

CORPOS DE FRAÇÕES NÃO COMUTATIVOS

VITOR DE OLIVEIRA FERREIRA

RESUMO. Veremos como a construção do corpo de frações de um domínio de integridade comutativo se generaliza para o contexto de anéis não necessariamente comutativos. Especial atenção será devotada aos chamados anéis de polinômios “skew”, uma generalização natural dos anéis de polinômios usuais, que reparte com esses muitas propriedades aritméticas. Como aplicação das técnicas apresentadas, veremos que, mesmo quando existe, o “corpo de frações” de um domínio de integridade não comutativo não é necessariamente único.

INTRODUÇÃO

Este texto contém o material apresentado no minicurso de mesmo título ministrado pelo autor na *XXIII Semana de Matemática* do Departamento de Matemática da UFRN, realizada em Natal, RN, no período de 17 a 21 de outubro de 2011.

O autor agradece aos organizadores do evento pelo convite.

1. DOMÍNIOS DE INTEGRIDADE COMUTATIVOS

Por convenção, todos os anéis tratados neste texto serão associativos e conterão um elemento identidade não nulo que é herdado por subanéis e preservado por homomorfismos. O conjunto dos elementos não nulos em um anel R será denotado por R^\times .

Um anel comutativo R é, por definição, um *domínio de integridade* se R não contiver divisores de zero, isto é, se para todos $a, b \in R$, $ab = 0$ implicar $a = 0$ ou $b = 0$.

Em um domínio de integridade R se $a, b, c \in R$ são tais que $ac = bc$ e $c \neq 0$, então $a = b$. Dizemos que em R temos “cancelamento”.

Exemplos. (1) Corpos são domínios de integridade. (Lembremos que um anel comutativo R é um *corpo* se para todo $a \in R, a \neq 0$, existir $a^{-1} \in R$ tal que $aa^{-1} = 1$.)

(2) O anel dos números inteiros \mathbb{Z} é um domínio de integridade.

(3) Se \mathbb{k} é um corpo, o anel dos polinômios em uma indeterminada

$$\mathbb{k}[x] = \{\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n : n \geq 0, \alpha_i \in \mathbb{k}\}$$

sobre \mathbb{k} é um domínio de integridade.

Todo subanel de um domínio de integridade é um domínio de integridade. Em particular, todo subanel de um corpo é um domínio de integridade. O teorema abaixo mostra que os subanéis de corpos são, na realidade, todos os domínios de integridade.

Teorema 1. *Um anel comutativo R é um domínio de integridade se, e somente se, existir um corpo K e um homomorfismo injetor $R \rightarrow K$.*

Demonstração. A condição é claramente suficiente, como já observamos acima. Para demonstrar que é também necessária, procedemos à construção do “corpo de frações” de R . (Daremos uma definição precisa abaixo.)

Definimos no conjunto $R \times R^\times$ a seguinte relação:

$$(a, b) \sim (c, d) \iff ad = bc.$$

Essa relação é reflexiva e simétrica, pois R é comutativo, e é transitiva, pois $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$ implicam $adf = bcf = bde$ e, por cancelamento de d , segue $(a, b) \sim (e, f)$. Em outras palavras, \sim é uma relação de equivalência no conjunto $R \times R^\times$.

Dado $(a, b) \in R \times R^\times$, a classe de equivalência de (a, b) com respeito à relação \sim será denotada por $[(a, b)]$, isto é, $[(a, b)] = \{(c, d) \in R \times R^\times : ad = bc\}$. No conjunto quociente $(R \times R^\times)/\sim = \{[(a, b)] : (a, b) \in R \times R^\times\}$, definimos duas operações binárias, $+$ (soma) e \cdot (multiplicação), da seguinte maneira,

$$[(a, b)] + [(c, d)] = [(ad + cb, bd)] \quad \text{e} \quad [(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

Observe que as classes de equivalência que ocorrem nos lados direitos das igualdades acima estão bem definidas, uma vez que como $b, d \in R^\times$ e R é um domínio de integridade, $bd \in R^\times$.

Como nas definições de soma e multiplicação acima fizemos escolhas de representantes das classes de equivalência que estavam sendo operadas, é necessário mostrar que as definições não dependem das escolhas desses representantes. Assim, dados $(a, b), (a', b'), (c, d), (c', d') \in R \times R^\times$ tais que $(a, b) \sim (a', b')$ e $(c, d) \sim (c', d')$, temos $(ad + cb)b'd' = ab'dd' + cd'bb' = ba'dd' + dc'bb' = (a'd' + c'b')bd$ e, portanto, $(ad + cb, bd) \sim (a'd' + c'b', b'd')$. A verificação de que a multiplicação também independe da escolha dos representantes é semelhante.

É uma verificação rotineira o fato de que com as operações definidas acima, o conjunto $(R \times R^\times)/\sim$, que denotaremos de agora em diante por $\text{Frac}(R)$, é um anel comutativo com elemento neutro $[(0, 1)]$ e identidade $[(1, 1)]$. Ainda, $\text{Frac}(R)$ é um corpo, uma vez que se $[(a, b)] \neq [(0, 1)]$, então $a \neq 0$ e, portanto, $[(b, a)] \in \text{Frac}(R)$. (Veja o Exercício 1 abaixo.)

Finalmente, a função $\lambda: R \rightarrow \text{Frac}(R)$, definida por $\lambda(a) = [(a, 1)]$, para todo $a \in R$, é um homomorfismo injetor (Exercício 1). \square

Os elementos de $\text{Frac}(R)$ são denotados usualmente por frações, $\frac{a}{b} = [(a, b)]$. O homomorfismo injetor λ construído acima é chamado *imersão canônica* de R em $\text{Frac}(R)$.

Exercício 1. No contexto da construção de $\text{Frac}(R)$ a partir do domínio de integridade R na demonstração do Teorema 1, demonstre que $[(0, 1)] = [(0, b)]$ e $[(1, 1)] = [(b, b)]$, qualquer que seja $b \in R^\times$. Mostre também que $[(a, b)] = [(0, 1)]$ se, e somente se, $a = 0$. E conclua que se $a \in R^\times$, então $[(a, b)] \cdot [(b, a)] = [(1, 1)]$.

Mostre que a função $\lambda: R \rightarrow \text{Frac}(R)$ é um homomorfismo injetor.

A construção do corpo $\text{Frac}(R)$ apresentada acima foi descrita pela primeira vez por E. Steinitz em 1910 no contexto da aritmetização da análise, trabalho ao qual se dedicaram muitos matemáticos no final do século XIX (cf. [10]). Esse é o método ensinado em cursos de matemática nos dias de hoje e generaliza a construção do corpo dos números racionais a partir do domínio de integridade dos números inteiros (ver, por exemplo, [12, Section 21] ou, para um texto em português, [13, Seção III.5]).

Um segundo exemplo da aplicação desse método é o da construção do corpo $\mathbb{k}(x)$ das *frações racionais* em uma indeterminada sobre um corpo \mathbb{k} . Por definição,

$$\mathbb{k}(x) = \text{Frac}(\mathbb{k}[x]) = \left\{ \frac{f}{g} : f, g \in \mathbb{k}[x], g \neq 0 \right\}.$$

Nas aplicações, fazemos mais uso da seguinte propriedade “universal” do corpo $\text{Frac}(R)$ do que de sua construção propriamente dita.

Teorema 2. *Seja R um domínio de integridade. Então, dado um corpo K e um homomorfismo injetor $\varphi: R \rightarrow K$, existe um único homomorfismo $\psi: \text{Frac}(R) \rightarrow K$ tal que $\psi\lambda = \varphi$, onde $\lambda: R \rightarrow \text{Frac}(R)$ denota a imersão canônica.*

Observe que o homomorfismo ψ no enunciado do teorema acima será injetor, uma vez que tem como domínio um corpo.

Demonstração. Defina $\psi: \text{Frac}(R) \rightarrow K$ por $\psi\left(\frac{a}{b}\right) = \varphi(a)\varphi(b)^{-1}$, para todo $\frac{a}{b} \in \text{Frac}(R)$. Note que como $b \in R^\times$ e φ é injetor, $\varphi(b) \neq 0$ e, portanto, é inversível em K . A função ψ está bem definida, uma vez que se $\frac{a}{b} = \frac{a'}{b'}$, então $\varphi(a)\varphi(b') = \varphi(ab') = \varphi(a'b) = \varphi(a')\varphi(b)$ e, assim, $\varphi(a)\varphi(b)^{-1} = \varphi(a')\varphi(b')^{-1}$.

Além disso, ψ é um homomorfismo, pois $\psi\left(\frac{1}{1}\right) = \varphi(1)\varphi(1)^{-1} = 1$ e se $\frac{a}{b}, \frac{c}{d} \in \text{Frac}(R)$, temos

$$\begin{aligned}\psi\left(\frac{a}{b} + \frac{c}{d}\right) &= \psi\left(\frac{ad + cb}{bd}\right) = \varphi(ad + cb)\varphi(bd)^{-1} \\ &= (\varphi(a)\varphi(d) + \varphi(c)\varphi(b))\varphi(b)^{-1}\varphi(d)^{-1} \\ &= \varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1} \\ &= \psi\left(\frac{a}{b}\right) + \psi\left(\frac{c}{d}\right)\end{aligned}$$

e

$$\psi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \psi\left(\frac{ac}{bd}\right) = \varphi(ac)\varphi(bd)^{-1} = \varphi(a)\varphi(b)^{-1}\varphi(c)\varphi(d)^{-1} = \psi\left(\frac{a}{b}\right)\psi\left(\frac{c}{d}\right).$$

Finalmente, se $\rho: \text{Frac}(R) \rightarrow K$ é um homomorfismo que satisfaz $\rho\lambda = \varphi$, então, para todo $\frac{a}{b} \in \text{Frac}(R)$, temos

$$\begin{aligned}\rho\left(\frac{a}{b}\right) &= \rho\left(\frac{a}{1} \cdot \frac{1}{b}\right) = \rho\left(\frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1}\right) = \rho\left(\frac{a}{1}\right)\rho\left(\frac{b}{1}\right)^{-1} \\ &= \rho\lambda(a)\rho\lambda(b)^{-1} = \varphi(a)\varphi(b)^{-1} = \psi\left(\frac{a}{b}\right),\end{aligned}$$

ou seja, $\rho = \psi$. □

Uma consequência importante do teorema acima é o fato de o corpo $\text{Frac}(R)$ ser único, num sentido que será precisado no Corolário 3.

