Universidade Federal de Santa Catarina
Centro de Ciências Físicas e Matemáticas

Números de Liouville: o início da teoria transcendente.

Ben Hur Eidt

Florianópolis, 11 de julho de 2016

Sumário

.

1 Introdução

O objetivo desse trabalho é demonstrar que um determinado conjunto, idealizado por Liouville e por isso leva seu nome, tem a propriedade de que todos seus elementos são números transcendentes: números que de certa forma transcendem as operações algébricas. Como é citado em [2] podemos afirmar que a teoria sobre números transcendentes é pouco conhecida, apesar de muitos matemáticas darem suas contribuições com o assunto, como Cantor, Hilbert, Euler etc. Talvez um dos motivos seja a falta de teoremas centrais e fundamentais sobre o assunto, o que torna as demonstrações trabalhosas e incrementadas.

Iniciaremos nossa exposição provando resultados (de álgebra) sobre anéis de polinômios, estrutura a qual o leitor já deve possui certa familiaridade. Assumiremos alguns resultados e provaremos outros no capítulo relacionado à isso. Chamamos atenção para o lema de gauss e o teorema que o sucede.

No capítulo seguinte, apresentaremos o conceito de extensão de corpos e definiremos os conceitos de números transcendentes e algébricos demonstrando algumas propriedades dos mesmos. O capítulo acabará com a prova de que na verdade quase todos os números são transcendentes apesar de não dar nenhum exemplo.

Caberá ao próximo e último capítulo a demonstração do trabalho e do método feito por Liouville. Consequentemente, temos a exposição de vários números transcendentes.

Afirmamos que tentamos cobrir todos os detalhes de todas as demonstrações aqui feitas, preferindo pecar por excesso do que por falta, bem como sempre que possível fazer boas observações e guiar o leitor no desenvolvimento do trabalho. Uma boa leitura!

2 Irredutibilidade no Anel de polinômios

Comecemos fixando algumas notações que serão usadas e relembrando conceitos vistos nos primeiros cursos de álgebra que terão sua importância no decorrer desse texto. Nessa primeira parte, estamos interessados em expor várias propriedades do anel de polinômios e portanto algumas definições já irão ser feitas diretamente em $D[x]$: o anel de polinômios com coeficientes em D, que por sua vez denotará sempre um domínio a não ser que mencionemos o contrário.

Denotaremos o conjunto dos elementos inversíveis de D por $U(D)$, usaremos também a notação $\partial f(x)$ para denotar o grau do polinômio $f(x)$. Além disso, admitimos alguns conhecimentos prévios do leitor quanto à estruturas como anéis, domínios e corpos e uma noção básica sobre o anel de polinômios.

Dito isso, nossa primeira proposição diz respeito à relação que existe entre os elementos inversíveis de D e de $D[x]$.

Proposição 2.1. *Seja D um domínio de integridade. Então vale que $U(D) = U(D[x])$.*

Demonstração. ($\Rightarrow$) A ida é imediata, pois identificamos os elementos de D como os polinômios constantes de $D[x]$, logo, $D \subseteq D[x]$ e assim $U(D) \subseteq U(D[x])$.

($\Leftarrow$) Tome $f(x) \in U(D[x])$, assim $\exists g(x) \in (D[x])$ tal que $g(x)f(x) = 1$. Como D é um domínio, $D[x]$ também o é, portanto temos $g(x) \neq 0$ e $f(x) \neq 0$. Novamente por termos um domínio vale que $0 = \partial(1) = \partial(g(x)f(x)) = \partial(g(x)) + \partial(f(x))$. Disso, segue que $\partial(g(x)) = \partial(f(x)) = 0$, de modo que, $g(x) = a$ e $f(x) = b$ para certos $a, b \in D$ e assim $ab = 1$. Logo $f(x) = b \in U(D)$. ■

Agora precisamos criar a noção de irredutibilidade em $D[x]$, que nada mais é do que um caso particular da definição de elemento irredutível em um domínio qualquer. Para tanto, segue a

Definição 2.1. *Seja D um domínio. Dizemos que $p(x) \in D[x]$ é **irredutível** em $D[x]$ (ou **irredutível** sobre D) se:*

