INTEGRAÇÃO AUTOMÁTICA DE FUNÇÕES ELEMENTARES

S. C. COUTINHO

RESUMO. Estas notas foram reunidas para um mini-curso no Departamento de Matemática da Universidade Federal de Pernambuco em fevereiro de 2007. O tema é a integração automática de funções racionais, com ênfase nos métodos de Hermite e Lazard-Rioboo-Trager. Correções e sugestões são bem-vindas, e devem ser enviadas para o endereço eletrônico informado ao final do texto.

SUMÁRIO

1. INTRODUÇÃO

O problema a ser abordado nestas notas pode ser formulado da seguinte maneira.

Problema 1.1. *Calcular, em forma fechada, a integral de uma função dada.*

Como esta é uma formulação demasiadamente vaga, convém reescrevê-la em uma forma que nos permita abordar o problema com mais precisão.

Problema 1.2. *Dada uma classe $\mathcal{F}$ de funções e um elemento $f \in \mathcal{F}$, ache (se possível) um elemento de $\mathcal{F}$ que corresponda à integral de f.*

Date: 13 de fevereiro de 2007.

Este problema foi resolvido, no caso em que $\mathcal{F}$ é o conjunto dos polinômios em uma variável, por I. Newton e G. W. Leibniz, os fundadores do cálculo diferencial e integral. Como sabemos, a integral de um polinômio é sempre um outro polinômio, de maneira que o problema sempre tem solução neste caso especial.

O caso seguinte corresponde a considerar funções que podem ser representadas como quocientes de polinômios, as chamadas funções racionais. Contudo, neste caso, o problema 1.2 nem sempre tem solução.

Teorema 1.1. *A integral da função racional $1/x$ não é uma função racional.*

Demonstração. Procedendo por contradição, suponhamos que $1/x$ tem como integral a função racional $f(x)/g(x)$, onde $g \neq 0$ e $\mathrm{mdc}(f,g) = 1$. Observe que esta última condição nos diz meramente que a fração polinomial está escrita em forma reduzida. Derivando ambos os lados de

$$\int \frac{1}{x} dx = \frac{f}{g},$$

obtemos

$$\frac{1}{x} dx = \frac{f'g - fg'}{g^2}.$$

Eliminado o denominador,

$$g^2 = x(f'g - fg'). \tag{1}$$

Em particular x divide g^2. Como x é irredutível como polinômio, concluímos que x divide g. Fatorando a maior potência de x que divide g podemos escrever $g = x^k \overline{g}$, onde $\mathrm{mdc}(\overline{g}, x) = 1$ e $k \geq 1$. Substituindo esta expressão para g em (1),

$$x^{2k}\overline{g}^2 = x(f'x^k\overline{g} - fkx^{k-1}\overline{g} - fx^k\overline{g}').$$

Cancelando x^k de ambos os membros, resta

$$x^k\overline{g}^2 = f'x\overline{g} - fk\overline{g} - fx\overline{g}').$$

Mas, disto concluímos que x tem que dividir $f\overline{g}$. Contudo, $\overline{g}$ e x são primos entre si, de forma que x deveria dividir f: o que também não pode ocorrer uma vez que x divide g e $\mathrm{mdc}(f,g) = 1$ por hipótese.

Leibniz propôs um método de integração para funções racionais que consistia em decompor a função racional do integrando na forma de frações parciais, mas não chegou a completar os detalhes, que ficaram por conta de Johan Bernoulli. Em um artigo publicado na Acta Eruditorum em 1703, Bernoulli mostrou, em particular, que a integral de qualquer função racional pode ser escrita em termos de outras funções racionais e de seus logaritmos. Os detalhes do funcionamento do método de Bernoulli serão descritos na seção 5. Apesar de ser algorítmico, o método de Bernoulli não deveria ser utilizado porque requer que sejamos capazes de fatorar completamente um polinômio em seus fatores irredutíveis (de graus um ou dois) sobre os números reais. Infelizmente, este continua sendo o único método de integração de funções racionais mencionado nos cursos básicos de cálculo.

Em uma série de artigos publicados a partir de 1833, Joseph Liouville estabeleceu de maneira mais consistente as bases para a abordagem do problema 1.2 de uma maneira mais geral. No âmbito de um curso inicial de cálculo, este problema costuma ser abordado para a classe $\mathcal{E}$ das funções elementares; isto é, aquelas funções que podem ser escritas a partir de

polinômios, exponenciais, logaritmos, funções algébricas e trigonométricas,

combinadas pelas operações básicas usuais:

soma, subtração, multiplicação e divisão.

As *funções algébricas* mencionadas acima são aquelas que satisfazem equações polinomiais na variável y, cujos coeficientes são funções racionais em x. O exemplo mais óbvio, e que aparece com mais freqüência em cálculo, é $x^{1/n}$, que satisfaz $y^n - x = 0$.

Um dos principais resultados de Liouville consistiu em mostrar que a integral de certas funções elementares não é uma função elementar. Este é o caso, por exemplo, das integrais

$$\int e^{x^2} dx, \quad \int \frac{\operatorname{sen}(x)}{x} dx \quad \text{e} \quad \int \frac{1}{\log(x)} dx.$$

Aliás, todos ouvimos de nosso professor de cálculo I que "pode-se mostrar" que estas funções não têm integral elementar; mas poucos vimos uma demonstração. As últimas seções destas notas (ainda não escritas) tratarão em detalhe deste problema.

Muito do que se conhecia sobre o problema 1.2 até o fim do século XIX foi reunido no livro de G. H. Hardy *The integration of functions of a single variable*, publicado em 1905. Nele, Hardy expressa dúvidas quanto a viabilidade de um tratamento completamente algorítmico para o problema da integração. Depois disto esta área ficou adormecida por cerca de 40 anos, quando foi retomada por J. F. Ritt em seu tratamento da álgebra diferencial, assunto de que trataremos na seção (ainda não escrita). Finalmente, um procedimento geral de integração foi proposto por R. Risch em 1968. Nas décadas seguintes, vários aspectos práticos importantes deste procedimento foram elaborados de forma mais precisa e algorítmica por, entre outros, B. M. Trager, Rothstein, R. Rioboo e D. Lazard, no que diz respeito a funções racionais, e por J. H. Davenport, M. Bronstein e B. M. Trager, no que diz respeito a funções algébricas e transcendentes. Estes algoritmos estão atualmente disponíveis em vários sistemas de computação algébrica, entre eles o AXIOM e o MAXIMA, ambos em domínio público.

Na primeira parte destas discutiremos detalhadamente um algoritmo para integração de funções racionais. Já a segunda parte será dedicada a uma introdução elementar à álgebra diferencial, cujo ápice consistirá na demonstração do princípio de Liouville e em sua aplicação à demonstração de que a integral de algumas funções elementares não é, ela própria, elementar.

Diante disto, é razoável perguntar porque dar tanta ênfase à integração de funções racionais, a ponto de dedicar métade das notas apenas a este problema.

A resposta é que, generalizado de uma forma ou de outra, a integração de funções racionais desempenha um papel extremamente importante em várias fases do algoritmo de Risch. Para que a resposta não pareça apenas uma evasiva, mostraremos como utilizar reduzir o cáculo de certas integrais trigonométricas à integração de funções racionais.

2. WEIERSTRASS

No século XIX, K. Weierstrass propôs um procedimento para integrar funções trigonométricas da forma

$$\frac{F(\operatorname{sen}(\theta), \cos(\theta))}{d}\theta F(\operatorname{sen}(\theta), \cos(\theta)),$$

onde $F(x, y)$ é uma função racional nas variáveis x e y. Em outras palavras, $F(x, y)$ é o quociente de polinômios nas variáveis x e y.

A idéia de Weierstrass consiste em reduzir o problema à integração de funções racionais em apenas uma variável, que chamaremos de t. Para isto, Weierstrass utiliza as identidades trigonométricas em que o seno e o co-seno são expressos em termos da tangente da metade do ângulo. As fórmulas são,

$$\operatorname{sen}(\theta) = \frac{2u}{1+u^2} \quad \text{e} \quad \cos(\theta) = \frac{1-u^2}{1+u^2} \quad \text{onde} \quad u = \tan(\frac{\theta}{2}).$$

Como $x = 2\arctan(u)$, temos que

$$\frac{dx}{du} = \frac{2}{u^2+1},$$

de forma que

$$\int f(\operatorname{sen}(x), \cos(x))dx = \int f\left(\frac{2u}{1+u^2}, \frac{1-u^2}{1+u^2}\right)\frac{2}{1+u^2}du.$$

Para obter a primitiva desejada, basta calcular esta integral e substituir u por $\tan(x/2)$.

Por exemplo, digamos que queremos calcular a integral

$$\int \operatorname{sen}^2(x)dx.$$

Usando a substituição acima, obtemos

$$\int \operatorname{sen}^2(x)dx = \int \left(\frac{2t}{1+t^2}\right)^2 \frac{2}{1+t^2}dt = \int \frac{8t^2dt}{(1+t^2)^3},$$

que pode ser calculada usando os métodos a serem descritos nas seções seguintes; veja a seção 10 para o resultado da integral.

As fórmulas para a o seno e o co-seno em termos da tangente da metade do ângulo podem ser facilmente deduzidas das identidades trigonométricas usuais. Contudo, também podemos obtê-las de maneira puramente geométrica, diretamente em função do parâmetro t, sem precisar sequer mencionar tangentes e meio ângulos. Para isto, basta lembrar que a circunferência pode ser parametrizada na forma

$$x = \cos(\theta) \quad \text{e} \quad y = \operatorname{sen}(\theta).$$

Portanto, se formos capazes de inventar uma nova parametrização da forma

$$x = g_1(t) \quad \text{e} \quad y = g_2(t),$$

poderemos concluir que

$$\cos(\theta) = g_1(t) \quad \text{e} \quad \operatorname{sen}(\theta) = g_2(t),$$

sem nenhum custo adicional de cálculos com identidades trigonométricas.

A idéia para este tratamento geométrico consiste em traçar uma reta de inclinação t pelo ponto $(-1, 0)$ da circunferência trigonométrica. Esta reta vai cortar a circunferência em dois pontos, um dos quais é o próprio $(-1, 0)$; o outro ponto terá suas coordenadas expressas em termos de t. Como a reta passa pelo ponto $(-1, 0)$ e tem inclinação t, sua equação será

$$y = t(x + 1).$$

Substituindo isto na equação $x^2 + y^2 = 1$, da circunferência de raio um e centro na origem, obtemos a equação quadrática

$$(1 + t^2)x^2 + 2t^2 x + (t^2 - 1) = 0,$$

na variável x, cujas soluções são

$$x = -1 \quad \text{e} \quad x = \frac{1 - t^2}{1 + t^2}.$$

Como $x = -1$ corresponde ao ponto $(-1, 0)$–a partir do qual a reta foi desenhada– o ponto que desejamos terá coordenadas

$$x = \frac{1 - t^2}{1 + t^2} \quad \text{e} \quad y = t(1 + x) = \frac{2t}{1 + t^2};$$

que são as equações para seno e co-seno de θ que já havíamos obtido antes, através das identidades trignométricas.

Há uma grande vantagem desta maneira de proceder sobre a utilização de cálculos trigonométricos: ela pode ser generalizada a outras situações na qual o integrando corresponde à parte de uma curva algébrica. Neste caso, basta parametrizar a curva, como fizemos acima no caso da circunferência, e converter a integral em uma função racional de uma variável.

Para tornar o procedimento mais claro, vamos aplicá-lo à integral

$$\int \frac{1}{\sqrt{x^2 + x^3}} dx.$$

Para isto, denotamos por y a função que aparece no denominador do integrando,

$$y = \sqrt{x^2 + x^3}.$$

Elevando ambos os membros ao quadrado,

$$y^2 = x^3 + x^2.$$

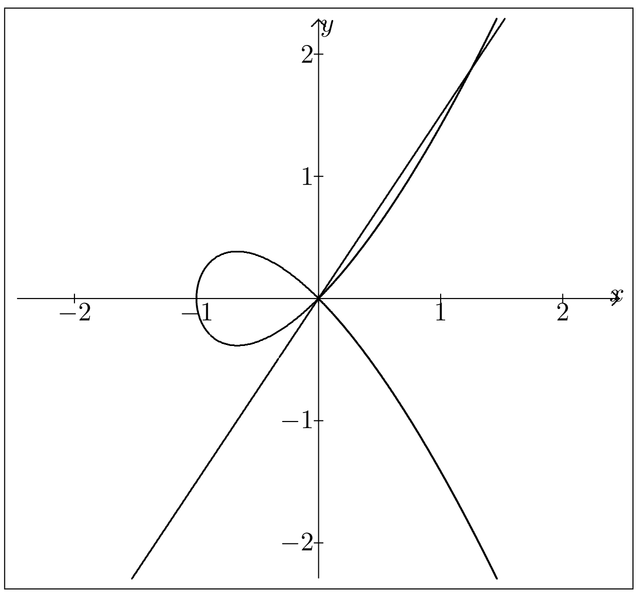
Portanto, trata-se de uma função algébrica que zera o polinômio

$$F(x, y) = y^2 - (x^3 + x^2).$$

Esta função é facilmente parametrizável, se utilizarmos um método semelhante ao já usado para a circunferência. Desta vez, tomamos a reta de inclinação t que passa pela origem,

$$y = tx.$$

Como mostra o gráfico, esta reta intersecta a curva em apenas um ponto, além da origem.