Dados um anel R , um par (K, ρ) , onde K é um corpo e $\rho: R \rightarrow K$ é um homomorfismo injetor, é um *corpo de frações* de R se para todo subcorpo K_0 de K tal que $\rho(R) \subseteq K_0$, tivermos $K_0 = K$. (Isso é o mesmo que dizer que K é gerado por $\rho(R)$ como um corpo.)

Vimos no Teorema 1 que um anel R é um domínio de integridade se, e somente se, R tiver um corpo de frações, uma vez que se $\rho: R \rightarrow K$ for um homomorfismo injetor de R em um corpo K , então o subcorpo de K gerado por $\rho(R)$ será um corpo de frações de R .

Ainda, se R é um domínio de integridade e se $\lambda: R \rightarrow \text{Frac}(R)$ é a imersão canônica, $(\text{Frac}(R), \lambda)$ é um corpo de frações de R , pois todo subcorpo de $\text{Frac}(R)$ que contiver $\lambda(R)$ deverá conter o conjunto $\{\lambda(a)\lambda(b)^{-1} : a, b \in R, b \neq 0\} = \text{Frac}(R)$.

Corolário 3. *Seja R um anel e seja (K, ρ) um corpo de frações de R . Então existe um isomorfismo $\psi: \text{Frac}(R) \rightarrow K$ tal que $\psi\lambda = \rho$, onde $\lambda: R \rightarrow \text{Frac}(R)$ denota a imersão canônica.*

Demonstração. Pelo Teorema 2, existe um homomorfismo (injetor) $\psi: \text{Frac}(R) \rightarrow K$ tal que $\psi\lambda = \rho$. Mas, $\psi(\text{Frac}(R))$ é um subcorpo de K que contém $\psi\lambda(R) = \rho(R)$. Portanto, $\psi(\text{Frac}(R)) = K$, isto é, ψ é também sobrejetor. □

Em vista do corolário acima, podemos chamar o corpo $\text{Frac}(R)$ construído a partir de um domínio de integridade R de *o corpo de frações de R* .

2. DOMÍNIOS DE ORE

Nesta seção veremos o que do que foi visto na seção anterior pode ser generalizado para o caso de anéis genéricos, não necessariamente comutativos. A pergunta mais natural, assim, é “quais são aqueles anéis que podem ser imersos em um corpo não necessariamente comutativo?”

Para abordar essa questão, vamos começar por precisar os termos utilizados.

Definição. Um anel R não necessariamente comutativo é um *domínio de integridade*, ou simplesmente, um *domínio*, se para todos $a, b \in R$, $ab = 0$ implicar $a = 0$ ou $b = 0$. (Esta é a mesma definição de domínio de integridade comutativo, exceto por não fazermos agora a exigência da comutatividade de R .)

Um anel R é um *anel com divisão* se todo elemento não nulo de R for inversível em R , ou seja, se para todo $a \in R$, $a \neq 0$, existir $a^{-1} \in R$ tal que $aa^{-1} = a^{-1}a = 1$. (Isto é, os anéis com divisão são justamente os “corpos não necessariamente comutativos”.)

É claro que os anéis com divisão comutativos são exatamente os corpos. O primeiro anel com divisão não comutativo foi construído por W. R. Hamilton em 1843 e é conhecido como o anel com divisão dos *quatérnios*. Esse anel é o conjunto $\mathbb{H}_{\mathbb{R}}$ formado por todas as combinações lineares reais dos símbolos $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$. Trata-se, então, de um espaço vetorial sobre \mathbb{R} de dimensão 4, com multiplicação satisfazendo as seguintes regras,

$$\mathbf{i}^2 = \mathbf{j}^2 = -\mathbf{1}, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k},$$

e $(\alpha\mathbf{x})(\beta\mathbf{y}) = (\alpha\beta)(\mathbf{xy})$, para todos $\alpha, \beta \in \mathbb{R}$ e $\mathbf{x}, \mathbf{y} \in \{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Observe que $\mathbb{H}_{\mathbb{R}}$ não é comutativo e é de fato um anel com divisão porque $\mathbf{1}$ é seu elemento identidade e dados $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ não todos nulos, temos

$$(\alpha\mathbf{1} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k})(\alpha\mathbf{1} - \beta\mathbf{i} - \gamma\mathbf{j} - \delta\mathbf{k}) = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)\mathbf{1}.$$

Teremos a oportunidade de encontrar o anel com divisão dos quatérnios novamente na próxima seção. (Para uma contextualização histórica da descoberta dos quatérnios, ver [19].)

Observemos que, assim como ocorria no caso comutativo, todo anel com divisão é um domínio e todo subanel de um domínio é ainda um domínio. Em particular, todo subanel de um anel com divisão é um domínio.

Porém, ao contrário do que acontece no caso comutativo, existem domínios que não podem ser imersos em um anel com divisão. O primeiro exemplo de um anel com essas características foi construído por A. I. Malcev em 1937. Neste texto, trataremos de um problema mais restrito e cujos detalhes apresentamos abaixo.

Suponha que R seja um anel e suponha que exista um anel com divisão Q que contém R como subanel e que satisfaz a seguinte condição: todo elemento de Q é da forma ab^{-1} , com $a, b \in R$, $b \neq 0$. Neste caso, dados $a, b \in R$ com $b \neq 0$, temos $b^{-1}a \in Q$ e, portanto, existem $c, d \in R$, $d \neq 0$, tais que $b^{-1}a = cd^{-1}$, o que implica $ad = bc$. Se $a \neq 0$, como R é um domínio (por ser um subanel de um anel com divisão), teremos $0 \neq ad = bc \in aR \cap bR$. O. Ore em 1931 observou que essa condição, juntamente com o fato de R não conter divisores de zero, é também suficiente para garantir que R seja imersível em um anel com divisão, como veremos abaixo.

Definição. Um anel R é um *domínio de Ore à direita* se R for um domínio e se para todos $a, b \in R^\times$, $aR \cap bR \neq \{0\}$.

Observe que um anel comutativo é um domínio de Ore à direita se, e somente se, for um domínio de integridade. Assim, domínios de Ore são uma generalização de domínios de integridade comutativos. Na próxima seção veremos exemplos de domínios de Ore não comutativos. Claro que, por simetria, podemos definir também domínios de Ore à esquerda.

Teorema 4. *Seja R um anel. Então existe um anel com divisão Q e um homomorfismo injetor $\lambda: R \rightarrow Q$ tais que todo elemento de Q pode ser escrito na forma $\lambda(a)\lambda(b)^{-1}$, com $a, b \in R$, $b \neq 0$ se, e somente se, R for um domínio de Ore à direita.*

Demonstração. No parágrafo que precede a definição de domínio de Ore à direita, vimos que a condição é necessária. A suficiência é demonstrada de maneira análoga à construção do corpo de frações de um domínio de integridade comutativo, porém as verificações dos detalhes são mais longas, como veremos abaixo.

Assim, assumamos que R é um domínio de Ore à direita e definamos no conjunto $R \times R^\times$ a seguinte relação:

$$(1) \quad (a, b) \sim (c, d) \iff \text{existem } u, v \in R^\times \text{ tais que } au = cv \text{ e } bu = dv.$$

Em outras palavras, e de maneira menos precisa, os pares (a, b) e (c, d) (que serão pensados como frações) estarão relacionados se quando colocados sobre o mesmo denominador, os numeradores coincidirem¹.

Mostremos que a relação definida em (1) é uma relação de equivalência. Ela é claramente simétrica. Dado $(a, b) \in R \times R^\times$, para mostrar que $(a, b) \sim (a, b)$, basta tomar $u = v = 1$ em (1). Finalmente, sejam $(a, b), (c, d), (e, f) \in R \times R^\times$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Então existem $u, v, s, t \in R^\times$ tais que

$$\begin{cases} au = cv \\ bu = dv \end{cases} \quad \text{e} \quad \begin{cases} cs = et \\ ds = ft \end{cases}$$

Pela condição de Ore, $vR \cap sR \neq \{0\}$ e, portanto, existem $p, q \in R$ tais que $vp = sq \neq 0$. Em particular, $p, q \in R^\times$. Assim, $a(up) = cvp = csq = e(tq)$ e $b(up) = dvp = dsq = f(tq)$. Como R é um domínio, $up, tq \in R^\times$. Segue $(a, b) \sim (e, f)$.

Denote por $(R \times R^\times)/\sim$ o conjunto quociente e por $[(a, b)]$ a classe de equivalência de $(a, b) \in R \times R^\times$ com respeito à relação \sim , isto é, $[(a, b)]$ é aquele elemento de $(R \times R^\times)/\sim$ definido por

$$[(a, b)] = \{(c, d) \in R \times R^\times : (c, d) \sim (a, b)\}.$$

Vamos, agora, definir operações binárias em $(R \times R^\times)/\sim$ com respeito às quais o conjunto quociente será um anel. Começamos por definir a adição. Assim, dados $(a, b), (c, d) \in R \times R^\times$ definimos

$$(2) \quad [(a, b)] + [(c, d)] = [(ae + cf, be)], \text{ onde } e, f \in R^\times \text{ são tais que } be = df.$$

Observe que como $b, d \in R^\times$, pela condição de Ore à direita, temos $bR \cap dR \neq \{0\}$ e, portanto, existem $e, f \in R$ tais que $be = df \neq 0$. Em particular, $e, f \in R^\times$.

É preciso mostrar que essa operação está bem definida, o que, neste caso, envolve a verificação de que a definição em (2) não depende da escolha dos elementos auxiliares e, f e que, além disso, não depende das escolhas dos representantes das classes de equivalência $[(a, b)]$ e $[(c, d)]$.

