangle$.

Para cada $a \in ker(\varphi) = \{a \in k\langle X\rangle : \overline{a} = 0\}$, $a \neq 0$, escolho $M(a)$ o máximo do conjunto $supp(a)$. Esse máximo existe e é único, pois $supp(a)$ é finito e a ordem $\leq$ em $\langle X\rangle$ é total. Defino, agora, o par $(W_a, f_a) \in \langle X\rangle \times k\langle X\rangle$, onde $W_a = M(a)$ e $f_a = M(a) - \lambda_{M(a)}^{-1} a$. Construo, assim, um conjunto $S = \{\sigma_a : a \in ker(\varphi) \text{ e } a \neq 0\}$, onde $\sigma_a = (W_a, f_a)$.

Temos, então, um sistema de redução S para $k\langle X\rangle$, uma ordem parcial de semigrupo $\leq$ em $\langle X\rangle$ com condição de cadeia descendente e tal que $\leq$ e S sejam compatíveis (por construção de S). Vejamos, agora, quais são os monômios irredutíveis segundo S. Seja Δ o conjunto dos monômios $A \in \langle X\rangle$ cujas imagens $\overline{A}$ são combinações lineares de imagens de monômios $B < A$. Denotemos por $\langle X\rangle_{irr}$ o conjunto complementar de Δ em $\langle X\rangle$. Afirmo que o conjunto $\langle X\rangle_{irr}$ é o conjunto dos monômios irredutíveis de $\langle X\rangle$ segundo S. De fato, seja $A \in \langle X\rangle$ tal que existam $n \in \mathbb{N}$, $\lambda_i \in k$ e $B_i \in \langle X\rangle$ $(i = 1, \ldots, n)$ que satisfaçam $B_i < A$ e $\overline{A} = \sum_{i=1}^{n} \lambda_i \overline{B_i}$. Então $\varphi(A - \sum_i \lambda_i B_i) = \overline{A} - \sum_i \lambda_i \overline{B_i} = 0$. Logo, $a = A - \sum_i \lambda_i B_i \in ker(\varphi)$. Assim, $W_a = A$ e, portanto, A é redutível. Por outro lado, se A é redutível, então existem $B, C \in \langle X\rangle$ e $a \in ker(\varphi)$ tais que $A = BW_aC$. Então

$$\begin{aligned}
\varphi(A - Bf_aC) &= \varphi(BW_aC - Bf_aC) \\
&= \varphi(B(W_a - f_a)C) \\
&= \varphi(B)\varphi(W_a - f_a)\varphi(C) \\
&= 0,
\end{aligned}$$

pois $\varphi(W_a - f_a) = \varphi(\lambda_{M(a)}^{-1} a) = \lambda_{M(a)}^{-1} \overline{a} = 0$. Logo, $\overline{A} = \overline{Bf_aC}$, que é combinação linear de imagens de monômios $< BW_aC = A$, pois, como $\leq$ e S são compatíveis, $\overline{f_a}$ é combinação linear de imagens de monômios $< W_a$. Denotamos por $k\langle X\rangle_{irr}$ o k-submódulo de $k\langle X\rangle$ gerado por $\langle X\rangle_{irr}$.

Vamos definir o ideal I do mesmo modo como o definimos na seção anterior, isto é, I é o ideal bilateral de $k\langle X\rangle$ gerado pelas diferenças $W_a - f_a$, com os pares $\sigma_a = (W_a, f_a)$ percorrendo o conjunto S. Afirma-se que $I = ker(\varphi)$. De fato, $I \subseteq ker(\varphi)$, pois

$\varphi(W_a - f_a) = 0$, para todo $\sigma_a \in S$. E $ker(\varphi) \subseteq I$, pois se $a \in ker(\varphi)$ e $a \neq 0$, então $a = \lambda_{M(a)}(W_a - f_a)$.

Vejamos, agora, que todo elemento de $k\langle X\rangle$ é de redução única. Sabemos que todo elemento de $k\langle X\rangle$ é de redução finita, pois $\langle X\rangle$ foi dotado de uma ordem parcial de semigrupo, $\leq$, com c.c.d. e, por construção do sistema de redução S, tem-se que $\leq$ e S são compatíveis (vide Lema 2.8). Assim sendo, seja $a \in k\langle X\rangle$ um elemento qualquer e $(r_1, \ldots, r_n)$ e $(s_1, \ldots, s_m)$ duas seqüências finais em a arbitrárias. Temos, então, $b = r_n \ldots r_1(a) \in k\langle X\rangle_{irr}$ e $b' = s_m \ldots s_1(a) \in k\langle X\rangle_{irr}$. Pelo Lema 2.4, sabemos que $b - a \in I = ker(\varphi)$ e que $a - b' \in I = ker(\varphi)$. Logo, $c = b - b' \in ker(\varphi)$. Suponhamos que $c \neq 0$. Neste caso, teríamos um par (W_c, f_c) em S, o que implicaria que c não seria irredutível. Isso contradiz o fato de b e b' serem irredutíveis e $k\langle X\rangle_{irr}$ um k-submódulo. Logo $c = 0$ e, portanto, a é de redução única.

Tendo em vista que todos os elementos de $k\langle X\rangle$ são de redução única, podemos aplicar o Teorema 2.1 e concluir que os elementos de $R \cong k\langle X\rangle / I$ têm uma forma normal.

De maneira análoga, se uma k-álgebra R é dada por geradores X e por relações $\{g_j = h_j : j \in J\}$, escolhemos uma boa ordem de semigrupo $\leq$ para $\langle X\rangle$ e para cada relação $g = h$ definimos um par (W, f), onde W é o monômio máximo (segundo a ordem $\leq$) do polinômio $g - h$ e $f = W - \lambda^{-1}(g - h)$, onde λ indica o coeficiente de W no polinômio $g - h$. Desta forma construímos parte do conjunto S. Para resolver as ambigüidades que surgirem, basta transformar as equações que delas derivam em pares do sistema de redução da mesma maneira. (Foi exatamente assim que procedemos no Capítulo 1.)

Teremos um sistema de redução S tal que $\leq$ e S sejam compatíveis. Além disso, todos os elementos de $k\langle X\rangle$ serão de redução única segundo S, pois S foi construído para que isso ocorresse. Dessa forma, os elementos de R terão uma forma normal.

2.2.3 Ordem parcial de semigrupo

Nesta subseção encontraremos condições suficientes para, dado um sistema de redução S, garantir a existência de uma ordem parcial de semigrupo $\leq$ em $\langle X\rangle$ com condição de cadeia descendente tal que $\leq$ e S sejam compatíveis.

Faremos alguns comentários preliminares sobre relações em conjuntos, que têm a finalidade de fixar algumas nomenclaturas e relembrar resultados básicos. Dado um con-

junto Y, um subconjunto R de $Y \times Y$ é chamando uma *relação* em Y. Dizemos que uma relação R é *transitiva* se $(x, y), (y, z) \in R$ implicar $(x, z) \in R$. Dada uma relação R qualquer em Y, sempre é possível construir uma relação transitiva que contenha R e que seja a "menor relação transitiva" em Y com essa propriedade. Isso é feito da seguinte maneira. Consideremos $\mathcal{U}$ o conjunto de todas as relações transitivas R' em Y tais que $R \subseteq R'$. O conjunto $\mathcal{U}$ é não vazio, pois $Y \times Y$ é uma relação transitiva em Y. Seja $T(R)$ a intersecção de todos os elementos de $\mathcal{U}$. A relação $T(R)$ é transitiva e contém R. Comumente, denomina-se $T(R)$ de *fecho transitivo* de R.

Dizemos que uma seqüência finita $(x_i, y_i)_{i=1}^n$ em R é uma *cadeia* finita se $y_i = x_{i+1}$, para $i = 1, \ldots, n-1$. Neste caso, costuma-se escrever a cadeia da seguinte maneira:

$$(x_1, x_2), (x_2, x_3), \ldots, (x_{n-2}, x_{n-1}), (x_{n-1}, x_n). \tag{2.2}$$

Definimos o *comprimento* da cadeia (2.2) como sendo o número de pares que a compõem, a saber, $n-1$. Define-se cadeia infinita de maneira análoga. No caso de cadeias infinitas, não há definição análoga de comprimento.

Há uma maneira de caracterizar o fecho transitivo de uma relação através de seus elementos. Dada uma relação R em Y, constrói-se o subconjunto T de $Y \times Y$ que contém todos os pares (x, y) para os quais exista uma cadeia finita do tipo (2.2) com $x_1 = x$ e $x_n = y$. Afirma-se que $T(R) = T$. É fácil ver que T é uma relação transitiva e que T contém R trivialmente. Logo, $T(R) \subseteq T$. Por outro lado, demonstra-se com facilidade que a relação T está contida em toda relação transitiva que contenha R. Logo, $T \subseteq T(R)$.

Uma relação R em um conjunto Y é dita *anti-reflexiva* se não contiver nenhum elemento da diagonal do conjunto $Y \times Y$, isto é, se não existir $x \in Y$ tal que $(x, x) \in R$. Dizemos que uma relação R tem *condição de cadeia* se dada qualquer cadeia infinita

$$(x_1, x_2), (x_2, x_3), \ldots, (x_n, x_{n+1}), \ldots$$

existir $i_0 \in \mathbb{N}$ tal que $(x_{i_0}, x_{i_0+1}) = (x_{i_0+n}, x_{i_0+n+1})$, para todo $n \in \mathbb{N}$, o que é equivalente a dizer que $x_i = x_{i_0}$, para todo $i \geq i_0$. Ressalta-se que se R é uma relação anti-reflexiva, dizer que R tem condição de cadeia é equivalente a dizer que R não contém cadeias infinitas.

Um resultado de demonstração elementar sobre cadeias e que nos será bastante útil no decorrer desta seção é aquele que afirma que uma relação qualquer tem condição de

cadeia se e somente se seu fecho transitivo tiver.

Seja k um anel associativo, comutativo com unidade e que **não contenha divisores de zero**. Seja S um sistema de redução para a k-álgebra livre $k\langle X\rangle$ gerada por um conjunto X dado. A álgebra $k\langle X\rangle$ é um k-módulo livre de base $\langle X\rangle$. Consideremos os funcionais lineares $C' : k\langle X\rangle \longrightarrow k$, onde C percorre $\langle X\rangle$, que são definidos na base $\langle X\rangle$ da seguinte maneira: $C'(C) = 1$ e $C'(B) = 0$, para $B \neq C$. Vamos definir uma relação R no conjunto $\langle X\rangle$. Um par $(D, C) \in \langle X\rangle \times \langle X\rangle$ será um elemento da relação R se existir uma redução r que atue não trivialmente em D tal que $C'(r(D)) \neq 0$, isto é, tal que C tenha coeficiente não nulo em $r(D)$. Seja $T(R)$ o fecho transitivo de R.

Lema 2.11 *Se todo elemento de $k\langle X\rangle$ é de redução finita, então (i) $T(R)$ é anti-reflexiva e (ii) $T(R)$ tem condição de cadeia.*

Prova (i) Primeiramente mostremos que R é anti-reflexiva. Suponha, por absurdo que exista um par $(C, C) \in R$. Então existe redução r tal que $C'(r(C)) \neq 0$. Logo, existem $\lambda \in k, \lambda \neq 0$ e $f \in k\langle X\rangle$, com $C'(f) = 0$, tais que $r(C) = \lambda C + f$. Assim, temos $r^n(C) = \lambda^n C + (\sum_{i=0}^{n-1} \lambda^i)f$, para todo $n \in \mathbb{N}$. Como k não contém divisores de zero, em particular não contém elementos nilpotentes não nulos; portanto $\lambda^n \neq 0$, qualquer que seja n. Então C não seria de redução finita. Suponha, agora, que exista um par $(C, C) \in T(R)$, ou seja, que exista uma cadeia finita

$$(C_1, C_2), (C_2, C_3), \ldots, (C_{n-1}, C_n) \tag{2.3}$$

em R tal que $C_1 = C = C_n$. A demonstração seguirá por indução no comprimento de (2.3), ou seja, $n - 1$. Se $n = 2$, teríamos $(C, C) \in R$, o que já vimos não ser possível. Suponha, por hipótese de indução, que não existam em R cadeias

$$(D_1, D_2), (D_2, D_3), \ldots, (D_{m-1}, D_m),$$

com $D_1 = D_m$ e $m < n$. Como para todo $i = 1, \ldots, n - 1$, temos $(C_i, C_{i+1}) \in R$, existem reduções r_i e elementos $\lambda_i \in k, \lambda_i \neq 0$, $f_i \in k\langle X\rangle$, com $C'_{i+1}(f_i) = 0$, tais que $r_i(C_i) = \lambda_i C_{i+1} + f_i$. Sabemos, também que $C'_i(f_i) = 0$, para todo i. Suponha que existam i, j, tais que $C'_j(f_i) \neq 0$. Isso implica que $(C_i, C_j) \in R$. Há dois casos a considerar. No primeiro caso, se $j > i + 1$, teríamos em R a cadeia

$$(C_1, C_2), \ldots, (C_{i-2}, C_{i-1}), (C_{i-1}, C_i), (C_i, C_j), (C_j, C_{j+1}), \ldots, (C_{n-1}, C_n),$$

que é uma cadeia de comprimento $(n-1)-(j-i-1) < n-1$ e tal que $C_1 = C_n = C$. Absurdo. No segundo caso, se $j < i$, teríamos em R a cadeia

$$(C_j, C_{j+1}), (C_{j+1}, C_{j+2}), \ldots, (C_{i-1}, C_i), (C_i, C_j),$$

que é uma cadeia de comprimento $i-j+1 < n-1$ (pois se $i = n$, então $j > 2$, e se $j = 1$, então $i < n-1$) e com o mesmo C_j nas "extremidades". Absurdo. Conclui-se, então, que $C_j'(f_i) = 0$, para $1 \leq i, j \leq n$. Portanto, pode-se mostrar que

$$(r_n \ldots r_1)^m (C_1) = (\lambda_n \ldots \lambda_1)^m C_n + g_m,$$

onde os polinômios g_m são tais que $C_i'(g_m) = 0$, para todo $i = 1, \ldots, n$ e todo $m \in \mathbb{N}$. Como k não contém divisores de zero, $(\lambda_n \ldots \lambda_1)^m \neq 0$, e, portanto, C_1 não seria de redução finita.

(ii) Basta, como mencionamos anteriormente, mostrar que R tem condição de cadeia. Como já sabemos que $T(R)$ (e, portanto, R) é anti-reflexiva, é suficiente mostrarmos que não existem cadeias infinitas em R. Suponhamos que exista uma cadeia infinita

$$(C_1, C_2), (C_2, C_3), \ldots, (C_n, C_{n+1}), \ldots$$

em R. Então existiriam reduções r_i $(i \in \mathbb{N})$ tais que $r_i(C_i) = \lambda_i C_{i+1} + f_i$, onde $\lambda_i \in k, \lambda_i \neq 0$ e $f_i \in k\langle X \rangle$, com $C_{i+1}'(f_i) = 0$. Vamos construir uma subcadeia infinita

$$(C_{j_1}, C_{j_2}), (C_{j_2}, C_{j_3}), \ldots, (C_{j_n}, C_{j_{n+1}}), \ldots$$

da cadeia acima. Tomamos $j_1 = 1$. Seja j_2 o máximo do conjunto $\{j \in \mathbb{N} : C_j'(r_{j_1}(C_{j_1})) \neq 0\}$. Esse conjunto é não vazio, pois $j_1 + 1$ pertence a ele, e é finito, pois $r_{j_1}(C_{j_1})$ é um polinômio e, portanto, uma combinação linear de monômios. Escolhido o índice j_n, tomamos j_{n+1} como sendo o máximo do conjunto $\{j \in \mathbb{N} : C_j'(r_{j_n}(C_{j_n})) \neq 0\}$. Esse máximo existe pois $j_n + 1$ pertence a esse conjunto, que é finito. Para cada $n \in \mathbb{N}$, indiquemos por $\mu_n \neq 0$ o coeficiente de $C_{j_{n+1}}$ em $r_{j_n}(C_{j_n})$. Por construção da subcadeia, temos que, para cada $n \in \mathbb{N}$, existe $g_n \in k\langle X \rangle$, com $C_j'(g_n) = 0$, para todo $j \geq j_n$ tal que,

$$r_{j_n}(C_{j_n}) = \mu_n C_{j_{n+1}} + g_n.$$

Nessas condições, temos

$$r_{j_n} \ldots r_{j_1}(C_{j_1}) = \mu_1 \ldots \mu_n C_{j_{n+1}} + \sum_{i=2}^{n} \mu_1 \ldots \mu_{i-1} g_i + g_1,$$

qualquer que seja $n \in \mathbb{N}$. Como k não contém divisores de zero, temos que o produto $\mu_1 \dots \mu_n$ é diferente de zero para todo n. Assim, C_{j_1} não seria de redução finita. Logo, $T(R)$ é anti-reflexiva. ■

Podemos concluir que se k não contiver divisores de zero, S for um sistema de redução para $k\langle X\rangle$ e todo elemento de $k\langle X\rangle$ for de redução finita, então existe uma ordem parcial de semigrupo, $\leq$, em $\langle X\rangle$ com condição de cadeia descendente tal que S e $\leq$ sejam compatíveis. Essa ordem é dada pelo lema abaixo.

Proposição 2.4 *Sejam k um anel associativo, comutativo, com unidade e que não contém divisores de zero e S um sistema de redução para $k\langle X\rangle$. Se todo elemento de $k\langle X\rangle$ for de redução finita, então a relação em $\langle X\rangle$ dada por $A \leq B$ se $(B, A) \in T(R)$ ou $A = B$ é uma ordem parcial de semigrupo com condição de cadeia descendente. Além disso, $\leq$ e S são compatíveis.*

Prova É conseqüência imediata do Lema 2.11 que $\leq$ é uma ordem parcial com condição de cadeia descendente. Mostremos que $\leq$ respeita a estrutura de semigrupo de $\langle X\rangle$. Sejam D, E elementos arbitrários de $\langle X\rangle$ e $A, B \in \langle X\rangle$ tais que $A < B$, isto é, tais que $(B, A) \in T(R)$. Então existe uma cadeia finita em R,

$$(C_1, C_2), (C_2, C_3), \dots, (C_{n-1}, C_n),$$

tal que $C_1 = B$ e $C_n = A$. Logo, para cada $i = 1, \dots, n$, existem uma redução $r_{A_i\sigma_iB_i}$ e elementos $\lambda_i \in k, \lambda_i \neq 0$ e $f_i \in k\langle X\rangle$, com $C'_{i+1}(f_i) = 0$, tais que $r_i(C_i) = \lambda_i C_{i+1} + f_i$. Portanto, $r_{DA_i\sigma_iB_iE}(DC_iE) = \lambda_i DC_{i+1}E + Df_iE$ e $(DC_{i+1}E)'(Df_iE) \neq 0$. Logo,

$$(DC_1E, DC_2E), (DC_2E, DC_3E), \dots, (DC_{n-1}E, DC_nE)$$

é uma cadeia em R, o que implica que $(DBE, DAE) = (DC_1E, DC_nE) \in T(R)$ e, portanto, $DAE < DBE$. A compatibilidade entre $\leq$ e S segue da construção de R. ■

Por outro lado, se k tem divisores de zero, $ab = 0$, por exemplo, então conseguimos construir a k-álgebra livre gerada pelo conjunto $\{u, x, y\}$, denotada por $k\langle u, x, y\rangle$ e o sistema de redução $S = \{\sigma, \tau\}$, onde $\sigma = (ux, auy)$ e $\tau = (yu, bxu)$. Assim, qualquer ordem parcial de semigrupo em $\langle u, x, y\rangle$ que seja compatível com S, isto é, tal que $uy < ux$ e $xu < yu$, iria implicar $uxu < uyu < uxu$, o que é absurdo. Apesar disso, todos os

elementos de $k\langle u,x,y\rangle$ são de redução finita segundo S. Esse fato será demonstrado em seguida.

Seja $A \in \langle u,x,y\rangle$ um monômio arbitrário e suponhamos, por absurdo, que A não seja de redução finita, isto é, que exista uma seqüencia infinita de reduções $(r_i)_{i\in\mathbb{N}}$ de modo que r_i atue não trivialmente em $r_{i-1}\dots r_1(A)$, para todo $i \in \mathbb{N}$. Vamos dividir o estudo dessa situação em três casos.