Substituindo na equação da curva, obtemos

$$t^2x^2 = x^2 + x^3.$$

Supondo $x \neq 0$, podemos cancelar x^2, que nos dá

$$x = t^2 - 1.$$

Logo,

$$y = t(t^2 - 1).$$

Voltando à integral, podemos escrevê-la na forma

$$\int \frac{1}{y} dx.$$

Mas, das expressões acima para x e y,

$$y = t(t^2 - 1) \quad \text{e} \quad dx = 2tdt.$$

Assim,

$$\int \frac{1}{y} dx = \int \frac{2tdt}{t(t^2-1)} = \int \frac{2dt}{(t^2-1)};$$

que é uma função racional muito fácil de integrar.

Infelizmente este procedimento não funcionará para qualquer função algébrica, porque nem todas as curvas algébricas podem ser parametrizadas a partir de funções racionais. Considere, por exemplo, a integral

$$\int \frac{1}{\sqrt{x^3+1}} dx.$$

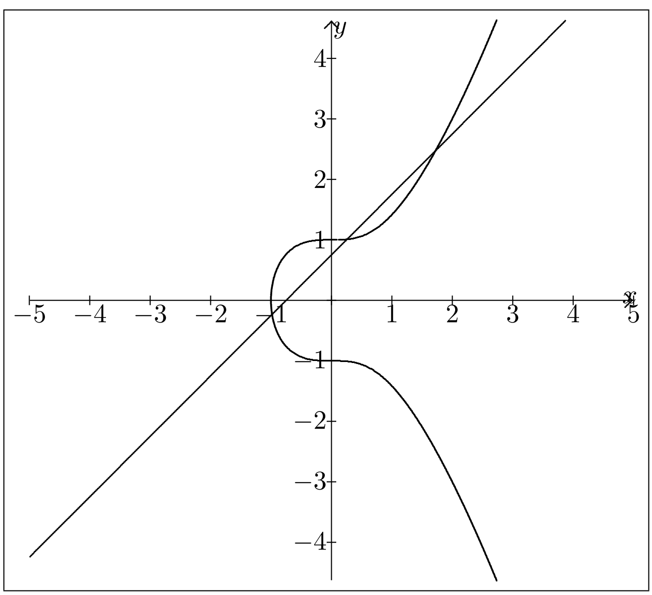
Se quiséssemos proceder como nos exemplos anteriores, deveríamos tomar

$$y = \sqrt{x^3+1};$$

que, elevado ao quadrado, nos dá a curva de equação,

$$y^2 = x^3 + 1.$$

Dado qualquer ponto desta curva, há sempre uma reta, passando por este ponto, que intersecta a curva em 3 pontos, como ilustra a figura abaixo.



Por causa disto, não podemos utilizar neste exemplo o mesmo método de parametrização adotado no caso da circunferência e da curva $y^2 = x^3 + x^2$. Na verdade, $y^2 = x^3 + 1$ não admite parametrização racional, como mostramos no próximo teorema.

Teorema 2.1. *A curva de equação $y^2 = x^3 + 1$ não admite parametrização em termos de funções racionais.*

Demonstração. Vamos proceder por contradição. Para isto suporemos que existem polinômios f, g e $h \neq 0$ em $\mathbb{R}[t]$, tais que as funções racionais

$$x = \frac{f}{h} \quad \text{e} \quad y = \frac{g}{h},$$

constituem uma parametrização da curva dada. Note que escolhemos escrever estas funções racionais em termos de um denominador comum h. Com isto, não podemos supor que estas duas frações de polinômios são reduzidas. O melhor que podemos fazer é escolher f, g e h de modo que

$$\operatorname{mdc}(f, g, h) = 1.$$

Substituindo as expressões para x e y na equação da curva e eliminando o denominador, obtemos

$$g^2 h = f^3 + h^3. \tag{2}$$

É conveniente separar a demonstração em dois casos que precisam ser tratados separadamente. Como veremos, o caso 2 é bem mais complicado que o caso 1.

CASO 1: $h \neq 0$ é constante.

Neste caso, absorvendo a constante h nos polinômios f e g, podemos escrever

$$g^2 = f^3 + 1,$$

Portanto,

$$f^3 = g^2 - 1 = (g - 1)(g + 1).$$

Como cada fator irredutível de f tem multiplicidade três e $g + 1$ e $g - 1$ são primos entre si, podemos concluir que existem polinômios a e b em $\mathbb{R}[t]$, tais que

$$g - 1 = a^3 \quad \text{e} \quad g + 1 = b^3.$$

Subtraindo a primeira destas expressões da segunda,

$$2 = a^3 - b^3 = (a - b)(a^2 + ab + b^2).$$

Mas isto só pode ocorrer se $a - b$ e $a^2 + ab + b^2$ são ambos constantes. Entretanto, neste caso, a e b seriam constantes e não teríamos uma curva, que é a contradição desejada.

CASO 2: $h \neq 0$ não é constante.

Não sendo constante, h admite um fator irredutível, digamos $p \in \mathbb{R}[t]$. Fatorando a maior potência de p que divide h, podemos escrever

$$h = p^k \overline{h}, \quad \text{onde} \quad \operatorname{mdc}(p, \overline{h}) = 1.$$

Substituindo isto em (2),

$$g^2 p^k \overline{h} = f^3 + p^{3k} \overline{h}^3; \tag{3}$$

donde concluímos que p divide f. Procedendo como para h, fatoramos a maior potência de p que divide f, o que nos dá

$$f = p^\ell \overline{f}, \quad \text{onde} \quad \operatorname{mdc}(p, \overline{f}) = 1.$$

Substituindo em (3),

$$g^2p^k\overline{h} = p^{3\ell}\overline{f}^3 + p^{3k}\overline{h}^3. \tag{4}$$

Mas isto implica que

$$h^k \quad \text{divide} \quad f^3 = p^{3\ell}\overline{f}^3$$

de modo que $k \leq 3\ell$. Isto nos permite cancelar p^k em (4), restando

$$g^2\overline{h} = p^{3\ell-k}\overline{f}^3 + p^{2k}\overline{h}^3.$$

Contudo, se k fosse *menor* que 3ℓ, p dividiria o lado esquerdo da equação; o que não é possível porque, por hipótese,

$$\mathrm{mdc}(p, \overline{h}) = 1,$$

ao passo que

$$\mathrm{mdc}(f, g, h) = 1,$$

e já verificamos que p divide f e h, de modo que já não pode dividir g. Logo, $k = 3\ell$. Como p representa um fator irredutível qualquer de h, concluímos que

> a multiplicidade de cada um dos fatores irredutíveis de h é múltiplo de 3.

Em outras palavras, $h = b^3$ para algum polinômio $b \in \mathbb{R}[t]$.

Substituindo $h = b^3$ em (2),

$$g^2b^3 = f^3 + b^9; \tag{5}$$

donde b^3 divide f^3. Mas isto só pode ocorrer se b divide f. Escrevendo,

$$f = b\tilde{f}, \quad \text{para algum} \quad \tilde{f} \in \mathbb{R}[t],$$

(5) transforma-se em

$$g^2b^3 = b^3\tilde{f}^3 + b^9;$$

da qual podemos cancelar b^3, obtendo

$$g^2 = \tilde{f}^3 + b^6.$$

que pode ser reescrita como

$$g^2 - b^6 = \tilde{f}^3.$$

Fatorando o lado esquerdo desta última equação,

$$(g - b^3)(g + b^3) = \tilde{f}^3. \tag{6}$$

Contudo, $g - b^3$ e $g + b^3$ são primos entre si; caso contrário b e g não teriam um fator comum, afinal

$$\mathrm{mdc}(f, g, h) = 1,$$

e b divide $h = b^3$ e $f = b\tilde{f}$. Mas isto implica que cada fator irredutível do lado direito de (6) tem multiplicidade 3 e é fator de $g - b^3$ ou de $g + b^3$, *mas não de ambos*. Isto só é possível se $g - b^3$ e $g + b^3$ forem cubos; digamos

$$g - b^3 = a^3 \quad \text{e} \quad g + b^3 = c^3,$$

para certos polinômios $a, c \in \mathbb{R}[t]$. Além disso,

$$\operatorname{mdc}(a, c) = \operatorname{mdc}(g - b^3, g + b^3) = 1. \tag{7}$$

Logo,

$$g = a^3 + b^3 = c^3 - b^3,$$

donde

$$a^3 + 2b^3 = c^3.$$

Derivando esta equação em relação a t,

$$3a^2a' + 6b^2b' = 3c^2c'.$$

Destas duas últimas equações segue que $u = a^2$ e $v = b^2$ são soluções do sistema linear

$$au + 2bv = c^3$$

$$a'u + 2b'v = c^2c'.$$

Mas o determinante do sistema

$$\det \begin{bmatrix} a & 2b \\ a' & 2b' \end{bmatrix} = 2(ab' - a'b)$$

só é nulo se $b = 0$ ou a/b for uma constante. No primeiro caso, o denominador h seria nulo; no segundo, teríamos uma contradição com (7). Mas se o sistema tem determinante não nulo, então suas soluções são únicas e podemos deduzir da regra de Cramer que

$$\det \begin{bmatrix} a & 2b \\ a' & 2b' \end{bmatrix} b^2 = \det \begin{bmatrix} a & c^3 \\ a' & c^2 \end{bmatrix}.$$

Logo,

$$2b^2(ab' - a'b) = c^2(ac' - a'c). \tag{8}$$

Entretanto, (7) implica que

$$\operatorname{mdc}(b, c) = 1;$$

de modo que

$$b^2 \quad \text{divide} \quad (ac' - a'c).$$

Assim,

$$2\operatorname{grau}(b) \leq \operatorname{grau}(a) + \operatorname{grau}(c) - 1,$$

Por outro lado, igualando graus dos dois lados da equação (8), e eliminando os termos comuns, verificamos que

$$\operatorname{grau}(b) = \operatorname{grau}(c).$$

Combinando as duas últimas expressões,

$$\operatorname{grau}(b) \leq \operatorname{grau}(a) - 1.$$

Contudo, repetindo o mesmo argumento para calcular $u = a^2$ a partir da regra de Cramer deduzimos que

$$\operatorname{grau}(b) = \operatorname{grau}(a),$$

que nos dá a contradição desejada.

Para não encerrarmos a seção em uma nota negativa, aqui vai uma boa notícia: existe um critério relativamente simples para detectar se uma dada curva algébrica pode ou não ser parametrizada por funções racionais. Mais precisamente, seja $F(x, y)$ um polinômio com coeficientes reais, nas variáveis x e y. A *curva algébrica* C definida por F em $\mathbb{R}^2$ é o conjunto dos pontos $p \in \mathbb{R}^2$ nos quais o polinômio F se anula; em símbolos

$$C = \{p \in \mathbb{R}^2 : F(p) = 0\}.$$

Dizemos que uma tal curva é *singular* se $\nabla F(p) = 0$ para algum $p \in C$. Caso contrário a curva é *não singular*. Isto é, o gradiente de uma curva algébrica não singular é sempre não nulo. Como o gradiente corresponde ao vetor normal à curva, isto significa que a curva tem vetores normais e tangentes não nulos em todos os seus pontos. Portanto, geometricamente falando, uma curva é não singular se cada um de seus pontos tem uma tangente bem definida. Das curvas analisadas acima,

$$x^2 + y^2 = 1 \quad \text{e} \quad y^2 = x^3 + 1$$

não são singuares, ao passo que $y^2 = x^3 + x^2$ é singular.

O *gênero* de uma curva algébrica não singular C é o número

$$g(C) = \frac{1}{2}(d-1)(d-2),$$

onde d é o grau do polinômio F que define C. Observe que as curvas não singulares de graus um (retas) e dois (cônicas, incluindo a circunferência) têm gênero zero, ao passo que qualquer curva de grau maior ou igual a 3 tem gênero maior que zero. O gênero também pode ser definido para curvas algébricas singulares, mas a fórmula é bem mais complicada porque precisamos de somar parcelas para dar conta do comportamento das singularidades. Para mais detalhes veja, por exemplo, [4, p. 30]. Em nosso contexto a importância do gênero é explicada pelo seguinte teorema.

Teorema 2.2. *Uma curva algébrica admite uma parametrização racional se, e somente se, seu gênero é zero.*

A demonstração deste teorema depende de conceitos e resultados de geometria algébrica e está fora do alcance destas notas.

3. Fatorações sem quadrados

O objetivo desta seção é de estabelecer a chamada *fatoração sem quadrados* (ou livre de quadrados) de um polinômio em uma variável.

Seja, pois, g um polinômio do anel $K[x]$, onde K é um corpo. Fatorando g, obtemos

$$g = cp_1^{e_1} \cdots p_s^{e_s} \in K[x], \tag{9}$$

onde $c \in K \setminus \{0\}$, $p_1, \dots, p_s$ são polinômios irredutíveis de $K[x]$, e os expoentes $e_1, \dots, e_s$ são todos positivos. A *parte livre de quadrados* de g é igual a

$$\mathrm{lq}(g) = p_1 \cdots p_s.$$

Em outras palavras, a parte livre de quadrados é igual ao produto dos fatores irredutíveis de g tomados com multiplicidade um.