Sejam então $e, f, e', f' \in R^\times$ tais que $be = df$ e $be' = df'$. Pela condição de Ore à direita, existem $r, s \in R^\times$ tais que $er = e's$. Assim, $dfr = ber = be's = df's$ e, como $d \neq 0$, segue $fr = f's$. Portanto, $(ae + cf)r = (ae' + cf')s$ e $(be)r = (be')s$. Logo, $(ae + cf, be) \sim (ae' + cf', be')$.

Mostremos, agora, que a definição em (2) não depende da escolha dos representantes no primeiro termo. Assim, sejam $(a, b), (a', b'), (c, d) \in R \times R^\times$ tais que $(a, b) \sim (a', b')$. Então existem $p, q \in R^\times$ tais que $ap = a'q$ e $bp = b'q$. Pela condição de Ore à direita, $dR \cap b'pR \neq \{0\}$ e, portanto, existem $x, y \in R^\times$ tais que $dx = b'py = b'qy$. Logo, pelo que vimos no parágrafo anterior, $(ae + cf, be) \sim (apy + cx, b'py)$ e $(a'e + cf, b'e) \sim (a'qy + cx, b'qy)$, onde $e, f \in R^\times$ são tais que $be = df$. Mas $apy = a'qy$ e, portanto, $(apy + cx, b'py) = (a'qy + cx, b'qy)$. Logo $(ae + cf, be) \sim (a'e + cf, b'e)$.

Observe que a definição da adição em (2) é simétrica e, assim, também independe da escolha de representantes do segundo termo.

Passamos, agora, à definição da multiplicação em $(R \times R^\times)/\sim$. Sejam $(a, b), (c, d) \in R \times R^\times$. Definimos

$$(3) \quad [(a, b)] \cdot [(c, d)] = [(af, de)], \text{ onde } e \in R^\times, f \in R \text{ são tais que } ce = bf.$$

Aqui, se $c \in R^\times$, pela condição de Ore à direita, existem $e, f \in R^\times$ tais que $ce = bf$, ao passo que se $c = 0$, basta tomar $f = 0$ e $e = 1$.

Novamente, é necessário mostrar que a definição de multiplicação em (3) não depende das escolhas nem dos elementos auxiliares e, f , nem dos representantes das classes de equivalência. Essa verificação será deixada a cargo do leitor, assim como as verificações das demais afirmações não demonstradas nos próximos três parágrafos (veja o Exercício 2 abaixo).

¹Observe, também, que se R for um domínio de integridade comutativo, essa é exatamente a mesma relação de equivalência que definimos na demonstração do Teorema 1.

Afirmamos que com as operações definidas em (2) e (3), o conjunto $(R \times R^\times)/\sim$ é um anel associativo com elemento neutro para a adição $[(0, 1)]$, identidade $[(1, 1)]$ e tal que $-[(a, b)] = [(-a, b)]$, para todos $(a, b) \in R \times R^\times$. Esse anel será denotado por $Q_d(R)$.

Observe que $Q_d(R)$ é um anel com divisão, uma vez que se $[(a, b)] \neq [(0, 1)]$, então $a \neq 0$ e, portanto, $(b, a) \in R \times R^\times$. Assim, $[(a, b)] \cdot [(b, a)] = [(b, a)] \cdot [(a, b)] = [(1, 1)]$.

Finalmente, considere a função $\lambda: R \rightarrow Q_d(R)$ definida por $\lambda(a) = [(a, 1)]$, para todo $a \in R$. Então λ é um homomorfismo de anéis porque $\lambda(1) = [(1, 1)]$ e se $a, c \in R$, então $\lambda(a + c) = [(a + c, 1)] = [(a, 1)] + [(c, 1)]$ (tomando $e = f = 1$ em (2)) e $[\lambda(a)\lambda(c)] = [(a, 1)] \cdot [(c, 1)]$ (tomando $e = 1, f = c$ em (3)). Além disso, λ é injetor pois se $a \in R$ é tal que $[(0, 1)] = \lambda(a) = [(a, 1)]$, então $a = 0$. Por fim, dado $[(a, b)] \in Q_d(R)$, temos $[(a, b)] = [(a, 1)] \cdot [(1, b)] = [(a, 1)] \cdot [(b, 1)]^{-1} = \lambda(a)\lambda(b)^{-1}$. \square

Exercício 2. Com a notação da demonstração do Teorema 4 acima, demonstre as afirmações abaixo.

- (1) A definição de multiplicação no conjunto $(R \times R^\times)/\sim$ em (3) não depende nem das escolhas dos elementos auxiliares e, f , nem dos representantes das classes de equivalência.
- (2) $[(a, b)] + [(0, 1)] = [(a, b)]$, para todos $(a, b) \in R \times R^\times$.
- (3) $[(a, b)] = [(ac, bc)]$, para todos $(a, b) \in R \times R^\times$ e $c \in R^\times$.
- (4) $[(a, b)] \cdot [(1, 1)] = [(1, 1)] \cdot [(a, b)] = [(a, b)]$, para todos $(a, b) \in R \times R^\times$.
- (5) Para todo $b \in R^\times$, $[(b, b)] = [(1, 1)]$.
- (6) Com as operações definidas em (2) e (3), $(R \times R^\times)/\sim$ é um anel associativo com unidade.
- (7) Para todo $(a, b) \in R \times R^\times$, $[(a, b)] = [(0, 1)]$ se, e somente se, $a = 0$. Use esse fato para mostrar que $Q_d(R)$ é, de fato, um anel com divisão.

O método de Ore, descrito acima, foi completamente incorporado na teoria de anéis não comutativos e sua descrição pode ser encontradas em vários livros introdutórios sobre o assunto, como, por exemplo, [7], [18] e [22]. Seguimos neste texto, a apresentação da teoria encontrada em [21, Section 4].

A exemplo do que ocorre no caso comutativo, $Q_d(R)$ também satisfaz uma propriedade universal.

Teorema 5. *Seja R um domínio de Ore à direita. Então, dado um anel com divisão D e um homomorfismo injetor $\varphi: R \rightarrow D$, existe um único homomorfismo $\psi: Q_d(R) \rightarrow D$ (que é injetor, pois D é um anel com divisão) tal que $\psi\lambda = \varphi$, onde $\lambda: R \rightarrow Q_d(R)$ é o homomorfismo definido na demonstração do Teorema 4.*

Exercício 3. Demonstre o Teorema 5. (Sugestão: Defina $\psi([(a, b)]) = \lambda(a)\lambda(b)^{-1}$, para cada $(a, b) \in R \times R^\times$, e tente imitar a demonstração do Teorema 2.)

A definição de corpo de frações de um domínio de integridade comutativo, que vimos na Seção 1, faz sentido no contexto não comutativo.

Definição. *Seja R um anel não necessariamente comutativo. Um par (ρ, D) , onde D é um anel com divisão e $\rho: R \rightarrow D$ é um homomorfismo injetor, é um anel com divisão de frações de R se para todo subanel com divisão D_0 de D tal que $\rho(R) \subseteq D_0$, tivermos $D_0 = D$.*

Exercício 4. *Seja R um domínio de Ore à direita e seja $\lambda: R \rightarrow Q_d(R)$ o homomorfismo definido na demonstração do Teorema 4.*

- (1) Mostre que $(\lambda, Q_d(R))$ é um anel com divisão de frações de R .
- (2) Mostre que dado um anel com divisão de frações (ρ, D) de R , existe um único isomorfismo $\psi: Q_d(R) \rightarrow D$ tal que $\psi\lambda = \rho$.

Novamente, em vista do item (2) do Exercício 4, $Q_d(R)$ é chamado de o anel com divisão de frações do domínio de Ore à direita R e λ é chamado *imersão canônica* de R em $Q_d(R)$. É

comum utilizarmos o termo *corpo de frações* de R para nos referirmos a $Q_d(R)$, mesmo $Q_d(R)$ não sendo necessariamente um anel comutativo.

Se R é um domínio de Ore à esquerda, seu anel com divisão de frações é denotado por $Q_e(R)$.

Exercício 5. Mostre que se R é um domínio de Ore à direita e à esquerda, então $Q_d(R) \cong Q_e(R)$.

Exercício 6. Mostre que se R é um domínio de integridade comutativo, então $\text{Frac}(R) \cong Q_d(R)$.

A caracterização feita por Ore daqueles domínios R que têm anéis com divisão de frações cujos elementos são escritos na forma ab^{-1} , com $a, b \in R$, $b \neq 0$, passou aproximadamente 20 anos em hibernação no ambiente matemático. Foi apenas a partir dos trabalhos de A. Goldie nas décadas de 1950–60 que as ideias de Ore foram retomadas e proporcionaram um grande impulso no desenvolvimento do estudo de anéis noetherianos não necessariamente comutativos, uma área da álgebra que permanece vibrante até os dias de hoje. Para as contribuições de Goldie à teoria de anéis, ver [11]; para introduções (bastante completas) à teoria de anéis noetherianos não comutativos, indicamos [15] e [20].

Observação. O problema geral de descrição de quais são aqueles domínios que têm um anel com divisão de frações foi completamente resolvido por P. M. Cohn em 1971. A obra [5] contém a teoria desenvolvida por Cohn para a solução desse problema, entre outros resultados sobre anéis com divisão e anéis relacionados².

3. ANÉIS DE POLINÔMIOS SKEW

Nesta seção veremos que uma construção que generaliza a construção do anel de polinômios em uma indeterminada sobre um corpo fornece uma vasta família de exemplos de domínios de Ore.