1o. caso: Existem $i,j \in \mathbb{N}$ e $A_i, B_i, A_j, B_j \in \langle u,x,y\rangle$ tais que $r_i = r_{A_i\sigma B_i}$ e $r_j = r_{A_j\tau B_j}$. Tomamos $l = max\{i,j\}$. Então $r_l\dots r_1(A) = (ab)cA'$, para algum $c \in k$ e $A' \in \langle u,x,y\rangle$. Logo $r_l\dots r_1(A) = 0$ e, assim, r_{l+1} atua trivialmente em $r_l\dots r_1(A)$. Contradição.

2o. caso: Em $(r_i)_{i\in\mathbb{N}}$ temos apenas reduções que envolvem o elemento $\sigma \in S$, isto é, $r_i = r_{A_i\sigma B_i}$ $(A_i, B_i \in \langle u,x,y\rangle)$, para todo $i \in \mathbb{N}$. Vamos indicar por $gr_z(A)$, onde $z \in \{u,x,y\}$, o grau de z em A, isto é, o número de vezes que z aparece em A. Assim, se $gr_x(A) = n$, então pode-se afirmar que r_{n+1} atua trivialmente em $r_n\dots r_1(A)$, pois vale, em geral, $gr_x(r_i\dots r_1(A)) = gr_x(r_{i-1}\dots r_1(A)) - 1$, para todo i. Logo, como $gr_x(r_n\dots r_1(A)) = 0$, $r_n\dots r_1(A)$ não envolve a letra x e, portanto, r_{n+1} tem que atuar trivialmente em $r_n\dots r_1(A)$. Contradição.

3o. caso: Em $(r_i)_{i\in\mathbb{N}}$ temos apenas reduções que envolvem o elemento $\tau \in S$. Esse caso é análogo ao anterior.

Provamos que todo monômio de $\langle X\rangle$ é de redução finita. Então pode-se concluir que todo elemento de $k\langle X\rangle$ é de redução finita. Mas, apesar disso, a ordem $\leq$ e o sistema de redução S não são compatíveis, o que foi devido ao fato de k conter divisores de zero.

Capítulo 3

Aplicações

Este capítulo será todo dedicado a apresentar algumas aplicações do Teorema 2.1 demonstrado no capítulo anterior. Cada uma das aplicações terá uma seção dedicada exclusivamente a ela, entretanto alguma superposição entre as seções pode ocorrer. A primeira seção apresenta uma demonstração do clássico Teorema de Poincaré-Birkhoff-Witt baseada nas idéias introduzidas no capítulo anterior. A segunda seção apresenta resultados de natureza mais prática que auxiliam o cálculo necessário para verificar resolubilidade de ambigüidades. No final dessa última seção encontra-se um exemplo de aplicação dos resultados apresentados.

3.1 O Teorema de Poincaré-Birkhoff-Witt (PBW)

Começaremos por introduzir e fixar algumas definições e notações comuns ao estudo de álgebras não-associativas.

Seja k um anel associativo, comutativo e com unidade. Uma *álgebra de Lie sobre* k $\mathcal{L}$ é uma álgebra (não-associativa) sobre k que satisfaz as seguintes condições, chamadas *condições de Lie*:

$$x^2 = 0 \tag{3.1}$$

$$(xy)z + (yz)x + (zx)y = 0 \tag{3.2}$$

para todos x, y, z elementos de $\mathcal{L}$. A identidade (3.2) é conhecida como *identidade de Jacobi.*

Deste ponto em diante consideraremos o anel k fixado e diremos simplesmente *álgebra de Lie* quando quisermos nos referir a uma álgebra de Lie sobre k e *álgebra* para nos referirmos a uma k-álgebra. Sub-álgebras de uma álgebra de Lie são definidas de maneira natural.

Se $\mathcal{L}$ é uma álgebra de Lie e $x, y \in \mathcal{L}$, pela condição (3.1), temos

$$xy = -yx. \tag{3.3}$$

Quando a característica de $\mathcal{L}$ é diferente de 2, a identidade (3.3) é equivalente à condição (3.1), podendo substituí-la na definição de álgebra de Lie.

Podemos construir uma álgebra de Lie a partir de uma álgebra associativa de uma maneira simples. Seja $\mathcal{U}$ uma álgebra associativa. Dados dois elementos arbitrários de $\mathcal{U}$, x, y, definimos o *produto de Lie* ou *comutador* de x e y por

$$[x, y] = xy - yx.$$

Verifica-se facilmente que [,] satisfaz as condições sobre o produto em uma álgebra e satisfaz também as condições (3.1) e (3.2). A álgebra de Lie obtida de $\mathcal{U}$ através da substituição do produto original pelo produto de Lie é chamada *a álgebra de Lie* da álgebra associativa $\mathcal{U}$ e é denotada por $\mathcal{U}_L$. Por causa desse tipo de construção é comum denotarmos o produto em uma álgebra de Lie por $[x, y]$. Essa será a notação utilizada no resto desta seção.

Seja $\mathcal{L}$ é uma álgebra de Lie arbitrária. Um par $(\mathcal{U}, i)$, onde $\mathcal{U}$ é uma álgebra associativa e $i : \mathcal{L} \longrightarrow \mathcal{U}_L$ um homomorfismo de álgebras de Lie, ou seja, uma aplicação k-linear que satisfaz $i([a, b]) = i(a)i(b) - i(b)i(a)$, para todos $a, b \in \mathcal{L}$, é dito uma *álgebra envolvente universal* de $\mathcal{L}$ se, dados $\mathcal{A}$, uma álgebra associativa, e $\theta : \mathcal{L} \longrightarrow \mathcal{A}_L$, um homomorfismo de álgebras de Lie, existir um único homomorfismo de álgebras associativas $\theta' : \mathcal{U} \longrightarrow \mathcal{A}$ tal que $\theta = \theta' i$. Graficamente, essa condição é equivalente à comutatividade do seguinte diagrama.

$$\begin{tikzcd}
\mathcal{L} \arrow[r, "i"] \arrow[dr, "\theta"'] & \mathcal{U}_L = \mathcal{U} \arrow[d, "\theta'"] \\
& \mathcal{A}_L = \mathcal{A}
\end{tikzcd}$$

Uma álgebra envolvente universal de uma álgebra de Lie tem muitas propriedades (ver [9, pp. 151–156]), entre elas a seguinte. Dada uma álgebra de Lie $\mathcal{L}$, se existir uma álgebra envolvente universal $(\mathcal{U}, i)$ de $\mathcal{L}$, então ela é única a menos de isomorfismo, isto é, se $(\mathcal{U}', j)$ for outra álgebra envolvente universal de $\mathcal{L}$, existe um único isomorfismo $j' : \mathcal{U} \longrightarrow \mathcal{U}'$ tal que $j = j'i$. Por esse motivo, costuma-se chamar uma álgebra envolvente universal de $\mathcal{L}$ de *a* álgebra envolvente universal de $\mathcal{L}$.

Seja agora $\mathcal{L}$ uma álgebra de Lie sobre k que é livre como k-módulo com base X. Deste ponto em diante só trabalharemos com essa álgebra de Lie.

Seja $k\langle X\rangle$ a k-álgebra associativa livre gerada por X, tal como no capítulo anterior. Podemos identificar $\mathcal{L}$ com o k-submódulo de $k\langle X\rangle$ gerado por X e, assim, teremos o produto de Lie operando sobre os elementos desse submódulo.

Seja I o ideal (bilateral) de $k\langle X\rangle$ gerado por todos os elementos da forma

$$ab - ba - [a, b],$$

onde a e b percorrem $\mathcal{L}$, e seja $k[\mathcal{L}] = k\langle X\rangle/I$. Se indicarmos por $i : \mathcal{L} \longrightarrow k\langle X\rangle$ a inclusão de $\mathcal{L}$ em $k\langle X\rangle$ e por $\pi : k\langle X\rangle \longrightarrow k[\mathcal{L}]$ a projeção canônica de $k\langle X\rangle$ em $k[\mathcal{L}]$, então $j = \pi i : \mathcal{L} \longrightarrow (k\langle X\rangle/I)_L$ é um homomorfismo de álgebras de Lie e o par $(k[\mathcal{L}], j)$ é a álgebra envolvente universal de $\mathcal{L}$. De fato, dados $\mathcal{A}$ uma álgebra associativa e $\theta : \mathcal{L} \longrightarrow \mathcal{A}_L$ um homomorfismo de álgebras de Lie, pela propriedade universal de que goza $k\langle X\rangle$, a função $\theta|_X : X \longrightarrow \mathcal{A}$, restrição de θ a X, pode ser estendida de maneira única a um homomorfismo de álgebras associativas $\theta' : k\langle X\rangle \longrightarrow \mathcal{A}$, o que quer dizer que o homomorfismo θ' satisfaz $\theta|_X = \theta' i|_X$, onde $i|_X$ indica a restrição de i a X, ou seja, a inclusão de X em $k\langle X\rangle$. Como X gera $\mathcal{L}$, θ' também satisfaz $\theta = \theta' i$. Assim, se $a, b \in \mathcal{L}$, então

$$\begin{aligned}
\theta'(ab - ba - [a, b]) &= \theta'(a)\theta'(b) - \theta'(b)\theta'(a) - \theta'([a, b]) \\
&= \theta' i(a)\theta' i(b) - \theta' i(b)\theta' i(a) - \theta' i([a, b]) \\
&= \theta(a)\theta(b) - \theta(b)\theta(a) - \theta([a, b]) \\
&= 0.
\end{aligned}$$

Logo, $I \subseteq ker(\theta')$ e, portanto, a função $\theta'' : k[\mathcal{L}] \longrightarrow \mathcal{A}$ dada por $\theta''(f + I) = \theta'(f)$ é um homomorfismo de álgebras associativas que verifica $\theta' = \theta''\pi$. Assim, $\theta = \theta' i =$

$(\theta''\pi)i = \theta''(\pi i) = \theta''j$. Além disso, θ'' é o único homomorfismo de álgebras associativas $\varphi : k[\mathcal{L}] \longrightarrow \mathcal{A}$ que verifica $\theta = \varphi j$, pois $k[\mathcal{L}]$ é gerada por $j(\mathcal{L})$ como k-álgebra.

Dado $a \in \mathcal{L}$, denotaremos $a' = a + I$.

Seja $\preceq$ uma ordem total em X. Pela k-bilinearidade do produto de Lie $[\ ,\ ]$ em $\mathcal{L}$ e do comutador $xy - yx$, o ideal I pode ser gerado pelos elementos $xy - yx - [x, y]$ com $x, y \in X$. Pela antisimetria de $[\ ,\ ]$ e do comutador $xy - yx$, os elementos acima com $x \prec y$ geram todo o ideal.

É conveniente ressaltar que a álgebra de Lie $\mathcal{L}$ com que estamos trabalhando nesta seção é, por definição, livre como k-módulo. O estudo de objetos livres é bastante difícil e questões sobre o caráter livre de objetos relacionados a um objeto livre dado, na maioria dos casos mais genéricos, ainda não têm resposta. O Teorema PBW responde uma questão dessa natureza em um caso específico.

Teorema 3.1 (PBW) *A álgebra $k[\mathcal{L}]$ olhada como k-módulo é livre de base consistindo de todos os produtos $x'y' \ldots z'$ tais que $x, y, \ldots, z \in X$ com $x \preceq y \preceq \cdots \preceq z$ e do elemento $1 + I$, onde 1 é o elemento unidade de $k\langle X\rangle$.*

Prova Seja S o sistema de reduções que consiste dos pares

$$\sigma_{yx} = (W_{\sigma_{yx}}, f_{\sigma_{yx}}),$$

onde $W_{\sigma_{yx}} = yx$ e $f_{\sigma_{yx}} = xy - [x, y]$, para todos $x, y \in X$ tais que $x \prec y$. Dessa maneira, o ideal I definido acima é o ideal gerado pelas diferenças $W_\sigma - f_\sigma$, onde σ percorre o conjunto S.

Vejamos quais são os elementos irredutíveis de $k\langle X\rangle$ segundo o sistema de redução S definido acima. Para tanto, basta verificarmos quais são os monômios irredutíveis segundo S. Primeiramente observamos que o monômio 1 (ou seja, a palavra vazia) é trivialmente irredutível. Além disso, todos os monômios do tipo $x_1x_2 \ldots x_n$, com $x_i \in X$ e $x_i \preceq x_{i+1}$, para $i = 1, \ldots, n-1$ são irredutíveis, pois os elementos de S só atuam em monômios $y_1y_2 \ldots y_m$ onde há ao menos uma inversão do tipo $y_{j+1} \prec y_j$. É fácil ver que esses são os únicos monômios irredutíveis segundo S.

Definimos o *índice* de um monômio $x_1x_2 \ldots x_n \in X$, denotado por $ind(x_1x_2 \ldots x_n)$, como o número de pares (i, j) tais que $i < j$ e $x_j \prec x_i$. Mais precisamente,

$$ind(x_1x_2 \ldots x_n) = \sum_{i<j} \varepsilon_{ij}, \quad \text{onde } \varepsilon_{ij} = \begin{cases} 0 & \text{se } x_i \preceq x_j \\ 1 & \text{se } x_j \prec x_i \end{cases}.$$

Por exemplo, $ind(x_1x_2\ldots x_n) = 0$ se $x_1 \preceq x_2 \preceq \cdots \preceq x_n$ e $ind(x_1x_2\ldots x_n) = \frac{n(n-1)}{2}$ se $x_n \prec x_{n-1} \prec \cdots \prec x_1$. O *comprimento* de um monômio $A = x_1x_2\ldots x_n$, onde $x_i \in X$, é o número natural definido por $cpt(A) = n$. Convencionamos que o comprimento da palavra vazia 1 é zero, isto é, $cpt(1) = 0$. (A palavra vazia 1 será o único monômio cujo comprimento é zero.) Diremos que dois monômios $A, B \in \langle X\rangle$ são do mesmo *tipo*, se $A = x_1x_2\ldots x_n$, com $x_i \in X$ e $B = x_{\tau(1)}x_{\tau(2)}\ldots x_{\tau(n)}$, onde τ é uma permutação dos números $1, 2, \ldots, n$, ou mais resumidamente, $\tau \in S_n$. Quando A e B são do mesmo tipo é imediato que $cpt(A) = cpt(B)$.

Vamos introduzir uma ordem parcial $\leq$ no conjunto $\langle X\rangle$ dos monômios da seguinte maneira. Dados dois monômios $A, B \in \langle X\rangle$, definimos $A < B$ se $cpt(A) < cpt(B)$ ou se A e B são do mesmo tipo e $ind(A) < ind(B)$. A ordem parcial em $\langle X\rangle$ com que trabalharemos será dada por

$$A \leq B \text{ se e somente se } A < B \text{ ou } A = B.$$

Faremos a seguir algumas verificações que nos garantirão a inclusão dessa situação como caso particular da situação no enunciado do Teorema 2.1.

(i) $\leq$ é uma ordem parcial de semigrupo em $\langle X\rangle$: A função $cpt : \langle X\rangle \longrightarrow \mathbb{N}$ definida acima goza da seguinte propriedade. Se $P, M \in \langle X\rangle$, então $cpt(PM) = cpt(P) + cpt(M)$, isto é, *cpt é aditiva.* Sejam D e E dois monômios arbitrários de $\langle X\rangle$. Suponha que $A, B \in \langle X\rangle$ são monômios tais que $A < B$. Se $cpt(A) < cpt(B)$, então $cpt(DAE) = cpt(D) + cpt(A) + cpt(E) < cpt(D) + cpt(B) + cpt(E) = cpt(DBE)$. Portanto, neste caso, $DAE < DBE$. Suponha agora que $A = x_1x_2\ldots x_n, B = x_{\tau(1)}x_{\tau(2)}\ldots x_{\tau(n)}$ ($\tau \in S_n$) e $ind(A) < ind(B)$. É imediato que DAE e DBE são do mesmo tipo. Neste ponto introduziremos uma nova função de duas variáveis, $Ind : \langle X\rangle \times \langle X\rangle \longrightarrow \mathbb{N}$, que nos auxiliará a mostrar que $ind(DAE) < ind(DBE)$, apesar desse fato parecer óbvio à primeira vista. Dados dois monômios $P = y_1y_2\ldots y_n$ e $M = z_1z_2\ldots z_m$ ($y_i, z_j \in X$), definimos o *índice relativo* de P em relação a M por

$$Ind(P, M) = \sum_{i,j} \eta_{i,j}, \text{ onde } \eta_{i,j} = \begin{cases} 0 & \text{se } y_i \preceq z_j \\ 1 & \text{se } z_j \prec y_i \end{cases}.$$

É imediato verificar que, se $P, P', M, M' \in \langle X\rangle$ são monômios tais que P e P' são do mesmo tipo e M e M' são do mesmo tipo, então $Ind(P, M) = Ind(P', M) = Ind(P, M') =$

$Ind(P', M')$. De verificação um pouco mais trabalhosa, porém não mais complicada, é a validade da seguinte fórmula:

$$ind(PM) = ind(P) + ind(M) + Ind(P, M).$$

Tendo em mãos tais identidades, sobre o caso que estamos estudando, podemos afirmar que $Ind(A, E) = Ind(B, E)$ e que $Ind(D, AE) = Ind(D, BE)$. Assim,

$$\begin{aligned} ind(DAE) &= ind(D) + ind(AE) + Ind(D, AE) \\ &= ind(D) + ind(A) + ind(E) + Ind(A, E) + Ind(D, AE) \\ &< ind(D) + ind(B) + ind(E) + Ind(B, E) + Ind(D, BE) = ind(DBE), \end{aligned}$$

e, portanto, $DAE < DBE$.

(ii) $\leq$ *e* S *são compatíveis:* Seja $\sigma_{yx} \in S$ um elemento arbitrário. Por definição de S, temos $x \prec y$ e, usando as notações do capítulo anterior, $W_{\sigma_{yx}} = yx$ e $f_{\sigma_{yx}} = xy - [x, y]$. Como $xy < yx$ (pois $ind(xy) = 0$ e $ind(yx) = 1$) e $[x, y] \in \mathcal{L}$ (portanto $[x, y] = \sum_i \lambda_i z_i$, com $\lambda_i \in k$ e $z_i \in \mathcal{L}$ e, assim, $cpt(z_i) = 1 < 2 = cpt(yx)$, para todo i, donde conclui-se que $z_i < yx$ para todo i), temos que $f_{\sigma_{yx}}$ é combinação linear de monômios $< W_{\sigma_{yx}}$.

(iii) $\leq$ *tem condição de cadeia descendente:* Conseqüência imediata da definição da ordem parcial $\leq$.

Em vista de *(i)*, *(ii)*, *(iii)* acima, já podemos aplicar o Teorema 2.1 à nossa situação. O que faremos em seguida é estudar as ambigüidades de S (e concluir que todas elas são resolúveis com respeito a $\leq$). Porém, antes disso, faremos uma observação que resultará de muita ajuda nesse estudo.

Sejam $a, b \in \mathcal{L}$ e $C \in \langle X \rangle$ um monômio de comprimento maior do que 2 (ou seja, $cpt(C) > 2$). Afirmo que $ab - ba - [a, b] \in I_C$. De fato, sejam $x, y \in X$ dois elementos (distintos) da base de $\mathcal{L}$ arbitrários. Se $y \prec x$, então $xy - yx - [x, y] = xy - (yx - [y, x]) = W_{\sigma_{xy}} - f_{\sigma_{xy}} \in I_C$, pois $cpt(W_{\sigma_{xy}}) = 2 < cpt(C)$, o que implica $W_{\sigma_{xy}} < C$. Se, por outro lado, $x \prec y$, então $xy - yx - [x, y] = -(yx - (xy - [x, y])) = -(W_{\sigma_{yx}} - f_{\sigma_{yx}})$ e, novamente, $xy - yx - [x, y] \in I_C$. Pela bilinearidade de $ab - ba - [a, b]$, como I_C é um submódulo, segue o resultado.

No caso em que estamos estudando não existem ambigüidades de inclusão, pois todos os monômios W_σ, com $\sigma \in S$, têm o mesmo comprimento, a saber, $cpt(W_\sigma) = 2$. Verifica-se por inspeção nos elementos σ de S que as ambigüidades de superposição que ocorrem

em S são precisamente as 5-uplas

$$(\sigma_{zy}, \sigma_{yx}, z, y, x),$$

com $x, y, z \in X$ e $x \prec y \prec z$. Passemos a estudá-las.