Para poder utilizar a parte livre de quadrados na prática, precisamos de um procedimento para calculá-la sem precisar fatorar o polinômio. Um tal procedimento existe, e é bastante simples. O algoritmo se baseia na seguinte fórmula. Suponha que g se fatora como na equação (9). Então,

$$g' = \frac{dg}{dx} = \sum_{j=1}^{s} e_j c p_1^{e_1} \cdots p_j^{e_j - 1} \cdots p_s^{e_s} =$$

$$c p_1^{e_1-1} \cdots p_s^{e_s-1} \sum_{j=1}^{s} e_j p_1 \cdots p_{j-1} p_{j+1} \cdots p_s.$$

Note que a j-ésima parcela do somatório não inclui o fator p_j; de modo que

$$\mathrm{mdc}\left(g, \sum_{j=1}^{s} e_j p_1 \cdots p_{j-1} p_{j+1} \cdots p_s\right) = 1.$$

Portanto,

$$\mathrm{mdc}(g, g') = p_1^{e_1-1} \cdots p_s^{e_s-1}.$$

Logo,

$$f = \frac{g}{\mathrm{mdc}(g, g')} = c p_1 \cdots p_s;$$

isto é,

$$\mathrm{lq}(g) = g/\mathrm{lc}(g).$$

Mas o máximo divisor comum, para polinômios em uma variável, pode ser calculado sem a necessidade de fatorar os polinômios. Para isto basta usar o algoritmo euclidiano para polinômios em uma variável.

Algoritmo 3.1 (Remoção de quadrados)**.** *Dado o gerador g de um ideal I de $K[x]$, o algoritmo tem como saída o polinômio* $\mathrm{lq}(g)$.

Etapa 1: *Use o algoritmo euclidiano para calcular* $d = \mathrm{mdc}(g, g')$.
Etapa 2: *Calcule $f = g/d$.*
Etapa 3: *Retorne* $\mathrm{lq}(g) = f/\mathrm{lc}(f)$.

Por exemplo, se

$$g = x^9 + 7x^8 + 21x^7 + 39x^6 + 55x^5 + 61x^4 + 51x^3 + 33x^2 + 16x + 4,$$

então,

$$g' = \frac{dg}{dx} = 9x^8 + 56x^7 + 147x^6 + 234x^5 + 275x^4 + 244x^3 + 153x^2 + 66x + 16.$$

Aplicando o algoritmo euclidiano, obtemos

$$\mathrm{mdc}(g, dg/dx) = x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2.$$

Efetuando a divisão de g pelo máximo divisor comum,

$$x^4 + 3x^3 + 3x^2 + 3x + 2.$$

Como este polinômio já é mônico, não precisamos dividi-lo por seu coeficiente líder; assim

$$\mathrm{lq}(g) = x^4 + 3x^3 + 3x^2 + 3x + 2.$$

O algoritmo anterior também pode ser usado para calcular uma espécie de fatoração parcial de um polinômio $g \in K[x]$. Digamos que

$$g = p_1^{e_1} \cdots p_s^{e_s}$$

é a fatoração completa de g em $K[x]$. A *fatoração livre de quadrados* de f é

$$g = g_1 g_2^2 \cdots g_m^m,$$

onde g_i é o produto dos fatores irredutíveis de g cuja multiplicidade é i e

$$m = \mu(g) = \max\{e_1, \ldots, e_s\}$$

é a *multiplicidade máxima* de g. Além de poder ser obtida a um custo muito baixo, esta fatoração tem a vantagem de agrupar os fatores de f de acordo com sua multiplicidade.

Como vimos anteriormente, se

$$g = p_1^{e_1} \cdots p_s^{e_s}$$

então,

$$\mathrm{mdc}(g, g') = p_1^{e_1-1} \cdots p_s^{e_s-1}.$$

Assim, um fator irredutível que tem multiplicidade k em f, terá multiplicidade $k-1$ em $\mathrm{mdc}(g, g')$. Desta forma, para determinar o produto dos polinômios irredutíveis que aparecem com multiplicidade k na fatoração de g basta calcular os que aparecem com multiplicidade $k-1$ na fatoração de $\mathrm{mdc}(g, g')$. Em particular,

$$\mu(\mathrm{mdc}(g, g')) = \mu(f) - 1 = m - 1.$$

Temos, então, um procedimento que nos permite reduzir o problema a um polinômio cuja multiplicidade máxima é menor que a de g.

Para converter este procedimento em um algoritmo, basta-nos encontrar uma maneira de calcular o produto g_1 dos fatores de multiplicidade 1. Porém, a parte livre de quadrados de $\mathrm{mdc}(g, g')$ contém apenas aqueles fatores irredutíveis cuja multiplicidade em g é maior que um. Desta forma,

$$g_1 = \frac{\mathrm{lq}(g)}{\mathrm{lq}(\mathrm{mdc}(g, g'))}.$$

Podemos sistematizar este algoritmo da seguinte forma.

Algoritmo 3.2. *Dado um polinômio $g \in K[x]$, o algoritmo calcula sua fatoração livre de quadrados*
$$g = \mathrm{lc}(g) \cdot g_1 g_2^2 \cdots g_m^m,$$
onde g_i é o produto dos fatores irredutíveis de g cuja multiplicidade é i.

Etapa 1: *Inicialize a lista $\mathcal{L}$ com $\mathrm{lc}(g)$ e a variável G com g.*
Etapa 2: *Calcule $D = \mathrm{mdc}(G, G')$.*
Etapa 3: *Se $D = 1$ acrescente G ao final de $\mathcal{L}$, retorne $\mathcal{L}$ e páre.*
Etapa 4: *Acrescente $\mathrm{lq}(G)/\mathrm{lq}(D)$ ao final da lista $\mathcal{L}$.*
Etapa 5: *Faça $G = D$ e volte à Etapa 2.*

Note que a saída do algoritmo é a lista
$$\mathcal{L} = [\mathrm{lc}(g), g_1, g_2, \dots, g_m].$$
Portanto, o i-ésimo o elemento da lista corresponde ao produto g_i dos fatores que aparecem em g com multiplicidade i. Assim, podemos determinar a multiplicidade do fator pela sua posição na lista. Por exemplo, seja
$$g = x^9 + 7x^8 + 21x^7 + 39x^6 + 55x^5 + 61x^4 + 51x^3 + 33x^2 + 16x + 4.$$
o mesmo polinômio utilizado no exemplo anterior. Neste caso a lista $\mathcal{L}$ é inicializada como
$$\mathcal{L} = [1],$$
já que $G = g$ é mônico. Aplicando o algoritmo a g, temos os seguintes passos:

Primeiro passo: Já vimos, anteriormente, que
$$D = \mathrm{mdc}(G, G') = x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2;$$
e que
$$\mathrm{lq}(G) = x^4 + 3x^3 + 3x^2 + 3x + 2.$$
Utilizando o algoritmo 3.1, obtemos
$$\mathrm{lq}(D) = x^4 + 3x^3 + 3x^2 + 3x + 2;$$
donde
$$g_1 = 1.$$
Portanto g não tem fatores irredutíveis com multiplicidade um. Ao final deste passo
$$G = x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2,$$
$$\mathcal{L} = [1, 1].$$

Segundo passo: Desta vez, temos que
$$D = \mathrm{mdc}(G, G') = x + 1,$$
ao passo que
$$\mathrm{lq}(G) = x^4 + 3x^3 + 3x^2 + 3x + 2$$
e
$$\mathrm{lq}(D) = x + 1.$$

Efetuando a divisão, obtemos

$$g_2 = x^3 + 2x^2 + x + 2.$$

Ao final do segundo passo

$$\begin{aligned} G &= x + 1, \\ \mathcal{L} &= [1, 1, x^3 + 2x^2 + x + 2]. \end{aligned}$$

Terceiro passo: Como $G' = 1$,

$$D = \mathrm{mdc}(G, G') = 1,$$

e resta-nos apenas acrescentar $G = x + 1$ ao final da lista, obtendo

$$\mathcal{L} = [1, 1, x^3 + 2x^2 + x + 2, x + 1].$$

O resultado obtido pelo algoritmo significa que

$$g = (x^3 + 2x^2 + x + 2)^2 (x + 1)^3,$$

como é fácil comprovar, efetuando a multiplicação.

4. Resultante

A noção de resultante foi introduzida no século XIX mas, durante a maior parte do século XX, não gozou de muito boa fama, até que foi reinstaurada por conta de suas inúmeras aplicações em computação algébrica.

Seja D um domínio e $f, g \in D[x]$. Explicitando os coeficientes de f e g temos que

$$f = a_s x^s + \cdots + a_1 x + a_0 \quad \text{e} \quad g = b_t x^t + \cdots + b_1 x + b_0,$$

onde os as e bs pertencem a D e $a_n b_m \neq 0$. A *resultante de f e g em relação a x* é o determinante da matriz de Sylvester, definida como

$$S = \left[\begin{array}{cccccccc} a_s & a_{s-1} & \cdots & a_1 & a_0 & \cdots & 0 & 0 \\ 0 & a_s & a_{s-1} & \cdots & a_1 & a_0 \cdots & 0 & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_s & a_{s-1} & \cdots & a_1 & a_0 \\ b_t & b_{t-1} & \cdots & b_1 & b_0 & \cdots & 0 & 0 \\ 0 & b_t & b_{t-1} & \cdots & b_1 & b_0 \cdots & 0 & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & b_t & b_{t-1} & \cdots & b_1 & b_0 \end{array}\right] \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} t \text{ linhas} \\ \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} s \text{ linhas} \end{array}$$

Observe que os coeficientes de f aparecem nas primeiras t linhas da matriz–onde $t = \mathrm{grau}(g)$–sempre deslocados de uma casa para a direita em relação à linha imediatamente acima. Da mesma forma, os coeficientes de g aparecem nas primeiras s linhas da matriz–onde $s = \mathrm{grau}(f)$–também deslocados de uma casa para a direita em relação à linha imediatamente acima. Em particular, S é uma matriz quadrada $s + t$.

Denotando a resultante definida acima por $\text{res}_x(f, g)$, temos que

$$\text{res}_x(f, g) = det(S)$$

é um elemento do domínio D. Precisaremos de algumas propriedades da resultante, que passamos a enunciar e provar.

Propriedade. *Se $f, g \in D[x]$, podemos calcular $A, B \in D[x]$ tais que $Af + Bg = \text{res}_x(f, g)$.*

Demonstração. Multiplicando

$$a_s x^s + \cdots + a_1 x + a_0 = f$$

por x^i, com $0 \leq i \leq t - 1$ e

$$b_t x^t + \cdots + b_1 x + b_0 = g,$$

por x^j, com $0 \leq j \leq s - 1$, obtemos um sistema

$$\begin{aligned}
a_s x^{s+t-1} + a_{s-1} x^{s+t-2} + \cdots + a_1 x^t + a_0 x^{t-1} &= x^{t-1} f \\
a_s x^{s+t-2} + a_{s-1} x^{s+t-3} + \cdots + a_1 x^{t-1} + a_0 x^{t-2} &= x^{t-2} f \\
\vdots \qquad\quad \vdots \quad &\ \ \vdots \\
a_s x^s + \cdots + a_1 x + a_0 &= f \\
b_t x^{t+s-1} + b_{t-1} x^{s+t-2} + \cdots + b_1 x^s + b_0 x^{s-1} &= x^{s-1} g \\
b_t x^{s+t-2} + b_{t-1} x^{s+t-3} + \cdots + b_1 x^{s-1} + b_0 x^{s-2} &= x^{s-2} g \\
\vdots \qquad\quad \vdots \quad &\ \ \vdots \\
b_t x^t + \cdots + b_1 x + b_0 &= g
\end{aligned}$$

que pode ser expresso, em forma matricial, como

$$S \begin{bmatrix} x^{s+t-1} \\ x^{s+t-2} \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} x^{t-1} f \\ \vdots \\ f \\ x^{s-1} g \\ \vdots \\ g \end{bmatrix}$$

Aplicando o método de Cramer para resolver este sistema relativamente à sua última componente, obtemos

$$\operatorname{res}_x(f,g) = \det(S) = \left[\begin{array}{c|c} & x^{t-1}f \\ & \vdots \\ & f \\ \widehat{S} & x^{s-1}g \\ & \vdots \\ & g \end{array}\right],$$

onde $\widehat{S}$ é a matriz $(s+t)\times(s+t-1)$ obtida de S pela remoção de sua última coluna. Para obter a fórmula desejada basta expandir o determinante da matriz da direita pela sua última coluna e observar que cada uma das parcelas estará multiplicada por f ou por g.

A próxima propriedade justifica o interesse da noção de resultante em álgebra e geometria.

Propriedade. *Dois polinômios $f, g \in D[x]$ têm um fator não constante comum se, e somente se,* $\operatorname{res}_x(f,g) = 0$.

Demonstração. Suponhamos que f e g tenham um fator não constante h em comum. Mas, pela propriedade 4, podemos escrever

$$\operatorname{res}_x(f,g) = Af + Bg$$

onde $A, B \in D[x]$. Como h divide f e g, então divide $Af + Bg$. Portanto, h divide $\operatorname{res}_x(f,g)$. Contudo, h é não constante por hipótese, ao passo que a resultante é um elemento de D. Mas isto só é possível se a resultante for nula.