1. *$p(x)$ não é o polinômio nulo.*
2. *$p(x) \notin U(D[x])$ ($p(x)$ não é inversível).*
3. *Se $p(x) = f(x)g(x)$ com $f(x) \in D[x]$ e $g(x) \in D[x]$ então $f(x) \in U(D[x])$ ou $g(x) \in U(D[x])$ ($f(x)$ é inversível ou $g(x)$ é inversível).*

Graças a proposição 2.1 podemos reescrever as duas últimas condições da definição anterior como: "$p(x) \notin U(D)$"e "Se $p(x) = f(x)g(x)$ então $f(x) \in U(D)$ ou $g(x) \in U(D)$". De maneira natural segue a

Definição 2.2. *Seja D um domínio. Dizemos que $p(x) \in D[x]$ é **redutível** em $D[x]$ (ou **redutível** sobre D) se:*

1. *$p(x)$ não é o polinômio nulo.*
2. *$p(x) \notin U(D[x])$ ($p(x)$ não é inversível).*
3. *Existem $f(x)$ e $g(x)$ não inversíveis em $D[x]$ tais que $p(x) = f(x)g(x)$.*

Observe que pelo que foi dito acima o polinômio nulo e os polinômios inversíveis são os únicos que não respeitam nenhuma das definições. Assim, todos os outros polinômios podem ser classificados de acordo com uma, e apenas uma, das definições acima.

Se pensaremos que D possui a estrutura de corpo, vemos que os polinômios constantes ($p(x) = a$) não são irredutíveis nem redutíveis, pois todo elemento de $D^* = D - \{0\}$ é inversível.

Em geral, verificar a irredutibilidade de polinômios quaisquer é uma tarefa complicada. Apesar disso, de acordo com o grau do polinômio podemos obter resultados sobre sua irredutibilidade ou não, começamos com a

Proposição 2.2. *Seja K um corpo de $p(x) \in K[x]$. Se $\partial p(x) = 1$ então $p(x)$ é irredutível.*

Demonstração. Suponha $p(x) = g(x)f(x)$, daí temos $\partial(g(x)f(x)) = \partial g(x) + \partial f(x) = 1$, ou seja, $\partial g(x) = 0$ ou $\partial f(x) = 0$. Logo, $f(x)$ ou $g(x)$ é um polinômio constante, como K é corpo, segue que $p(x)$ é irredutível. ■

Além disso, observe que se $\partial f(x) > 1$ e $f \in D[x]$ possui uma raiz, digamos α, em D então $f(x) = (x - \alpha)g(x)$, o que nos diz que $\partial g(x) \geq 1$ visto que $\partial(x - \alpha) = 1$. Ou seja, o que acabamos de dizer é que nessa situação o polinômio $p(x)$ não é irredutível, pois foi decomposto como produto de dois polinômios não inversíveis.

Para os casos em que os polinômios tem grau 2 ou 3 temos também a

Proposição 2.3. *Seja $f(x) \in K[x]$ um polinômio que não tenha raizes em K e tal que $\partial f(x) = 2$ ou $\partial f(x) = 3$. Então, $f(x)$ é irredutível.*

Demonstração. Suponha, por absurdo, $f(x)$ redutível em ambos os casos.

Se $\partial f(x) = 2$, escrevemos $f(x) = g(x)h(x)$. Daí, $\partial f(x) = \partial g(x) = 1$. Assim, $h(x) = ax + b$ e $g(x) = cx + d$, mas $\dfrac{-b}{a}$ é raiz de $h(x)$ e $\dfrac{-c}{d}$ é raiz de $g(x)$. O que é um absurdo pois assim seriam raízes de $f(x)$.

Se $\partial f(x) = 3$ escrevemos novamente $f(x) = g(x)h(x)$. Daí, $\partial g(x) = 2$ e $\partial h(x) = 1$ ou $\partial g(x) = 1$ e $\partial h(x) = 2$. Em ambos os casos, novamente, teremos uma raiz do polinômio de grau 1, ou seja, conseguiremos uma raiz de $f(x)$. Absurdo. ■

Definição 2.3. *Um polinômio $p(x) = a_o + a_1x + a_2x^2 \ldots + a_nx^n$, com coeficientes em um domínio D, é dito ser mônico se $a_n = 1$.*

Definição 2.4. *Um polinômio $p(x) \in \mathbb{Z}[x]$ é dito primitivo se o máximo divisor comum de seus coeficientes for* 1.