Seja $(\sigma_{zy}, \sigma_{yx}, z, y, x)$ uma ambigüidade de superposição em S. Para podermos afirmar sobre a resolubilidade de $(\sigma_{zy}, \sigma_{yx}, z, y, x)$ com respeito à ordem $\leq$, precisamos analisar o elemento $r_{1\sigma_{zy}x}(zyx) - r_{z\sigma_{yx}1}(zyx) = (yzx - [y,z]x) - (zxy - z[x,y])$. Tendo em vista o Lema 2.6 do capítulo anterior, vamos realizar mais algumas reduções nos elementos $yzx - [y,z]x$ e $zxy - z[x,y]$. Comecemos por $yzx - [y,z]x$:

$$\begin{aligned} r_{y\sigma_{zx}1}(yzx - [y,z]x) &= r_{y\sigma_{zx}1}(yzx) - [y,z]x \\ &= yxz - y[x,z] - [y,z]x. \end{aligned}$$

Vamos realizar mais uma redução para obtermos um termo xyz.

$$\begin{aligned} r_{1\sigma_{yx}z}(yxz - y[x,z] - [y,z]x) &= r_{1\sigma_{yx}z}(yxz) - y[x,z] - [y,z]x \\ &= xyz - [x,y]z - y[x,z] - [y,z]x. \end{aligned}$$

Procederemos de maneira análoga com $zxy - z[x,y]$ a fim de "reduzí-lo" a um elemento que contenha um termo xyz:

$$\begin{aligned} r_{1\sigma_{zx}y}(zxy - z[x,y]) &= r_{1\sigma_{zx}y}(zxy) - z[x,y] \\ &= xzy - [x,z]y - z[x,y]. \end{aligned}$$

Apliquemos agora a redução

$$\begin{aligned} r_{x\sigma_{zy}1}(xzy - [x,z]y - z[x,y]) &= r_{x\sigma_{zy}1}(xzy) - [x,z]y - z[x,y] \\ &= xyz - x[y,z] - [x,z]y - z[x,y]. \end{aligned}$$

Temos, assim,

$$\begin{aligned} & r_{1\sigma_{yx}z} r_{y\sigma_{zx}1}(yzx - [y,z]x) - r_{x\sigma_{zy}1} r_{1\sigma_{zx}y}(zxy - z[x,y]) \\ &= (xyz - [x,y]z - y[x,z] - [y,z]x) - (xyz - x[y,z] - [x,z]y - z[x,y]) \\ &= (x[y,z] - [y,z]x) - (y[x,z] - [x,z]y) - (z[x,y] - [x,y]z). \end{aligned}$$

Como $cpt(zyx) = 3 > 2$, pela observação feita acima, temos

$$\begin{aligned} x[y,z] - [y,z]x - [x,[y,z]] &\in I_{zyx} \\ y[x,z] - [x,z]y - [y,[x,z]] &\in I_{zyx} \\ z[x,y] - [x,y]z - [z,[x,y]] &\in I_{zyx}. \end{aligned}$$

Mas, pela anti-simetria de [,] e pela identidade de Jacobi,

$$-[x,[y,z]] + [y,[x,z]] + [z,[x,y]] = -([x,[y,z]] + [y,[z,x]] + [z,[x,y]]) = 0.$$

Logo,

$$\begin{aligned} &(x[y,z] - [y,z]x) - (y[x,z] - [x,z]y) - (z[x,y] - [x,y]z) \\ &= (x[y,z] - [y,z]x - [x,[y,z]]) - (y[x,z] - [x,z]y - [y,[x,z]]) \\ &\quad - (z[x,y] - [x,y]z - [z,[x,y]]) \in I_{zyx}. \end{aligned}$$

Portanto, pelo Lema 2.6, a ambigüidade $(\sigma_{zy}, \sigma_{yx}, z, y, x)$ é resolúvel com respeito a $\leq$. Logo, todas as ambigüidades de S são resolúveis com respeito a $\leq$. Pela equivalência $(a') \Leftrightarrow (c)$ do Teorema 2.1, as imagens dos monômios irredutíveis de $k\langle X\rangle$ segundo S formam uma base para $k[\mathcal{L}]$. ■

Existem várias outras demonstrações desse teorema. Uma de especial simplicidade e clareza é a que aparece em [9, Sec V.2], também apresentada em [8, Sec II.4].

3.2 Identidades

A aplicação do Teorema 2.1 a algumas situações mais particulares, que são justamente aquelas em que o Teorema se mostrará mais útil, revela que a verificação das hipóteses acerca da condição de cadeia da ordem parcial de semigrupo e da compatibilidade dessa ordem com o sistema de redução são um tanto quanto elementares. No entanto, para obtermos a informação sobre a existência de uma base formada por classes de elementos irredutíveis é necessário, ainda, que se verifique a redutibilidade única de todos os elementos de $k\langle X\rangle$ ou a resolubilidade de todas as ambigüidades do sistema de redução. Essas verificações são sensivelmente mais trabalhosas e mais complexas que as citadas anteriormente. Para tanto, nesta seção, vamos introduzir alguns resultados que

apresentam condições equivalentes às que afirmam sobre a resolubilidade de ambigüidades com respeito à ordem introduzida, aproveitando-se de identidades sabidamente válidas em $k\langle X\rangle$, e que facilitam um pouco o trabalho de verificação dessas condições. No que segue, k é um anel associativo, comutativo e com unidade.

Lema 3.1 *Sejam S um sistema de redução em uma álgebra livre $k\langle X\rangle$ e $\leq$ uma ordem parcial de semigrupo em $\langle X\rangle$ de modo que $\leq$ e S sejam compatíveis. Seja (σ, τ, A, B, C) uma ambigüidade de superposição (resp. inclusão) de S e suponha que*

$$f_1 + f_2 + \cdots + f_n = 0 \tag{3.4}$$

seja uma equação em $k\langle X\rangle$ tal que apenas dois termos dela, digamos f_i e f_j (com $i < j$), envolvam o monômio ABC com coeficiente diferente de 0, e, ainda, que esses coeficientes sejam elementos inversíveis de k. Então a ambigüidade (σ, τ, A, B, C) é resolúvel com respeito a $\leq$ se e somente se

$$f_1 + \cdots + r_{A\sigma 1}(f_i) + \cdots + r_{1\sigma C}(f_j) + \cdots + f_n \in I_{ABC}. \tag{3.5}$$

(Formulação análoga para o caso de uma ambigüidade de inclusão.)

Prova Suponhamos que o coeficiente de ABC em f_i seja λ. Portanto o coeficiente de ABC em f_j é $-\lambda$, uma vez que somente nos termos f_i e f_j os coeficientes de ABC são não nulos. A demonstração será feita apenas para o caso de ambigüidades de superposição. A demonstração para uma ambigüidade de inclusão é totalmente análoga.

Suponhamos que a ambigüidade (σ, τ, A, B, C) seja resolúvel com respeito a $\leq$. Então $f_\sigma C - Af_\tau \in I_{ABC}$, o que implica que $r_{1\sigma C}(f_i) - r_{A\tau 1}(f_i) = \lambda(f_\sigma C - Af_\tau) \in I_{ABC}$. Por outro lado, como vale (3.4), temos $f_1 + \cdots + r_{A\tau 1}(f_i) + \cdots + r_{A\tau 1}(f_j) + \cdots + f_n = r_{A\tau 1}(f_1 + \cdots + f_n) = 0 \in I_{ABC}$. Logo $f_1 + \cdots + r_{A\tau 1}(f_i) + \cdots + r_{1\sigma C}(f_j) + \cdots + f_n = (r_{1\sigma C}(f_i) - r_{A\tau 1}(f_i)) + (f_1 + \cdots + r_{A\tau 1}(f_i) + \cdots + r_{A\tau 1}(f_j) + \cdots + f_n) \in I_{ABC}$.

Suponhamos, agora, que vale a fórmula (3.5). Por (3.4), temos $f_1 + \cdots + r_{A\tau 1}(f_i) + \cdots + r_{A\tau 1}(f_j) + \cdots + f_n = r_{A\tau 1}(f_1 + \cdots + f_n) = 0 \in I_{ABC}$. Assim, $r_{1\sigma C}(f_i) - r_{A\tau 1}(f_i) = (f_1 + \cdots + r_{1\sigma C}(f_i) + \cdots + r_{A\tau 1}(f_j) + \cdots + f_n) - (f_1 + \cdots + r_{A\tau 1}(f_i) + \cdots + r_{A\tau 1}(f_j) + \cdots + f_n) \in I_{ABC}$, pois estamos supondo que vale (3.5). Logo, $f_\sigma C - Af_\tau = \lambda^{-1}(r_{1\sigma C}(f_i) - r_{A\tau 1}(f_i)) \in I_{ABC}$. Isso demonstra o lema. ■

A seguir, serão enunciados e demonstrados três corolários do Lema 3.1 que têm como exclusiva finalidade especializar esse lema para o caso da aplicação que será apresentada

no final desta seção. A frase "Sejam S um sistema de redução em uma álgebra livre $k\langle X\rangle$ e $\leq$ uma ordem parcial de semigrupo em $\langle X\rangle$ de modo que $\leq$ e S sejam compatíveis." que consta do enunciado do Lema 3.1 será tomada como hipótese para todos os corolários subsequentes. Deve-se ressaltar ainda que o símbolo $[x,y]$ significará, nesta seção, o comutador de x e y, isto é, $[x,y] = xy - yx$, uma vez que não estamos mais tratando de álgebras de Lie.

Corolário 3.1 *Suponha que existam $x, y, z \in X$ tais que $yxz < zyx$ e $xzy < zyx$ e que o sistema de redução S contenha os pares*

$$\begin{aligned} \sigma &= (zy, yz - a) \\ \tau &= (yx, xy - b), \end{aligned}$$

com $a, b \in k\langle X\rangle$. Então a ambigüidade (σ, τ, z, y, x) é resolúvel com respeito a $\leq$ se e somente se

$$[x,a] + [y,[z,x]] + [z,b] \in I_{zyx}. \tag{3.6}$$

Prova Denotemos $f_1 = [x,[y,z]]$, $f_2 = [y,[z,x]]$, $f_3 = [z,[x,y]]$. Então, como toda álgebra associativa satisfaz a identidade de Jacobi para o comutador, temos

$$f_1 + f_2 + f_3 = 0.$$

Verifica-se facilmente que os coeficientes de zyx em f_1, f_2, f_3 são respectivamente $1, 0, -1$. Pelo Lema 3.1, (σ, τ, z, y, x) é resolúvel com respeito a $\leq$ se e somente se

$$r_{1\sigma x}(f_1) + f_2 + r_{z\tau 1}(f_3) \in I_{zyx}. \tag{3.7}$$

Resta, portanto, verificar que (3.7) $\Longleftrightarrow$ (3.6). Vejamos, $r_{1\sigma x}(f_1) + f_2 + r_{z\tau 1}(f_3) = -(xzy + ax) + f_2 + (zb + yxz)$. Como $xzy < zyx$, temos $xzy - xyz + xa = x(zy - (yz - a)) = x(W_\sigma - f_\sigma) \in I_{zyx}$. Analogamente, como $yxz < zyx$, temos $-yxz + xyz - bz = -(yx - (xy - b))z = -(W_\tau - f_\tau) \in I_{zyx}$. Portanto, $(xzy + xa) - (yxz + bz) = (xzy - xyz + xa) + (-yxz + xyz - bz) \in I_{zyx}$.

Logo, $-(xzy + ax) + f_2 + (zb + yxz) \in I_{zyx} \Longleftrightarrow \{(-(xzy + ax) + f_2 + (zb + yxz)\} + \{(xzy + xa) - (yxz + bz)\} \in I_{zyx}$. Mas $\{(-(xzy + ax) + f_2 + (zb + yxz)\} + \{(xzy + xa) - (yxz + bz)\} = (xa - ax) + f_2 + (zb - bz)$. Assim,

$$r_{1\sigma x}(f_1) + f_2 + r_{z\tau 1}(f_3) \in I_{zyx} \Longleftrightarrow [x,a] + [y,[z,x]] + [z,b] \in I_{zyx}$$

e o corolário está demonstrado. ■

Lembremos que se R é uma k-álgebra associativa e se $x \in R$, a função $ad\ x : R \longrightarrow R$ definida por $(ad\ x)(y) = [x, y]$, para $y \in R$, é uma **derivação** em R, isto é, $ad\ x$ é k-linear e satisfaz $(ad\ x)(yz) = (ad\ x)(y)z + y(ad\ x)(z)$. Essa função é chamada *derivação interna determinada por* x ou, mais simplesmente, *função adjunta determinada por* x.

Corolário 3.2 *Suponha que a característica do anel k seja um primo ímpar p (isso será denotado por car $k = p$), isto é, k é uma $\mathbb{Z}_p$-álgebra comutativa. Suponha, ainda, que $x, y \in X$ são elementos tais que $xy < yx$ (resp. $yx < xy$) e que o sistema de redução S contenha os pares*

$$\begin{aligned} \sigma &= (yx, xy - a) \quad (resp.\ (xy, yx + a)) \\ \tau &= (x^p, b), \end{aligned}$$

com $a, b \in k\langle X\rangle$. Então a ambigüidade $(\sigma, \tau, y, x, x^{p-1})$ (resp. $(\tau, \sigma, x^{p-1}, x, y)$) é resolúvel com respeito a $\leq$ se e somente se

$$(ad\ x)^{p-1}(a) - (ad\ b)(y) \in I_{yx^p}\ (resp.\ I_{x^py}). \tag{3.8}$$

Prova A demonstração da versão deste corolário contida nos parênteses é análoga à original e, portanto, será suprimida. Verifica-se que em uma álgebra associativa sobre um anel R de característica p, p primo ímpar, vale a seguinte identidade:

$$(ad\ a)^p(b) = (ad\ a^p)(b),$$

para todo $a, b \in R$.(Ver [9, p. 186 (60)].) Em particular, no nosso caso, vale

$$(ad\ x)^p(y) - (ad\ x^p)(y) = 0.$$

Denotaremos $f_1 = (ad\ x)^p(y)$ e $f_2 = -(ad\ x^p)(y)$. Como os coeficientes de yx^p em f_1 e f_2 são, respectivamente, -1 e 1, podemos aplicar o Lema 3.1 e concluir que $(\sigma, \tau, y, x, x^{p-1})$ é resolúvel com respeito a $\leq$ se e somente se

$$r_{1\sigma x^{p-1}}((ad\ x)^p(y)) - r_{y\tau 1}((ad\ x^p)(y)) \in I_{yx^p}. \tag{3.9}$$

Novamente, é suficiente, portanto, mostrarmos a equivalência (3.8) $\Longleftrightarrow$ (3.9).

Primeiramente, como $r_{y\tau 1}((ad\ x^p)(y)) = r_{y\tau 1}(x^p y - yx^p) = x^p y - yb$, temos

$$r_{y\tau 1}((ad\ x^p)(y)) - (ad\ b)(y) \in I_{yx^p},$$

pois $r_{y\tau 1}((ad\ x^p)(y)) - (ad\ b)(y) = x^p y - yb - by + yb = (x^p - b)y$ e $x^p y < yx^p$, uma vez que $xy < yx$ e $\leq$ é ordem parcial de semigrupo.

Por outro lado, demonstra-se por indução finita que $r_{1\sigma x^{n-1}}((ad\,x)^n(y)) - (ad\,x)^{n-1}(a) \in I_{yx^n}$, para todo $n > 1$. (Ver Apêndice no final deste capítulo.) Em particular, temos

$$r_{1\sigma x^{p-1}}((ad\ x^p)(y)) - (ad\ x)^{p-1}(a) \in I_{yx^p}.$$

Logo, podemos escrever

$$\begin{aligned}(ad\ x)^{p-1}(a) - (ad\ b)(y) &= \{r_{1\sigma x^{p-1}}((ad\ x^p)(y)) - r_{y\tau 1}((ad\ x^p)(y))\} \\ &\quad - \{r_{1\sigma x^{p-1}}((ad\ x^p)(y)) - (ad\ x)^{p-1}(a)\} \\ &\quad + \{r_{y\tau 1}((ad\ x^p)(y)) - (ad\ b)(y)\}\end{aligned}$$

e, portanto, tendo em vista as considerações anteriores, segue que

$$(ad\ x)^{p-1}(a) - (ad\ b)(y) \in I_{yx^p} \Longleftrightarrow r_{1\sigma x^{p-1}}((ad\ x)^p(y)) - r_{y\tau 1}((ad\ x^p)(y)) \in I_{yx^p},$$

o que demonstra o corolário. ■

Corolário 3.3 *Seja $x \in X$ e n um inteiro positivo. Suponha que o sistema de redução S contenha um par do tipo*

$$\sigma = (x^n, a),$$

com $a \in k\langle X\rangle$. Então todas as ambigüidades do tipo $(\sigma, \sigma, x^i, x^{n-i}, x^i)$, para $i < n$, são resolúveis com respeito a $\leq$ se e somente se

$$[a, x] \in I_{x^{n+1}} \tag{3.10}$$

Prova Toda álgebra associativa R satisfaz $[z^m, z^j] = 0$, qualquer que seja $z \in R$ e para todo $m, j \in \mathbb{N}$. Logo, em $k\langle X\rangle$ vale a equação $x^{n+i} - x^{i+n} = [x^n, x^i] = 0$, para todo $i \in \mathbb{N}$. É evidente que não há distinção entre x^{n+i} e x^{i+n}, mas as notações diferenciadas serão mantidas por motivos de conveniência. Fixado $i \in \mathbb{N}$, denotaremos $f_1 = x^{n+i}$ e $f_2 = x^{i+n}$. Como os coeficientes de x^{n+i} $(= x^{i+n})$ em f_1 e f_2 são respectivamente 1 e -1,

podemos aplicar o Lema 3.1. Assim, uma ambigüidade $(\sigma, \sigma, x^i, x^{n-i}, x^i)$ é resolúvel com respeito a $\leq$ se e somente se

$$r_{1\sigma x^i}(x^{n+i}) - r_{x^i\sigma 1}(x^{i+n}) \in I_{x^{n+i}}. \tag{3.11}$$

Assim, resta-nos demonstrar a equivalência (3.10) $\Longleftrightarrow$ (3.11). Vejamos, $r_{1\sigma x^i}(x^{n+i}) = ax^i$ e $r_{x^i\sigma 1}(x^{i+n}) = x^i a$. Dessa maneira, temos $r_{1\sigma x^i}(x^{n+i}) - ax^i = 0 \in I_{x^{n+i}}$ e $r_{x^i\sigma 1}(x^{i+n}) - x^i a = 0 \in I_{x^{n+i}}$. Portanto, podemos escrever

$$\begin{aligned} [a, x^i] \;=\; ax^i - x^i a \;=\; & \{r_{1\sigma x^i}(x^{n+i}) - r_{x^i\sigma 1}(x^{i+n})\} \\ & - \{r_{1\sigma x^i}(x^{n+i}) - ax^i\} \\ & + \{r_{x^i\sigma 1}(x^{i+n}) - x^i a\}, \end{aligned}$$

o que implica

$$[a, x^i] \in I_{x^{n+i}} \Longleftrightarrow r_{1\sigma x^i}(x^{n+i}) - r_{x^i\sigma 1}(x^{i+n}) \in I_{x^{n+i}}.$$

Se mostramos que

$$[a, x^i] \in I_{x^{n+i}} \Longleftrightarrow [a, x] \in I_{x^{n+1}},$$

para todo $i \in \mathbb{N}$, a demonstração do corolário estará terminada. De fato, a prova é feita por indução em $i \in \mathbb{N}$. Se $[a, x^i] \in I_{x^{n+i}}$, então $ax^{i+1} - x^i ax \in I_{x^{n+i+1}}$ e $xax^i - x^{i+1}a \in I_{x^{n+i+1}}$. Portanto, $[a, x^{i+1}] + (xax^i - x^i ax) \in I_{x^{n+i+1}}$. Mas $xax^i - x^i ax = x[a, x^{i-1}]x \in I_{x^{n+i+1}}$, por hipótese de indução e pelo Lema 2.7. ■

Utilizaremos, agora, o Teorema 2.1 e os corolários do Lema 3.1 para efetuar o cálculo de uma base para uma álgebra definida por geradores e relações. Essa álgebra aparece em um artigo de Taft e Wilson [17], no qual os autores apresentam o primeiro exemplo de uma álgebra de Hopf de dimensão finita sobre um corpo de característica p, p primo, e que tem algumas propriedades que eles buscavam. Essa álgebra será introduzida no exemplo abaixo.