Precisamos de uma última propriedade, um pouco mais técnica, que será necessária na demonstração do teorema 9.1.

Propriedade. *Se $f, g \in D[x]$, então*

$$\operatorname{res}_x(f,g) = a_s g(\alpha_1)\cdots g(\alpha_s)$$

onde a_s é o coeficiente líder de f e $\alpha_1, \ldots, \alpha_s$ são suas raízes.

Antes de encerrar precisamos introduzir uma generalização da noção de resultante, a chamada subresultante. Mais uma vez estaremos supondo que $f, g \in D[x]$, e que D é um domínio. A *k-ésima subresultante de f e g*, que será denotada por $S_k(f,g)$, é o determinante da matriz

$$\begin{bmatrix} a_s & a_{s-1} & \cdots & \cdots & a_1 & a_{2k-s} & x^{s-k-1}f \\ 0 & a_s & a_{s-1} & \cdots & a_2 & a_{2k-s-1} & x^{s-k-2}f \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \vdots & 0 & a_s & a_{k+1} & f \\ b_t & b_{t-1} & \cdots & \vdots & b_1 & b_{2k-t} & x^{t-k-1}g \\ 0 & b_t & b_{t-1} & \cdots & b_2 & b_{2k-t-1} & x^{t-k-2}g \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \\ 0 & \cdots & \vdots & 0 & b_t & b_{k+1} & g \end{bmatrix},$$

onde consideramos todos os coeficientes cujos índices são negativos como sendo nulos. Comparando esta matriz com a matriz do sistema construído como parte da demonstração da propriedade 4, vemos que

$$S_0(f,g) = \mathrm{res}_x(f,g).$$

Expandindo o determinante da matriz acima pela última coluna, podemos calcular polinômios $A_k, B_k \in D[x]$, tais que

$$A_k f + B_k g = S_k(f,g). \tag{10}$$

Além disso, não é difícil verificar que S_k tem grau k. O resultado mais importante sobre subresultantes que utilizaremos adiante é o seguinte teorema.

Teorema 4.1. *Seja $\sigma : A \to B$ um homomorfismo entre dois domínios e $\overline{\sigma} : A[x] \to B[x]$ sua extensão aos anéis de polinômios correspondentes. Se $f, g \in A[x]$ são polinômios não nulos e f e $\overline{\sigma}(f)$ têm o mesmo grau, então*

$$\overline{\sigma}(S_j(f,g)) = c_j S_j(f,g)$$

para alguma constante $c_j \in B$ para todo

$$0 \leq j \leq \min\{\mathrm{grau}(f), \mathrm{grau}(g)\}.$$

5. Bernoulli

Antes de mais nada, uma observação sobre notação. Ao longo de todas as notas, usaremos tanto df/dx, quanto $f'(x)$, para denotar a derivada de uma função f, na variável x.

Podemos escrever uma função racional $f \in \mathbb{R}(x)$ na forma $f = N/D$, onde $N, D \in \mathbb{R}[x]$ e $D \neq 0$. Se N tem grau maior do que D, podemos dividi-los obtendo

$$N = DQ + R, \ \text{ onde } \ R = 0 \ \text{ ou } \ \mathrm{grau}(R) < \mathrm{grau}(D).$$

Assim,

$$f = \frac{N}{D} = \frac{DQ+R}{D} = Q + \frac{R}{D},$$

de forma que

$$\int f dx = \int Q dx + \int \frac{R}{D} dx.$$

Como Q é um polinômio, não há dificuldade em integrá-lo. Portanto, para obter a integral de f basta integrar R/D, onde R tem grau menor que D.

Para isto, começamos fatorando D. Como estamos trabalhando com funções reais, a fatoração terá que ser sobre $\mathbb{R}[x]$. Portanto, esperamos encontrar entre os fatores de D polinômios de grau um ou dois, já que estas são as únicas possibilidades quando o polinômio é irredutível sobre $\mathbb{R}$. Digamos que

$$D = (x - \alpha_1)^{r_1} \cdots (x - \alpha_m)^{r_m} (x^2 + a_1 x + b_1)^{s_1} \cdots (x^2 + a_n x + b_n)^{s_n}.$$

A partir desta fatoração podemos escrever a decomposição em frações parciais de R/D. As parcelas nesta decomposição são de dois tipos, dependendo do seu denominador. Para os fatores de grau um temos parcelas da forma

$$\frac{c_{ik}}{(x - \alpha_i)^k} \quad \text{onde} \quad 1 \leq k \leq r_i \ \text{ e } \ c_{ik}, \alpha_i \in \mathbb{R}.$$

Já os fatores de grau dois dão origem a parcelas do tipo

$$\frac{d_{ik} x + c_{i\ell}}{(x^2 + a_i x + b_i)^\ell} \quad \text{onde} \quad 1 \leq \ell \leq s_i \ \text{ e } \ d_{ik}, c_{ik}, a_i, b_i \in \mathbb{R}.$$

Antes de prosseguir, vejamos um exemplo. Seja

$$f = \frac{x^2 + 3}{x^6 - 3x^2 - 2}. \tag{11}$$

Como o numerador de f já tem grau menor que o seu denominador, não precisamos efetuar nenhuma divisão. Passamos, assim, diretamente à fatoração do denominador, que é

$$x^6 - 3x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 1)^2.$$

A decomposição em frações parciais correspondente será

$$\frac{5\sqrt{2}}{36} \left(\frac{1}{x - \sqrt{2}} - \frac{1}{x + \sqrt{2}} \right) - \frac{5}{9} \left(\frac{1}{x^2 + 1} \right) - \frac{2}{3} \left(\frac{1}{(x^2 + 1)^2} \right).$$

Voltemos ao caso geral, analisado acima. Tendo em mãos a decomposição em frações parciais de R/Q basta integrá-la termo a termo. Portanto, reduzimos o problema à integração de funções racionais dos seguintes tipos

$$\frac{1}{(x - \alpha)^k} \ \text{ e } \ \frac{ax + b}{(x^2 + \alpha x + \beta)^k},$$

onde a, b, α e β são números reais, e $k \geq 2$ é um inteiro positivo. Trataremos cada um destes casos separadamente. Em primeiro lugar, uma simples integração por substituição nos dá

$$\int \frac{dx}{(x - \alpha)^k} = \begin{cases} -\frac{(x-\alpha)^{1-k}}{k-1} & \text{se } k > 1 \\ \log(x - \alpha) & \text{se } k = 1. \end{cases} \tag{12}$$

Passando ao segundo caso, precisamos integrar

$$\int \frac{ax+b}{(x^2+\alpha x+\beta)^k}dx,$$

onde $k \geq 1$. Para simplificar a notação, denotaremos o numerador por f e o denominador por g. Então, $g' = 2x + \alpha$, de modo que

$$f = ax + b = \frac{a}{2}g' + b - \frac{a}{2}.$$

Portanto,

$$\int \frac{f}{g^k}dx = \frac{a}{2}\int \frac{g'}{g^k}dx + \left(b - \frac{a}{2}\right)\int \frac{1}{g^k}dx.$$

Contudo,

$$\int \frac{g'}{g^k}dx = \begin{cases} \log g & \text{se } \ k = 1 \\ \frac{1}{(1-k)}g^{1-k} & \text{se } \ k \geq 2. \end{cases}$$

Assim, basta calcular

$$\int \frac{1}{g^k}dx$$

para encerrar o problema. Mas, completando quadrados em g, obtemos

$$g = \left(x + \frac{\alpha}{2}\right)^2 + \beta - \frac{\alpha^2}{4}.$$

Fazendo, agora, a mudança de variáveis

$$x = \left(\frac{4\beta - \alpha^2}{4}\right)^{-1/2} y - \alpha/2,$$

a integral se reescreve como

$$\int \frac{1}{g^k}dx = \left(\frac{4}{4\beta - \alpha^2}\right)^{k/2}\int \frac{1}{(y^2+1)^k}dy,$$

o que reduz o problema à integração de $1/(y^2+1)^k$.

Fazemos esta integração em duas etapas: reduzimos, recursivamente, ao caso $k = 1$ e, então, calculamos este caso explicitamente. Porém,

$$\frac{d}{dy}\arctan y = \frac{1}{1+y^2}, \tag{13}$$

de forma que

$$\int \frac{1}{y^2+1}dy = \arctan y, \tag{14}$$

resolvendo assim o caso $k = 1$. Para obter a fórmula de redução, integramos $1/(y^2+1)^{k-1}$ por partes, o que nos dá

$$\int \frac{1}{(y^2+1)^{k-1}}dy = \frac{y}{(y^2+1)^{k-1}} + 2(k-1)\int \frac{y^2}{(y^2+1)^k}dy. \tag{15}$$

Somando e subtraindo 1 do numerador y^2, e efetuando os cancelamentos necessários, temos que

$$\int \frac{y^2 dy}{(y^2+1)^k} = \int \frac{dy}{(y^2+1)^{k-1}} - \int \frac{dy}{(y^2+1)^k} dy.$$

Substituindo em (15),

$$\int \frac{dy}{(y^2+1)^{k-1}} = \frac{y}{(y^2+1)^{k-1}} + \int \frac{2(k-1)dy}{(y^2+1)^{k-1}} - \int \frac{2(k-1)dy}{(y^2+1)^k}.$$

Resolvendo para a integral de $1/(y^2+1)^k$, obtemos a fórmula de redução desejada

$$\int \frac{dy}{(y^2+1)^k} = \frac{y}{2(k-1)(y^2+1)^{k-1}} + \frac{2k-3}{2(k-1)} \int \frac{dy}{(y^2+1)^{k-1}}.$$

Ao invés de substituir estas equações umas nas outras para obter uma fórmula recursiva geral de redução, é preferível efetuar as substituições uma a uma à medida que o processo vai sendo realizado. Desta forma é mais fácil acompanhar a mecânica do prcedimento. Vamos aplicar este método à integral da função f definida em (11). Usando a decomposição em frações parciais, vemos que f tem como primitiva

$$\frac{5\sqrt{2}}{36}\left(\int \frac{dx}{x-\sqrt{2}} - \int \frac{dx}{x+\sqrt{2}}\right) - \frac{5}{9}\int \frac{dx}{x^2+1} - \frac{2}{3}\int \frac{dx}{(x^2+1)^2}. \tag{16}$$

Cada uma destas integrais será calculada separadamente, usando o algoritmo de Bernoulli, como o descrevemos acima. Em primeiro lugar,

$$\int \frac{1}{x-\sqrt{2}}dx = \log(x-\sqrt{2}) \text{ e } \int \frac{1}{x+\sqrt{2}}dx = \log(x+\sqrt{2}), \tag{17}$$

não oferece nenhuma dificuldade. Já a terceira integral é calculada usando (14),

$$\int \frac{1}{x^2+1}dx = \arctan(x).$$

Usando a fórmula de redução na última integral da equação (16),

$$\int \frac{dx}{(x^2+1)^2} = \frac{1}{2}\int \frac{dx}{(x^2+1)} + \frac{x}{2(x^2+1)} = \frac{1}{2}\left(\arctan x + \frac{x}{(x^2+1)}\right).$$

Substituindo tudo de volta na integral original e efetuando as reduções necessárias, obtemos a seguinte primitiva para f,

$$\frac{5\sqrt{2}}{36}\left(\log(x-\sqrt{2}) - \log(x+\sqrt{2})\right) - \frac{8}{9}\arctan(x) - \frac{1}{3}\frac{x}{(x^2+1)}.$$

Usando, finalmente, as propriedades dos logaritmos, temos que

$$\int \frac{x^2+3}{x^6-3x^2-2}dx = \frac{5\sqrt{2}}{36}\log\left(\frac{x-\sqrt{2}}{x+\sqrt{2}}\right) - \frac{8}{9}\arctan(x) - \frac{1}{3}\frac{x}{(x^2+1)}.$$

Uma maneira de evitar a fórmula de redução é admitir funções de variável complexa. Se fizermos isto, a primeira coisa a ser simplificada é a decomposição de f em frações parciais, que passa a ser

$$\frac{5\sqrt{2}}{36}\left(\frac{1}{x-\sqrt{2}}-\frac{1}{x+\sqrt{2}}\right)+ \\ \frac{4}{9}\left(\frac{i}{x-i}-\frac{i}{x+i}\right)+ \\ \frac{1}{6}\left(\frac{1}{(x-i)^2}+\frac{1}{(x+i)^2}\right).$$

Neste caso podemos usar o equivalente da fórmula (12) para cada uma das parcelas. Fazendo isto, e agrupando os logaritmos, obtemos a seguinte primitiva para f,

$$\frac{5\sqrt{2}}{36}\log\left(\frac{x-\sqrt{2}}{x+\sqrt{2}}\right)+\frac{4}{9}i\log\left(\frac{x-i}{x+i}\right)-\frac{1}{6}\left(\frac{1}{(x-i)}+\frac{1}{(x+i)}\right).$$

Como você vê, não há nenhum arco tangente à vista! Contudo, a integral de uma função real acabou dando uma função complexa, o que não é muito agradável. Contudo, se as duas fórmulas que obtivemos para a primitiva de f estão corretas, então devem diferir apenas por uma constante; e é isto que mostraremos a seguir.