Proposição 2.4 (Lema de Gauss)**.** *O Produto de dois polinômios primitivos é um polinômio primitivo.*

Demonstração. Suponha que não seja assim. Sejam $f(x) = a_0 + a_1x + \ldots + a_nx^n$ e $g(x) = b_0 + b_1x + \ldots + b_mx^m$ dois polinômios primitivos tais que $f(x)g(x) = c_0 + c_1x + \ldots + c_{n+m}x^{n+m}$ não seja primitivo, então existe um número primo p tal que $p|c_i$ para todo $i \in \{\ 0, 1, 2 \ldots n + m\}$. Considere portanto o morfismo

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$
$$\sum_{i=0}^{n} a_ix^i \mapsto \sum_{i=0}^{n} \overline{a_i}x^i$$

Aplicando em $f(x)g(x)$ veja que $\varphi(f(x)g(x)) = \varphi(f(x))\varphi(g(x)) = 0$. Dai do fato de $\mathbb{Z}_p[x]$ ser um domínio devemos ter $\varphi(f(x)) = \overline{p} = \overline{0}$ ou $\varphi(g(x)) = \overline{p} = \overline{0}$. Consideremos $f(x) = \overline{0}$, isso significa que $f(x)$ quando visto como polinômio em $\mathbb{Z}_p[x]$ via morfismo é o polinômio identicamente nulo, ou seja, quando olhamos $p(x)$ em $\mathbb{Z}[x]$ todos seus coeficientes devem ser múltiplos de p, o que é um absurdo pois $f(x)$ é primitivo. O mesmo argumento é válido se $g(x) = \overline{0}$. ■

Com a proposição acima seremos agora capazes de provar um dos resultados mais famosos sobre irredutibilidade, que confronta os conceitos de irredutibilidade em $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$.

Teorema 2.1 (irred sobre $\mathbb{Z} \Rightarrow$ irred sobre $\mathbb{Q}$)**.** *Seja $p(x) \in \mathbb{Z}[x]$ um polinômio irredutível sobre $\mathbb{Z}$, de grau maior ou igual a 1, então $p(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. Suponha que $p(x)$ seja redutível sobre $\mathbb{Q}$, escreva portanto $p(x) = g(x)h(x)$, $g(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \frac{a_2}{b_2}x^2 \ldots \frac{a_n}{b_n}x^n$ e $h(x) = \frac{c_0}{d_0} + \frac{c_2}{d_1}x + \frac{c_2}{d_2}x^2 \ldots \frac{c_m}{d_m}x^m$ onde $\partial g(x) \geq 1$ e $\partial h(x) \geq 1$. Seja $\alpha = mmc(b_0, b_1, b_2, \ldots b_n)$ e $\beta = mmc(d_0, d_1, d_2, \ldots d_n)$.

Portanto $\alpha g(x)$ é primitivo e $\beta h(x)$ também, de modo que $\alpha g(x)\beta h(x) = \alpha\beta p(x)$ é primitivo pelo lema de Gauss. Ora, sendo assim devemos ter $\alpha = \pm 1$ e $\beta = \pm 1$ de modo que $g(x) \in \mathbb{Z}[x]$ e $h(x) \in \mathbb{Z}[x]$ e portanto $p(x) \in \mathbb{Z}[x]$, mas, por hipótese $p(x)$ é irredutível sobre $\mathbb{Z}$, assim chegamos em um absurdo. Portanto $p(x)$ é irredutível sobre $\mathbb{Q}$. ■

Podemos nos perguntar se a recíproca do teorema acima é válida, a resposta é não, considere por exemplo o polinômio $2x + 2$ que é irredutível em $\mathbb{Q}[x]$ mas não é irredutível em $\mathbb{Z}[x]$ pois pode ser fatorado da seguinte forma: $2x + 2 = 2(x + 1)$. Perceba que na verdade o que está por trás disso é o fato de 2 não ser inversível em $\mathbb{Z}$. Adicionando uma certa restrição conseguiremos uma espécie de recíproca para o teorema 2.1. Assim temos o

Teorema 2.2. *Seja $p(x) \in \mathbb{Z}[x]$ um polinômio irredutível sobre $\mathbb{Z}$, de grau maior igual a 1 e primitivo, então as irredutibilidades sobre $\mathbb{Z}$ e sobre $\mathbb{Q}$ são equivalentes.*

Demonstração. O teorema 2.1 já nos garante que o se o polinômio for irredutível sobre $\mathbb{Z}$ então ele será irredutível sobre $\mathbb{Q}$.