Seja \mathbb{k} um corpo e seja σ um endomorfismo de \mathbb{k} , isto é, $\sigma: \mathbb{k} \rightarrow \mathbb{k}$ é um homomorfismo. (Repare que, porque \mathbb{k} é um corpo, σ é necessariamente injetor.) Considere o conjunto $\mathbb{k}[x; \sigma]$ formado por todos os polinômios na indeterminada x com coeficientes em \mathbb{k} à esquerda das potências de x ,

$$\mathbb{k}[x; \sigma] = \{ \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n : n \geq 0, \alpha_i \in \mathbb{k} \}.$$

A estrutura aditiva com a qual $\mathbb{k}[x; \sigma]$ será munido é a mesma que tem o anel de polinômios usual, isto é, dois elementos de $\mathbb{k}[x; \sigma]$ são somados somando coeficientes dos termos de mesmo grau. Definiremos, porém, uma multiplicação em $\mathbb{k}[x; \sigma]$ que levará em conta a ação de σ e fará de $\mathbb{k}[x; \sigma]$ um anel não necessariamente comutativo. Assim, dados $f, g \in \mathbb{k}[x; \sigma]$, digamos

$$f = \sum_{i=0}^n \alpha_i x^i \quad \text{e} \quad g = \sum_{j=0}^m \beta_j x^j,$$

definimos

$$fg = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} \alpha_i \sigma^i(\beta_j) \right) x^k.$$

Ou seja, a multiplicação em $\mathbb{k}[x; \sigma]$ é aquela função bilinear em $\mathbb{k}[x; \sigma]$ que satisfaz

$$x\alpha = \sigma(\alpha)x, \quad \text{para todo } \alpha \in \mathbb{k}, \quad \text{e} \quad x^i x^j = x^{i+j}, \quad \text{para todos } i, j \geq 0.$$

O conjunto $\mathbb{k}[x; \sigma]$ com as operações de adição e multiplicação definidas acima é um anel associativo com unidade. (Verifique essa afirmação.) Além disso, se $\sigma = I_{\mathbb{k}}$ é o endomorfismo identidade de \mathbb{k} , então $\mathbb{k}[x; \sigma] = \mathbb{k}[x]$, o anel de polinômios usual. Mas se $\sigma \neq I_{\mathbb{k}}$, então $\mathbb{k}[x; \sigma]$ não é um anel comutativo.

O anel $\mathbb{k}[x; \sigma]$ é chamado *anel de polinômios skew*, ou *extensão de Ore*, e foi definido pela primeira vez por Ore em 1933, justamente com o intuito de exemplificar o seu método de construção de corpos de frações não comutativos.

²Uma versão atualizada de [5] é o livro [8].

Vamos definir uma função grau $\text{gr}: \mathbb{k}[x; \sigma] \rightarrow \mathbb{N} \cup \{-\infty\}$ de maneira análoga ao caso comutativo: dado $f = \sum_{i=0}^n \alpha_i x^i \in \mathbb{k}[x; \sigma]$, com $\alpha_n \neq 0$, definimos $\text{gr}(f) = n$ e definimos $\text{gr}(0) = -\infty$. Aqui, $\mathbb{N} \cup \{-\infty\}$ deve ser entendido apenas como o conjunto dos números naturais \mathbb{N} acrescido de um símbolo $-\infty$ sujeito às seguintes condições: $z + (-\infty) = (-\infty) + z = -\infty$, para todo $z \in \mathbb{N} \cup \{-\infty\}$ e $-\infty < n$, para todo $n \in \mathbb{N}$.

Proposição 6. A função $\text{gr}: \mathbb{k}[x; \sigma] \rightarrow \mathbb{N} \cup \{-\infty\}$ tem as seguintes propriedades:

- (i) $\text{gr}(f + g) \leq \max\{\text{gr}(f), \text{gr}(g)\}$ e
- (ii) $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$,

para todos $f, g \in \mathbb{k}[x; \sigma]$.

Demonstração. Ambos os itens são verdadeiros se $f = 0$ ou $g = 0$, como é fácil de verificar. Suponha, então, que $f, g \in \mathbb{k}[x; \sigma]$ sejam tais que

$$f = \alpha_0 + \cdots + \alpha_n x^n, \text{ com } \alpha_n \neq 0, \text{ e } g = \beta_0 + \cdots + \beta_m x^m, \text{ com } \beta_m \neq 0.$$

- (i) Temos $f + g = \gamma_0 + \cdots + \gamma_t x^t$, onde $t = \max\{n, m\}$ e $\gamma_i = \alpha_i + \beta_i$ com a convenção de que $\alpha_i = 0$ se $i > n$ e $\beta_i = 0$ se $i > m$. Segue que $\text{gr}(f + g) \leq t$.
- (ii) Temos

$$fg = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} \alpha_i \sigma^i(\beta_j) \right) x^k = \sum_{k=0}^{n+m-1} \left(\sum_{i+j=k} \alpha_i \sigma^i(\beta_j) \right) x^k + \alpha_n \sigma^n(\beta_m) x^{n+m}.$$

Como σ é injetor, segue $\alpha_n \sigma^n(\beta_m) \neq 0$. Portanto $\text{gr}(fg) = n + m = \text{gr}(f) + \text{gr}(g)$. □

Uma consequência imediata do item (ii) da proposição acima é o fato de $\mathbb{k}[x; \sigma]$ ser um domínio. Na verdade, veremos que é possível deduzir da existência de uma função grau muito mais sobre as propriedades algébricas de $\mathbb{k}[x; \sigma]$.

Definição. Um anel R é um domínio de ideais à esquerda principais se R for um domínio e se para todo ideal à esquerda I de R , existir $a \in R$ tal que $I = Ra$.

Corolário 7. Se \mathbb{k} é um corpo e σ é um endomorfismo de \mathbb{k} , então $\mathbb{k}[x; \sigma]$ é um domínio de ideais à esquerda principais.

Demonstração. Já vimos que decorre do item (ii) da Proposição 6 que R é um domínio. Para mostrar que todo ideal à esquerda de $\mathbb{k}[x; \sigma]$ é principal, mostraremos que $\mathbb{k}[x; \sigma]$ satisfaz um algoritmo de divisão com respeito à função grau, mais precisamente, mostremos que dados $f, g \in \mathbb{k}[x; \sigma]$, $g \neq 0$, existem $q, r \in \mathbb{k}[x; \sigma]$ tais que

$$f = qg + r, \text{ com } \text{gr}(r) < \text{gr}(g).$$

De fato, se $\text{gr}(f) < \text{gr}(g)$, basta tomar $q = 0$ e $r = f$. Suponhamos, então, que $\text{gr}(f) \geq \text{gr}(g)$, digamos

$$f = \alpha_0 + \cdots + \alpha_n x^n, \text{ com } \alpha_n \neq 0, \quad g = \beta_0 + \cdots + \beta_m x^m, \text{ com } \beta_m \neq 0$$

e $n \geq m$. Procedemos por indução em $n - m$. Se $n - m = 0$, então basta tomar $q = \alpha_n \beta_n^{-1}$ e $r = f - \alpha_n \beta_n^{-1} g$. Suponha, então, que $n - m \geq 1$ e seja $f_1 = f - \alpha_n x^{n-m} \beta_m^{-1} g$. Se $\text{gr}(f_1) < \text{gr}(g)$, tome $q = \alpha_n x^{n-m} \beta_m^{-1}$ e $r = f_1$, caso contrário, como $\text{gr}(f_1) < \text{gr}(f)$, por hipótese de indução, existem $q_1, r \in \mathbb{k}[x; \sigma]$ tais que

$$f_1 = q_1 g + r, \text{ com } \text{gr}(r) < \text{gr}(g).$$

Portanto, $f = (\alpha_n x^{n-m} \beta_m^{-1} + q_1)g + r$ e $\text{gr}(r) < \text{gr}(g)$.

Agora, vejamos porque $\mathbb{k}[x; \sigma]$ é um domínio de ideais à esquerda principais. Seja I um ideal à esquerda de $R = \mathbb{k}[x; \sigma]$. Se $I = \{0\}$, então, $I = R0$. Se $I \neq \{0\}$, tome $g \in I$, $g \neq 0$, com $\text{gr}(g)$ mínimo entre os graus dos elementos não nulos de I . Mostremos que $I = Rg$. De fato, se $f \in I$, então, com vimos acima, existem $q, r \in \mathbb{k}[x; \sigma]$ tais que $f = qg + r$, com $\text{gr}(r) < \text{gr}(g)$. Logo $r = f - qg \in I$, pois I é um ideal à esquerda. Como $\text{gr}(r) < \text{gr}(g)$, devemos ter $r = 0$. Portanto, $f = qg \in Rg$. □

Para concluir que anéis de polinômios skew são exemplos de domínios de Ore, resta demonstrarmos o resultado abaixo.

Teorema 8. *Todo domínio de ideais à esquerda principais é um domínio de Ore à esquerda.*

Demonstração. Seja R um domínio de ideais à esquerda principais e sejam $a, b \in R^\times$. Precisamos mostrar que $Ra \cap Rb \neq \{0\}$. Suponha, por contradição, que $Ra \cap Rb = \{0\}$. Seja I o ideal à esquerda de R gerado por a e b , isto é, $I = Ra + Rb$. Por hipótese, existe $c \in R$ tal que $I = Rc$. Como $a \in I$, temos $a = xc$, para algum $x \in R$. (Note que $x \neq 0$, uma vez que $a \in R^\times$.) Além disso, por definição de I , existem $y, z \in R$ tais que $c = ya + zb$. Portanto, $a = xc = xya + xzb$. Logo, $(1 - xy)a = xzb \in Ra \cap Rb = \{0\}$. Donde segue $xzb = 0$ e isso implica $z = 0$, pois $x \neq 0$ e $b \neq 0$. Porém, nesse caso, teríamos $c = ya \in Ra$ e, assim, $b \in Rc \subseteq Ra$, implicando $0 \neq b \in Ra \cap Rb = \{0\}$, o que é impossível. Logo $Ra \cap Rb \neq \{0\}$. \square

O corolário abaixo segue imediatamente do Teorema 8 e do Corolário 7.

Corolário 9. *Se \mathbb{k} é um corpo e σ é um endomorfismo de \mathbb{k} , então $\mathbb{k}[x; \sigma]$ é um domínio de Ore à esquerda.* \square

Um comentário importante é que nem sempre nas condições do Corolário 9 o anel de polinômios skew será um domínio de Ore à direita. Essa assimetria será explorada na próxima seção. Uma condição necessária para garantir a assimetria está apresentada abaixo.