EXEMPLO: Seja k um corpo de característica $p \neq 2$ e seja R a k-álgebra presentada por geradores x, y, z e relações

$$\begin{aligned} &[x, y] = x, \quad [y, z] = -z, \quad [x, z] = x^2/2, \\ &x^p = 0, \qquad y^p = y, \qquad z^p = 0. \end{aligned}$$

Afirma-se que R tem dimensão p^3, como k-espaço vetorial, com base

$$\{x^\alpha y^\beta z^\gamma : 0 \leq \alpha, \beta, \gamma < p\}.$$

Faremos uma demonstração da afirmação acima. Comecemos por construir a k-álgebra livre gerada por $\{x, y, z\}$, que será denotada por $k\langle x, y, z\rangle$, e um sistema de redução $S = \{\sigma_i : 1 \leq i \leq 6\}$, onde os pares σ_i são definidos da seguinte maneira:

$$\begin{array}{lll} \sigma_1 = (x^p, 0), & \sigma_2 = (y^p, y), & \sigma_3 = (z^p, 0) \\ \sigma_4 = (yx, xy - x), & \sigma_5 = (zy, yz + z), & \sigma_6 = (zx, xz - x^2/2). \end{array}$$

O semigrupo $\langle x, y, z\rangle$ será dotado de uma ordem parcial $\leq$, que é definida como segue. Dados $A, B \in \langle x, y, z\rangle$, defino $A < B$ se e somente se $cpt(A) < cpt(B)$ ou $cpt(A) = cpt(B)$ e A precede B lexicograficamente em relação à seguinte ordem total definida em $\{x, y, z\}$: $x < y < z$.

Verifica-se facilmente que $\leq$ é uma ordem parcial de semigrupo, que $\leq$ tem condição de cadeia descendente e que $\leq$ e S são compatíveis. Os monômios irredutíveis segundo S são justamente aqueles da base alegada, pois eles são obviamente irredutíveis e um monômio irredutível não pode conter subpalavras dos tipos yx, zy, zx e nem potências de x, y e z maiores do que p.

Neste ponto já temos verificadas todas as hipóteses do Teorema 2.1. Provaremos em seguida que todas as ambigüidades de $k\langle x, y, z\rangle$ são resolúveis segundo S e, então, poderemos concluir sobre a base de monômios irredutíveis.

Primeiramente, pode-se notar que S não contém ambigüidades de inclusão, pois não existem σ_i e σ_j $(i \neq j)$, em S tais que W_{σ_i} seja subpalavra de W_{σ_j}. As ambigüidades de superposição de S, como é fácil de se verificar estudando dois a dois os pares de S, estão listadas abaixo.

$$\begin{array}{llll} (i) & (\sigma_1, \sigma_1, x^i, x^{p-i}, x^i) & (vi) & (\sigma_6, \sigma_1, z, x, x^{p-1}) \\ (ii) & (\sigma_2, \sigma_2, y^i, y^{p-i}, y^i) & (vii) & (\sigma_5, \sigma_2, z, y, y^{p-1}) \\ (iii) & (\sigma_3, \sigma_3, z^i, z^{p-i}, z^i) & (viii) & (\sigma_2, \sigma_4, y^{p-1}, y, x) \\ (iv) & (\sigma_5, \sigma_4, z, y, x) & (ix) & (\sigma_3, \sigma_5, z^{p-1}, z, y) \\ (v) & (\sigma_4, \sigma_1, y, x, x^{p-1}) & (x) & (\sigma_3, \sigma_6, z^{p-1}, z, x) \end{array}$$

As três primeiras ambigüidades na realidade são famílias de ambigüidades indexadas por i. Por exemplo, para a família (i), para cada $i < p$, temos uma ambigüidade de

superposição. Vamos utilizar a equivalência $(a') \Longleftrightarrow (c)$ do Teorema 2.1. Para afirmar sobre a redutibilidade das ambigüidades com respeito a $\leq$, utilizaremos os corolários do Lema 3.1.

As ambigüidades (i) são resolúveis com respeito a $\leq$, pois

$$[0, x] = 0 \in I_{x^{p+1}} \quad \text{(Corolário 3.3)}.$$

As ambigüidades (ii) são resolúveis com respeito a $\leq$, pois

$$[y, y] = 0 \in I_{y^{p+1}} \quad \text{(Corolário 3.3)}.$$

As ambigüidades (iii) são resolúveis com respeito a $\leq$, pois

$$[0, z] = 0 \in I_{z^{p+1}} \quad \text{(Corolário 3.3)}.$$

A ambigüidade (iv) é resolúvel com respeito a $\leq$, pois

$$\begin{aligned} [x, -z] + [y, [z, x]] + [z, x] &= 2[z, x] + [y, [z, x]] \\ &= 2zx - 2xz - zxy + xzy + yzx - yxz. \end{aligned}$$

Logo,

$$\begin{aligned} [x, -z] + [y, [z, x]] + [z, x] &= 2(zx - (xz - x^2/2)) - (zx - (xz - x^2/2))y \\ &= + y(zx - (xz - x^2/2)) - \frac{1}{2}(yx - (xy - x))x \\ &= - \frac{1}{2}x(yx - (xy - x)). \end{aligned}$$

Assim, como $zx, zxy, yzx, yx^2, xyx < zyx$, temos $[x, -z] + [y, [z, x]] + [z, x] \in I_{zyx}$ (Corolário 3.1).

A ambigüidade (v) é resolúvel com respeito a $\leq$, pois

$$(ad\ x)^{p-1}(x) - (ad\ 0)(y) = 0 \in I_{yx^p} \quad \text{(Corolário 3.2)}.$$

A ambigüidade (vi) é resolúvel com respeito a $\leq$, pois

$$(ad\ x)^{p-1}(x^2/2) - (ad\ 0)(z) = 0 \in I_{zx^p} \quad \text{(Corolário 3.2)}.$$

A ambigüidade (vii) é resolúvel com respeito a $\leq$, pois vale em geral

$$(ad\ y)^n(z) + (ad\ y)^{n-1}(z) \in I_{zy^{n+1}}, \tag{3.12}$$

para todo $n > 2$. Esse fato pode ser demonstrado por indução finita em n. Denotemos $\varphi_n(y,z) = (ad\ y)^n(z) + (ad\ y)^{n-1}(z)$ e mostremos que $\varphi_n(y,z) \in I_{zy^{n+1}}$, para todo $n > 2$. De fato, $\varphi_2(y,z) = y^2z - 2yzy + zy^2 + yz - zy = (zy - (yz+z))y - y(zy - (yz+z))$. Como $zy^2, yzy < zy^3$, temos $\varphi_2(y,z) \in I_{zy^3}$. Observe, agora, que

$$\begin{aligned}
\varphi_{n+1}(y,z) &= (ad\ y)^{n+1}(z) + (ad\ y)^n(z) \\
&= y(ad\ y)^n(z) - (ad\ y)^n(z)y + y(ad\ y)^{n-1}(z) - (ad\ y)^{n-1}(z)y \\
&= y\{(ad\ y)^n(z) + (ad\ y)^{n-1}(z)\} - \{(ad\ y)^n(z) + (ad\ y)^{n-1}(z)\}y,
\end{aligned}$$

ou seja, $\varphi_{n+1}(y,z) = (ad\ y)(\varphi_n(y,z))$, o que, em vista do Lema 2.7, dá conta do passo de indução.

Tendo em mãos a fórmula (3.12), podemos demonstrar, também por indução finita, que

$$(ad\ y)^{2n}(z) + (ad\ y)(z) \in I_{zy^{2n+1}}, \tag{3.13}$$

para todo $n \in \mathbb{N}$. O caso $n = 1$ já foi verificado acima. Suponha, agora, que a fórmula (3.13) é válida para $n = t$ e mostremos sua validade para $n = t+1$. Temos

$$\begin{aligned}
(ad\ y)^{2(t+1)}(z) + (ad\ y)(z) &= \{(ad\ y)^{2t+2}(z) + (ad\ y)^{2t+1}(z)\} - \{(ad\ y)^{2t+1}(z) \\
&= + (ad\ y)^{2t}(z)\} + \{(ad\ y)^{2t}(z) + (ad\ y)(z)\}.
\end{aligned}$$

Por (3.12), temos $(ad\ y)^{2t+2}(z) + (ad\ y)^{2t+1}(z) \in I_{zy^{2t+3}}$ e $(ad\ y)^{2t+1}(z) + (ad\ y)^{2t}(z) \in I_{zy^{2t+2}} \subseteq I_{zy^{2t+3}}$, e, por hipótese de indução, temos $(ad\ y)^{2t}(z) + (ad\ y)(z) \in I_{zy^{2t+1}} \subseteq I_{zy^{2t+3}}$. Assim o resultado está demonstrado.

Se particularizarmos a fórmula (3.13) para $n = (p-1)/2$, obtemos $(ad\ y)^{p-1}(z) + (ad\ y)(z) \in I_{zy^p}$ e, portanto,

$$(ad\ y)^{p-1}(-z) - (ad\ y)(z) = -((ad\ y)^{p-1}(z) + (ad\ y)(z)) \in I_{zy^p},$$

o que, pelo Corolário 3.2, garante a resolubilidade da ambigüidade (vii) com respeito a $\leq$.

A ambigüidade $(viii)$ é resolúvel com respeito a $\leq$, pois prova-se de maneira análoga ao que foi feito acima que vale, em geral, a fórmula

$$(ad\ y)^{2n}(x) + (ad\ y)(x) \in I_{y^{2n+1}x}, \tag{3.14}$$

para todo $n \in \mathbb{N}$. Novamente, especializando (3.14) para $n = (p-1)/2$, obtemos

$$(ad\ y)^{p-1}(-x) - (ad\ y)(x) = -((ad\ y)^{p-1}(x) + (ad\ y)(x)) \in I_{y^p x},$$

e a resolubilidade da ambigüidade $(viii)$ está verificada via o Corolário 3.2.

A ambigüidade (ix) é resolúvel com respeito a $\leq$, pois

$$(ad\ z)^{p-1}(z) - (ad\ 0)(y) = 0 \in I_{z^p y} \quad \text{(Corolário 3.2)}.$$

O Corolário 3.2 afirma que a ambigüidade (x) será resolúvel com respeito a $\leq$ se e somente se $(ad\ z)^{p-1}(-x^2/2) - (ad\ 0)(x) \in I_{z^p x}$, ou seja, é suficiente verificarmos que $(ad\ z)^{p-1}(x^2/2) \in I_{z^p x}$. Ainda não consegui encontrar uma demonstração para esse fato, mas creio que em pouco tempo devo obtê-la. A maior dificuldade deste caso em comparação com os nove anteriores deve-se ao fato de termos que efetuar cálculos de potências de $ad\ z$ em $x^2/2$ e não mais em x ou y como havia sido feito anteriormente. O fato de Taft e Wilson terem obtido uma demonstração alternativa de que esta álgebra tem dimensão p^3 leva-nos a crer que de fato (x) é resolúvel. No entanto, a demonstração daqueles dois autores não é feita por intermédio do Lema do Diamante, o que a torna inadaptável a esse caso.

Concluindo que a ambigüidade (x) é resolúvel com respeito a $\leq$ e, portanto, que todas as ambigüidades de S são resolúveis com respeito a $\leq$, pelo Teorema 2.1, podemos afirmar que o conjunto das classes dos monômios irredutíveis segundo S, $\{x^\alpha y^\beta z^\gamma + I : 0 \leq \alpha, \beta, \gamma < p\}$, forma uma base para $R = k\langle X\rangle / I$ como k-espaço vetorial e, portanto, a dimensão de R sobre k é p^3.

OBSERVAÇÃO: Se no enunciado do Lema 3.1 adicionarmos a hipótese de que todos os monômios $< ABC$ são de redução única, o que em geral será verdade em toda aplicação útil desse lema, então a hipótese de que dois coeficientes $\neq 0$ de ABC em (3.4) sejam inversíveis de k pode ser enfraquecida, exigindo-se, então, apenas que esses coeficientes não sejam divisores de zero em k.

De fato, suponha que todos os monômios $< ABC$ sejam de redução única. Então temos

$$I_{ABC} = ker(r_S|_{M_{ABC}}),$$

onde M_{ABC} denota o k-submódulo de $k\langle X\rangle$ gerado pelos monômios $< ABC$. Provemos o resultado acima. Por hipótese, o domínio de r_S contém M_{ABC}. Denotemos $g = r_S|_{M_{ABC}}$ e

mostremos que $I_{ABC} = ker(g)$. Por um lado, se $D(W_\sigma - f_\sigma)E \in I_{ABC}$, em particular, temos $DW_\sigma E < ABC$ e, portanto, $DW_\sigma E \in M_{ABC}$. Pelo Lema 2.1, $Df_\sigma E = r_{D\sigma E}(DW_\sigma E)$ é de redução única e vale

$$r_S(Df_\sigma E) = r_S(r_{D\sigma E}(DW_\sigma E)) = r_S(DW_\sigma E).$$

Como $r_S(Df_\sigma E) = g(Df_\sigma E)$, pois $Df_\sigma E \in M_{ABC}$ pela compatibilidade de $\leq$ e S, e $r_S(DW_\sigma E) = g(DW_\sigma E)$, temos $g(D(W_\sigma - f_\sigma)E) = g(DW_\sigma E) - g(Df_\sigma E) = 0$. Logo, $I_{ABC} \subseteq ker(g)$. Por outro lado, se $a \in ker(g)$, então $a \in M_{ABC}$, isto é, a é combinação linear de monômios $< ABC$, e $r_S(a) = 0$. Se tomarmos $(r_1, \ldots, r_n)$ uma seqüencia final em a, temos, pelo Corolário 2.1,

$$a = a - r_S(a) = a - r_n \ldots r_1(a) \in I_{ABC}.$$

Logo, $ker(g) \subseteq I_{ABC}$.

Voltando agora para o nosso problema inicial, fazendo as mudanças propostas acima no enunciado do Lema 3.1 e tomando α como coeficiente de ABC em f_i, se vale (3.5), podemos escrever $\alpha(f_\sigma C - ABC) = r_{1\sigma C}(f_i) - f_i$ e $-\alpha(Af_\tau - ABC) = r_{A\tau 1}(f_j) - f_j$. Assim, $(f_1 + \cdots + r_{1\sigma C}(f_i) + \cdots + r_{A\tau 1}(f_j) + \cdots + f_n) - (f_1 + \cdots + f_n) = \alpha(f_\sigma C - ABC) - \alpha(Af_\tau - ABC) = \alpha(f_\sigma C - Af_\tau)$. Logo, como $I_{ABC} = ker(r_S|_{M_{ABC}})$ e a expressão do lado esquerdo da equação acima pertence a I_{ABC}, temos

$$\alpha r_S(f_\sigma C - Af_\tau) = r_S(\alpha(f_\sigma C - Af_\tau)) = 0.$$

Como $k\langle X\rangle$ é um k-módulo livre, $k\langle X\rangle$ não tem torção, o que, sendo k um anel sem divisores de zero, implica $r_S(f_\sigma C - Af_\tau) = 0$ e, portanto, $f_\sigma C - Af_\tau \in ker(r_S|_{M_{ABC}}) = I_{ABC}$, o que significa que a ambigüidade (σ, τ, A, B, C) é resolúvel com respeito a $\leq$. A afirmação recíproca do Lema 3.1 já prescidia do fato de α ser inversível.

Trabalhamos em toda esta seção com *identidades* em $k\langle X\rangle$. Pode, no entanto, haver situações em que é necessário trabalhar-se com *equações* que se sabe serem válidas no anel R $(= k\langle X\rangle/I)$. Pode-se adaptar o Lema 3.1 para este caso também desde que se possa garantir que a equação em questão deriva de uma fórmula restritiva em $k\langle X\rangle$, como impõe a expressão (3.15) abaixo.

Corolário 3.4 *O Lema 3.1 continua válido se (3.4) é enfraquecido para*

$$f_1 + \cdots + f_n \in I_{ABC}. \tag{3.15}$$

Prova Basta observar que $I_{ABC} \subseteq M_{ABC}$ e, portanto, $r_{A\tau 1}(f_1 + \cdots + f_n) = f_1 + \cdots + f_n \in I_{ABC}$. O resto da prova é idêntico ao que foi feito na prova do Lema 3.1. ■

APÊNDICE

Neste apêndice, nas hipóteses do Corolário 3.2, mostraremos o seguinte

RESULTADO 2: $r_{1\sigma x^{n-1}}((ad\ x)^n(y)) - (ad\ x)^{n-1}(a) \in I_{yx^n}$, para todo $n > 1$.

Para tanto será necessário mostrarmos primeiramente o

RESULTADO 1: $x\{(ad\ x)^n - (ad\ x)^{n-1}(a)\} \in I_{yx^{n+1}}$, para todo $n > 1$.

Demonstrações

1: Vamos definir uma família de funções. Para cada $n > 1$, seja $\varphi_n(x, y, a)$ definida da seguinte maneira.

$$\varphi_n(x, y, a) = x\{(ad\ x)^n - (ad\ x)^{n-1}(a)\}.$$

Queremos, então, mostrar que $\varphi_n(x, y, a) \in I_{yx^{n+1}}$, para todo $n > 1$.

Para $n = 2$, temos

$$\begin{aligned}
\varphi_2(x, y, a) &= x\{(ad\ x)^2(y) - (ad\ x)(a)\} \\
&= x\{(x^2y - 2xyx + yx^2) - (xa - ax)\} \\
&= x\{-x(yx - (xy - a)) + (yx - (xy - a))x\} \\
&= -x^2(yx - (xy - a)) + x(yx - (xy - a))x,
\end{aligned}$$

mas, como $x^2yx < yx^3$, temos $-x^2(yx - (xy - a)) \in I_{yx^3}$ e, como $xyx^2 < yx^3$, temos $x(yx - (xy - a))x \in I_{yx^3}$. Logo, $\varphi_2(x, y, a) \in I_{yx^3}$.

Mostremos, agora, que

$$\varphi_{n+1}(x, y, a) = (ad\ x)(\varphi_n(x, y, a)). \tag{3.16}$$

De fato,

$$\varphi_{n+1}(x, y, a) = x\{(ad\ x)^{n+1}(y) - (ad\ x)^n(a)\}$$

$$
\begin{aligned}
&= x\{x(ad\ x)^n(y) - (ad\ x)^n(y)x\} - x\{x(ad\ x)^{n-1}(a) - (ad\ x)^{n-1}(a)x\} \\
&= x\{x\{(ad\ x)^n(y) - (ad\ x)^{n-1}(a)\}\} - \{x\{(ad\ x)^n(y) - (ad\ x)^{n-1}(a)\}\}x \\
&= (ad\ x)(\varphi_n(x, y, a).
\end{aligned}
$$

Tendo em vista a equação (3.16) e o Lema 2.7, segue o resultado desejado.

2: Para $n = 2$, temos

$$
\begin{aligned}
r_{1\sigma x}((ad\ x)^2(y)) - (ad\ x)(a) &= r_{1\sigma x}(x^2 - 2xyx + yx^2) - xa + ax \\
&= x^2y - 2xyx + (xy - a)x - xa + ax \\
&= -x(yx - (xy - a)).
\end{aligned}
$$

Como $xyx < yx^2$, segue $r_{1\sigma x}((ad\ x)^2(y)) - (ad\ x)(a) \in I_{yx^2}$.