Suponha agora que $p(x)$ seja irredutível em $\mathbb{Q}$. Daí, se $p(x) = f(x)g(x)$, com $f(x) \in \mathbb{Z}[x]$ e $g(x) \in \mathbb{Z}[x]$, (em particular $f(x)$ e $g(x)$ podem ser vistos como elementos em $\mathbb{Q}[x]$) temos que $f(x)$ é inversível ou $g(x)$ é inversível, ou seja, um dos dois é um polinômio constante. Sem perda de generalidade assuma $f(x) = a$. Então $p(x) = ag(x)$, de modo que a divide todos os coeficientes de $p(x)$, mas $p(x)$ é primitivo, assim $a = \pm 1$. Portanto $f(x) = \pm 1$ é inversível em $\mathbb{Z}[x]$. Logo, $p(x)$ é irredutível sobre $\mathbb{Z}[x]$. ■

Por fim, apresentamos um dos mais famosos critérios de irredutibilidade.

Teorema 2.3 (Critério de Einsenstein)**.** *Seja $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \mathbb{Z}[x]$ um polinômio de grau n. Se existe um número primo, p, tal que:*

- *$p \mid a_i$ para qualquer $i \in \{0, 1, 2, \ldots, n-1\}$*
- *$p \nmid a_n$*
- *$p^2 \nmid a_0$*

então $p(x)$ é irredutível sobre $\mathbb{Q}[x]$.

Demonstração. Suponha que $p(x)$ seja redutível, portanto podemos escrever

$$p(x) = h(x)g(x) = (b_0 + b_1x + b_2x^2 + \ldots + b_lx^l)(c_0 + c_1x + c_2x^2 + \ldots + c_jx^j)$$

com $b_l \neq 0$, $c_j \neq 0$, $\partial h(x) \geq 1$, $\partial g(x) \geq 1$ e $\partial p(x) = l + j = n$. Observando que o termo livre da variável x é dado por $a_0 = b_0c_0$ vemos que não podemos ter p dividindo b_0 e c_0 simultaneamente pois $p^2 \nmid a_0$. Mas $p \mid b_0c_0$, suponha portanto, sem perda de generalidade que $p \mid c_0$. Seja m o menor valor de k para o qual $p \nmid c_k$, daí temos $m \geq 1$ e certamente

$$a_m = b_0c_m + b_1c_{m-1} + b_2c_{m-2} + \ldots + b_{m-1}c_1 + b_mc_0$$

Observe agora que $p \mid a_m$ e $p \mid c_{m-1}, \ldots, p \mid c_0$. Portanto $p \mid b_0c_m$ o que é um absurdo, pois $p \nmid b_0$ e $p \nmid c_m$ e p é um número primo. ■

O critério acima nos ajuda na verificação da irredutibilidade de vários polinômios. Além disso, podemos juntar o critério de Einsenstein e os teoremas anteriores para verificar a irredutibilidade em $\mathbb{Z}[x]$.

Exemplo 2.1. *O polinômio* $2x^7+3x^5+3 = p(x) \in \mathbb{Z}[x]$ *é irredutível sobre* $\mathbb{Q}$ *pelo critério de Einsenstein aplicado para* $p = 3$. *Além disso, é primitivo e portanto é irredutível em* $\mathbb{Z}[x]$.

Exemplo 2.2. $10x^{11} + 6x^3 + 6$ *é irredutível sobre* $\mathbb{Q}$ *utilizando o critério de Einsenstein para* $p = 3$. *Apesar disso, não é irredutível sobre* $\mathbb{Z}$ *pois* $10x^{11}+6x^3+6 = 2(5x^{11}+3x^3+3)$.