Proposição 10. *Seja \mathbb{k} um corpo e seja σ um endomorfismo de \mathbb{k} . Se σ não é sobrejetor, $\mathbb{k}[x; \sigma]$ não é um domínio de Ore à direita.*

Demonstração. Denote $R = \mathbb{k}[x; \sigma]$. Se σ não é sobrejetor, existe $\gamma \in \mathbb{k}$ tal que $\gamma \notin \sigma(\mathbb{k})$. Mostraremos que $xR \cap \gamma xR = \{0\}$, apesar de $x, \gamma x \in R^\times$. Suponha que $xR \cap \gamma xR \neq \{0\}$. Então existem $f, g \in R$ tais que $xf = \gamma xg \neq 0$. Digamos que

$$f = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n, \text{ com } \alpha_n \neq 0, \quad \text{e} \quad g = \beta_0 + \beta_1 x + \cdots + \beta_m x^m, \text{ com } \beta_m \neq 0.$$

Então

$$xf = \sigma(\alpha_0)x + \sigma(\alpha_1)x^2 + \cdots + \sigma(\alpha_n)x^{n+1}$$

e

$$\gamma xg = \gamma\sigma(\beta_0)x + \gamma\sigma(\beta_1)x^2 + \cdots + \gamma\sigma(\beta_m)x^{m+1}.$$

Logo, $n = m$ e $\sigma(\alpha_n) = \gamma\sigma(\beta_n)$ e, portanto, $\gamma = \sigma(\alpha_n\beta_n^{-1}) \in \sigma(\mathbb{k})$, o que é uma contradição. Logo, $xR \cap \gamma xR = \{0\}$ e, assim, R não é um domínio de Ore à direita. \square

Na realidade, a sobrejetividade de σ na proposição acima é condição necessária e suficiente para que $\mathbb{k}[x; \sigma]$ seja um domínio de ideais à direita principais (veja [16, Proposition 1.1.14] ou [7, Theorem 5.8]).

Abaixo veremos alguns exemplos historicamente importantes de construções baseadas em extensões de Ore.

Exemplos. (1) Seja \mathbb{C} o corpo dos números complexos e seja $\tau: \alpha + \beta i \mapsto \alpha - \beta i$ a conjugação complexa ($\alpha, \beta \in \mathbb{R}$). O polinômio $1 + x^2 \in \mathbb{C}[x; \tau]$ é central (isto é, comuta com todos os elementos de $\mathbb{C}[x; \tau]$), assim, o ideal à esquerda $(1 + x^2)\mathbb{C}[x; \tau]$ é um ideal bilateral e existe um isomorfismo de anéis

$$\frac{\mathbb{C}[x; \tau]}{(1 + x^2)\mathbb{C}[x; \tau]} \cong \mathbb{H}_{\mathbb{R}}.$$

(2) Seja \mathbb{Q} o corpo dos números racionais e considere o endomorfismo σ do corpo das funções racionais $\mathbb{Q}(t)$ definido por $\sigma(h(t)) = h(2t)$, para todo $h(t) \in \mathbb{Q}(t)$. D. Hilbert em 1899 usa um “complemento” (em um certo sentido que não será precisado aqui) do anel com divisão de frações de $\mathbb{Q}(t)[x; \sigma]$ para produzir o primeiro exemplo de um anel com divisão ordenado que não fosse comutativo. (Ver [6] para outros comentários sobre o desenvolvimento histórico da teoria de anéis com divisão.)

- (3) Em ambos os exemplos acima consideramos anéis de polinômios skew que envolvem endomorfismos sobrejetores. Seja \mathbb{k} um corpo qualquer (por exemplo, $\mathbb{k} = \mathbb{Q}$) e considere o endomorfismo η de do corpo $\mathbb{k}(t)$ das frações racionais sobre \mathbb{k} dado por $\eta(h(t)) = h(t^2)$, para todo $h(t) \in \mathbb{k}(t)$. Então η não é sobrejetor e, portanto, $\mathbb{k}(t)[x; \eta]$ é um exemplo de um domínio de Ore à esquerda que não é um domínio de Ore à direita. Consideraremos esse anel de polinômios skew novamente quando tratarmos de construir um corpo de frações da álgebra associativa livre na Seção 5.

Exercício 7. Seja \mathbb{k} um corpo e seja $\mathbb{k}(t)$ o corpo das frações racionais sobre \mathbb{k} , isto é,

$$\mathbb{k}(t) = \left\{ \frac{f(t)}{g(t)} : f(t), g(t) \in \mathbb{k}[t], g(t) \neq 0 \right\}.$$

Mostre que a função

$$\begin{aligned} \eta: \mathbb{k}(t) &\longrightarrow \mathbb{k}(t) \\ \frac{f(t)}{g(t)} &\longmapsto \frac{f(t^2)}{g(t^2)} \end{aligned}$$

é um homomorfismo que não é sobrejetor. (*Sugestão:* Utilize um argumento sobre os graus para mostrar que não existem polinômios $f(t), g(t) \in \mathbb{k}[t]$, com $g(t) \neq 0$, tais que $f(t^2) = tg(t^2)$ e conclua que $t \notin \eta(\mathbb{k}(t))$.)

4. A ÁLGEBRA ASSOCIATIVA LIVRE

Apresentaremos nesta seção um importante exemplo de um domínio que não é um domínio de Ore, a álgebra associativa livre.

Nesta seção \mathbb{k} sempre denotará um corpo.

Sejam u, v duas indeterminadas, ou *letras*, como as chamaremos de agora em diante. Considere o conjunto

$$M = \{z_1 \dots z_k : k \geq 0, z_i \in \{u, v\}\}$$

formado por todas as sequências finitas de elementos do conjunto $\{u, v\}$. Ou seja, M é o conjunto de todas as *palavras* nas letras u e v , incluindo a palavra vazia, que será denotada por e . Se $m = z_1 \dots z_k \in M$, chamamos k de *comprimento* de m e escrevemos $\text{cpt}(m) = k$; por definição, $\text{cpt}(e) = 0$. Existe uma operação binária associativa $*$ em M dada por justaposição de palavras: se $m = z_1 \dots z_k$ e $n = w_1 \dots w_s$, então

$$m * n = z_1 \dots z_k w_1 \dots w_s.$$

A *álgebra associativa livre nas indeterminadas u e v sobre \mathbb{k}* é o conjunto $\mathbb{k}\langle u, v \rangle$ formado por todas as combinações lineares de elementos de M com coeficientes em \mathbb{k} , isto é,

$$\mathbb{k}\langle u, v \rangle = \left\{ \sum_{m \in M} \alpha_m m : m \in M, \alpha_m \in \mathbb{k} \text{ e } \{m \in M : \alpha_m \neq 0\} \text{ é finito} \right\}.$$

Está subentendido nesta definição que os elementos de M são linearmente independentes sobre \mathbb{k} , ou, dito de outra maneira, dados $f = \sum_{m \in M} \alpha_m m, g = \sum_{m \in M} \beta_m m$, temos $f = g$ se, e somente se, $\alpha_m = \beta_m$, para todo $m \in M$.

Se $f = \sum_{m \in M} \alpha_m m \in \mathbb{k}\langle u, v \rangle$, o conjunto $\{m \in M : \alpha_m \neq 0\}$ é usualmente chamado de *suporte* de f e é denotado por $\text{sup}(f)$.

Assim, os elementos de $\mathbb{k}\langle u, v \rangle$ nada mais são do que polinômios com coeficientes do corpo \mathbb{k} nas indeterminadas *não comutativas* u e v . Definimos em $\mathbb{k}\langle u, v \rangle$ operações binárias de adição de multiplicação de modo a dotar $\mathbb{k}\langle u, v \rangle$ de uma estrutura de anel. A adição é definida por adição de coeficientes correspondentes, isto é,

$$\sum_{m \in M} \alpha_m m + \sum_{m \in M} \beta_m m = \sum_{m \in M} (\alpha_m + \beta_m) m.$$

E a multiplicação é definida por distributividade a partir da seguinte regra de multiplicação de elementos com um único termo:

$$\alpha m \cdot \beta n = (\alpha\beta)(m * n),$$

para todos $\alpha, \beta \in \mathbb{k}$ e $m, n \in M$.

Exercício 8. Mostre que com as operações definidas acima, $\mathbb{k}\langle u, v \rangle$ é um anel (associativo) com unidade $1e$, que não é comutativo, uma vez que $uv \neq vu$. Mostre que a função $\mathbb{k} \rightarrow \mathbb{k}\langle u, v \rangle, a \mapsto ae$, é um homomorfismo injetor.

Deste ponto em diante, quando for conveniente, identificaremos \mathbb{k} com sua imagem em $\mathbb{k}\langle u, v \rangle$ por intermédio do homomorfismo injetor mencionado no exercício acima. Em particular, o elemento identidade de $\mathbb{k}\langle u, v \rangle$ será identificado com $1 \in \mathbb{k}$.

O anel $\mathbb{k}\langle u, v \rangle$ também é dotado de uma função grau $\text{gr}: \mathbb{k}\langle u, v \rangle \rightarrow \mathbb{N} \cup \{-\infty\}$, definida da seguinte maneira,

$$\text{gr}(f) = \begin{cases} \max\{\text{cpt}(m) : m \in \text{sup}(f)\} & \text{se } f \neq 0, \\ -\infty & \text{se } f = 0. \end{cases}$$

Por exemplo, $\text{gr}(1 + u - uv + vu + vu^2) = 3$.

Exercício 9. Mostre que a função $\text{gr}: \mathbb{k}\langle u, v \rangle \rightarrow \mathbb{N} \cup \{-\infty\}$ definida acima tem as seguintes propriedades: para todos $f, g \in \mathbb{k}\langle u, v \rangle$,

- (i) $\text{gr}(f + g) \leq \max\{\text{gr}(f), \text{gr}(g)\}$,
- (ii) $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.