Para isto precisamos apenas considerar o que ocorre com as três últimas parcelas, já que a primeira coincide nas duas fórmulas. Contudo,

$$\frac{1}{(x-i)}+\frac{1}{(x+i)}=\frac{2x}{(x^2+1)},$$

de forma que o problema se reduz a expressar

$$\log\left(\frac{x-i}{x+i}\right)$$

em termos de arcos tangentes. Para isto, podemos usar o seguinte lema.

Lema 5.1. *Se $g \in \mathbb{R}(x)$ e $g^2 \neq -1$, então*

$$i\frac{d}{dx}\log\left(\frac{g+i}{g-i}\right)=2\frac{d}{dx}\arctan(g).$$

Demonstração. Derivando $\log(g-i/g+i)$ em relação a x, obtemos

$$\frac{g-i}{g+i}\frac{g'(g-i)-g'(g+i)}{(g-i)^2}=2i\frac{g'}{g^2+1}.$$

Portanto,

$$i\frac{d}{dx}\log\left(\frac{g+i}{g-i}\right)=\frac{2g'}{g^2+1},$$

que, por sua vez, é igual à derivada de $2\arctan(g)$, pela regra da cadeia.

Aplicando o lema, vemos que, a menos de uma constante, a função

$$i \log(x - i/x + i)$$

é igual a $2 \arctan(x)$. Juntando tudo o que fizemos, concluímos que

$$\int f dx = \frac{5\sqrt{2}}{36} \log\left(\frac{x-\sqrt{2}}{x+\sqrt{2}}\right) - \frac{8}{9}\arctan(x) - \frac{1}{6}\frac{2x}{(x^2+1)},$$

que é igual ao resultado obtido pelo método de Bernoulli. Na prática, é desta última maneira que vamos proceder. Isto é, faremos a integração em termos de logaritmos, admitindo argumentos e coeficientes complexos, se necessário. Ao final, convertemos o resultado em uma função real usando o lema 5.1. Como veremos, isto pode causar alguns problemas; mas tudo a seu tempo.

Encerramos esta seção enunciando o teorema que resulta de nossa excursão pelos números complexos. Para prová-lo, basta calcular, termo a termo, as primitivas da decomposição em frações parciais sobre $\mathbb{C}$ do integrando.

Teorema 5.2. *Sejam N e D polinômios com coeficientes reais e tais que* $\mathrm{grau}(N) < \mathrm{grau}(D)$ *e seja*

$$D = (x - \alpha_1)^{e_1} \cdots (x - \alpha_d)^{e_d},$$

onde $\alpha_1, \ldots, \alpha_d$ são complexos distintos, e $e_1, \ldots, e_d$ são inteiros positivos. Então

$$\int \frac{N}{D} dx = g + \sum_{i=1}^{d} c_i \log(x - \alpha_i),$$

onde $g \in \mathbb{R}(x)$ e $c_i \in \mathbb{C}$, para $1 \leq i \leq d$. Além disso, $g = 0$ caso $e_i = 1$ para todo $1 \leq i \leq d$.

Demonstração. A decomposição em frações parciais de N/D será uma soma de termos da forma

$$\frac{c}{(x-\alpha)^k},$$

onde $c, \alpha \in \mathbb{C}$ e $k > 0$ é um número inteiro. Pela fórmula (12), a integral desta função racional será outra função racional se $k > 1$. Caso contrário, a integral será um logaritmo. Como a fórmula geral segue da integração de cada parcela da decomposição em frações parciais, o teorema esta provado.

6. Funções elementares

Como conseqüência do algoritmo de Bernoulli, temos que a integral de qualquer função racional com coeficientes reais pode ser escrita como a soma de funções racionais, logaritmos e arcos tangentes. Estas três são típicos representantes das funções tradicionalmente estudadas nos cursos de cálculo, e que chamamos de funções elementares. Como vamos usar este conceito de maneira sistemática, é conveniente defini-lo de maneira mais precisa.

Uma função de uma variável é *elementar* se pode ser definida a partir das funções

- racionais;

- algébricas;
- trigonométricas diretas e inversas;
- exponencial e logaritmo;

pela aplicação recursiva das operações de adição, subtração, multiplicação, divisão e composição de funções.

Das quatro categorias básicas de funções, apenas a segunda precisa de esclarecimentos adicionais. Dizemos que uma função f na variável (real) x é *algébrica* se existe polinômio um polinômio irredutível $G(x, y) \in \mathbb{R}[x, y]$ tal que

$$G(x, f(x)) = 0,$$

para todo x no domínio de f. Por exemplo, $\sqrt{x}$ é algébrica, já que satisfaz o polinômio irredutível $F(x, y) = y^2 - x$. As funções racionais também são algébricas. De fato, se $p, q \in \mathbb{R}[x]$ e $q \neq 0$, então a função racional p/q satisfaz o polinômio $p - qy$. Em particular, vemos que as classes de funções básicas que aparecem na definição de funções elementares não são mutuamente exclusivas. Com um pouco de esforço (que não faremos aqui) pode-se mostrar que:

> toda função construída a partir das quatro operações aritméticas elementares, da extração de raízes e da composição de funções, é algébrica.

Contudo, a recíproca desta afirmação é falsa.

Por outro lado, nem todas as funções são algébricas, um fato que já havia sido notado por I. Newton. O que Newton observou é que toda função algébrica satisfaz a seguinte propriedade.

Proposição 6.1. *Se o gráfico de uma função algébrica corta uma reta do plano em uma quantidade infinita de pontos, então o gráfico é a própria reta.*

Demonstração. Seja f uma função algébrica e $G \in \mathbb{R}[x, y]$ um polinômio irredutível tal que $G(x, f(x)) = 0$ para todo ponto do domínio de f. Digamos que r é uma reta do plano que intersecta o gráfico de f em uma infinidade de pontos. Note que r não pode ser uma reta vertical porque o gráfico de uma função não corta nenhuma reta vertical em mais de um ponto. Assim, podemos supor que r tem equação $y = ax + b$, onde $a, b \in \mathbb{R}$.

Considere, agora, um ponto de abscissa x_0 que esteja na interseção do gráfico de f com a reta r. Para que isto ocorra, devemos ter que $f(x_0) = ax_0 + b$, donde

$$G(x_0, ax_0 + b) = 0.$$

Em outras palavras, x_0 é raiz do polinômio de uma variável $q(t) = G(t, at+b)$. Se há infinitos pontos de interseção, então q tem infinitas raízes. Mas isto só pode ocorrer se q for identicamente nulo. Neste caso, dividindo G por $y - ax - b$, obtemos

$$G = Q \cdot (y - ax - b) + R, \text{ onde } Q, R \in \mathbb{R}[x, y].$$

Note que esta divisão é possível porque $y - ax - b$ é mônico como polinômio em y.

Contudo, como o resto R é um polinômio cujo grau em y é menor que o de $y - ax - b$, concluímos que R contém apenas a variável x. Substituindo $y = ax + b$ na equação acima, e levando em conta que $G(x, ax + b) = 0$, verificamos que $R = 0$. Portanto,

$$G = Q \cdot (y - ax - b),$$

o que contradiz o fato de G ser irredutível e completa a demonstração da proposição.

Usando esta proposição, verificamos que uma função periódica, como o seno ou o co-seno, não pode ser algébrica, já que seu gráfico corta alguma reta horizontal em uma infinidade de pontos. Uma função que não é algébrica ' é conhecida como *transcendente*. As funções exponencial e logaritmo também são transcendentes. Contudo, como não são periódicas, não podemos provar isto usando a proposição 6.1. Para uma demonstração da transcendência da exponencial, do logaritmo, e de outras funções correlatas, veja [4, p. 44, §16].

Voltando ao que dizíamos no início da seção, segue do algoritmo de Bernoulli que a primitiva de uma função racional pode ser escrita como soma de uma função racional (e, portanto, algébrica) com arcos tangentes e logaritmos (que são transcendentes). Isto sugere a pergunta

> é possível reformular a parte transcendente da integral, total ou parcialmente, usando funções racionais?

A resposta é não, mas prová-la requer técnicas que estão além dos limites deste livro. Por isso vamos nos contentar em mostrar que a parte transcendente não pode ser *igual* a nenhuma função racional. Um tratamento completo desta questão pode ser encontrado em [REF].

Proposição 6.2. *Sejam α_i e c_i números complexos, $1 \leq i \leq d$. Se os α_i são todos distintos e $\sum_{i=1}^{d} c_i \log(x - \alpha_i)$ é uma função racional, então $c_i = 0$ para todo $1 \leq i \leq d$.*

Demonstração. Suponhamos, por contradição, que

$$\sum_{i=1}^{d} c_i \log(x - \alpha_i) = p/q,$$

onde $p, q \in \mathbb{C}[x]$ e $\operatorname{mdc}(p, q) = 1$. Derivando ambos os lados, temos que

$$\sum_{i=1}^{d} \frac{c_i}{x - \alpha_i} = \frac{p'q - pq'}{q^2}. \tag{18}$$

Digamos que $(x-\beta)$ é um fator cuja multiplicidade na fatoração de q é r. Logo a multiplicidade de $x - \beta$ na fatoração de q' é $r - 1$. Portanto, como p e q são primos entre si, a maior potência de $x - \beta$ que divide $p'q - pq'$ é $(x - \beta)^{r-1}$. Assim, expressando o lado direito da equação (18) em forma reduzida, vemos que seu denominador contém um fator $(x - \beta)^{r+1}$, obtido do cancelamento do $(x - \beta)^{r-1}$ do numerador, com o $(x - \beta)^{2r}$ do denominador. Contudo, expressando o lado esquerdo de (18) em forma reduzida, não encontramos nenhum fator com multiplicadade superior a um. Portanto, $r + 1 = 1$, donde $r = 0$. Mas isto significa que q é constante e podemos absorvê-lo no p. Fazendo isto (18) se reduz a

$$\sum_{i=1}^{d} \frac{c_i}{x - \alpha_i} = p'.$$

Multiplicando por $(x - \alpha_k)$, para algum $1 \leq k \leq d$,

$$c_k + \sum_{i \neq k} \frac{c_i(x - \alpha_k)}{x - \alpha_i} = p'(x - \alpha_k).$$

Mas, fazendo $x = \alpha_k$ nesta expressão, obtemos $c_k = 0$. Como isto vale para todo $1 \leq k \leq d$, a demonstração está completa.

Com o que vimos até agora, o resultado do algoritmo de Bernoulli pode ser reformulado como a afirmação de que a integral de uma função racional consiste de duas partes. A parte algébrica, que é uma função racional, e a parte transcendente, que é uma soma de logaritmos e arcos tangentes. Nas próximas três seções estudaremos algoritmos eficientes que nos permitirão calcular cada uma destas partes.

7. Hermite

Embora o procedimento de Bernoulli nos dê um algoritmo, ele é pouco eficiente, já que demanda uma fatoração completa do denominador sobre $\mathbb{R}$. Entretanto, como C. Hermite observou em 1872, é possível obter a parte racional da integral de $f \in \mathbb{R}(x)$, e o integrando da parte transcendente, sem que seja necessário fatorar o denominador de f em termos de seus fatores irredutíveis. O procedimento originalmente proposto por Hermite começa por calcular a decomposição em frações parciais que resulta da fatoração livre de quadrados do denominador. Entretanto, é possível reformular este procedimento de maneira a evitar esta decomposição. É precisamente este o caminho que seguiremos aqui.

Seja K um subcorpo de $\mathbb{C}$. Na prática estaremos interessados no caso em que $K = \mathbb{Q}$. Retomando a notação do início da seção, digamos que

$$f = N/D, \text{ com } N, D \in K[x] \text{ e } \operatorname{grau}(N) < \operatorname{grau}(D).$$

Observe que, desta vez, estamos assumindo que tanto o numerador quanto o denominador de f têm coeficientes no corpo K. Ao invés de fatorar D completamente, calcularemos apenas sua fatoração sem quadrados, definida na seção 1. Seja

$$D = D_1 D_2^2 \cdots D_m^m$$

esta decomposição. Lembre-se que isto significa que D_i é o produto de todos os fatores irredutíveis, de multiplicidade i, na fatoração de D. Além disso, sabemos do algoritmo 3.2 da página 14, que esta fatoração pode ser obtida calculando apenas com elementos do corpo K.

Se $m = 1$, então D tem apenas fatores com multiplicidade um e, pelo teorema 5.2, sua integral é uma soma de logaritmos. Nossa meta é reduzir, passo a passo, a integral de N/D ao cálculo da primitiva de uma função racional cujo denominador é livre de quadrados. A cada passo a integral é reescrita como uma soma de duas parcelas. A primeira é uma função racional, ao passo que a segunda é a primitiva de uma outra função racional. Entretanto, a nova função racional da qual precisamos achar a primitiva terá um denominador cuja multiplidade máxima (definida na página 13) é menor que a do passo anterior. O processo termina quando a função racional que ainda falta integrar tem denominador livre de quadrados. Neste estágio teremos obtido

$$\int \frac{N}{D} dx = Q + \int \frac{\hat{N}}{\hat{D}},$$

onde $Q \in K(x)$ e $\hat{D}$ é livre de quadrados. A primitiva de $\hat{N}/\hat{D}$ corresponde à parte transcendente da integral de N/D, ao passo que Q nos dá sua parte racional. Portanto, o algoritmo que estamos prestes a descrever nos dará

- a parte racional da integral de N/D;
- a função racional cuja integral corresponde à parte transcendente da integral de N/D.