Exemplo 2.3 (Fábrica de irracionais)**.** *O polinômio* $x^2 - 2m$ *para* m *ímpar é irredutível em* $\mathbb{Z}[x]$ *e* $\mathbb{Q}[x]$ *(*$p = 2$ *e primitivo). Veja que como o polinômio acima é irredutível sobre* $\mathbb{Q}$ *suas raízes não podem ser racionais. Logo* $\sqrt{2}$, $\sqrt{6}$, $\sqrt{10}$, $\sqrt{14}$, $\sqrt{18}$ ... *são números irracionais.*

Exemplo 2.4 (Aumentado a fábrica de irracionais)**.** *O polinômio* $x^n - 2m$ *para* m *ímpar e* $n \geq 2$ *é irredutível pelo mesmo motivo do exemplo acima e novamente todas suas raízes são irracionais.*

3 Extensões de corpos, números algébricos e transcendentes

O presente capítulo será destinado para a apresentação de algumas definições, motivações e teoremas, que, dentre outras coisas, visam garantir a existência e classificar quantitativamente os números transcendentes.

Definição 3.1. *Uma extensão de um corpo F é um par (i, F) onde $i : F \to E$ é um homomorfismo injetor.*

Observando que $i(F) \subseteq E$ é um subcorpo, iremos cometer um abuso de notação e escrever $F \subset E$ para nos referirmos a extensão. Veja que podemos abrir mão da estrutura multiplicativa do corpo E e pensá-lo como um F-espaço vetorial. Nesse caso denotaremos por $[E : F] = dim_F E$, a dimensão de E como um F-espaço vetorial. Diremos também que a extensão $F \subset E$ é finita se $[E : F] = n < \infty$

Definição 3.2 (Números algébricos e transcendentes)**.** *Dada $K \subset L$ uma extensão de corpos, dizemos que $\alpha \in L$ é **algébrico** sobre K quando existe $f(x) \in K[x]$ tal que $f(\alpha) = 0$. Caso tal polinômio não exista dizemos que α é **transcendente** sobre K.*

Definição 3.3. *Se $\alpha \in L$ é algébrico sobre K, então um polinômio mônico $p(x) \in K[x]$ de grau mínimo que admite α como raíz é chamado de polinômio minimal de α sobre K.*

Proposição 3.1. *Seja $K \subset L$ uma extensão de corpos e $\alpha \in L$ um número algébrico sobre K com polinômio minimal $p(x) \in K[x]$. Assim dado $f(x) \in K[x]$ vale que:*

$$f(\alpha) = 0 \Leftrightarrow p(x) \mid f(x)$$

Demonstração. ($\Rightarrow$) Se $p(x) \mid f(x)$ então existe $g(x)$ tal que $p(x)g(x) = f(x)$, em especial para $x = \alpha$ segue que $f(\alpha) = p(\alpha)g(\alpha) = 0$.

($\Leftarrow$) Suponha agora que $f(\alpha) = 0$. Usando a divisão euclidiana podemos obter $q(x)$ e $r(x)$ tais que $f(x) = q(x)p(x) + r(x)$ com $0 \leq \partial r < \partial p$. Daí, para $x = \alpha$ obtemos que $r(\alpha) = 0$. Porém, $p(x)$ é o polinômio minimal de α sobre K, logo $r(x) \equiv 0$, ou seja, $r(x)$ é o polinômio identicamente nulo. Portanto $p(x) \mid f(x)$ como queríamos demonstrar. ■

A proposição acima nos auxilia em mais duas belas conclusões que vem em forma de uma proposição.

Proposição 3.2. *Nos moldes da hipótese da proposição anterior, α possui um único polinômio minimal sobre K e o mesmo é irredutível.*

Demonstração. Sejam $p_1(x)$ e $p_2(x)$ ambos polinômios minimais de α sobre K. Daí pela proposição anterior $p_1(x) = g(x)p_2(x)$ e $p_2(x) = h(x)p_1(x)$ donde segue que $p_1(x) = g(x)h(x)p_1(x)$ e portanto olhando para os graus vemos que $\partial(g(x)h(x)) = 0$ e portanto $\partial g(x) = \partial h(x) = 0$. Desse modo $g(x)$ e $h(x)$ são polinômios constantes. Lembre também que $p_1(x)$ e $p_2(x)$ são mônicos e por isso só nos resta a opção $g(x) = h(x) \equiv 1$. Daí, $p_1(x) = p_2(x)$.