Como vimos na seção anterior, a condição (ii) do exercício acima garante que $\mathbb{k}\langle u, v \rangle$ é um domínio. Porém $\mathbb{k}\langle u, v \rangle$ não é um domínio de Ore à esquerda, nem à direita, pois é claro que $u\mathbb{k}\langle u, v \rangle \cap v\mathbb{k}\langle u, v \rangle = \{0\}$ e $\mathbb{k}\langle u, v \rangle u \cap \mathbb{k}\langle u, v \rangle v = \{0\}$.

Há duas outras propriedades satisfeitas pela álgebra livre que serão utilizadas mais adiante e estão enunciadas abaixo.

Lema 11. *Todo elemento de $\mathbb{k}\langle u, v \rangle$ se escreve de maneira única na forma*

$$\alpha + ug + vh,$$

onde $\alpha \in \mathbb{k}, g, h \in \mathbb{k}\langle u, v \rangle$.

Demonstração. Dado $f = \sum_{m \in M} \alpha_m m$, seja $g = \sum_{m \in M} \alpha_{um} m$ e seja $h = \sum_{m \in M} \alpha_{vm} m$. Então, $f = \alpha_e + ug + vh$. A unicidade segue da unicidade da decomposição de f como soma de múltiplos escalares dos elementos de M . \square

De modo simétrico, também temos decomposição única de elementos de $\mathbb{k}\langle u, v \rangle$ na forma $\beta + g'u + h'v$, com $\beta \in \mathbb{k}$ e $g', h' \in \mathbb{k}\langle u, v \rangle$.

No Exercício 8, vimos que existe um homomorfismo $\mu: \mathbb{k} \rightarrow \mathbb{k}\langle u, v \rangle$, definido por $\mu(\alpha) = \alpha e$, para todo $\alpha \in \mathbb{k}$. É fácil ver que $\mu(\alpha)f = f\mu(\alpha)$, para todos $\alpha \in \mathbb{k}$ e $f \in \mathbb{k}\langle u, v \rangle$. Isso faz de $\mathbb{k}\langle u, v \rangle$ uma \mathbb{k} -álgebra, conforme a definição abaixo.

Definição. Um anel R dado com um homomorfismo $\mu: \mathbb{k} \rightarrow R$ tal que $\mu(\alpha)r = r\mu(\alpha)$, para todos $\alpha \in \mathbb{k}$ e $r \in R$ é chamado uma \mathbb{k} -álgebra. Se R e S são \mathbb{k} -álgebras com homomorfismos $\mu_R: \mathbb{k} \rightarrow R$ e $\mu_S: \mathbb{k} \rightarrow S$, dizemos que um homomorfismo de anéis $\phi: R \rightarrow S$ é um *homomorfismo de \mathbb{k} -álgebras* se $\phi\mu_R = \mu_S$.

Exercício 10. Seja R uma \mathbb{k} -álgebra. Mostre que se R for um domínio de Ore à direita, então existe uma estrutura natural de \mathbb{k} -álgebra em $Q_d(R)$ com respeito à qual a imersão canônica $\lambda: R \rightarrow Q_d(R)$ é um homomorfismo de \mathbb{k} -álgebras.

Lema 12. *Se R é uma \mathbb{k} -álgebra e $\iota: \{u, v\} \rightarrow R$ é uma função, então existe um único homomorfismo de \mathbb{k} -álgebras $\phi: \mathbb{k}\langle u, v \rangle \rightarrow R$ tal que $\phi(u) = \iota(u)$ e $\phi(v) = \iota(v)$.*

Demonstração. Defina uma função $\bar{\iota}: M \rightarrow R$ da seguinte maneira, $\bar{\iota}(e) = 1$ e $\bar{\iota}(z_1 \dots z_r) = \iota(z_1) \dots \iota(z_r)$. Seja $\mu_R: \mathbb{k} \rightarrow R$ o homomorfismo que dota R de uma estrutura de \mathbb{k} -álgebra. Então, a função $\phi: \mathbb{k}\langle u, v \rangle \rightarrow R$ dada por

$$\phi \left(\sum_{m \in M} \alpha_m m \right) = \sum_{m \in M} \mu_R(\alpha_m) \bar{\iota}(m)$$

é um homomorfismo de álgebras com a propriedade desejada. (Verifique essa afirmação.) Além disso, qualquer outro homomorfismo de álgebras $\mathbb{k}\langle u, v \rangle \rightarrow R$ que coincide com ϕ nos elementos u e v coincidirá também nos elementos de M e, portanto, em todos os elementos de $\mathbb{k}\langle u, v \rangle$. \square

Observação. O anel $\mathbb{k}\langle u, v \rangle$ é também chamado de \mathbb{k} -álgebra livre de posto 2, pois o conjunto de letras $\{u, v\}$ tem dois elementos. Poderíamos considerar álgebras livres cujos elementos são combinações lineares sobre \mathbb{k} de palavras formadas por letras de um alfabeto de tamanho arbitrário (infinito, até) e o posto da álgebra livre seria, então, a cardinalidade desse alfabeto. Assim, a álgebra livre de posto 1 é justamente o anel de polinômios em uma indeterminada sobre \mathbb{k} . Essa é a única álgebra livre comutativa. Existem versões dos Lemas 11 e 12 para álgebras livres de postos arbitrários.

5. CORPOS DE FRAÇÕES DA ÁLGEBRA ASSOCIATIVA LIVRE

Como vimos na seção anterior, a álgebra livre $\mathbb{k}\langle u, v \rangle$ não é um domínio de Ore. Nesta seção veremos que, ainda assim, $\mathbb{k}\langle u, v \rangle$ tem um anel com divisão de frações.

Começaremos com um critério para identificar álgebras livres como subálgebras de outros anéis.

Definição. Seja R um anel e seja S um subanel de R . Dados $a_1, \dots, a_n \in R$, diremos que o conjunto $\{a_1, \dots, a_n\}$ é *linearmente independente à direita sobre S* se para todos $b_1, \dots, b_n \in S$, $a_1 b_1 + \dots + a_n b_n = 0$ implicar $b_1 = \dots = b_n = 0$. O conjunto $\{a_1, \dots, a_n\}$ é *linearmente dependente à direita sobre S* se não for linearmente independente à direita sobre S .

Exercício 11. Seja R um domínio. Mostre que R é um domínio de Ore à direita se, e somente se, para todos $a, b \in R$, o conjunto $\{a, b\}$ for linearmente dependente à direita sobre R .

O critério abaixo foi obtido por A. V. Jategaonkar em 1969.

Lema 13. *Seja \mathbb{k} um corpo e seja R uma \mathbb{k} -álgebra. Sejam $a, b \in R$. Se $\{a, b\}$ é linearmente independente à direita sobre R , então existe um homomorfismo injetor de \mathbb{k} -álgebras $\phi: \mathbb{k}\langle u, v \rangle \rightarrow R$ tal que $\phi(u) = a$ e $\phi(v) = b$.*

Demonstração. Pelo Lema 12, existe um único homomorfismo de \mathbb{k} -álgebras $\phi: \mathbb{k}\langle u, v \rangle \rightarrow R$ que satisfaz $\phi(u) = a$ e $\phi(v) = b$. Mostremos que ϕ é injetor. Suponha, por absurdo, que $\ker \phi \neq \{0\}$ e tome $f \in \ker \phi, f \neq 0$, de grau mínimo n , digamos. Pelo Lema 11, podemos escrever f na forma $f = \alpha + ug + vh$, com $\alpha \in \mathbb{k}, g, h \in \mathbb{k}\langle u, v \rangle$. Se $g = h = 0$, teríamos $\mu_R(\alpha) = \phi(f) = 0$, onde $\mu_R: \mathbb{k} \rightarrow R$ denota o homomorfismo que define a estrutura de \mathbb{k} -álgebra em R . Como μ_R é injetor (pois tem como domínio um corpo), seguiria $\alpha = 0$, o que é impossível, pois $f \neq 0$. Assuma, assim, que $g \neq 0$, por exemplo. (O argumento é análogo se $h \neq 0$.) Temos, portanto,

$$\begin{aligned} 0 &= \phi(f)\phi(v) = \phi(fv) = \phi(\alpha v + ugv + v hv) \\ &= \phi(u(gv) + v(\alpha + hv)) = a\phi(gv) + b\phi(\alpha + hv). \end{aligned}$$

Como $\{a, b\}$ é linearmente independente à direita sobre R segue, em particular, que $\phi(gv) = 0$.

Novamente, sejam $\beta \in \mathbb{k}$ e $p, q \in \mathbb{k}\langle u, v \rangle$ tais que $g = \beta + up + vq$. Temos

$$0 = \phi(gv) = \phi(\beta v + upv + vqv) = a\phi(pv) + b\phi(\beta + qv).$$

Assim, $pv, \beta + qv \in \ker \phi$. Como $\text{gr}(g) \leq n - 1$, segue $\text{gr}(p), \text{gr}(q) \leq n - 2$ e, portanto $\text{gr}(pv), \text{gr}(\beta + qv) \leq n - 1$. Pela minimalidade do grau de f , temos, necessariamente, $pv = 0$

e $\beta + qv = 0$. A unicidade do Lema 11 garante, portanto, que $\beta = 0$ e $p = q = 0$. Daí segue $g = 0$, uma contradição.

Portanto, ϕ é injetor. \square

Um domínio R que não é um domínio de Ore à direita contém, pelo Exercício 11, um par de elementos $\{a, b\}$ que é linearmente independente à direita sobre R . O Lema 13 tem, assim, a seguinte consequência.