Continuando a assumir que a função a ser integrada é N/D e que

$$D = D_1 D_2^2 \cdots D_m^m$$

é a decomposição sem quadrados do seu denominador. Seja

$$U = \frac{D}{D_m^m} = D_1 D_2^2 \cdots D_{m-1}^{m-1}.$$

Como $\operatorname{mdc}(D_i, D_m) = 1$, para todo $1 \leq i \leq m-1$, e como D_m não tem quadrados, podemos concluir que D_m e

$$U(D_m)' = D_1 D_2^2 \cdots D_{m-1}^{m-1} D_m'$$

têm que ser primos entre si. Portanto, pelo algoritmo euclidiano estendido, podemos calcular polinômios α_0 e β_0, tais que

$$\alpha_0 U D_m' + \beta_0 D_m = 1.$$

Multiplicando por N,

$$(N\alpha_0) U D_m' + (N\beta_0) D_m = N.$$

Entretanto, precisamos de cuidados extra para garantir que, ao final de um passo da redução, o numerador do integrando tenha grau menor que seu denominador. Para isso, dividimos $N\alpha_0$ por D_m, obtendo r como resto e q como divisor. Desta forma,

$$N = (N\alpha_0) U D_m' + (N\beta_0) D_m = r U D_m' + (N\beta_0 + q U D_m') D_m.$$

Portanto, fazendo $\alpha = r$ e $\beta = N\beta_0 + qUD_m'$ temos que

$$\alpha U D_m' + \beta D_m = N \text{ com } \operatorname{grau}(\alpha) < \operatorname{grau}(D_m), \tag{19}$$

já que α é o resto (não nulo) de uma divisão por D_m. Com isto,

$$(m-1)\frac{N}{D} = (m-1)\left(\frac{\alpha U D_m' + \beta D_m}{U D_m^m}\right);$$

donde,

$$(m-1)\frac{N}{D} = \frac{(m-1)\alpha D_m'}{D_m^m} + \frac{(m-1)\beta}{U D_m^{m-1}}.$$

Substituindo, agora,

$$\frac{d}{dx}\left(\frac{\alpha}{D_m^{m-1}}\right) = \frac{\alpha'}{D_m^{m-1}} - \frac{(m-1)\alpha D_m'}{D_m^m}.$$

na equação anterior, obtemos

$$(m-1)\frac{N}{D} = \left(\frac{\alpha'}{D_m^{m-1}} - \frac{d}{dx}\left(\frac{\alpha}{D_m^{m-1}}\right)\right) + \frac{(m-1)\beta}{U D_m^{m-1}}.$$

Desta forma,

$$(m-1)\frac{N}{D} = \frac{\alpha' U + (m-1)\beta}{U D_m^{m-1}} - \frac{d}{dx}\left(\frac{\alpha}{D_m^{m-1}}\right).$$

Assim,

$$\int \frac{N}{D} dx = \frac{1}{m-1}\left(\int \frac{\alpha' U + (m-1)\beta}{U D_m^{m-1}} dx\right) - \frac{\alpha}{D_m^{m-1}}.$$

Como,

$$U D_m^{m-1} = D_1 D_2^2 \cdots (D_{m-1} D_m)^{m-1},$$

sua multiplicidade máxima é

$$\mu(U D_m^{m-1}) = m-1,$$

como queríamos.

Ainda precisamos nos certificar que o numerador $\alpha' U + (m-1)\beta$ tem grau menor que o denominador $U D_m^{m-1}$. Contudo, de (19), temos que

$$\mathrm{grau}(\beta D_m) \leq \max\{\mathrm{grau}(\alpha U D_m'), \mathrm{grau}(N)\}.$$

Mas,

$$\mathrm{grau}(\alpha U D_m') = \mathrm{grau}(\alpha) + \mathrm{grau}(U) + \mathrm{grau}(D_m')$$

Contudo, $\mathrm{grau}(\alpha) < \mathrm{grau}(D_m)$ e $m \geq 2$, de forma que

$$\mathrm{grau}(\alpha U D_m') < \mathrm{grau}(U D_m^2) - 1 < \mathrm{grau}(U D_m^m).$$

Como N também tem grau menor que $D = U D_m^m$,

$$\mathrm{grau}(\beta D_m) \leq \mathrm{grau}(D).$$

Portanto,

$$\mathrm{grau}(\beta) \leq \mathrm{grau}(D) - \mathrm{grau}(D_m) < \mathrm{grau}(U D_m^{m-1}),$$

Finalmente,

$$\mathrm{grau}(\alpha' U + (m-1)\beta) \leq \max\{\mathrm{grau}(\alpha') + \mathrm{grau}(U), \mathrm{grau}(\beta)\},$$

e levando em conta a desigualdade para o grau de α mais uma vez, obtemos

$$\mathrm{grau}(\alpha' U + (m-1)\beta) < \max\{\mathrm{grau}(UD_m), \mathrm{grau}(UD_m^{m-1})\};$$

donde

$$\mathrm{grau}(\alpha' U + (m-1)\beta) < \mathrm{grau}(UD_m^{m-1}),$$

como precisávamos mostrar.

O algoritmo que resulta do processo de redução descrito acima pode ser formulado da seguinte maneira.

Algoritmo 7.1 (Algoritmo de Hermite)**.** *Dada uma função racional $f = N/D$, com $N, D \in K[x]$ e $\mathrm{grau}(N) < \mathrm{grau}(D)$ o algoritmo calcula a parte racional da primitiva de N/D, juntamente com o integrando da parte transcendente.*

Etapa 1: *Inicialize $R = 0$ e $j = m$.*

Etapa 2: *Calcule a fatoração sem quadrados de $D_1 D_2^2 \cdots D_m^m$ de D e seja $\mathcal{L}$ a lista $[D_1, \ldots, D_m]$.*

Etapa 3: *Se $j = 1$ imprima R e N/D.*

Etapa 4: *Se $\mathrm{grau}(D_j) = 0$, faça $j = j - 1$, e volte à Etapa 3.*

Etapa 5: *Faça*

$$V = D_j \text{ e } U = D/V^j.$$

Etapa 6: *Aplicando o algoritmo euclidiano estendido a UV' e V, calcule polinômios A e B tais que*

$$AUV' + BV = 1.$$

Etapa 7: *Calcule o quociente Q da divisão de NA por V e faça*

$$\alpha = NA - QV \text{ e } \beta = NB + QUV'.$$

Etapa 8: *Faça*

$$\begin{aligned} R &= R - \frac{\alpha}{V^{j-1}} \\ N &= \alpha' U + (j-1)\beta \\ D &= UV^{j-1} \text{ e} \\ j &= j - 1, \end{aligned}$$

e retorne à Etapa 2.

Resta-nos descrever um exemplo para que você possa ver este algoritmo em ação. Digamos que $N = 1$ e que D corresponde ao polinômio cuja fatoração sem quadrados é

$$D = (x+1)(x^2+2)^2(x^3+3)^3.$$

Desta forma, no primeiro laço,

$$j = 3,\ V = x^3 + 3 \text{ e } U = (x+1)(x^2+2)^2.$$

Assim, $UV' = 3x^2(x+1)(x^2+2)^2$ e, pelo algoritmo euclidiano estendido

$$A = \frac{5}{5202}x^2 + \frac{67}{5202}x - \frac{3}{578}$$
$$B = -\frac{5}{1734}x^6 - \frac{12}{289}x^5 - \frac{10}{289}x^4 - \frac{41}{289}x^3 + \frac{6}{289}x^2 + \frac{1}{3}$$

Multiplicando por $N = 1$ e dividindo o coeficiente de UV' por V, obtemos

$$\alpha = A \text{ e } \beta = B,$$

donde

$$R = \left(-\frac{5}{10404}x^2 - \frac{67}{10404}x + \frac{3}{1156}\right)/(x^6 + 6x^3 + 9)$$
$$N = -\frac{5}{2601}x^6 - \frac{355}{10404}x^5 - \frac{253}{10404}x^4 - \frac{292}{2601}x^3 + \frac{131}{2601}x^2 + \frac{77}{2601}x + \frac{934}{2601}$$
$$D = (x+1)((x^2+2)(x^3+3))^2.$$

Para o segundo laço, repetimos o processo anterior com os valores de N e D obtidos ao final do primeiro laço. Temos, assim,

$$j = 2,\ V = (x^2+2)(x^3+3) \text{ e } U = (x+1).$$

Assim, $UV' = (5x^4+6x^2+6x)(x+1)$ e, pelo algoritmo euclidiano estendido

$$A = -\frac{65}{10404}x^4 + \frac{50}{2601}x^3 - \frac{1}{306}x^2 + \frac{43}{10404}x + \frac{5}{578}$$
$$B = \frac{325}{10404}x^4 - \frac{75}{1156}x^3 - \frac{545}{5202}x^2 - \frac{5}{578}x + \frac{1}{6}$$

de modo que

$$\alpha = \frac{521}{795906}x^4 + \frac{8423}{795906}x^3 - \frac{689}{93636}x^2 + \frac{22217}{1591812}x - \frac{54}{4913}$$
$$\beta = -\frac{2605}{795906}x^4 - \frac{22360}{397953}x^3 - \frac{21497}{1591812}x^2 + \frac{4225}{265302}x - \frac{467}{7803},$$

donde R tem por numerador

$$-\frac{521}{795906}x^7 - \frac{8423}{795906}x^6 + \frac{689}{93636}x^5 - \frac{6527}{795906}x^4 + \\ - \frac{14431}{530604}x^3 + \frac{185}{7803}x^2 - \frac{29051}{530604}x + \frac{375}{9826}$$

e por denominador $x^8 + 2x^6 + 6x^5 + 12x^3 + 9x^2 + 18$, ao passo que

$$N = -\frac{521}{795906}x^4 - \frac{5789}{265302}x^3 + \frac{5615}{1591812}x^2 + \frac{8047}{530604}x + \frac{117485}{1591812}$$
$$D = (x+1)(x^2+2)(x^3+3).$$

No próximo laço já temos $j = 1$, de forma que a parte racional da integral é dada pelo valor de R acima, e o integrando da parte transcendente é

$$\frac{-\frac{521}{795906}x^4 - \frac{5789}{265302}x^3 + \frac{5615}{1591812}x^2 + \frac{8047}{530604}x + \frac{117485}{1591812}}{(x+1)(x^2+2)(x^3+3)}.$$

8. Rothstein e Trager

Como dissemos ao final da seção 5, determinaremos a parte transcendente da integral de uma função racional em termos de logaritmos. Para isto, precisamos fatorar completamente o denominador da função racional. Contudo, tendo aplicado primeiro o algoritmo de Hermite, podemos assumir que o denominador a ser fatorado é livre de quadrados. Em outras palavras, o denominador se escreve como um produto de termos lineares *distintos*. Entretanto, chegados a este ponto, nos vemos forçados a lidar com números não racionais em nossos procedimentos. Note que isto ocorre mesmo sem estivermos supondo que a função racional a ser integrada tem coeficientes racionais.

Infelizmente não há uma maneira geral (e exata) de representar um número não racional no computador. Por outro lado, todos os números não racionais que aparecem nestes algoritmos são raízes de alguma equação polinomial com coeficientes racionais. Isto nos permite chegar a uma solução intermediária, que consiste em não explicitar estes números, dizendo apenas que correspondem às raízes de uma certa equação polinomial em uma variável, com coeficientes polinomiais.

Para poder tornar mais preciso o que precisa ser feito, devemos relembrar o que já sabemos sobre a parte transcendente da integral. Suponha que N e D são polinômios em $K[x]$ que satisfazem

- $\text{grau}(N) < \text{grau}(D)$ e
- D é mônico e livre de quadrados.

Neste caso, pelo teorema 5.2,

$$\int \frac{N}{D} dx = \sum_{i=1}^{d} c_i \log(x - \alpha_i),$$

onde os cs e αs são números complexos, e $\alpha_i \neq \alpha_j$ se $i \neq j$. Se, porventura, houver $i \neq j$ para os quais $c_i = c_j$, podemos agrupá-los escrevendo

$$c_i \log(x - \alpha_i) + c_j \log(x - \alpha_j) = (c_i + c_j) \log((x - \alpha_i)(x - \alpha_j)).$$

Fazendo isto quantas vezes forem necessárias podemos reescrever a integral acima na forma

$$\int \frac{N}{D} dx = \sum_{i=1}^{s} c_i \log(v_i), \tag{20}$$

onde $s \leq d$, os cs são todos distintos e os v_i são mônicos, livres de quadrados e primos entre si. Estas últimas condições sobre v_i decorrem das hipóteses feitas sobre D.

De acordo com (20) precisamos apenas determinar os s pares (c_i, v_i) para calcular completamente a integral. A estratégia consistirá em achar um polinômio de $\mathbb{Q}[x]$ cujas raízes são exatamente os cs, e em seguida descrever um procedimento que nos permita calcular o polinômio v correspondente a um dado valor de c. Este é o conteúdo do próximo teorema, que foi provado, independentemente, por M. Rothstein e B. Trager em 1976.