Suponhamos, agora, que o Resultado 2 seja válido para $n = t$ e mostremos sua validade para $n = t + 1$.

$$
\begin{aligned}
r_{1\sigma x^t}((ad\ x)^{t+1}(y)) &= r_{1\sigma x^t}(x(ad\ x)^t(y) - (ad\ x)^t(y)x) \\
&= x(ad\ x)^t(y) - r_{1\sigma x^t}((ad\ x)^t(y)x) \\
&= x(ad\ x)^t(y) - \{r_{1\sigma x^{t-1}}((ad\ x)^t(y))\}x.
\end{aligned}
$$

Logo,

$$
\begin{aligned}
&r_{1\sigma x^t}((ad\ x)^{t+1}(y)) - (ad\ x)^t(a) = \\
&= x(ad\ x)^t(y) - \{r_{1\sigma x^{t-1}}((ad\ x)^t(y)\}x - x(ad\ x)^{t-1}(a) + (ad\ x)^{t-1}(a)x \\
&= x\{(ad\ x)^t(y) - (ad\ x)^{t-1}(a)\} - \{r_{1\sigma x^{t-1}}((ad\ x)^t(y)) - (ad\ x)^t(a)\}x.
\end{aligned}
$$

Pelo Resultado 1, $x\{(ad\ x)^t(y) - (ad\ x)^{t-1}(a)\} \in I_{yx^{t+1}}$, e, por hipótese de indução, $r_{1\sigma x^{t-1}}((ad\,x)^t(y)) - (ad\,x)^t(a) \in I_{yx^t}$, portanto, $\{r_{1\sigma x^{t-1}}((ad\,x)^t(y)) - (ad\,x)^t(a)\}x \in I_{yx^{t+1}}$. E o Resultado 2 está provado.

Capítulo 4

Generalização para k-anéis

Neste capítulo faremos uma generalização bem natural dos resultados da primeira seção do segundo capítulo, isto é, vamos generalizar o Lema do Diamante. Durante todo este capítulo, k será apenas um anel associativo com unidade. A comutatividade de k não mais será hipótese nas duas próximas seções. A primeira seção deste capítulo tratará da generalização do Lema do Diamante propriamente dita; a segunda apresentará uma aplicação dessa generalização.

4.1 Estrutura de bimódulos para k-anéis

Seja k um anel (não necessariamente comutativo) associativo com unidade. Um *k-anel* é um par ordenado (R, ϕ_R), onde R é uma anel associativo com unidade e $\phi_R : k \longrightarrow R$ é um homomorfismo de anéis, levando o elemento unidade de k no elemento unidade de R. Dados dois k-anéis (R, ϕ_R) e (S, ϕ_S), definimos um *homomorfismo de k-anéis* $g : (R, \phi_R) \longrightarrow (S, \phi_S)$ como sendo um homomorfismo de anéis $g : R \longrightarrow S$ levando o elemento unidade de R no elemento unidade de S e que faz comutar o diagrama abaixo.

$$\begin{tikzcd} R \arrow[rr, "g"] & & S \\ & k \arrow[ul, "\phi_R"] \arrow[ur, "\phi_S"'] & \end{tikzcd}$$

Existe uma formulação equivalente para a definição de k-anel. Dizemos, alternativamente, que um anel associativo com unidade R é um k-anel se R for também um k-bimódulo e satisfizer as condições

$$\lambda(xy) = (\lambda x)y, \quad (x\lambda)y = x(\lambda y), \quad (xy)\lambda = x(y\lambda),$$

para todos $\lambda \in k$ e $x, y \in R$.

Sejam X um conjunto e $(M_x)_{x\in X}$ uma família arbitrária de k-bimódulos indexada por X. Formemos o semigrupo livre com unidade gerado por X, que será denotado por $\langle X\rangle$.

Para cada $A = x_1 \dots x_n \in \langle X\rangle$ $(x_i \in X)$, considere o produto tensorial (sobre k) $P_A = M_{x_1} \otimes \cdots \otimes M_{x_n}$. O grupo abeliano P_A é um k-bimódulo, definindo-se a ação de escalares $\lambda, \mu \in k$ em um elemento gerador $m_1 \otimes \dots \otimes m_n$ $(m_i \in M_{x_i})$ de P_A por

$$\lambda(m_1 \otimes \cdots \otimes m_n)\mu = (\lambda m_1) \otimes \cdots \otimes (m_n\mu)$$

e estendendo-a linearmente. Essa ação está bem definida (ver [10, p. 135, Prop. 3.6]). Assim, posso escrever todo elemento de P_A na forma

$$\sum_{i=1}^{l} m^i_{x_1} \otimes \cdots \otimes m^i_{x_n},$$

onde $m^i_{x_j} \in M_{x_j}$ para todo $i = 1, \dots, l$ e $j = 1, \dots, n$. Ressalva-se que essa forma não é única. Com esta notação estamos denotando $P_1 = k$ e $P_x = M_x$, para todo $x \in X$. Observe que, a partir da definição de P_A, podemos afirmar que $P_A \otimes P_B = P_{AB}$.

Considere agora a soma direta externa da família $(P_A)_{A\in\langle X\rangle}$, isto é, o k-bimódulo $\bigoplus_{A\in\langle X\rangle} P_A$ (ou apenas $\bigoplus_{\langle X\rangle} P_A$). Os elementos de $\bigoplus_{\langle X\rangle} P_A$ são famílias $(a_A)_{A\in\langle X\rangle}$, onde $a_A \in P_A$ e o conjunto $supp((a_A)_{A\in\langle X\rangle}) = \{A \in \langle X\rangle : a_A \neq 0\}$, chamado *suporte* da família $(a_A)_{A\in\langle X\rangle}$, é finito. Por simplicidade, denotarei os elementos de $\bigoplus_{\langle X\rangle} P_A$ por (a_A) apenas, deixando para indicar o conjunto percorrido pelos índices apenas quando for estritamente necessário.

Lembremos que a estrutura de k-bimódulo de $\bigoplus_{\langle X\rangle} P_A$ é dada por $(a_A) + (b_A) = (a_A + b_A)$ e, se $\lambda, \mu \in k$, então $\lambda(a_A)\mu = (\lambda a_A \mu)$. Além disso, podemos dotar $\bigoplus_{\langle X\rangle} P_A$ de uma multiplicação, como em [16, pp. 121–122, Prop. 1.9.13], dada por

$$(a_A) \otimes (b_B) = (c_C), \text{ onde } c_C = \sum_{AB=C} a_A \otimes b_B.$$

A notação $a_A \otimes b_B$ indica o elemento de P_{AB} definido da seguinte maneira. Se $a = \sum_i m^i_{x_1} \otimes \cdots \otimes m^i_{x_n} \in P_A = M_{x_1} \otimes \cdots \otimes M_{x_n}$ e $b = \sum_j m^j_{x'_1} \otimes \cdots \otimes m^j_{x'_p} \in P_B = M_{x'_1} \otimes \cdots \otimes M_{x'_p}$, então

$$a_A \otimes b_B = \sum_{i,j} m^i_{x_1} \otimes \cdots \otimes m^i_{x_n} \otimes m^j_{x'_1} \otimes \cdots \otimes m^j_{x'_p}.$$

Afirma-se que $\bigoplus_{\langle X \rangle} P_A$ dotado da multiplicação $\otimes$ é um anel associativo, cuja unidade é o elemento (a_A), com $a_1 = 1 \in k$ e $a_A = 0$ se $A \neq 1$. Podemos definir uma aplicação $\varphi : k \longrightarrow \bigoplus_{\langle X \rangle} P_A$, dada por $\varphi(\lambda) = (a_A)$, onde $a_1 = \lambda$ e $a_A = 0$ se $A \neq 1$. Verifica-se facilmente que φ é um homomorfismo de anéis (é na realidade um monomorfismo de anéis) e que $\varphi(1) = 1$. Logo, $(\bigoplus_{\langle X \rangle} P_A, \varphi)$ é um k-anel. Observe que a estrutura de k-bimódulo de $\bigoplus_{\langle X \rangle} P_A$ pode ser dada por intermédio de sua estrutura de k-anel, definindo-se $\lambda(a_A)\mu = \varphi(\lambda) \otimes (a_A) \otimes \varphi(\mu)$, para $\lambda, \mu \in k$ e $(a_A) \in k\langle M \rangle$.

Para cada $B \in \langle X \rangle$, podemos considerar o homomorfismo de k-bimódulos

$$\begin{array}{ccc} P_B & \longrightarrow & \bigoplus_{\langle X \rangle} P_A \\ b & \longmapsto & (a_A), \end{array}$$

onde $a_B = b$ e $a_A = 0$ se $A \neq B$. Como, para todo $B \in \langle X \rangle$, o homomorfismo acima é injetor, podemos considerar P_B como um sub-k-bimódulo de $\bigoplus_{\langle X \rangle} P_A$. Mais geralmente, se Y é um subconjunto não vazio de $\langle X \rangle$, então pode-se considerar o k-bimódulo $\bigoplus_{B \in Y} P_B$ como sub-k-bimódulo de $\bigoplus_{\langle X \rangle} P_A$, através do monomorfismo

$$\begin{array}{ccc} \bigoplus_Y P_B & \longrightarrow & \bigoplus_{\langle X \rangle} P_A \\ (b_B) & \longmapsto & (a_A), \end{array}$$

onde $a_B = b_B$, para todo $B \in Y$ e $a_A = 0$ se $A \notin Y$.

Definidas as operações no k-anel $\bigoplus_{\langle X \rangle} P_A$, se (a_A) é um elemento arbitrário, podemos escrever

$$(a_A) = \sum_{A \in supp((a_A))} a_A.$$

Assim, $\bigoplus_{\langle X \rangle} P_A$ é gerado, como k-bimódulo, pelo conjunto $\{a_A \in P_A : A \in \langle X \rangle\}$. Deste ponto em diante, quando não houver possibilidade de dúvida, indicarei simplesmente $(a_A) = \sum_A a_A$, quando quiser dizer $(a_A) = \sum_{A \in supp((a_A))} a_A$. Esse abuso de notação tem a vantagem de facilitar a leitura do texto. Mais ainda, quando a soma em questão estiver

sujeita a alguma restrição, por exemplo, se $B \in \langle X \rangle$ e quisermos escrever

$$\sum_{\substack{A \in supp((a_A)) \\ A \neq B}} a_A,$$

escreveremos apenas $\sum_{A \neq B} a_A$. Dada uma família (a_A), cada um dos elementos $a_A \in P_A$ tal que $A \in supp((a_A))$ é denominado a *componente homogênea* de (a_A) em P_A.

O k-anel $\bigoplus_{\langle X \rangle} P_A$ é chamado de *k-anel tensorial* do k-bimódulo $M = \bigoplus_{x \in X} M_x$. Define-se de maneira geral o k-anel tensorial de um k-bimódulo arbitrário M como sendo o k-anel $T(M) = \bigoplus_{i \in \mathbb{N}_0} (\otimes^i M)$, onde

$$\otimes^i M = \underbrace{M \otimes \ldots \otimes M}_{i},$$

$\otimes^1 M = M$ e $\otimes^0 M = k$. Indicando-se por $\alpha : M \longrightarrow T(M)$, a injeção natural de $\otimes^1 M = M$ em $T(M)$, o k-anel tensorial $T(M)$ tem a seguinte propriedade universal. Para todo k-anel R e todo homomorfismo de k-bimódulos $\phi : M \longrightarrow R$, existe um único homomorfismo de k-anéis $\overline{\phi} : T(M) \longrightarrow R$ que faz comutar o diagrama abaixo.

$$\begin{tikzcd} M \arrow[r, "\alpha"] \arrow[dr, "\phi"'] & T(M) \arrow[d, "\overline{\phi}"] \\ & R \end{tikzcd}$$

De fato, dados um k-anel R e um homomorfismo de k-bimódulos $\phi : M \longrightarrow R$, para cada $n \geq 2$, considere a aplicação $\phi_n : M \times \ldots \times M \longrightarrow R$ dada por $\phi_n(x_1, \ldots, x_n) = \phi(x_1) \ldots \phi(x_n)$. As aplicações ϕ_n são n-lineares sobre k e, portanto, para cada n, existe um único homomorfismo de grupos abelianos $\overline{\phi_n} : \otimes^n M \longrightarrow R$, que é também um homomorfismo de k-bimódulos, tal que $\phi_n = \overline{\phi_n}\theta$, onde $\theta(x_1, \ldots, x_n) = x_1 \otimes \cdots \otimes x_n$. Assim, para todo $n \geq 2$, temos

$$\overline{\phi_n}(x_1 \otimes \cdots \otimes x_n) = \phi(x_1) \ldots \phi(x_n).$$

Tomando $\overline{\phi_1} = \phi$ e $\overline{\phi_0}$ como sendo a identidade do anel k, como $T(M)$ é a soma direta dos k-bimódulos $\otimes^n M$, existe um único homomorfismo de k-bimódulos $\overline{\phi} : T(M) \longrightarrow S$ tal que, para todo $n \geq 0$, $\overline{\phi_n} = \overline{\phi}\alpha_n$, onde α_n indica a injeção natural de $\otimes^n M$ em $T(M)$

(e, portanto, $\alpha_1 = \alpha$). É imediato verificar que $\overline{\phi}$ é um homomorfismo de k-anéis. Além disso, temos $\overline{\phi}\alpha = \overline{\phi}\alpha_1 = \overline{\phi_1} = \phi$. A aplicação $\overline{\phi}$ é o único homomorfismo de k-anéis $\psi : T(M) \longrightarrow S$ tal que $\psi\alpha = \phi$, pois $T(M)$ é gerado, como k-anel, por $\alpha(M) \cup 1$. Essa caracterização do k-anel tensorial de um k-bimódulo é análoga à de uma k-álgebra tensorial, no caso comutativo (ver [8, I.12]); na realidade, o conceito de k-anel é uma generalização do conceito de k-álgebra.

Neste capítulo denotaremos o k-anel tensorial $\bigoplus_{\langle X\rangle} P_A$ por $k\langle M\rangle$. De agora em diante, para simplificar a linguagem, diremos apenas "anel tensorial" no lugar de "k-anel tensorial".

Um *sistema de redução* para $k\langle M\rangle$ será um conjunto S de pares $\sigma = (W_\sigma, f_\sigma)$, onde $W_\sigma \in \langle X\rangle$ e $f_\sigma : P_{W_\sigma} \longrightarrow k\langle M\rangle$ é um homomorfismo de k-bimódulos.

Dados $A, B \in \langle X\rangle$ e $\sigma \in S$, definimos a *redução* $r_{A\sigma B} : k\langle M\rangle \longrightarrow k\langle M\rangle$, como sendo o homomorfismo de k-bimódulos que atua nos somandos diretos de $k\langle M\rangle$ da seguinte maneira: $r_{A\sigma B}(a) = a$, para todo $a \in P_C$ com $C \neq AW_\sigma B$ e para cada $d \in P_{AW_\sigma B}$, definimos $r_{A\sigma B}(d) = P_A \otimes f_\sigma \otimes P_B(d)$, onde $P_A \otimes f_\sigma \otimes P_B$ é o homomorfismo de k-bimódulos de domínio $P_{AW_\sigma B} = P_A \otimes P_{W_\sigma} \otimes P_B$ e contradomínio $k\langle M\rangle$ e que atua em geradores $a \otimes c \otimes b$ de $P_A \otimes P_{W_\sigma} \otimes P_B$ ($a \in P_A$, $c \in P_{W_\sigma}$, $b \in P_B$) da seguinte maneira:

$$P_A \otimes f_\sigma \otimes P_B(a \otimes c \otimes b) = a \otimes f_\sigma(c) \otimes b.$$

Dizemos que uma redução $r_{BW_\sigma C}$ *atua trivialmente* em um elemento (a_A) se $a_{BW_\sigma C} = 0$ (e portanto, $r_{BW_\sigma C}((a_A)) = (a_A)$). Caso contrário, dizemos que $r_{BW_\sigma C}$ *atua não trivialmente* em (a_A). Neste caso, se escrevermos $(a_A) = \sum_A a_A$, temos:

$$r_{B\sigma C}((a_A)) = \sum_{A \neq BW_\sigma C} a_A + P_B \otimes f_\sigma \otimes P_C(a_{BW_\sigma C}).$$

Considere o subconjunto de $\langle X\rangle$ formado pelos monômios que contêm, para algum $\sigma \in S$, W_σ como subpalavra. Vamos denotar por $\langle X\rangle_{irr}$ o complementar desse subconjunto em $\langle X\rangle$, isto é, os elementos de $\langle X\rangle_{irr}$ são aqueles monômios C para os quais não existem $A, B \in \langle X\rangle$ e $\sigma \in S$ tais que $C = AW_\sigma B$. Na realidade, $\langle X\rangle_{irr}$ é apenas o conjunto de monômios C para os quais todas as reduções $r_{A\sigma B}$ atuam trivialmente nos elementos de P_C. Definimos o sub-k-bimódulo $k\langle M\rangle_{irr}$ de $k\langle M\rangle$ por $k\langle M\rangle_{irr} = \bigoplus_{A \in \langle X\rangle_{irr}} P_A$. Os elementos de $k\langle M\rangle_{irr}$ serão denominados elementos *irredutíveis* de $k\langle M\rangle$ (segundo S), pois novamente, não há redução que atue não trivialmente neles.

Um elemento $(a_A) \in k\langle M\rangle$ é dito de *redução finita* se, dada qualquer seqüência infinita de reduções $(r_i)_{i\in\mathbb{N}}$, existir $i_0 \in \mathbb{N}$ tal que r_i atue trivialmente em $r_{i-1}\dots r_1((a_A))$, para todo $i > i_0$. Assim, como no Capítulo 2, o conjunto dos elementos de redução finita de $k\langle M\rangle$ forma um sub-k-bimódulo.

Dado um elemento $(a_A) \in k\langle M\rangle$, uma seqüência finita de reduções $(r_1,\dots,r_n)$ é dita *final* em (a_A) se $r_n\dots r_1((a_A)) \in k\langle M\rangle_{irr}$.

Enunciaremos uma seqüência de resultados análogos aos enunciados no Capítulo 2, que, tendo demonstrações identicas às daquele capítulo, conterão na sua prova apenas a referência ao resultado do Capítulo 2 cuja demonstração é a mesma. É evidente que algumas modificações na notação serão necessárias nessas demonstrações, por exemplo, onde se lê $k\langle X\rangle$, leia-se $k\langle M\rangle$. Como essas modificações são óbvias, elas serão deixadas por conta do leitor.

Proposição 4.1 *Se $(a_A) \in k\langle M\rangle$ é de redução finita, então existe uma seqüencia final em (a_A).*

Prova Ver Proposição 2.1. ■

Um elemento (a_A) de redução finita será dito de *redução única* se, dadas duas seqüências finais arbitrárias em (a_A), $(r_1,\dots,r_n)$ e $(s_1,\dots,s_m)$, tivermos $r_n\dots r_1((a_A)) = s_m\dots s_1((a_A))$. Esse valor comum será denotado por $r_S((a_A))$.

Lema 4.1 *Sejam $(a_A) \in k\langle M\rangle$ e $(r_i)_{i=1}^n$ uma seqüência finita qualquer de reduções. Denotemos $r = r_n\dots r_1$. Valem as seguintes implicações:*

(i) se (a_A) é de redução finita, então $r((a_A))$ é de redução finita;

(ii) se (a_A) é de redução única, então $r((a_A))$ é de redução única e $r_S(r((a_A))) = r_S((a_A))$.

Prova Ver Lema 2.1. ■

Lema 4.2 *O conjunto dos elementos de redução única de $k\langle M\rangle$ é um sub-k-bimódulo e r_S é um homomorfismo de k-bimódulos desse sub-bimódulo em $k\langle M\rangle_{irr}$.*

Prova Ver Lema 2.2. ■

O próximo lema é uma versão do Lema 2.3 que necessita de mais do que algumas modificações óbvias e, portanto, será demonstrado. Um resultado geral sobre o cálculo

de reduções será demonstrado anteriormente, pois ele auxilia a compreensão de algumas passagens da demonstração do Lema 4.3 e de alguns outros resultados posteriores.