Para a segunda parte observe que se o polinômio minimal $p(x)$, único pelo que foi feito acima, fosse redutível, teríamos $p(x) = h(x)g(x)$ com $\partial g(x) \geq 1$ e $\partial h(x) \geq 1$, daí para $x = \alpha$ temos $h(\alpha)g(\alpha) = 0$ e então $h(\alpha) = 0$ ou $g(\alpha) = 0$, o que nos dá uma contradição através da minimalidade de p pois $\partial h(x) < \partial p(x)$ e $\partial g(x) < \partial p(x)$. ■

Apesar das definições acima nos permitirem trabalhar com 2 corpos quaisquer, iremos pensar, de agora em diante na extensão $\mathbb{Q} \subset \mathbb{C}$. Assim diremos simplesmente que α é algébrico, de modo que ficará subentendido que $\alpha \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$. Do mesmo modo usaremos o conceito de número transcendente.

Exemplo 3.1. *Todo número racional é algébrico. Tomando* $\frac{p}{q} \in \mathbb{Q}$ *vemos que tal número é raiz de* $p(x) = qx - p$.

Exemplo 3.2. *Os números* i *e* $\cos\left(\frac{\pi}{2016}\right) + i \sin\left(\frac{\pi}{2016}\right)$ *são algébricos pois são raizes de* $p(x) = x^2 + 1$ *e* $p(x) = x^{4032} - 1$

Exemplo 3.3. $\sqrt{7 - 2\sqrt{10}}$ *é algébrico pois é raiz de* $x^4 - 14x^2 + 9$.

Iremos denotar o conjunto dos números algébricos por $\overline{\mathbb{Q}}$ e o conjunto dos números transcendentes por $\mathbb{T}$.

É relativamente simples encontrarmos e citarmos exemplos de números algébricos. O mesmo não acontece com os números transcendentes. Até o momento não temos nenhum exemplo e na verdade ainda nem temos certeza se a definição de número transcendente não é vazia, ou seja, será que existem números transcendentes?

Guiados por essa pergunta caminharemos agora buscando informações que possam responde-la. O seguinte teorema nos dá informações sobre a natureza quantitativa dos números algébricos.

Teorema 3.1. *O conjunto dos números algébricos,* $\overline{\mathbb{Q}}$*, é enumerável.*

Demonstração. Considere o polinômio $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ de grau n, denote como R_p o conjunto das raízes de p. Como $\mathbb{Q}$ é corpo, segue que $|R_p| \leq n$.

Afirmação: Para qualquer $n \in \mathbb{N}$ existe apenas uma quantidade enumerável de polinômios em $\mathbb{Q}[x]$ com grau n. De fato, considere o conjunto $X_n = \{p \in \mathbb{Q}[x] : \partial p(x) = n\}$ e a função:

$$\varphi : \underbrace{\mathbb{Q} \text{ x } \mathbb{Q} \text{ x } \mathbb{Q} \text{ x } \ldots \text{ x } \mathbb{Q}^*}_{n+1 \text{ vezes}} \to X_n$$

$$(a_0, a_1, a_2, \ldots, a_n) \mapsto a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

A importância de usarmos $\mathbb{Q}^*$ é a garantia de que o grau do polinômio seja n. Veja que φ é injetora pois se $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$ então, por igualdade de polinômios, temos $a_0 = b_0$, $a_1 = b_1, \ldots, a_n = b_n$. φ também é sobrejetora pois se $p(x) = c_0 + c_1x + c_2x^2 + \ldots + c_nx^n \in X_n$ vemos que $p(x) = \varphi(c_0, c_1, c_2, \ldots c_n)$.

Logo φ é uma bijeção. Além disso, $\underbrace{\mathbb{Q} \text{ x } \mathbb{Q} \text{ x } \mathbb{Q} \text{ x } \ldots \text{ x } \mathbb{Q}^*}_{n+1 \text{ vezes}}$ é enumerável pois $\mathbb{Q}$ o é. Portanto X_n é enumerável.

Definindo agora $A_n = \bigcup_{p\,:\,\partial p = n} R_p$ vemos que A_n é enumerável pois é escrito como uma união enumerável de conjuntos finitos. Agora perceba que $\overline{\mathbb{Q}} = \bigcup_{n \in \mathbb{N}} A_n$ que é enumerável pois é escrito como uma união enumerável de enumeráveis. ■

O leitor deve ter percebido que na demonstração acima usamos alguns resultados sobre enumerabilidade de conjuntos, caso haja interesse por parte mesmo sobre os teoremas e proposições usadas recomendamos [3].