Corolário 14. *Seja \mathbb{k} um corpo e seja R uma \mathbb{k} -álgebra que é um domínio, mas que não é um domínio de Ore à direita. Então existe um homomorfismo injetor de \mathbb{k} -álgebras $\mathbb{k}\langle u, v \rangle \rightarrow R$.* \square

De posse do resultado acima, Jategaonkar observa que uma \mathbb{k} -álgebra que é domínio de Ore à esquerda R , mas não é um domínio de Ore à direita fornece uma imersão da álgebra livre $\mathbb{k}\langle u, v \rangle$ em um anel com divisão, dada pela composição

$$\mathbb{k}\langle u, v \rangle \hookrightarrow R \hookrightarrow Q_e(R),$$

onde o primeiro homomorfismo existe pelo Corolário 14 e o segundo, pelo Teorema 5. Um exemplo de uma tal álgebra foi visto na Seção 3: o endomorfismo σ do corpo das frações racionais $\mathbb{k}(t)$ sobre \mathbb{k} que satisfaz $\sigma(t) = t^2$ não é sobrejetor. Logo $R = \mathbb{k}(t)[x; \sigma]$ é uma \mathbb{k} -álgebra (verifique essa afirmação) que é um domínio de Ore à esquerda mas não é um domínio de Ore à direita. Portanto, existe um homomorfismo injetor $\mathbb{k}\langle u, v \rangle \rightarrow Q_e(\mathbb{k}(t)[x; \sigma])$.

A construção de uma imersão da álgebra livre em um anel com divisão pelo método de Jategaonkar tem antecedentes históricos. A primeira construção de um anel com divisão que contém um subanel isomorfo a uma álgebra livre foi apresentada por R. Moufang em 1937, porém seu método era diferente (cf. [6]).

6. A NÃO UNICIDADE DO CORPO DE FRAÇÕES DA ÁLGEBRA LIVRE

Lembremos que um anel com divisão D é um anel com divisão de frações de um anel R se existir um homomorfismo injetor $\rho: R \rightarrow D$ tal que D seja gerado, como anel com divisão, por $\rho(R)$, isto é, tal que seja D o menor subanel com divisão de D que contém $\rho(R)$. (Já tínhamos encontrado essa definição na Seção 2, quando mostramos que se R é um domínio de Ore à direita, então $Q_d(R)$ é um anel com divisão de frações de R .) Assim, um anel R tem um anel com divisão de frações se, e somente se, existir um homomorfismo injetor de R em um anel com divisão. É claro que ser um domínio é condição necessária para um anel ter um anel com divisão de frações. Também já fora mencionado na Seção 2 que essa condição não é suficiente no caso não comutativo.

Diremos que dois anéis com divisão (ρ_1, D_1) e (ρ_2, D_2) de um anel R são *isomorfos* se existir um isomorfismo $\varphi: D_1 \rightarrow D_2$ tal que $\varphi\rho_1 = \rho_2$. Vimos que dois corpos de frações de um domínio de integridade comutativo são sempre isomorfos (Corolário 3) e que dois anéis com divisão de frações de um domínio de Ore (à direita ou à esquerda) são sempre isomorfos (Exercício 4).

Nesta seção veremos que a álgebra livre $\mathbb{k}\langle u, v \rangle$ tem uma família infinita de anéis com divisão de frações não dois a dois isomorfos. Para tanto faremos uma elaboração da construção do anel com divisão que contém a álgebra livre visto na seção anterior. As ideias que serão apresentadas aqui foram propostas pela primeira vez por J. L. Fisher em 1971. Seguiremos a apresentação de [18, Section 9C].

Começemos por demonstrar um resultado que em conjunto com o Lema 13 estabelece um critério de identificação de geradores de uma álgebra livre em anéis de polinômios skew.

Durante o restante desta seção \mathbb{k} denotará um corpo.

Lema 15. *Seja σ um endomorfismo de \mathbb{k} e sejam $\alpha, \beta \in \mathbb{k}$. Se $\{\alpha, \beta\}$ é um conjunto linearmente independente sobre $\sigma(\mathbb{k})$, então $\{\alpha x, \beta x\}$ é linearmente independente à direita sobre $\mathbb{k}[x; \sigma]$.*

Demonstração. Sejam $f, g \in \mathbb{k}[x; \sigma]$ tais que $\alpha x f + \beta x g = 0$. Devemos mostrar que $f = g = 0$. Sejam $\gamma_0, \dots, \gamma_n, \delta_0, \dots, \delta_n \in \mathbb{k}$ tais que

$$f = \gamma_0 + \dots + \gamma_n x^n \quad \text{e} \quad g = \delta_0 + \dots + \delta_n x^n.$$

(Não exigimos que $\gamma_n = 0$ ou que $\delta_n = 0$, apenas que as representações de f e g tenham o mesmo número de termos, o que é sempre possível.) Então

$$\begin{aligned} 0 &= \alpha x f + \beta x g \\ &= (\alpha \sigma(\gamma_0) + \beta \sigma(\delta_0))x + (\alpha \sigma(\gamma_1) + \beta \sigma(\delta_1))x^2 \\ &\quad + \dots + (\alpha \sigma(\gamma_n) + \beta \sigma(\delta_n))x^{n+1}. \end{aligned}$$

Portanto, $\alpha \sigma(\gamma_i) + \beta \sigma(\delta_i) = 0$, para todo $i = 0, \dots, n$. Como $\{\alpha, \beta\}$ é linearmente independente sobre $\sigma(\mathbb{k})$, segue $\sigma(\gamma_i) = \sigma(\delta_i) = 0$, para todo $i = 0, \dots, n$. Pela injetividade de σ , obtemos $f = g = 0$. \square

Seja $K = \mathbb{k}(t)$ o corpo das frações racionais sobre \mathbb{k} . Para cada inteiro $n \geq 2$, denote por σ_n o endomorfismo de K que satisfaz $\sigma_n(t) = t^n$ e seja $R_n = K[x; \sigma_n]$ o anel de polinômios skew.

Lema 16. O conjunto $\{x, tx\} \subseteq R_n$ é linearmente independente à direita sobre R_n .

Demonstração. O conjunto $\{1, t\} \subseteq K$ é linearmente independente sobre $\sigma(K)$, pois se existissem $f, g, p, q \in \mathbb{k}[t]$, $g, q \neq 0$ tais que

$$1\sigma\left(\frac{f}{g}\right) + t\sigma\left(\frac{p}{q}\right) = 0,$$

teríamos $-f(t^n)q(t^n) = tp(t^n)g(t^n)$, o que é impossível se a combinação linear não for trivial, pois nesse caso, o lado esquerdo da última igualdade teria grau múltiplo de n , enquanto o lado direito teria grau congruente a 1 módulo n . Segue, portanto, do Lema 15 que $\{x, tx\}$ é um subconjunto de R_n linearmente independente à direita sobre R_n . \square

Pelo Lema 13, existe um homomorfismo injetor de \mathbb{k} -álgebras $\rho_n: \mathbb{k}\langle u, v \rangle \rightarrow R_n$ tal que $\rho_n(u) = x, \rho_n(v) = tx$. Ainda, como R_n é um domínio de Ore à esquerda, existe um homomorfismo injetor $\lambda_n: R_n \rightarrow D_n$, onde D_n denota o anel com divisão $Q_e(R_n)$ de frações de R_n . Seja $\varepsilon_n = \lambda_n \rho_n$.

Lema 17. (ε_n, D_n) é um corpo de frações de $\mathbb{k}\langle u, v \rangle$.

Demonstração. Seja F um subanel com divisão de D_n tal que $\varepsilon_n(\mathbb{k}\langle u, v \rangle) \subseteq F$. Mostremos que $F = D_n$. Com efeito,

$$\lambda_n(x) = \lambda_n \rho_n(u) = \varepsilon_n(u) \in \varepsilon_n(\mathbb{k}\langle u, v \rangle) \subseteq F$$

e

$$\lambda_n(t)\lambda_n(x) = \lambda_n(tx) = \lambda_n \rho_n(v) = \varepsilon_n(v) \in \varepsilon_n(\mathbb{k}\langle u, v \rangle) \subseteq F.$$

Portanto, $\lambda_n(t) = (\lambda_n(t)\lambda_n(x))\lambda_n(x)^{-1} \in F$, uma vez que F é um anel com divisão e $\lambda_n(x) \neq 0$, pois λ_n é injetor. Como λ_n é um homomorfismo de \mathbb{k} -álgebras (por ser uma composta de homomorfismos de \mathbb{k} -álgebras), segue $\lambda_n(\mathbb{k}(t)) \subseteq F$. Portanto, F contém $\lambda_n(\mathbb{k}(t)[x; \sigma])$ e, sendo um anel com divisão, deve conter D_n . \square

Teorema 18. Com a notação acima, se $m \neq n$, não existe um homomorfismo de anéis $\psi: D_m \rightarrow D_n$ tal que $\psi \varepsilon_m = \varepsilon_n$. (E, portanto, (ε_m, D_m) e (ε_n, D_n) são corpos de frações de $\mathbb{k}\langle u, v \rangle$ não isomorfos.)