Sejam $A, B, L, M \in \langle X \rangle$ monômios arbitrários e σ um elemento qualquer de S. Então vale a seguinte fórmula:

$$r_{LA\sigma BM}(a \otimes b \otimes c) = a \otimes r_{A\sigma B}(b) \otimes c, \tag{4.1}$$

quaisquer que sejam $a \in P_L$, $b \in P_{AW_\sigma B}$, $c \in P_M$. De fato, como $b \in P_{AW_\sigma B} = P_A \otimes P_{W_\sigma} \otimes P_B$, existem $n \in \mathbb{N}$ e elementos $b_i^A \in P_A$, $b_i^{W_\sigma} \in P_{W_\sigma}$, $b_i^B \in P_B$ $(i = 1, \ldots, n)$, tais que

$$b = \sum_{i=1}^{n} b_i^A \otimes b_i^{W_\sigma} \otimes b_i^B,$$

Assim,

$$\begin{aligned} r_{LA\sigma BM}(a \otimes b \otimes c) &= r_{LA\sigma BM}(a \otimes (\sum_i b_i^A \otimes b_i^{W_\sigma} \otimes b_i^B) \otimes c) \\ &= r_{LA\sigma BM}(\sum_i a \otimes b_i^A \otimes b_i^{W_\sigma} \otimes b_i^B \otimes c). \end{aligned}$$

Como $r_{LA\sigma BM}$ é um homomorfismo de k-bimódulos, temos

$$r_{LA\sigma BM}(\sum_i a \otimes b_i^A \otimes b_i^{W_\sigma} \otimes b_i^B \otimes c) = \sum_i r_{LA\sigma BM}(a \otimes b_i^A \otimes b_i^{W_\sigma} \otimes b_i^B \otimes c).$$

Como, para cada $i = 1, \ldots, n$, temos $a \otimes b_i^A \in P_L \otimes P_A = P_{LA}$ e $b_i^B \otimes c \in P_B \otimes P_M = P_{BM}$, aplicando a definição da ação de uma redução, obtemos

$$r_{LA\sigma BM}(a \otimes b_i^A \otimes b_i^{W_\sigma} \otimes b_i^B \otimes c) = a \otimes b_i^A \otimes f_\sigma(b_i^{W_\sigma}) \otimes b_i^B \otimes c$$

e, portanto,

$$\begin{aligned} r_{LA\sigma BM}(\sum_i a \otimes b_i^A \otimes b_i^{W_\sigma} \otimes b_i^B \otimes c) &= \sum_i a \otimes b_i^A \otimes f_\sigma(b_i^{W_\sigma}) \otimes b_i^B \otimes c \\ &= a \otimes (\sum_i b_i^A \otimes f_\sigma(b_i^{W_\sigma}) \otimes b_i^B) \otimes c. \end{aligned}$$

Basta, agora, notar que, por definição, $\sum_{i=1}^{n} b_i^A \otimes f_\sigma(b_i^{W_\sigma}) \otimes b_i^B = r_{A\sigma B}(b)$.

Lema 4.3 *Suponha que $(a_A), (b_B), (c_C) \in k\langle M \rangle$ sejam elementos não nulos tais que, para todas as componentes homogêneas a_A, b_B, c_C de $(a_A), (b_B), (c_C)$, respectivamente, em qualquer dos somandos P_A, P_B, P_C de $k\langle M \rangle$, o produto $a_A \otimes b_B \otimes c_C$ seja de redução única. Seja r uma composição qualquer de reduções. Então $(a_A) \otimes r((b_B)) \otimes (c_C)$ é de redução única e $r_S((a_A) \otimes r((b_B)) \otimes (c_C)) = r_S((a_A) \otimes (b_B) \otimes (c_C))$.*

Prova Seja $r_{D\sigma E}$ uma redução qualquer e a_A, b_B, c_C elementos arbitrários dos sub-bimódulos P_A, P_B, P_C, respectivamente. Mostremos que $a_B \otimes r_{D\sigma E}(b_B) \otimes c_C = r_{AD\sigma EC}(a_A \otimes b_B \otimes c_C)$. De fato, se $B \neq DW_\sigma E$, então $r_{D\sigma E}(b_B) = b_B$ e, portanto, $a_A \otimes r_{D\sigma E}(b_B) \otimes c_C = a_A \otimes b_B \otimes c_C$. Neste caso, temos $ABC \neq ADW_\sigma EC$, o que implica que $r_{AD\sigma EC}(a_A \otimes b_B \otimes c_C) = a_A \otimes b_B \otimes c_C = a_A \otimes r_{D\sigma E}(b_B) \otimes c_C$. Por outro lado, se $B = DW_\sigma E$, então $b_B \in P_{DW_\sigma E}$, o que implica

$$a_A \otimes r_{D\sigma E}(b_B) \otimes c_C = r_{AD\sigma EC}(a_A \otimes b_B \otimes c_C),$$

por (4.1). Vejamos agora o caso em que temos $a_A \in P_A, c_C \in P_C$ e $b = (b_B)$ é um elemento arbitrário de $k\langle M\rangle$. Neste caso ainda vale que

$$a_A \otimes r_{D\sigma E}(b) \otimes c_C = r_{AD\sigma EC}(a_A \otimes b \otimes c_C),$$

pois podemos escrever $(b_B) = \sum_B b_B$ e, como $r_{D\sigma E}$ é um homomorfismo de k-bimódulos, temos

$$\begin{aligned} a_A \otimes r_{D\sigma E}((b_B)) \otimes c_C &= a_A \otimes r_{D\sigma E}(\sum_B b_B) \otimes c_C \\ &= a_A \otimes (\sum_B r_{D\sigma E}(b_B)) \otimes c_C \\ &= \sum_B a_A \otimes r_{D\sigma E}(b_B) \otimes c_C. \end{aligned}$$

Como, pelo que vimos acima, $a_A \otimes r_{D\sigma E}(b_B) \otimes c_C = r_{AD\sigma EC}(a_A \otimes b_B \otimes c_C)$, temos

$$\begin{aligned} a_A \otimes r_{D\sigma E}((b_B)) \otimes c_C &= \sum_B r_{AD\sigma EC}(a_A \otimes b_B \otimes c_C) \\ &= r_{AD\sigma EC}(\sum_B a_A \otimes b_B \otimes c_C) \\ &= r_{AD\sigma EC}(a_A \otimes (\sum_B b_B) \otimes c_C) \\ &= r_{AD\sigma EC}(a_A \otimes (b_B) \otimes c_C). \end{aligned}$$

De maneira análoga ao que fizemos na demonstração do Lema 2.3 e tendo em vista o Lema 4.1(ii), se temos $a_A \in P_A$, $b_B \in P_B$ e $c_C \in P_C$, podemos concluir que $a_A \otimes r(b_B) \otimes c_C$ é de redução única, quando $a_A \otimes b_B \otimes c_C$ o for, e que $r_S(a_A \otimes r(b_B) \otimes c_C) = r_S(a_A \otimes b_B \otimes c_C)$. Dados agora $(a_A), (b_B), (c_C)$ elementos arbitrários de $k\langle M\rangle$, escrevendo-os como soma de suas componentes homogêneas, podemos repetir o final da demonstração do Lema 2.3. ■

Uma 5-upla (σ, τ, A, B, C), onde $\sigma, \tau \in S$ e $A, B, C \in \langle X\rangle$ é dita uma *ambigüidade de superposição* (resp. *ambigüidade de inclusão*) se $W_\sigma = AB$ e $W_\tau = BC$ (resp. $W_\sigma = B$

e $W_\tau = ABC$). Uma ambigüidade de superposição (resp. de inclusão) (σ, τ, A, B, C) será dita *resolível* se, para todo $d \in P_{ABC}$, existirem composições de reduções r e r' tais que $r(r_{1\sigma C}(d)) = r'(r_{A\tau 1}(d))$ (resp. $r(r_{A\sigma B}(d)) = r'(r_{1\tau 1}(d))$).

Dada uma ordem parcial de semigrupo em $\langle X \rangle$, $\leq$, dizemos que $\leq$ e S são *compatíveis* se $f_\sigma(P_{W_\sigma}) \subseteq \bigoplus_{A<W_\sigma} P_A$, para todo $\sigma = (W_\sigma, f_\sigma) \in S$.

Como fizemos no Capítulo 2, vamos definir o ideal I de $k\langle M \rangle$ como sendo o ideal (bilateral) gerado pelo conjunto

$$\{(a_A) - r_{B\sigma C}((a_A)) : (a_A) \in k\langle M \rangle, B, C \in \langle X \rangle, \sigma \in S\}.$$

Para elementos (a_A) e reduções $r_{B\sigma C}$ tais que $r_{B\sigma C}$ atua trivialmente em (a_A), temos $(a_A) - r_{B\sigma C}((a_A)) = 0$ e, portanto, essas diferenças não contribuem para o ideal I. Logo, podemos considerar apenas as diferenças $(a_A) - r_{B\sigma C}((a_A))$, para as quais $r_{B\sigma C}$ atua não trivialmente em (a_A). Neste caso, se escrevermos $(a_A) = \sum_A a_A$, teremos

$$\begin{aligned}
(a_A) - r_{B\sigma C}((a_A)) &= \sum_A a_A - r_{B\sigma C}(\sum_A a_A) \\
&= \sum_A a_A - \sum_A r_{B\sigma C}(a_A) \\
&= a_{BW_\sigma C} - r_{B\sigma C}(a_{BW_\sigma C}).
\end{aligned}$$

Logo, pode-se caracterizar I como o ideal gerado pelo conjunto $\{d - r_{B\sigma C}(d) : B, C \in \langle X \rangle, \sigma \in S, d \in P_{BW_\sigma C}\}$. Afirma-se, então, que I é o ideal gerado pelo conjunto

$$\{e - f_\sigma(e) : \sigma \in S, e \in P_{W_\sigma}\}.$$

A demonstração desse fato é simples e não será feita aqui. Como k-bimódulo, I é gerado pelo conjunto

$$\{a \otimes (e - f_\sigma(e)) \otimes b : A, B \in \langle X \rangle, \sigma \in S, e \in P_{W_\sigma}, a \in P_A, b \in P_B\}.$$

Se temos uma ordem parcial de semigrupo $\leq$ em $\langle X \rangle$ e um sistema de redução S tais que $\leq$ e S sejam compatíveis, então, para cada $C \in \langle X \rangle$, definimos o sub-k-bimódulo I_C de $k\langle M \rangle$ gerado por

$$\{d - r_{A\sigma B}(d) : A, B \in \langle X \rangle, \sigma \in S, AW_\sigma B < C, d \in P_{AW_\sigma B}\}.$$

Novamente, prova-se que I_C é o sub-k-bimódulo gerado pelos elementos $a \otimes (e - f_\sigma(e)) \otimes b$, onde $A, B \in \langle X \rangle$ e $\sigma \in S$ são tais que $AW_\sigma B < C$ e a, b, e percorrem P_A, P_B, P_{W_σ}, respectivamente.

Dados um sistema de redução S e uma ordem parcial de semigrupo $\leq$ em $\langle X\rangle$, tais que $\leq$ e S sejam compatíveis, dizemos que uma ambigüidade de superposição (resp. de inclusão) (σ, τ, A, B, C) é *resolível com respeito a* $\leq$ se $(r_{1\sigma C} - r_{A\tau 1})(P_{ABC}) \subseteq I_{ABC}$ (resp. $(r_{A\sigma C} - r_{1\tau 1})(P_{ABC}) \subseteq I_{ABC}$).

Fixemos um sistema de redução S para $k\langle M\rangle$ e uma ordem parcial de semigrupo $\leq$ para $\langle X\rangle$ tais que $\leq$ e S sejam compatíveis. Vamos continuar enunciando resultados análogos aos do Capítulo 2.

Se temos $r = r_n \dots r_1$, uma composição arbitrária de reduções, então, vale que $(a_A) - r((a_A)) \in I$, onde (a_A) é um elemento qualquer de $k\langle M\rangle$. De fato, por definição de I, temos $(a_A) - r_1((a_A)) \in I$ e $r_{i-1} \dots r_1((a_A)) - r_i r_{i-1} \dots r_1((a_A)) \in I$, para todo $i = 2, \dots n$. Logo, $(a_A) - r((a_A)) = [(a_A) - r_1((a_A))] + [r_1((a_A)) - r_2 r_1((a_A))] + \dots + [r_{n-1} \dots r_1((a_A)) - r_n \dots r_1((a_A))] \in I$. Essa afirmação é análoga à do Lema 2.4.

Se $(a_A) \in \bigoplus_{A<E} P_A$, para algum $E \in \langle X\rangle$, então afirma-se que $r_{B\sigma C}((a_A)) \in \bigoplus_{A<E} P_A$, qualquer que seja a redução $r_{B\sigma C}$. Se $BW_\sigma C \notin supp((a_A))$, o resultado é trivial. Senão, escrevemos $(a_A) = \sum_A a_A$ e temos

$$r_{B\sigma C}((a_A)) = \sum_{A \neq BW_\sigma C} a_A + r_{B\sigma C}(a_{BW_\sigma C}).$$

Como $a_{BW_\sigma C} \in P_{BW_\sigma C} = P_B \otimes P_{W_\sigma} \otimes P_C$, existem $n \in \mathbb{N}$ e $a_i^B \in P_B$, $a_i^{W_\sigma} \in P_{W_\sigma}$, $a_i^C \in P_C$ $(i = 1, \dots, n)$, tais que

$$a_{BW_\sigma C} = \sum_{i=1}^{n} a_i^B \otimes a_i^{W_\sigma} \otimes a_i^C.$$

Assim, $r_{B\sigma C}(a_{BW_\sigma C}) = \sum_i a_i^B \otimes f_\sigma(a_i^{W_\sigma}) \otimes a_i^C$. Como, por hipótese, $\leq$ e S são compatíveis, temos $f_\sigma(a_i^{W_\sigma}) \in \bigoplus_{D<W_\sigma} P_D$ para todo $i = 1, \dots, n$, o que implica que $a_i^B \otimes f_\sigma(a_i^{W_\sigma}) \otimes a_i^C \in P_B \otimes (\bigoplus_{D<W_\sigma} P_D) \otimes P_C = \bigoplus_{D<W_\sigma} P_{BDC}$. Usando que $\leq$ é uma ordem parcial de semigrupo em $\langle X\rangle$, para cada $D < W_\sigma$ temos $BDC < BW_\sigma C$. Mas $BW_\sigma C < E$, pois $(a_A) \in \bigoplus_{A<E} P_A$. Logo, $\bigoplus_{D<W_\sigma} P_{BDC}$ está contido em $\bigoplus_{A<E} P_A$. Portanto, $r_{B\sigma C}(a_{BW_\sigma C}) \in \bigoplus_{A<E} P_A$.

Sabemos que $(a_A) - r_{B\sigma C}((a_A)) = 0$, se $a_{BW_\sigma C} = 0$, ou $= a_{BW_\sigma C} - r_{B\sigma C}(a_{BW_\sigma C})$, se $a_{BW_\sigma C} \neq 0$. No primeiro caso, é evidente que $(a_A) - r_{B\sigma C}((a_A)) \in I_E$. No segundo caso, temos o mesmo resultado, pois $BW_\sigma C < E$, por hipótese.

Vamos enunciar no lema abaixo os resultados provados acima.

Lema 4.4 *Sejam $r_{B\sigma C}$ uma redução, $E \in \langle X \rangle$ e $(a_A) \in \bigoplus_{A<E} P_A$. Então valem:*

(i) $r_{B\sigma C}((a_A)) \in \bigoplus_{A<E} P_A$;

(ii) $(a_A) - r_{B\sigma C}((a_A)) \in I_E$. ■

O lema acima é análogo ao Lema 2.5 do Capítulo 2 e, como aquele, tem um corolário imediato.

Corolário 4.1 *Se $r = r_n \ldots r_1$ é uma composição qualquer de reduções, $E \in \langle X \rangle$ e $(a_A) \in \bigoplus_{A<E} P_A$, então $(a_A) - r((a_A)) \in I_E$.* ■

Os próximos dois resultados são análogos à Proposição 2.2 e ao Lema 2.7.

Proposição 4.2 *Toda ambigüidade resolúvel de S é resolúvel com respeito a $\leq$.*

Prova Seja (σ, τ, A, B, C) uma ambigüidade de superposição de S. Precisamos mostrar que, dado $a \in P_{ABC}$, $r_{1\sigma C}(a) - r_{A\tau 1}(a) \in I_{ABC}$. Por um lado, como $a \in P_{ABC} = P_{W_\sigma} \otimes P_C$, existem $n \in \mathbb{N}$ e elementos $a_i^{W_\sigma} \in P_{W_\sigma}$, $a_i^C \in P_C$, $(i = 1, \ldots, n)$ tais que

$$a = \sum_{i=1}^{n} a_i^{W_\sigma} \otimes a_i^C.$$

Temos, então,

$$r_{1\sigma C}(a) = \sum_i f_\sigma(a_i^{W_\sigma}) \otimes a_i^C.$$

Por compatibilidade de $\leq$ e S, tem-se $f_\sigma(a_i^{W_\sigma}) \in \bigoplus_{D<W_\sigma} P_D$. Logo $r_{1\sigma C}(a)$ pertence ao sub-k-bimódulo $\bigoplus_{D<W_\sigma} P_D \otimes P_C = \bigoplus_{D<W_\sigma} P_{DC}$. Como $D < W_\sigma$, então $DC < W_\sigma C = ABC$. Portanto $r_{1\sigma C}(a) \in \bigoplus_{D<ABC} P_D$. Demonstra-se, analogamente, que $r_{A\tau 1}(a) \in \bigoplus_{D<ABC} P_D$. Por hipótese, (σ, τ, A, B, C) é resolúvel, portanto existem composições de reduções, r e r', tais que $r(r_{1\sigma C}(a)) = r'(r_{A\tau 1}(a))$. Pelo Corolário 4.1, temos que $r_{1\sigma C}(d) - r(r_{1\sigma C}(d)) \in I_{ABC}$ e que $r'(r_{A\tau 1}(d)) - r_{A\tau 1}(d) \in I_{ABC}$, o que demonstra a proposição para o caso de ambigüidades de superposição. A demonstração no caso de ambigüidades de inclusão é análoga. ■

Lema 4.5 *Seja $D \in \langle X \rangle$. Se $(a_A) \in k\langle M \rangle$ é tal que $(a_A) \in I_D$, então $l \otimes (a_A) \otimes m \in I_{LDM}$, para todos $L, M \in \langle X \rangle$ e todos $l \in P_L, m \in P_M$.*

Prova Se $(a_A) \in I_D$, então existem $n \in \mathbb{N}$ e para cada $i = 1, \ldots, n$, $\sigma_i \in S$, $B_i, C_i \in \langle X \rangle$ com $B_i W_{\sigma_i} C_i < D$ $(i = 1, \ldots, n)$ e elementos $b_i \in P_{B_i}$, $c_i \in P_{C_i}$, $d_i \in P_{W_{\sigma_i}}$ tais que

$$(a_A) = \sum_{i=1}^{n} b_i \otimes (d_i - f_{\sigma_i}(d_i)) \otimes c_i.$$

Assim,

$$\begin{aligned} l \otimes (a_A) \otimes m &= l \otimes (\sum_i b_i \otimes (d_i - f_{\sigma_i}(d_i)) \otimes c_i) \otimes m \\ &= \sum_i l \otimes b_i \otimes (d_i - f_{\sigma_i}(d_i)) \otimes c_i \otimes m. \end{aligned}$$

Como $l \otimes b_i \in P_L \otimes P_{B_i} = P_{LB_i}$ e $c_i \otimes m \in P_{C_i} \otimes P_M = P_{C_i M}$ e, como, para cada i, $B_i W_{\sigma_i} C_i < D$ implica $LB_i W_{\sigma_i} C_i M < LDM$, segue que $l \otimes (a_A) \otimes m \in I_{LDM}$. ■

O princípio de indução (Proposição 2.3) enunciado no Capítulo 2, sendo apenas um resultado sobre conjuntos ordenados, continuará sendo válido no contexto deste capítulo.

Passaremos agora a estudar condições suficientes para garantir que um elemento $(a_A) \in k\langle M \rangle$ seja de redução finita. Suponha que o conjunto $\langle X \rangle$ seja dotado de uma ordem parcial de semigrupo, $\leq$, **com condição de cadeia descendente** e tal que $\leq$ e S sejam compatíveis. Afirma-se que, neste caso, para todo monômio minimal D em $\langle X \rangle$, todos os elementos de P_D são de redução única (em particular, de redução finita). De fato, seja D um monômio minimal em $\langle X \rangle$ e seja $d \in P_D$ um elemento arbitrário. Se d for irredutível, então d é necessariamente de redução única. Suponhamos que d não seja irredutível, isto é, que exista redução $r_{B\sigma C}$ que atue não trivialmente em d. Se este é o caso, então temos $D = BW_\sigma C$. Assim, $d \in P_{BW_\sigma C} = P_B \otimes P_{W_\sigma} \otimes P_C$ e, portanto, posso escrever d na forma

$$d = \sum_{i=1}^{n} d_i^B \otimes d_i^{W_\sigma} \otimes d_i^C,$$

onde $d_i^B \in P_B$, $d_i^{W_\sigma} \in P_{W_\sigma}$, $d_i^C \in P_C$. Dessa maneira, temos

$$r_{B\sigma C}(d) = \sum_i d_i^B \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^C.$$

Como $\leq$ e S são compatíveis, $f_\sigma(P_{W_\sigma}) \subseteq \bigoplus_{E<W_\sigma} P_E$, o que implica que $d_i^B \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^C$ pertence a $\bigoplus_{E<W_\sigma} P_{BEC}$, que, por sua vez está contido em $\bigoplus_{E<D} P_E = \{0\}$. Logo, $r_{B\sigma C}(d) = 0$ e, portanto, é de redução única.