Teorema 8.1 (Rothstein e Trager). *Sejam N e D polinômios co-primos em $K[x]$ que satisfazem*

- $\mathrm{grau}(N) < \mathrm{grau}(D)$ *e*
- *D é mônico e livre de quadrados.*

Então

$$\int \frac{N}{D} dx = \sum_{i=1}^{s} c_i \log(v_i), \tag{21}$$

onde

(1) *os c_is são as raízes de* $\mathrm{res}_x(D, N - yD')$, *e*

(2) $v_i = \mathrm{mdc}(D, N - c_i D')$,

para cada $1 \leq i \leq d$.

Note que estamos assumindo, conforme explicado acima, que os v_i são não constantes, mônicos, livres de quadrados e primos entre si. Além disso, (1) nos diz que a resultante não tem nenhuma raiz além dos c_is.

Demonstração. Em primeiro lugar, sabemos pelo algoritmo de Bernoulli que a primitiva de N/D pode ser escrita na forma da identidade do teorema. Derivando ambos os lados da identidade proposta no teorema, obtemos

$$\frac{N}{D} = \sum_{i=1}^{s} c_i \frac{v_i'}{v_i}. \tag{22}$$

De fato, esta última igualdade é equivalente à identidade (21). Rearrumando o lado direito da desigualdade para que tenha um denominador comum, obtemos

$$\frac{N}{D} = \frac{\sum_{i=1}^{s} c_i v_i' u_i}{v_1 \cdots v_s}, \tag{23}$$

onde u_i é o produto de todos os vs, *exceto* v_i. Em particular, isto significa que v_j divide todas as parcelas da soma

$$\sum_{i=1}^{s} c_i v_i' u_i$$

exceto a i-ésima. Portanto,

$$\mathrm{mdc}(v_i, \sum_{i=1}^{s} c_i v_i' u_i) = 1.$$

Como os vs são primos entre si, podemos concluir que

$$\mathrm{mdc}(v_1 \cdots v_s, \sum_{i=1}^{s} c_i v_i' u_i) = 1.$$

Mas, N e D também são primos entre si e D é mônico. Assim, da igualdade (23), segue que

$$D = v_1 \cdots v_s \quad \text{e que} \quad N = \sum_{i=1}^{s} c_i v_i' u_i. \tag{24}$$

Com isto estamos prontos para provar (2). A derivada de D pode ser escrita na forma

$$D' = \sum_{i=1}^{s} u_i v_i',$$

de modo que, usando (24) agrupando os termos comuns,

$$N - yD' = \sum_{i=1}^{s} (c_i - y) v_i' u_i. \tag{25}$$

Isolando a j-ésima parcela,

$$N - yD' = \sum_{i \neq j} (c_i - y) v_i' u_i + (c_i - y) v_j' u_j. \tag{26}$$

Como v_j divide todos os u_is, exceto u_j, concluímos que v_j divide a primeira parcela da soma. Fazendo, agora, $y = c_j$, a segunda parcela se anula, e temos que v_j divide $N - c_j D'$. Contudo, se $k \neq j$, o polinômio v_k não divide $(c_j - c_k) v_k' u_k$, que é não nula já que, por hipótese, $c_j \neq c_k$. Resumindo,

$$\text{mdc}(v_\ell, N - c_j D') = \begin{cases} 1 & \text{se} \quad \ell \neq j \\ v_j & \text{se} \quad \ell = j. \end{cases}$$

Disto podemos concluir que

$$v_j = \text{mdc}(v_1 \cdots v_s, N - c_j D') = \text{mdc}(D, N - c_j D');$$

o que prova (2).

Para provar (1) observe primeiramente que, segundo (2), os polinômios D e $N - c_j D'$ (na variável x) têm um fator comum para cada $1 \leq j \leq s$. Portanto, a resultante destes dois polinômios deve ser nula; isto é

$$\text{res}_x(D, N - c_j D') = 0 \quad \text{para cada} \quad 1 \leq j \leq s.$$

Em outras palavras, cada c_j é raiz de

$$R(y) = \text{res}_x(D, N - yD'),$$

que é um polinômio na variável y. Resta-nos, apenas, provar que R não admite raízes além dos c_j. Para isto o mesmo argumento já usado acima, só que trás para a frente.

Seja, pois, c uma raiz de R. Como

$$\text{res}_x(D, N - cD') = R(c) = 0,$$

os polinômios D e $N - cD'$ admitem fatores comuns não constantes. Seja v um fator irredutível dentre estes. Prosseguimos usando as fórmulas (26). Em primeiro lugar, como v divide

$$D = v_1 \cdots v_s,$$

e os v_is são primos entre si, temos que v divide apenas um dos termos, digamos v_k. Por outro lado, v divide $N - cD'$, que é igual a

$$\sum_{i=1}^{s} (c_i - c) v_i' u_i,$$

por (26). Contudo, v divide v_k, que divide cada um dos u_is, exceto u_k. Portanto, para que v divida

$$N - cD' = \sum_{i \neq k} (c_i - c) v_i' u_i + (c_k - c) v_k' u_k,$$

é necessário que $c_k - c = 0$; mostrando, assim, que R não tem raízes além dos c_is.

Obtemos com isto uma versão do algoritmo de Rothstein-Trager. A versão padrão, implementada em sistemas de computação algébrica como o AXIOM utiliza resultantes, em vez de bases de Gröbner. Veja os exercícios ??? para mais detalhes.

Algoritmo 8.2 (Algoritmo de Rothstein-Trager)**.** *Dados polinômios N e D em $K[x]$ que satisfazem*

- $\mathrm{grau}(N) < \mathrm{grau}(D)$ *e*
- *D é mônico e livre de quadrados,*

o algoritmo calcula pares $(c_j, v_j) \in \mathbb{C} \times \mathbb{C}[x]$, tais que

$$\int \frac{N}{D} dx = \sum_{i=1}^{s} c_i \log(v_i).$$

Etapa 1: *Calcule a resultante $R = \mathrm{res}_x(D, N - yD')$.*
Etapa 2: *Para cada raiz c de R, calcule*

$$v_c = \mathrm{mdc}(N - cD', D).$$

Etapa 3: *Imprima cada c com seu respectivo v_c.*

Aplicaremos este algoritmo à integral

$$\int \frac{-\frac{13385}{1591812}x^4 - \frac{38497}{530604}x^3 + \frac{92473}{397953}x^2 + \frac{60551}{530604}x - \frac{59363}{1591812}}{(x+1)(x^2+2)(x^3+3)} dx,$$

obtida ao final da seção 7. Neste exemplo, o numerador da função a ser integrada é

$$N = -\frac{13385}{1591812}x^4 - \frac{38497}{530604}x^3 + \frac{92473}{397953}x^2 + \frac{60551}{530604}x - \frac{59363}{1591812}$$

e o denominador é

$$D = (x+1)(x^2+2)(x^3+3).$$

Calculando a resultante

$$R = y^6 - \frac{8917240841513}{52724672145101952}y^4 - \frac{21633427966541}{5765442899066898 4512}y^3 +$$

$$\frac{1699777407653}{819974101200625557504}y^2 - \frac{3306713087191}{29888055988762801571 0208}y -$$

$$\frac{7211969}{574549326965836247 04}$$

O polinômio R pode ser fatorado como

$$\left(y - \frac{1}{72}\right)\left(y^2 - \frac{5122}{751689}y + \frac{1}{36992}\right)$$
$$\left(y^3 + \frac{13833}{668168}y^2 + \frac{2718605}{19727326116}y + \frac{7211969}{21571831107846}\right)$$

Portanto, $c_1 = 1/72$; de modo que

$$v_1 = \operatorname{mdc}(N - \frac{1}{72}D', D) = x + 1.$$

Com isto, uma das parcelas da parte transcendente será igual a

$$\frac{1}{72}\log(x+1).$$

Ao usar o mesmo método para obter as demais parcelas, precisaríamos calcular máximos divisores comuns de polinômios sobre extensões do tipo $\mathbb{Q}[\alpha]$, onde α é a raiz de um dos outros fatores irredutíveis de r. Isto é possível mas, felizmente, não é necessário, como veremos na próxima seção. O "felizmente"da afirmação acima se deve ao custo computacional dos cálculos realizados em extensões de corpos.

9. LAZARD, RIOBOO E TRAGER

No final da década de 1980, D. Lazard e R. Rioboo [6], inventaram um algoritmo capaz de determinar a parte transcendente da integral de uma função racional, sem efetuar cálculos em extensões do corpo de base. Pouco depois, descobriram que B. Trager havia implementado o mesmo algoritmo no sistema de computação algébrica SCRATCHPAD, precursor do atual AXIOM. O algoritmo de Lazard-Rioboo-Trager utiliza subresultantes (definidas na seção 4) e é baseado no seguinte teorema.

Teorema 9.1 (Lazard, Rioboo e Trager)**.** *Sejam N e D polinômios coprimos em $K[x]$ que satisfazem*

- $\operatorname{grau}(N) < \operatorname{grau}(D)$ *e*

- *D é mônico e livre de quadrados.*

Seja $S_i(x,y) \in \mathbb{Q}[x,y]$ a i-ésima subresultante (em relação à variável x) de $N - yD'$ e seja
$$R(y) = \mathrm{res}_x(N - yD', D).$$
Se a fatoração livre de quadrados de $R(y)$ é $R_1 R_2^2 \cdots R_m^m$, então
$$\int \frac{N}{D} dx = \sum_{i=1}^{m} \left(\sum_{c:R_i(c)=0} c \log(S_i(x,c)) \right).$$

Observe que x e y aparecem na notação da subresultante $S_i(x,y)$ para indicar que se trata de um polinômio nestas variáveis. Na verdade esta é a subresultante de D e $N - yD'$, considerados como polinômios na variável x, cujos coeficientes são polinômios em $\mathbb{Q}[y]$.

Demonstração. Seja c uma raiz de R de multiplicidade k–que é, portanto, raiz de R_k. Precisamos, apenas, mostrar que
$$\mathrm{mdc}(D, N - cD') = a_k S_k(x,c) \quad \text{para algum} \quad a_k \in \mathbb{C};$$
porque o resultado do teorema segue desta igualdade e do teorema 8.1–levando em conta, é claro, que constantes não interferem na integral.

Pela propriedade 4 da resultante,
$$R(y) = a \prod_{b:D(b)=0} (N(b) - yD'(b)),$$
onde $a \in \mathbb{R}$. Como estamos supondo que c é uma raiz de multiplicidade k, há k valores de b que são raízes comuns de D e de $N - yD'$. Denotando por $b_1, \dots, b_k$ este valores, concluímos que também são raízes de $\mathrm{mdc}(D, N - cD')$. Observe que, como D é livre de quadrados, os b_is são todos distintos. Logo, estas são todas as raízes de $\mathrm{mdc}(D, N - cD')$, mesmo se as contamos com multiplicidade. Portanto,

(27) $$\mathrm{grau}(\mathrm{mdc}(D, N - cD')) = k.$$

É chegado o momento de introduzir subsresultantes. Para isto, construímos primeiro o homomorfismo
$$\sigma_c : \mathbb{C}[y] \to \mathbb{C},$$
que manda y em c. Em seguida, estendemos este homomorfismo a
$$\overline{\sigma_c} : \mathbb{C}[y,x] \to \mathbb{C}[x].$$
De acordo com o teorema 4.1, existe uma constante $d_k \in \mathbb{C}$, tal que
$$\overline{\sigma}(S_k(x,y)) = d_k \overline{S_k}(x),$$
onde $\overline{S_k}(x)$ é a k-ésima subresultante de
$$\overline{\sigma}(D) \quad \text{e} \quad \overline{\sigma}(N - yD')) = N - cD'.$$
Contudo,
$$\overline{\sigma}(S_k(x,y)) = S_k(x,c);$$

de modo que

$$S_k(x,c) = d_k\overline{S_k}(x). \tag{28}$$

Em particular, estes dois polinômios têm o mesmo grau, que é igual a k.

Utilizando, agora, a equação (10), podemos calcular polinômios A_k e B_k de $\mathbb{Q}[x]$, para os quais vale a identidade

$$A_k \cdot D + B_k \cdot (N - cD') = \overline{S_k}(x).$$

Como $\mathrm{mdc}(D, N-cD')$ divide cada uma das parcelas desta soma, concluímos que divide a soma. Portanto, $\mathrm{mdc}(D, N-cD')$ divide $\overline{S_k}(x)$. Entretanto, estes dois polinômios têm grau k, de forma que diferem apenas por um múltiplo constante; isto é,

$$\mathrm{mdc}(D, N - cD') = e_k\overline{S_k}(x).$$

Combinando esta última equação com (28), obtemos

$$\mathrm{mdc}(D, N - cD') = e_k d_k S_k(x,c),$$

como desejávamos mostrar.