Demonstração. Para todo inteiro $r \geq 2$, temos

$$\begin{aligned}
(\varepsilon_r(u)^{-1}\varepsilon_r(v))^r &= (\lambda_r(x)^{-1}\lambda_r(tx))^r = (\lambda_r(x)^{-1}\lambda_r(t)\lambda_r(x))^r \\
&= \lambda_r(x)^{-1}\lambda_r(t)^r\lambda_r(x) = \lambda_r(x)^{-1}\lambda_r(t^r x) \\
&= \lambda_r(x)^{-1}\lambda_r(\sigma_r(t)x) = \lambda_r(x)^{-1}\lambda_r(xt) \\
&= \lambda_r(x)^{-1}\lambda_r(x)\lambda_r(t) = \lambda_r(t) \\
&= \lambda_r(t)\lambda_r(x)\lambda_r(x)^{-1} = \lambda_r(tx)\lambda_r(x)^{-1} \\
&= \varepsilon_r(v)\varepsilon_r(u)^{-1}.
\end{aligned}$$

Se existisse um homomorfismo de anéis $\psi: D_m \rightarrow D_n$ tal que $\psi\varepsilon_m = \varepsilon_n$, teríamos, portanto,

$$\begin{aligned}
(\varepsilon_n(u)^{-1}\varepsilon_n(v))^m &= (\psi\varepsilon_m(u)^{-1}\psi\varepsilon_m(v))^m = \psi\left((\varepsilon_m(u)^{-1}\varepsilon_m(v))^m\right) \\
&= \psi(\varepsilon_m(v)\varepsilon_m(u)^{-1}) = \varepsilon_n(v)\varepsilon_n(u)^{-1} \\
&= (\varepsilon_n(u)^{-1}\varepsilon_n(v))^n.
\end{aligned}$$

Mas lembremos que $\varepsilon_n(u)^{-1}\varepsilon_n(v) = \lambda_n(x)^{-1}\lambda_n(t)\lambda_n(x)$ e, assim,

$$\begin{aligned}
\lambda_n(x)^{-1}\lambda_n(t)^m\lambda_n(x) &= (\lambda_n(x)^{-1}\lambda_n(t)\lambda_n(x))^m = (\lambda_n(x)^{-1}\lambda_n(t)\lambda_n(x))^n \\
&= \lambda_n(x)^{-1}\lambda_n(t)^n\lambda_n(x).
\end{aligned}$$

Isso implica $\lambda_n(t^m) = \lambda_n(t^n)$. Mas como λ_n é injetor, teríamos $t^m = t^n$ em R_n , uma contradição. \square

7. COMENTÁRIOS FINAIS

- (1) Mencionamos na Seção 2 que existem domínios que não têm anéis com divisão de frações. O primeiro exemplo foi construído por Malcev em 1937 e trata-se de um domínio cujo monóide multiplicativo não pode ser imerso em um grupo. Os detalhes dessa construção podem ser encontrados, por exemplo, em [18, Section 9B]. Em 1967, três matemáticos, L. A. Bokut, A. J. Bowtell e A. A. Klein, de maneira independente, apresentaram exemplos de domínios cujos monóides multiplicativos são imersíveis em grupos e ainda assim, eles não têm anéis com divisão de frações. Para outros comentários sobre essas construções, ver [5], pp. 486-7.
- (2) Não podemos falar em o anel de frações da álgebra livre $\mathbb{k}\langle u, v \rangle$, pois como vimos na Seção 6, ela tem infinitos anéis com divisão não isomorfos entre si. Porém, como mostrou S. A. Amitsur em 1966, existe um anel com divisão de frações de $\mathbb{k}\langle u, v \rangle$, chamado *corpo universal de frações* de $\mathbb{k}\langle u, v \rangle$ a partir do qual todos os demais anéis de frações de $\mathbb{k}\langle u, v \rangle$ podem ser obtidos por “especializações”. O corpo universal de frações de uma álgebra livre é único a menos de isomorfismos. (Ver [1].)
- (3) Nas décadas 1960–70, P. M. Cohn desenvolve a teoria de “anéis de ideais livres” e mostra que todos eles têm corpos universais de frações sobre os quais todas as matrizes plenas são inversíveis e, assim, o corpo universal de frações de uma álgebra livre pode ser obtido por inversão não de elementos mas sim de matrizes. A referência principal para a teoria de anéis de ideais livres é [5].
- (4) Existe uma versão mais geral da construção de anéis de polinômios skew. Seja R um anel, seja σ um endomorfismo de R e seja δ uma σ -derivada de R , isto é, $\delta: R \rightarrow R$ é uma função que satisfaz
 - (a) $\delta(a + b) = \delta(a) + \delta(b)$ e
 - (b) $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$,
para todos $a, b \in R$. Então o conjunto dos polinômios

$$R[x; \sigma, \delta] = \{a_0 + a_1x + \cdots + a_nx^n : n \geq 0, a_i \in R\}$$

tem uma estrutura de anel associativo com unidade com multiplicação satisfazendo

$$xa = \sigma(a)x + \delta(a), \quad a \in R.$$

Se R for um domínio de Ore à esquerda e σ for injetor, $R[x; \sigma, \delta]$ será também um domínio de Ore à esquerda. Além disso, se R for um anel com divisão, então $R[x; \sigma, \delta]$ será um domínio de ideais à esquerda principais, que não é um domínio de ideais à direita principais se σ não for sobrejetor. (Ver, por exemplo, [7, Section 5.2].)

Um exemplo importante de uma álgebra que é um anel de polinômios skew com derivação é a chamada *primeira álgebra de Weyl*,

$$A_1(\mathbb{k}) = \mathbb{k}[t] \left[x; I, \frac{d}{dt} \right],$$

onde \mathbb{k} denota um corpo, $I: \mathbb{k}[t] \rightarrow \mathbb{k}[t]$ o endomorfismo identidade e $\frac{d}{dt}: \mathbb{k}[t] \rightarrow \mathbb{k}[t]$ a derivada usual no anel de polinômios $\mathbb{k}[t]$. Assim, $A_1(\mathbb{k})$ é a \mathbb{k} -álgebra gerada por x e t , sujeitos à relação

$$xt - tx = 1.$$

Essa álgebra tem papel de relevância na teoria quântica e foi considerada pela primeira vez na década de 1920.

Mais recentemente, vários exemplos de grupos quânticos foram construídos por meio de extensões de Ore. (Ver [17].)

- (5) Anéis com divisão de frações de domínios de Ore são frequentemente anéis com divisão de dimensão infinita sobre seus centros. Essa é uma das razões pelas quais sabe-se pouco acerca da estrutura deles. Anéis com divisão de dimensão finita, por outro lado, são bem mais conhecidos. Para um panorama da história dos anéis com divisão de dimensão finita, ver [2]. O livro [16] contém uma apresentação bem completa (com demonstrações) de boa parte da teoria mencionada em [2].
- (6) Um exemplo do tipo de dificuldade encontrado na teoria de anéis com divisão de dimensão infinita é ilustrado pela seguinte conjectura (proposta por L. Makar-Limanov em 1984): se D é um anel com divisão de dimensão finita sobre seu centro k e D é finitamente gerado como anel com divisão sobre k , então D contém uma subálgebra livre de posto 2. (Para maiores detalhes sobre esse problema e outros problemas relacionados, incluindo soluções parciais deles, ver [14] e [3].)

Incluímos entre as referências deste texto, além de livros e artigos diretamente citados, outros trabalhos relacionados com os temas tratados e que podem ser de interesse do leitor.

REFERÊNCIAS

- [1] S. A. AMITSUR, Rational identities and applications to algebra and geometry, *Journal of Algebra* **3** (1966), 304-359.
- [2] ———, Highlights in the history of finite-dimensional central division algebras, *Ring Theory 1989 (Ramat Gan and Jerusalem, 1988/1989)*, 404-430, Israel Mathematics Conference Proceedings, Volume **1**, Weizmann, Jerusalem, 1989.
- [3] J. P. BELL, D. ROGALSKI, Free subalgebras of quotient rings of Ore extensions, arXiv:1101.5829v2.
- [4] P. M. COHN, Rings of fractions, *American Mathematical Monthly* **78** (1971), 596-615.
- [5] ———, *Free Rings and Their Relations*, Second edition, London Mathematical Society Monographs, Volume **19**, Academic Press, Inc., London, 1985.
- [6] ———, A brief history of infinite-dimensional skew fields, *The Mathematical Scientist* **17** (1992), no. 1, 1-14.
- [7] ———, *An Introduction to Ring Theory*, Springer Undergraduate Mathematics Series, Springer, London, 2000.
- [8] ———, *Free Ideal Rings and Localization in General Rings*, New Mathematical Monographs, Volume **3**, Cambridge University Press, Cambridge, 2006.
- [9] ———, Localization in general rings, a historical survey, *Non-commutative Localization in Algebra and Topology*, 5-23, London Mathematical Society Lecture Note Series, Volume **330**, Cambridge University Press, Cambridge, 2006.
- [10] S. C. COUTINHO, Quotient rings of noncommutative rings in the first half of the 20th century, *Archive for History of Exact Sciences* **58** (2004), no. 3, 255-281.

- [11] S. C. COUTINHO, J. C. MCCONNELL, The quest for quotient rings (of noncommutative Noetherian rings), *Amererican Mathematical Monthly* **110** (2003), no. 4, 298-313.
- [12] J. B. FRALEIGH, *A First Course in Abstract Algebra*, Seventh edition, Addison Wesley, Boston, MA, 2003.
- [13] A. GONÇALVES, *Introdução à Álgebra*, Quinta edição, Projeto Euclides, IMPA, Rio de Janeiro, 2001.
- [14] J. Z. GONÇALVES, M. SHIRVANI, A survey on free objects in division rings and in division rings with an involution, *Communications in Algebra*, no prelo.
- [15] K. R. GOODEARL, R. B. WARFIELD JR., *An Introduction to Noncommutative Noetherian Rings*, Second edition, London Mathematical Society Student Texts, Volume **61**, Cambridge University Press, Cambridge, 2004.
- [16] N. JACOBSON, *Finite-dimensional Division Algebras over Fields*, Springer-Verlag, Berlin, 1996.
- [17] C. KASSEL, *Quantum Groups*, Graduate Texts in Mathematics, Volume **155**, Springer-Verlag, New York, 1995.
- [18] T. Y. LAM, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, Volume **189**, Springer-Verlag, New York, 1999.
- [19] ———, Hamilton's quaternions, *Handbook of Algebra*, Volume **3**, 429-454, North-Holland, Amsterdam, 2003.
- [20] J. C. MCCONNELL, J. C. ROBSON, *Noncommutative Noetherian Rings*, With the cooperation of L. W. Small, Revised edition, Graduate Studies in Mathematics, Volume **30**, American Mathematical Society, Providence, RI, 2001.
- [21] D. S. PASSMAN, *The Algebraic Structure of Group Rings*, Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985.
- [22] L. H. ROWEN, *Ring Theory*, Student edition, Academic Press, Inc., Boston, MA, 1991.
- [23] B. STENSTRÖM, *Rings of Quotients*, An Introduction to Methods of Ring Theory, Die Grundlehren der Mathematischen Wissenschaften, Band **217**, Springer-Verlag, New York-Heidelberg, 1975.

DEPARTAMENTO DE MATEMÁTICA, IME-USP, CAIXA POSTAL 66281, SÃO PAULO - SP, 05314-970
 E-mail: vofer@ime.usp.br