O lema seguinte afirma que a c.c.d. sobre $\leq$, com $\leq$ e S compatíveis, é condição suficiente para garantir a redutibilidade finita para todos os elementos de $k\langle M \rangle$.

Lema 4.6 *Se $\leq$ é uma ordem parcial de semigrupo em $\langle X\rangle$ com c.c.d. tal que $\leq$ e S sejam compatíveis, então todo elemento de $k\langle M\rangle$ é de redução finita.*

Prova Mostraremos por indução em $\langle X\rangle$ que, para cada $A \in \langle X\rangle$, todos os elementos de P_A são de redução finita. Sabe-se que para os elementos minimais de $\langle X\rangle$ o resultado é verdadeiro. Seja, então, $D \in \langle X\rangle$ não minimal e suponhamos que para todo $A < D$ os elementos de P_A sejam de redução finita. Tomemos d um elemento arbitrário de P_D. Seja $(r_i)_{i\in\mathbb{N}}$ uma seqüência infinita de reduções. Precisamos encontrar $i_0 \in \mathbb{N}$ tal que r_i atue trivialmente em $r_{i-1}\dots r_1(d)$, para todo $i > i_0$. Se r_i atua trivialmente em $r_{i-1}\dots r_1(d)$ para todo $i \in \mathbb{N}$, então basta tomar $i_0 = 1$. Senão, seja j_0 o menor j tal que r_j atue não trivialmente em $r_{j-1}\dots r_1(d)$. Pela compatibilidade de $\leq$ e S, temos que $r_{j_0}(d) = r_{j_0}r_{j_0-1}\dots r_1(d)$ pertence a $\bigoplus_{C<D} P_C$, ou seja, podemos escrever $r_{j_0}(d) = \sum_C d_C$, com $C < D$. Considere, agora, a seqüência infinita de reduções $(s_i)_{i\in\mathbb{N}}$, dada por $s_i = r_{j_0+i}$. Por hipótese, d_C é de redução finita, para todo $C \in supp(r_{j_0}(d))$, logo, para cada $C \in supp(r_{j_0}(d))$, existe $i(C)$ tal que s_i atua trivialmente em $s_{i-1}\dots s_1(d_C)$ para todo $i > i(C)$. Seja $i' = max\{i(C) : C \in supp(r_{j_0}(d))\}$. Então temos que s_i atua trivialmente em $s_{i-1}\dots s_1(d_C)$ para todo $i > i'$ e todo $C \in supp(r_{j_0}(d))$, ou seja, r_{j_0+i} atua trivialmente em $r_{j_0+i-1}\dots r_{j_0+1}(d_C)$, para todo $i > i'$ e todo $C \in supp(r_{j_0}(d))$. Portanto, r_{j_0+i} atua trivialmente em $\sum_C r_{j_0+i-1}\dots r_{j_0+1}(d_C)$, para todo $i > i'$. Mas $\sum_C r_{j_0+i-1}\dots r_{j_0+1}(d_C) = r_{j_0+i-1}\dots r_{j_0+1}(\sum_C d_C) = r_{j_0+i-1}\dots r_{j_0+1}(r_{j_0}(d)) = r_{j_0+i-1}\dots r_{j_0+1}r_{j_0}\dots r_1(d)$. Logo, basta tomar $i_0 = j_0 + i'$. Provamos, então, que d é de redução finita e, assim, podemos afirmar que todo elemento d em P_D é de redução finita. Como D foi escolhido arbitrariamente, temos que todo $a \in P_A$ é de redução finita, qualquer que seja $A \in \langle X\rangle$. Logo, todo elemento de $k\langle M\rangle$ é de redução finita, uma vez que os elementos $a \in P_A$ geram $k\langle M\rangle$ como k-bimódulo e o conjunto dos elementos de redução finita de $k\langle M\rangle$ forma um sub-k-bimódulo de $k\langle M\rangle$. ■

Tendo enunciado todas as definições e resultados preliminares análogos aos do Capítulo 2, já temos condição de enunciar e demonstrar um teorema cujo conteúdo é semelhante ao do Teorema 2.1.

Teorema 4.1 *Sejam k um anel associativo com unidade, $k\langle M\rangle$ o k-anel tensorial da soma direta M de uma família $(M_x)_{x\in X}$ de k-bimódulos, S um sistema de redução para $k\langle M\rangle$, I o ideal de $k\langle M\rangle$ gerado pelos elementos $a - f_\sigma(a)$, onde σ percorre o conjunto S*

e $a \in P_{W_\sigma}$, e $\leq$ uma ordem parcial de semigrupo em $\langle X \rangle$ com c.c.d. tal que $\leq$ e S sejam compatíveis. Então as condições abaixo são equivalentes.

(a) Todas as ambigüidades de S são resolúveis.

(a') Todas as ambigüidades de S são resolúveis com respeito a $\leq$.

(b) Todos os elementos de $k\langle M \rangle$ são de redução única.

(c) $k\langle M \rangle = k\langle M \rangle_{irr} \oplus I$.

Observe que a condição (c) é equivalente a dizer que o homomorfismo de k-bimódulos $\varphi : k\langle M \rangle_{irr} \longrightarrow k\langle M \rangle / I$, dado pela restrição a $k\langle M \rangle_{irr}$ da projeção canônica de $k\langle M \rangle$ sobre $k\langle M \rangle / I$, é um isomorfismo.

Prova A demonstração das equivalências seguirá o mesmo esquema utilizado na demonstração do Teorema 2.1, isto é,

$$\begin{array}{ccccc} (a) & \Rightarrow & (a') & & \\ & & \Downarrow & & \\ (a) & \Leftarrow & (b) & \Leftrightarrow & (c). \end{array}$$

Pelo Lema 4.6, podemos afirmar que todos os elementos de $k\langle M \rangle$ são de redução finita.

$(b) \Rightarrow (c)$: Estamos supondo que o domínio do homomorfismo de k-bimódulos r_S é $k\langle M \rangle$. Como $r_S(r_S((a_A))) = r_S((a_A))$, para todo $(a_A) \in k\langle M \rangle$, $r_S : k\langle M \rangle \longrightarrow k\langle M \rangle$ é uma projeção. É imediato que $Im(r_S) = k\langle M \rangle_{irr}$. Além disso, temos que $ker(r_S) = I$, pois se, por um lado, $r_S((a_A)) = 0$, então, temos $(a_A) = (a_A) - r_S((a_A)) \in I$. Por outro lado, se $a \otimes (e - f_\sigma(e)) \otimes b$ é um elemento gerador arbitrário de I, $r_S(a \otimes (e - f_\sigma(e)) \otimes b) = r_S(a \otimes e \otimes b) - r_S(a \otimes f_\sigma(e) \otimes b) = 0$, pelo Lema 4.3, uma vez que $f_\sigma(e) = r_{1\sigma 1}(e)$.

$(c) \Rightarrow (b)$: Análoga à demonstração de $(c') \Rightarrow (b)$ do Teorema 2.1.

$(a) \Rightarrow (a')$: Proposição 4.2.

$(b) \Rightarrow (a)$: Seja (σ, τ, A, B, C) uma ambigüidade de superposição de S e seja $d \in P_{ABC}$. Temos que mostrar que existem composições de reduções r e r', tais que $r(r_{1\sigma C}(d)) = r'(r_{A\tau 1}(d))$. Pelo Lema 4.1 (ou Lema 4.3), como d é de redução única por hipótese, $r_S(r_{1\sigma C}(d)) = r_S(d)$, isto é, dada uma seqüência final $(r_1, \ldots, r_n)$ em $r_{1\sigma C}(d)$, temos $r_n \ldots r_1(r_{1\sigma C}(d)) = r_S(d)$. Analogamente, se $(s_1, \ldots, s_m)$ é uma seqüência final em $r_{A\tau 1}(d)$, então $s_m \ldots s_1(r_{A\tau 1}(d)) = r_S(d)$. Logo, (σ, τ, A, B, C) é resolúvel. A demonstração para ambigüidades de inclusão é totalmente análoga.

$(a') \Rightarrow (b)$: Como o conjunto dos elementos de redução única de $k\langle M\rangle$ é um sub-k-bimódulo e os elementos $a \in P_A$, para todo $A \in \langle X\rangle$, formam um conjunto gerador para $k\langle M\rangle$, como k-bimódulo, provaremos, então, que dado $A \in \langle X\rangle$, cada $a \in P_A$ é de redução única. A prova será feita por indução em $\langle X\rangle$.

Seja $D \in \langle X\rangle$. Se D é minimal em $\langle X\rangle$, então já temos que todo $d \in P_D$ é de redução única. Suponhamos, então, que D não seja minimal em $\langle X\rangle$ e, por hipótese de indução, que todo $c \in P_C$, para $C < D$, seja de redução única. Isso implica que $\bigoplus_{A<D} P_A$ está contido no domínio de r_S. Mostremos inicialmente que I_D está contido em $ker(r_S)$. Seja $a \otimes (e - f_\sigma(e)) \otimes b$ um gerador de I_D, isto é, estamos tomando $a \in P_A, e \in P_{W_\sigma}, b \in P_B$, para $\sigma \in S$ e $A, B \in \langle X\rangle$ tais que $AW_\sigma B < D$. Como $a \otimes e \otimes b \in P_{AW_\sigma B}$ e $AW_\sigma B < D$, temos que $a \otimes e \otimes b$ é de redução única. Pelo Lema 4.3, $a \otimes f_\sigma(e) \otimes b = a \otimes r_{1\sigma 1}(e) \otimes b$ é de redução única e vale $r_S(a \otimes e \otimes b) = r_S(a \otimes f_\sigma(e) \otimes b)$. Logo, $I_D \subseteq ker(r_S)$.

Seja $d \in P_D$ um elemento arbitrário. Se d for irredutível, então d é de redução única. Suponhamos, então, que d não seja irredutível. Sejam $(r_i)_{i=1}^n$ e $(s_j)_{j=1}^m$ duas seqüências finais em d. Tomemos i_0 como sendo o menor i tal que r_i atue não trivialmente em $r_{i-1} \dots r_1(d)$ e j_0 o menor j tal que s_j atue não trivialmente em $s_{j-1} \dots s_1(d)$. Como já fizemos outras vezes, a compatibilidade entre $\leq$ e S permite-nos afirmar que $r_{i_0}(d) \in \bigoplus_{A<D} P_A$ e que $s_{j_0}(d) \in \bigoplus_{A<D} P_A$. Logo, $r_{i_0}(d)$ e $s_{j_0}(d)$ são de redução única. Assim, basta mostrarmos que $r_S(r_{i_0}(d)) = r_S(s_{j_0}(d))$, pois, como $r_n \dots r_1(d) \in k\langle M\rangle_{irr}$, temos que $r_S(r_{i_0}(d)) = r_n \dots r_1(d)$ e analogamente $r_S(s_{j_0}(d)) = s_m \dots s_1(d)$. Feitas essas considerações, como as seqüências finais em d tomadas são arbitrárias, basta verificarmos que

$$r_S(r_{L\sigma M'}(d)) = r_S(r_{L'\tau M}(d)),$$

onde $r_{L\sigma M'}$ e $r_{L'\tau M}$ são reduções que atuam não trivialmente em d. Observe que estamos automaticamente supondo que $D = LW_\sigma M' = L'W_\tau M$.

Como na demonstração de $(a') \Rightarrow (b)$ do Teorema 2.1, iremos supor, sem perda de generalidade, que $cpt(L) \leq cpt(L')$ e dividir a demonstração em três casos de acordo com as posições relativas de W_σ e W_τ.

1o. caso: $D = LABCM$, onde $L' = LA$, $M' = CM$, $W_\sigma = AB$ e $W_\tau = BC$, isto é, (σ, τ, A, B, C) é uma ambigüidade de superposição. Como $d \in P_{LABCM} = P_L \otimes P_{ABC} \otimes P_L$,

podemos escrever d na forma

$$d = \sum_i d_i^L \otimes d_i^{ABC} \otimes d_i^M,$$

onde $d_i^L \in P_L$, $d_i^{ABC} \in P_{ABC}$, $d_i^M \in P_M$. Assim, pela equação (4.1), temos

$$\begin{aligned} r_{L\sigma CM}(d) &= \sum_i d_i^L \otimes r_{1\sigma C}(d_i^{ABC}) \otimes d_i^M \\ r_{LA\tau M}(d) &= \sum_i d_i^L \otimes r_{A\tau 1}(d_i^{ABC}) \otimes d_i^M. \end{aligned}$$

Portanto, $r_{L\sigma M'}(d) - r_{L'\tau M}(d) = \sum_i d_i^L \otimes (r_{1\sigma C}(d_i^{ABC}) - r_{A\tau 1}(d_i^{ABC})) \otimes d_i^M$. Como, por hipótese, todas as ambigüidades de S são resolúveis segundo $\leq$, temos $(r_{1\sigma C} - r_{A\tau 1})(P_{ABC}) \subseteq I_{ABC}$, em particular, $r_{1\sigma C}(d_i^{ABC}) - r_{A\tau 1}(d_i^{ABC}) \in I_{ABC}$. Pelo Lema 4.5, para cada i, temos $d_i^L \otimes (r_{1\sigma C}(d_i^{ABC}) - r_{A\tau 1}(d_i^{ABC})) \otimes d_i^M \in I_{LABCM} = I_D$. Logo $r_{L\sigma M'}(d) - r_{L'\tau M}(d) \in I_D$. Portanto, como $I_D \subseteq ker(r_S)$, temos $r_S(r_{L\sigma M'}(d)) = r_S(r_{L'\tau M}(d))$.

2o. caso: $D = LABCM'$, onde $L' = LA$, $M = CM'$, $W_\sigma = ABC$ e $W_\tau = B$, isto é, (τ, σ, A, B, C) é uma ambigüidade de inclusão. Este caso é tratado de maneira análoga ao primeiro.

3o. caso: $D = LW_\sigma NW_\tau M$, onde $L' = LW_\sigma N$ e $M' = NW_\tau M$. Neste caso, como $d \in P_D = P_L \otimes P_{W_\sigma} \otimes P_N \otimes P_{W_\tau} \otimes P_M$, podemos escrever d na forma

$$d = \sum_i d_i^L \otimes d_i^{W_\sigma} \otimes d_i^N \otimes d_i^{W_\tau} \otimes d_i^M,$$

onde $d_i^L \in P_L$, $d_i^{W_\sigma} \in P_{W_\sigma}$, $d_i^N \in P_N$, $d_i^{W_\tau} \in P_{W_\tau}$, $d_i^M \in P_M$. Dessa maneira, temos

$$r_{L\sigma NW_\tau M}(d) = \sum_i d_i^L \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^N \otimes d_i^{W_\tau} \otimes d_i^M.$$

Como $\leq$ e S são compatíveis, temos que, para cada i, o elemento $d_i^L \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^N$ pertence a $\bigoplus_{W<W_\sigma} P_{LWN}$ e, portanto, para cada componente homogênea a de $d_i^L \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^N$ em um sub-k-bimódulo P_A (lembrando que $A \in \{LWN : W < W_\sigma\}$), o produto $a \otimes d_i^{W_\tau} \otimes d_i^M$ pertence ao sub-k-bimódulo $P_{AW_\tau M}$. Mas, como $A < LW_\sigma N$, temos $AW_\tau M < LW_\sigma NW_\tau M = D$. Portanto, por hipótese de indução, $a \otimes d_i^{W_\tau} \otimes d_i^M$ é de redução única e, pelo Lema 4.3, temos

$$\begin{aligned} r_S(d_i^L \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^N \otimes d_i^{W_\tau} \otimes d_i^M) &= r_S(d_i^L \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^N \otimes r_{1\tau 1}(d_i^{W_\tau}) \otimes a_i^M) \\ &= r_S(d_i^L \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^N \otimes f_\tau(d_i^{W_\tau}) \otimes d_i^M). \end{aligned}$$

Portanto, temos

$$r_S(r_{L\sigma NW_\tau M}(d)) = r_S(\sum_i d_i^L \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^N \otimes f_\tau(d_i^{W_\tau}) \otimes d_i^M). \tag{4.2}$$

De maneira análoga,

$$r_{LW_\sigma N\tau M}(d) = \sum_i d_i^L \otimes d_i^{W_\sigma} \otimes d_i^N \otimes f_\tau(d_i^{W_\tau}) \otimes d_i^M.$$

Usando o mesmo raciocínio acima para os elementos d_i^L, $d_i^{W_\sigma}$ e $a_i^N \otimes f_\tau(a_i^{W_\tau}) \otimes a_i^M$, concluímos que

$$r_S(r_{LW_\sigma N\tau M}(d)) = r_S(\sum_i d_i^L \otimes f_\sigma(d_i^{W_\sigma}) \otimes d_i^N \otimes f_\tau(d_i^{W_\tau}) \otimes d_i^M). \tag{4.3}$$

Em vista de (4.2) e (4.3), concluímos que

$$r_S(r_{L\sigma M'}(d)) = r_S(r_{L'\tau M}(d)),$$

o que termina a demonstração do teorema. ■

Alguns comentários merecem ser feitos. Primeiramente, é importante notar que essa é uma generalização bastante natural da situação do Capítulo 2, uma vez que as idéias centrais não dizem respeito à estrutura interna dos objetos em questão e sim às relações que existem entre eles. Prova disso é a grande facilidade encontrada na adaptação dos enunciados e demonstrações do Capítulo 2 para este. Vale a pena ressaltar também que esta é realmente uma generalização, pois, para obtermos o caso tratado no Capítulo 2, basta tomarmos k comutativo e $M_x = k$, para todo $x \in X$.

Em segundo lugar, deve-se ressaltar que o Teorema 4.1 não afirma sobre a existência de uma base formada por classes de elementos irredutíveis, como fazia o Teorema 2.1, isto é, ele não fornece formas normais para os elementos de $k\langle M\rangle/I$, mas apenas um resultado sobre a estrutura de $k\langle M\rangle/I$. No entanto, isso já é suficiente para algumas aplicações relevantes como veremos na seção seguinte.

Um último comentário diz respeito justamente a uma situação particular na qual o Teorema 4.1, de fato, afirma sobre a existência de uma base formada por classes de elementos irredutíveis. Para tanto, lembremos que se M_1 e M_2 são k-bimódulos que são livres como k-módulos à direita, com bases Z_1 e Z_2, respectivamente, então $M_1 \otimes M_2$ é um k-módulo à direita livre com base $\{z_1 \otimes z_2 : z_1 \in Z_1, z_2 \in Z_2\}$ (ver, por exemplo, [4, p. 142, Th. 14.8]). Temos, então, o seguinte corolário do Teorema 4.1.

Corolário 4.2 *Suponha que temos todas as hipóteses do Teorema 4.1 para $k\langle M\rangle$, S, $\leq$ e que para cada $x \in X$, o k-bimódulo M_x é livre como k-módulo à direita com base $Z(x)$, onde assumimos que os $Z(x)$ são dois a dois disjuntos. Então, se vale uma (e portanto todas elas) das condições (a), (a'), (b) ou (c), $k\langle M\rangle/I$ é livre como k-módulo à direita e tem como base o conjunto $\{\overline{z_1} \otimes \cdots \otimes \overline{z_n} : n \in \mathbb{N}_0, z_i \in Z(x_i), x_1 \ldots x_n \in \langle X\rangle_{irr}\}$, onde $\overline{z_i} = z_i + I$.*

Prova Basta notar que, nas condições acima, o conjunto $\{z_1 \otimes \cdots \otimes z_n : n \in \mathbb{N}_0, z_i \in Z(x_i), x_1 \ldots x_n \in \langle X\rangle_{irr}\}$ forma uma base para $k\langle M\rangle_{irr}$. ■

4.2 Aplicação: coprodutos de k-anéis

Seja k um anel associativo com unidade. Comecemos esta seção por introduzir uma caracterização mais categórica para o objeto $k\langle M\rangle$. Usaremos aqui a definição alternativa, porém equivalente, de k-anel citada no início da seção anterior, isto é, vamos dotar o anel S de uma estrutura de k-bimódulo dada por:

$$\eta a = \phi_S(\eta)a, \quad a\mu = a\phi_S(\mu),$$

para $\eta, \mu \in k$ e $a \in k\langle M\rangle$. Nessa definição, um homomorfismo de k-anéis $g : R \longrightarrow S$ é uma aplicação que é ao mesmo tempo um homomorfismo de k-bimódulos e um homomorfismo de anéis e que leva o elemento unidade de R no elemento unidade de S.