10. INTEGRAIS: DEFINIDAS E INDEFINIDAS

Como vimos nas seções anteriores, uma combinação dos algoritmos de Hermite e Lazard-Rioboo-Trager, nos permitem integrar automaticamente qualquer função racional. Voltando à integral

$$\int \mathrm{sen}^2(x)dx,$$

já considerada na seção 2, podemos finalmente calculá-la completamente. Usando a substituição de Weierstrass, temos a igualdade

$$\int \mathrm{sen}^2(x)dx = \int \frac{8u^2du}{(1+u^2)^3}.$$

Como o numerador tem grau menor que o denominador, não há necessidade de efetuar nenhuma divisão de polinômios. Contudo, o denominador tem fatores mútiplos, de forma que precisamos começar aplicando o algoritmo Hermite. Como a multiplicidade máxima dos fatores no denominador é três, o algoritmo de Hermite executará dois laços, dando como resultado

$$\frac{u^3-u}{u^4+2u^2+1} + \int \frac{du}{u^2+1}.$$

Portanto, por (13), temos que

$$\int \frac{8u^2du}{(1+u^2)^3} = \frac{u^3-u}{u^4+2u^2+1} + \arctan(u).$$

Substituindo $u = \tan(x/2)$, a integral final é

$$\frac{\tan(x/2)^3 - \tan(x/2)}{\tan(x/2)^4 + 2\tan(x/2)^2 + 1} + \arctan(\tan(x/2)).$$

Chegados a este ponto, talvez lhe venha o impulso de escrever $x/2$, em lugar de $\arctan(\tan(x/2))$. Contudo, isto só é verdadeiro se sabemos que $-\pi < x < \pi$. De fato, a tangente está definida em qualquer intervalo da forma $(-k\pi/2, k\pi/2)$, com k ímpar; ao passo que a imagem do arcotangente está toda contida em $(-\pi/2, \pi/2)$. Este detalhe torna-se particularmente relevante quando usamos primitivas para calcular integrais definidas.

Para analisar a relação entre integrais definidas e indefinidas, precisamos do chamado *teorema fundamental do cálculo*, que aprendemos em cálculo I. O teorema, que foi descoberto independentemente por Newton e Leibniz, pode ser enunciado da seguinte forma.

Teorema Fundamenal do Cálculo. *Sejam $I \subseteq \mathbb{R}$ um intervalo aberto e $f : I \to \mathbb{R}$ uma função contínua. Se $F : I \to \mathbb{R}$ é uma primitiva de f e $a, b \in I$, então*

$$\int_a^b f dx = F(b) - F(a).$$

Na prática, integrais definidas normalmente são calculadas usando métodos numéricos, e não o teorema fundamental do cálculo, veja ???? por exemplo. Contudo, como temos algoritmos que nos permitem determinar algumas primitivas de forma exata, parece razoável utilizá-las. O uso de primitivas é especialmente atrativo se precisamos calcular a integral da mesma função com vários limites de integração diferentes.

Apesar de parecer uma boa idéia, este método conduz a uma série de problemas. Por exemplo, vamos determinar

$$\int_1^2 \frac{x^4 - 3x^2 + 6}{x^6 - 5x^4 + 5x^2 + 4} dx.$$

Como o denominador do integrando é livre de quadrados, podemos utilizar diretamente o algoritmo de Lazard-Rioboo-Trager, que nos dá como primitiva

$$i\frac{1}{2}\log(x^3 + ix^2 - 3x - 2i) - i\frac{1}{2}\log(x^3 - ix^2 - 3x + 2i),$$

que é igual a

$$\frac{1}{2} i \log(\frac{g + i}{g - i}), \text{ onde } g = \frac{x^3 - 3x}{x^2 - 2}.$$

Aplicando, agora, o lema 5.1 concluímos que a primitiva é igual a

$$\arctan(\frac{x^3 - 3x}{x^2 - 2}).$$

Portanto, a integral desejada é

$$\arctan(\frac{x^3 - 3x}{x^2 - 2})|_1^2 = \arctan(1) - \arctan(2);$$

que é aproximadamente igual a $-0, 32175$. Contudo, se aplicarmos um método numérico ao cálculo desta integral, descobrimos que o resultado dá ????. A pergunta, naturalmente, é: onde está o erro?

Na verdade o erro está na escolha da primitiva usada na aplicação do teorema fundamental do cálculo. No exemplo acima, a função

$$\arctan(\frac{x^3 - 3x}{x^2 - 2})$$

tem uma singularidade em $\sqrt{2}$, que fica entre os limites de integração. Portanto, a primitiva não é contínua neste intervalo e, conseqüentemente, não podemos usá-la para calcular a integral definida no *intervalo dado*. Note, porém, que esta singularidade é um artefato do processo de integração em si. De fato, o denominador do integrando não tem nenhuma raiz real, de modo que a primitiva deveria estar definida em qualquer intervalo desejado. Chamaremos de *espúria* uma singularidade da primitiva que não é singularidade do integrando.

O exemplo apareceu originalmente na tese de doutorado de R. Rioboo. Nela, Rioboo descreve um algoritmo que permite representar a integral de qualquer função racional com *coeficientes reais* sem nenhuma singularidade espúria. Aplicado ao exemplo acima, o algoritmo de Rioboo nos dá a primitiva

$$\arctan\left(\frac{x^5 - 3x^3 + x}{2}\right) + \arctan(x^3) + \arctan(x),$$

que não tem nenhuma singularidade. A princípio isto pode parecer muito estranho. Afinal, duas primitivas diferem apenas por uma constante, e as constantes se cancelam quando fazemos a diferença dos seus valores nos limites de integração, não se cancelam? Entretanto, uma mera constante pode ser suficiente para remover uma singularidade de uma integral indefinida, ou introduzi-la. Este é, infelizmente, um fato raramente apresentado em um curso elementar de cáculo, apesar de sua importância nas aplicações. Como se trata de um algoritmo cuja descrição é bastante técnica, ainda que elementar, não apresentaremos o algoritmo de Rioboo aqui. Para uma descrição detalhada veja [1, capítulo 2, seção 2.8, p. 59].

Este mesmo problema torna-se muito mais agudo quando consideramos funções mais complicadas. Um tratamento detalhado do que acontece com as funções trigonométricas consideradas no início da seção, pode ser encontrado em [5]. Para o caso geral veja [3].

11. Ritt

Nesta seção introduzimos as noções básicas de álgebra diferencial, conforme formalizadas por J. F. Ritt a partir da década de 1940.

Um *corpo diferencial* é um corpo K ao qual está associada uma aplicação que satisfaz

$$d(a + b) = d(a) + d(b) \quad \text{e} \quad d(ab) = ad(b) + bd(a),$$

para todo $a, b \in K$. Dizemos que uma tal aplicação é uma *derivação* de K. O exemplo mais básico de corpo diferencial é $\mathbb{C}(x)$ com a derivação dada por d/dx. Outro corpo diferencial importante é $\mathcal{M}$, o corpo das funções meromorfas em x; isto é, aquelas que são quocientes de funções holomorfas. Neste caso, também, a derivação é d/dx. Nosso primeiro resultado mostra que as propriedades da derivação usual de $\mathcal{M}$ se estendem ao caso geral definido acima.

Proposição 11.1. *Seja K um corpo diferencial, munido de uma derivação d. Se $f, g \in K$ e n é um inteiro positivo, então:*

(1) $d(0) = d(1) = 0$;
(2) $d(-f) = -d(f)$;
(3) $d(f/g) = (fd(g) - gd(f))/g^2$;
(4) $d(f^n) = nf^{n-1}d(f)$.

Observe que os corpos $\mathbb{C}(x) \subseteq \mathcal{M}$ partilham uma mesma derivação. Podemos expressar isto de outra maneira dizendo que, a derivação de $\mathcal{M}$ restrita a $\mathbb{C}(x)$ coincide com a derivação originalmente definida em $\mathbb{C}(x)$. Isto sugere a seguinte definição. Sejam $K \subseteq L$ corpos diferenciais, cujas derivações são dadas, respectivamente, por d_K e d_L. Dizemos que a extensào de corpos $K \subset L$ é uma *extensão diferencial* se a derivação d_L restrita a K coincide com d_K; em outras palavras

$$d_L(a) = d_K(a) \quad \text{para todo} \quad a \in K.$$

Neste caso também dizemos que K é um *subcorpo diferencial* de L. O próximo teorema diz respeito a um caso importante desta definição.

Teorema 11.2. *Seja K um corpo diferencial, munido de uma derivação d. Se $K \subseteq L$ é uma extensão finita de corpos, então d pode ser estendida a uma derivação de L. Além do mais, esta extensão é única.*

O teorema pode ser reformulado, dizendo-se que toda extensão finita de corpos $K \subseteq L$ pode ser convertida–de maneira única–em uma extensão diferencial.

Demonstração. Como toda extensão finita pode ser escrita como uma extensão simples, existe $\theta \in L$ tal que $L = K[\theta]$. Além disso, como θ é algébrico sobre K, existe um polinômio

$$p(x) = a_n x^n + \cdots + a_0 \in K[x],$$

tal que $p(\theta) = 0$. Suponhamos, por um momento, que L admita uma derivação D que estende d, e vamos provar a unicidade a que se refere o teorema.

Aplicando D a

$$p(\theta) = a_n\theta^n + \cdots + a_0 = 0,$$

obtemos

$$D(a_n)\theta^n + \cdots + D(a_0) + na_n\theta^{n-1}D(\theta) + \cdots + a_1 D(\theta) + a_0 = 0.$$

Como D estende d e os a_js pertencem a K,

$$d(a_n)\theta^n + \cdots + d(a_0) + na_n\theta^{n-1}D(\theta) + \cdots + a_1 D(\theta) + a_0 = 0.$$

Explicitando o valor de $D(\theta)$ a partir da equação acima,

$$D(\theta) = \frac{d(a_n)\theta^n + \cdots + d(a_0) - a_0}{na_n\theta^{n-1} + \cdots + a_1}. \tag{29}$$

Resumindo, se D estende d, então $D(\theta)$ é dada pela equação (29). Contundo, todo elemento de $L = K(\theta)$ é uma expressão polinomial em θ. Portanto, usando as propriedades listadas na proposição 11.1, (29) basta para determinar completamente como D é calculado em L. Em particular, a um único D possível em L que estende d, a derivação em K, o que prova a unicidade. Tendo mostrado que há uma única maneira possível de definir D da maneira desejada, provamos a existência de D utilizando (29) como a fórmula que a define em L.

Seja K um corpo diferencial, munido de uma derivação d. O *subcorpo de constantes* de K é

$$K_0 = \{x \in K : d(x) = 0\}.$$

Como d se anula em K_0, é claro que este último é um subcorpo diferencial de K.

Teorema 11.3. *O corpo de constantes de $\mathbb{C}(x)$ é $\mathbb{C}$.*

Demonstração. Sejam f e $g \neq 0$ polinômios em $\mathbb{C}[x]$ e suponhamos que a função racional f/g pertence ao corpo de constantes de $\mathbb{C}(x)$. Como sempre, podemos supor que a fração f/g foi reduzida, de forma que $\mathrm{mdc}(f, g) = 1$. Neste caso,

$$d(f/g) = (fd(g) - gd(f))/g^2 = 0,$$

que só pode ocorrer se $fd(g) = gd(f)$. Como f e g são primos entre si, f tem que dividir $d(f)$ e g tem que dividir $d(g)$. Logo,

$$d(f) = hf \quad \text{e} \quad d(g) = hg.$$

Note que o mesmo h tem que aparecer como co-fator em ambas as igualdades para que $fd(g) = gd(f)$ seja verdadeira. Contudo, $d = d/dx$ é a derivação usual, de forma que

$$d(f) = \frac{df}{dx}$$

tem grau menor que f. Logo, $d(f) = hf$ só pode valer se

$$\frac{df}{dx} = h = 0;$$

donde

$$\frac{dg}{dx} = 0.$$

Mas um polinômio cuja derivada é nula tem que ser constante. Logo, f, g e, conseqüentemente, f/g pertencem a $\mathbb{C}(x)$.

Um argumento semelhante mostra que o corpo de constantes de $\mathcal{M}$ também é $\mathcal{C}$.

REFERÊNCIAS

[1] M. Bronstein, *Symbolic integration I: transcendental functions*, segunda edição, Springer (2005).

[2] G. Czichowski, A note on Gröbner bases and integration of rational functions, J. Symbolic Computation **20** (1995), 163–167.

[3] J. H. Davenport, *The difficulties of definite integration*, web????

[4] G. H. Hardy, *Integration of functions of a single variable*, segunda edição, Cambridge University Press (1928).

[5] D. J. Jeffrey e A. D. Rich, *The evaluation of trigonometric integrals avoiding spurious discontinuities*, ACM Trans. Math. Software, **20** (1994), 124–135.

[6] D. Lazard e R. Rioboo, *Integration of rational functions: rational computation of the logarithmic part*, **9** (1990), 113–115.

DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO, INSTITUTO DE MATEMÁTICA, UNIVERSIDADE FEDERAL DO RIO DE JANEIRO, P.O. BOX 68530, 21945-970 RIO DE JANEIRO, RJ, BRAZIL.

PROGRAMA DE ENGENHARIA DE SISTEMAS E COMPUTAÇÃO, COPPE, UFRJ, PO BOX 68511, 21941-972, RIO DE JANEIRO, RJ, BRAZIL.

E-mail address: `collier@impa.br`

URL: `http://www.dcc.ufrj.br/˜collier`