Dada uma família $(M_x)_{x\in X}$ de k-bimódulos, construímos, como na seção anterior o k-anel tensorial da soma direta dos módulos M_x, que é denotado por $k\langle M\rangle$. Se indicarmos por $i_x : M_x \longrightarrow k\langle M\rangle$ a injeção natural de M_x em $k\langle M\rangle$, que é um homomorfismo de k-bimódulos, podemos enunciar a seguinte propriedade universal para $k\langle M\rangle$. Seja R um k-anel e, para cada $x \in X$, seja $g_x : M_x \longrightarrow R$ um homomorfismo de k-bimódulos. Então existe um único homomorfismo de k-anéis $\overline{g} : k\langle M\rangle \longrightarrow R$ que satisfaz $\overline{g}i_x = g_x$, para todo $x \in X$.

Vamos indicar por M a soma direta $\bigoplus_{x\in X} M_x$ e por α a injeção natural de M em $T(M) = k\langle M\rangle$. Se, para cada $x \in X$, denotarmos por j_x a injeção natural de M_x em M, teremos $i_x = \alpha j_x$. Como M é a soma direta dos k-bimódulos M_x, existe um único homomorfismo de k-bimódulos $g : M \longrightarrow R$ tal que $gj_x = g_x$, para todo $x \in X$. Como

$k\langle M\rangle$ é o k-anel tensorial de M, existe um único homomorfismo de k-anéis $\overline{g} : k\langle M\rangle \longrightarrow R$ tal que $\overline{g}\alpha = g$, para cada $x \in X$. Temos, então, para cada $x \in X$,

$$g_x = gj_x = (\overline{g}\alpha)j_x = \overline{g}(\alpha j_x) = \overline{g}i_x.$$

A aplicação $\overline{g}$ é o único homomorfismo de k-anéis $\psi : k\langle M\rangle \longrightarrow R$ tal que $\psi i_x = g_x$, para todo $x \in X$, pois $k\langle M\rangle$ é gerado como k-anel por 1 e pelos elementos $i_x(m_x)$, com $x \in X$ e m_x percorrendo M_x.

Seja $(R_\lambda)_{\lambda\in\Lambda}$ uma família de k-anéis. Por um *coproduto* da família (R_λ) sobre k, denotado por $\coprod_k R_\lambda$, entende-se um conjunto $\{R, j_\lambda : \lambda \in \Lambda\}$, onde R é um k-anel e, para cada $\lambda \in \Lambda$, $j_\lambda : R_\lambda \longrightarrow R$ é um homomorfismo de k-anéis, tais que se S é um k-anel e $g_\lambda : R_\lambda \longrightarrow S$, $\lambda \in \Lambda$, são homomorfismos de k-anéis, então existe um único homomorfismo de k-anéis $g : R \longrightarrow S$ tal que $gj_\lambda = g_\lambda$, para cada $\lambda \in \Lambda$. Em termos de diagramas, essa condição é equivalente a dizer que todo diagrama

$$\begin{tikzcd} S & R \arrow[l, "g"'] \\ & R_\lambda \arrow[u, "j_\lambda"'] \arrow[ul, "g_\lambda"] \end{tikzcd}$$

é comutativo. Prova-se que se $\{R, j_\lambda\}$ e $\{R', j'_\lambda\}$ são dois coprodutos de (R_λ) sobre k, então existe um único isomorfismo $\theta : R \longrightarrow R'$ tal que $\theta j_\lambda = j'_\lambda$, para todo $\lambda \in \Lambda$. Em vista disso, diremos simplesmente *o* coproduto de (R_λ). É importante ressaltar que, nas categorias de k-anéis, coprodutos sempre existem (vide [6, p. 142, Th. III.6.1]).

Dizemos que um k-anel (R, ϕ_R) é *fiel* se o homomorfismo ϕ_R for injetor. Na definição alternativa que estamos adotando, isto é equivalente a dizer que o conjunto $Ann(R) = \{\eta \in k : \eta R = \{0\}\}$, chamado *anulador* de R, é o conjunto $\{0\}$. Nessas condições, podemos identificar o anel k com o subanel $\phi_R(k)$ e, assim, k será um sub-anel de R que, olhado como k-bimódulo, é também um sub-k-bimódulo de R, ou, mais simplesmente, um *sub-k-anel* de R.

Corolário 4.3 *Seja $(R_\lambda)_{\lambda\in\Lambda}$ uma família de k-anéis fiéis, dos quais k é um somando direto como k-bimódulo, isto é, existem k-bimódulos M_λ tais que $R_\lambda = k \bigoplus M_\lambda$. Então o coproduto $R = \coprod_k R_\lambda$ é isomorfo, como k-bimódulo, à soma direta de todos os produtos tensoriais $M_{\lambda_1} \otimes_k \cdots \otimes_k M_{\lambda_n}$, onde $n \geq 0$ e $\lambda_1, \ldots, \lambda_n \in \Lambda$, com dois λ_i's sucessivos diferentes. (Quando $n = 0$ estamos referindo-nos ao somando k.)*

Prova Sejam $\langle\Lambda\rangle$ o semigrupo livre com unidade gerado por Λ e $k\langle M\rangle$ o k-anel tensorial de $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$, isto é, $k\langle M\rangle = \bigoplus_{\langle\Lambda\rangle} P_A$, onde $A \in \langle\Lambda\rangle$, e se $A = \lambda_1 \ldots \lambda_n$, $P_A = M_{\lambda_1} \otimes_k \cdots \otimes_k M_{\lambda_n}$. Seja S o sistema de redução para $k\langle M\rangle$ formado pelos pares $\sigma_\lambda = (\lambda^2, m_\lambda)$, com $\lambda \in \Lambda$, onde $m_\lambda : M_\lambda \otimes_k M_\lambda \longrightarrow R_\lambda = k \bigoplus M_\lambda$ é o homomorfismo de k-bimódulos induzido pela multiplicação de R_λ, ou seja, se $x, y \in M_\lambda \subseteq R_\lambda$, então $m_\lambda(x \otimes y) = xy \in R_\lambda$. Nessas condições, se a e b são elementos arbitrários de R_λ, então, podemos escrever $a = \mu + x$ e $b = \mu' + x'$, com $\mu, \mu' \in k$ e $x, x' \in M_\lambda$. Logo,

$$\begin{aligned} a \otimes b &= \mu \otimes \mu' + \mu \otimes x' + x \otimes \mu' + x \otimes x' \\ &= \mu\mu' + \mu x' + x\mu' + x \otimes x'. \end{aligned}$$

Note que foi utilizado o fato de haver isomorfismos entre $k \otimes_k M_\lambda$ e M_λ e entre $M_\lambda \otimes_k k$ e M_λ que levam, respectivamente, $\mu \otimes x$ em μx e $x \otimes \mu$ em $x\mu$ quaisquer que sejam $\mu \in k$ e $x \in M_\lambda$. Calculando, agora, a redução $r_{1\sigma_\lambda 1}$ em $a \otimes b$, obtemos

$$\begin{aligned} r_{1\sigma_\lambda 1}(a \otimes b) &= \mu\mu' + \mu x' + x\mu' + m_\lambda(x \otimes x') \\ &= \mu\mu' + \mu x' + x\mu' + xx' \\ &= ab. \end{aligned}$$

Seja I o ideal de $k\langle M\rangle$ gerado pelos elementos $x \otimes y - m_\lambda(x \otimes y) = x \otimes y - xy$, com λ percorrendo o conjunto Λ e $x, y \in M_\lambda$. Em vista da observação acima, podemos dizer que I é o ideal de $k\langle M\rangle$ gerado pelos elementos da forma $a \otimes b - r_{1\sigma_\lambda 1}(a \otimes b) = a \otimes b - ab$, com $\lambda \in \Lambda$ e $a, b \in R_\lambda$.

Para cada $\lambda \in \Lambda$, seja $i_\lambda : R_\lambda \longrightarrow k\langle M\rangle$ a inclusão do sub-k-bimódulo $R_\lambda = k \bigoplus M_\lambda$ em $k\langle M\rangle$ e seja $\pi : k\langle M\rangle \longrightarrow k\langle M\rangle/I$ a projeção canônica. Afirma-se que $\{k\langle M\rangle/I, j_\lambda = \pi i_\lambda : \lambda \in \Lambda\}$ é o coproduto $\coprod_k R_\lambda$. De fato, sejam S um k-anel e, para cada λ, $g_\lambda : R_\lambda \longrightarrow S$ um homomorfismo de k-anéis. Se, para cada λ, indicarmos por $i_\lambda|_{M_\lambda}$ a restrição de i_λ a M_λ, então $i_\lambda|_{M_\lambda}$ será a inclusão de M_λ em $k\langle M\rangle$ e, portanto, pela propriedade universal de $k\langle M\rangle$, existirá um único homomorfismo de k-anéis $g : k\langle M\rangle \longrightarrow S$ tal que, para cada λ, temos $gi_\lambda|_{M_\lambda} = g_\lambda|_{M_\lambda}$, onde $g_\lambda|_{M_\lambda} : M_\lambda \longrightarrow S$ é o homomorfismo de k-bimódulos obtido por restrição de g_λ a M_λ. Ou seja, gi_λ e g_λ são homomorfismos de k-bimódulos de $R_\lambda = k \bigoplus M_\lambda$ em S que coincidem em M_λ e, além disso, temos que $gi_\lambda(1) = g(1) = 1 = g_\lambda(1)$, pois g_λ e g são homomorfismos de k-anéis. Portanto, devem coincidir em todo o domínio, isto é, $gi_\lambda = g_\lambda$. Ressalta-se que as aplicações i_λ, apesar

de serem homomorfismos de k-bimódulos, não são homomorfismos de k-anéis, porém, as aplicações $\pi i_\lambda : R_\lambda \longrightarrow k\langle M\rangle/I$ o são, uma vez que, fixado $\lambda \in \Lambda$ e dados $a, b \in R_\lambda$, temos

$$\begin{aligned} \pi i_\lambda(ab) &= \pi(ab) \\ &= ab + I \\ &= (a \otimes b) + I, \end{aligned}$$

pois $a \otimes b - ab \in I$. Logo, $\pi i_\lambda(ab) = (a + I) \otimes (b + I) = \pi(a) \otimes \pi(b) = \pi i_\lambda(a) \otimes \pi i_\lambda(b)$. Além disso, se a e b são elementos arbitrários de R_λ, para algum $\lambda \in \Lambda$, temos

$$\begin{aligned} g(a \otimes b - ab) &= g(a)g(b) - g(ab) \\ &= gi_\lambda(a)gi_\lambda(b) - gi_\lambda(ab) \\ &= g_\lambda(a)g_\lambda(b) - g_\lambda(ab) \\ &= 0, \end{aligned}$$

uma vez que g_λ é homomorfismo de k-anéis (em particular, de anéis) de R_λ em S. Logo, $I \subseteq ker(g)$. Portanto existe um único homomorfismo de k-anéis $\overline{g} : k\langle M\rangle/I \longrightarrow S$ tal que $\overline{g}\pi = g$. Assim, para cada λ, temos

$$g_\lambda = gi_\lambda = (\overline{g}\pi)i_\lambda = \overline{g}(\pi i_\lambda).$$

A situação acima está expressa na comutatividade do diagrama que segue.

$$\begin{tikzcd}
 & & k\langle M\rangle \arrow[dr, "\pi"] \arrow[dd, "g"] & \\
M_\lambda \arrow[urr, "i_\lambda|M_\lambda"] \arrow[drr, "g_\lambda|M_\lambda"'] & R_\lambda \arrow[ur, "i_\lambda"] \arrow[dr, "g_\lambda"] & & k\langle M\rangle/I \arrow[dl, "\overline{g}"] \\
 & & S &
\end{tikzcd}$$

A aplicação $\overline{g}$ é o único homomorfismo de k-anéis $\varphi : k\langle M\rangle/I \longrightarrow S$ que satisfaz $g_\lambda = \varphi(\pi i_\lambda)$, pois $k\langle M\rangle/I$ é gerado, como k-anel por $1 + I$ e pelos elementos $\pi i_\lambda(a_\lambda)$, com $\lambda \in \Lambda$ e a_λ percorrendo R_λ, uma vez que $k\langle M\rangle$ é gerado, como k-anel, por 1 e pelos

elementos $i_\lambda(m_\lambda) \in M_\lambda \subseteq R_\lambda$, com $\lambda \in \Lambda$ e m_λ percorrendo M_λ. Logo, $\{k\langle M\rangle/I, j_\lambda = \pi i_\lambda : \lambda \in \Lambda\}$ é de fato o coproduto da família (R_λ).

A relação $<$ em $\langle\Lambda\rangle$, definida por $A < B$ se $cpt(A) < cpt(B)$, para $A, B \in \langle\Lambda\rangle$, é uma ordem parcial estrita de semigrupo em $\langle\Lambda\rangle$. Além disso, a ordem parcial $\leq$ obtida de $<$, definindo-se $A \leq B$ se $A < B$ ou $A = B$, é uma ordem parcial de semigrupo em $\langle\Lambda\rangle$ que tem c.c.d. Como, para todo λ, temos $m_\lambda(P_{\lambda^2}) \subseteq R_\lambda = k \oplus M_\lambda \subseteq \bigoplus_{A<\lambda^2} P_A$, a ordem $\leq$ e o sistema de redução S são compatíveis.

Se A é um monômio arbitrário de $\langle\Lambda\rangle$, por definição dos operadores lineares m_λ, é fácil ver que os elementos de P_A são redutíveis se e somente se A contém como subpalavra um monômio do tipo λ^2, para algum $\lambda \in \Lambda$. Assim, o sub-k-bimódulo $k\langle M\rangle_{irr}$ dos elementos irredutíveis de $k\langle M\rangle$ segundo S é a soma direta dos produtos tensoriais $M_{\lambda_1} \otimes_k \cdots \otimes_k M_{\lambda_n}$, nos quais não há ocorrência de dois λ_i's sucessivos iguais.

Por inspeção nos pares $\sigma_\lambda = (\lambda^2, m_\lambda)$ de S, conclui-se que as ambigüidades do sistema de redução são exatamente as 5-uplas $(\sigma_\lambda, \sigma_\lambda, \lambda, \lambda, \lambda)$; ou seja, para cada $\lambda \in \Lambda$, temos uma ambigüidade do tipo acima e, além disso, essas são as únicas ambigüidades de S.

Agora, verificadas todas as hipótese do Teorema 4.1, para obter o resultado desejado, que é fornecido, neste caso, pela afirmação (c) do Teorema, devemos estudar, por exemplo, a resolubilidade das ambigüidades do sistema de redução. Mostraremos, assim, que todas as ambigüidades são resolúveis. Dado $\lambda \in \Lambda$, mostraremos que para cada $a \in P_{\lambda^3}$, existem composições de reduções r e r' tais que $r(r_{1\sigma_\lambda\lambda}(a)) = r'(r_{\lambda\sigma_\lambda 1}(a))$. Como as reduções são aplicações k-lineares, basta mostrarmos o resultado para geradores de P_{λ^3}, ou seja, sendo $P_{\lambda^3} = M_\lambda \otimes_k M_\lambda \otimes_k M_\lambda$, é suficiente mostrarmos que existem (composições de) reduções r e r' tais que $r(r_{1\sigma_\lambda\lambda}(x \otimes y \otimes z)) = r'(r_{\lambda\sigma_\lambda 1}(x \otimes y \otimes z))$, quaisquer que sejam $x, y, z \in M_\lambda$. Temos, por um lado, $r_{1\sigma_\lambda\lambda}(x \otimes y \otimes z) = r_{1\sigma_\lambda 1}(x \otimes y) \otimes z = xy \otimes z$, a primeira igualdade tendo sido obtida por intermédio de (4.1). Como $xy, z \in R_\lambda$, podemos aplicar a redução $r_{1\sigma_\lambda 1}$ ao elemento $xy \otimes z$. Assim obtemos

$$r_{1\sigma_\lambda 1}(r_{1\sigma_\lambda\lambda}(x \otimes y \otimes z)) = r_{1\sigma_\lambda 1}(xy \otimes z) = (xy)z.$$

Por outro lado, temos $r_{\lambda\sigma_\lambda 1}(x \otimes y \otimes z) = x \otimes r_{1\sigma_\lambda 1}(y \otimes z) = x \otimes yx$. E, portanto,

$$r_{1\sigma_\lambda 1}(r_{\lambda\sigma_\lambda 1}(x \otimes y \otimes z)) = r_{1\sigma_\lambda 1}(x \otimes yz) = x(yz).$$

Logo,

$$r_{1\sigma_\lambda 1}(r_{1\sigma_\lambda\lambda}(x \otimes y \otimes z)) = r_{1\sigma_\lambda 1}(r_{\lambda\sigma_\lambda 1}(x \otimes y \otimes z)),$$

o que quer dizer que a ambigüidade $(\sigma_\lambda, \sigma_\lambda, \lambda, \lambda, \lambda)$ é resolúvel. Portanto, como o λ escolhido foi arbitrário, todas as ambigüidades de S são resolúveis e, pelo Teorema 4.1 $(a) \Rightarrow (c)$, temos que $k\langle M\rangle/I = \coprod_k R_\lambda$ e $k\langle M\rangle_{irr}$ são isomorfos como k-bimódulos. ■

Bibliografia

[1] ADVANCED PROBLEM 5082, Amer. Math. Monthly **70** (1963), 335.

[2] ANICK, D. J., "On the homology of associative algebras", Trans. Amer. Math. Soc. **296**, No. 2 (1986), 641-659.

[3] BERGMAN, G. M., "The Diamond Lemma for ring theory", Adv. in Math. **29** (1978), 178-218.

[4] BLYTH, T. S., *Module Theory*, Clarendon, Oxford, 1977.

[5] LE BRUYN, L., "Homological properties of braided matrices", J. Algebra **170** (1994), 596-607.

[6] COHN, P. M., *Universal Algebra*, 2nd. edition, Mathematics and Its Aplications V. 6, D. Reidel, Dordrecht, 1981.

[7] COHN, P. M., *Free Rings and Their Relations*, 2nd. edition, Academic Press, London, 1985.

[8] COSTA, R., *Álgebras de Lie e Álgebras Associativas*, IV Escola de Álgebra, São Paulo, 1976.

[9] JACOBSON, N., *Lie Algebras*, Interscience, New York, 1962.

[10] JACOBSON, N., *Basic Algebra II*, W. H. Freeman, San Francisco, 1980.

[11] JOSEPH, A., "On the prime and primitive spectra of the algebra of functions on a quantum group", J. Algebra **169** (1994), 441-511.

[12] MAKAR-LIMANOV, L., "On subnormal subgroups of skew fields", J. Algebra **114** (1988), 261-267.

[13] MASUOKA, A., "Cleft extensions for a Hopf algebra generated by a nearly primitive element", Comm. Algebra **22**, Vol. 11 (1994), 4537-4559.

[14] MAULDON, J. G., "Nonorthogonal idempotents whose sum is idempotent", Amer. Math. Monthly **71** (1964), 963-973.

[15] NEWMAN, M. H., "On theories with combinatorial definition of 'equivalence'", Ann. Math. **43**, No. 2 (1942), 223-243.

[16] ROWEN, L., *Ring Theory*, Vol. 1, Academic Press, Boston, 1988.

[17] TAFT, E. J. & WILSON, R. L., "Hopf algebras with nonsemisimple antipode", Proc. Amer. Math. Soc. **49**, No. 2 (1975), 269-276.