Teorema 3.2. $\mathbb{T}$ *é não enumerável*

Demonstração. Veja que podemos identificar o conjunto dos números reais como a união dos reais algébricos e dos reais transcendentes. Como $\mathbb{R}$ é não enumerável e $\overline{\mathbb{Q}}$ é enumerável concluímos que $\mathbb{T}$ é não enumerável! ■

O que foi feito acima já nos diz que o conjunto dos números algébricos é pequeno, quando comparado ao conjunto dos números transcendentes. Inclusive em vez de usarmos o conjunto dos números reais na demonstração podíamos nos referir ao conjunto dos números complexos. Uma outra maneira de vermos isso é através do conceito de medida, mas antes uma definição.

Definição 3.4. *Dizemos que $A \subseteq \mathbb{R}^2$ tem medida nula (escrevemos $m(A) = 0$) se $\forall \epsilon > 0$ existe uma quantidade enumerável de bolas abertas $(B_n)_{n\in\mathbb{N}}$ tais que*

- $A \subseteq \bigcup\limits_{n\in\mathbb{N}} B_n$
- $\sum\limits_{n=1}^{\infty} \acute{A}rea(B_n) < \epsilon$

Diremos também que uma propriedade é satisfeita por **quase todos os números complexos**, se o conjunto, $A \subseteq \mathbb{C} \cong \mathbb{R}^2$, que não satisfizer essa propriedade possuir medida nula. Com as informações dadas podemos agora provar o

Teorema 3.3. *Quase todos os números são transcendentes.*

Demonstração. Perceba que devemos provar que $m(\overline{\mathbb{Q}}) = 0$. Fixe $\epsilon > 0$. Pelo teorema anterior, já sabemos que $\overline{\mathbb{Q}}$ é enumerável, portanto escreva $\overline{\mathbb{Q}} = \{a_1, a_2, a_3, \ldots\}$. Defina então as seguintes bolas abertas:

$$B_n = \{z \in \mathbb{C} : |z - a_n| < r_n\} \text{ onde } r_n = \frac{1}{n}\sqrt{\frac{3\epsilon}{\pi^3}}$$

(Afirmamos que fizemos a conta). Veja que $\overline{\mathbb{Q}} \subseteq \bigcup\limits_{n\in\mathbb{N}} B_n$ pois $a_n \in B_n$. Falta portanto provar que $\sum\limits_{n=1}^{\infty} \text{Área}(B_n) < \epsilon$, o que de fato acontece conforme atesta o desenvolvimento a seguir:

$$\text{Área} \bigcup_{n\in\mathbb{N}} B_n \leq \sum_{n=1}^{\infty} \text{Área}(B_n) = \sum_{n=1}^{\infty} \pi r_n^2 = \sum_{n=1}^{\infty} \pi \frac{1}{n^2}\frac{3\epsilon}{\pi^3} = \frac{3\epsilon}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2}$$

Agora usando (pesquise) que $\sum\limits_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ obtemos:

$$\frac{3\epsilon}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{3\epsilon}{\pi^2}\frac{\pi^2}{6} = \frac{\epsilon}{2} < \epsilon. \quad ■$$

Portanto $m(\overline{\mathbb{Q}}) = 0$. Nesse caso dizemos também que o conjunto $\mathbb{T}$ tem medida total, $m(\mathbb{T}) = \infty$.

De qualquer maneira, agora temos absoluta certeza que nossas definições não são vazias e podemos procurar números transcendentes. Essa será a tarefa do próximo capítulo.

4 Os números de Liouville

No capítulo anterior vimos que existem muito mais números transcendentes do que algébricos. Apesar disso, ainda não fomos capazes de explicitar nenhum deles. É aquela conversa: sabemos que eles existem mas ainda não conseguimos pegar nenhum na mão.

A reviravolta virá nesse capítulo, o último por sinal. O trabalho para encontrá-los foi originalmente feito por Liouville em 1844 e proporcionou os primeiros exemplos de números transcendentes.

A ideia foi encontrar alguma propriedade que é satisfeita por todos os números algébricos e portanto se algum número não a satisfizesse ele seria transcendente. Os teoremas e definições desse capítulo visam facilitar o caminho para a demonstração do teorema que consolidou o trabalho de Liouville. Nesse âmbito começamos com o

Teorema 4.1 (**Liouville**). *Seja α uma raiz irracional de um polinômio irredutível $P(x) \in \mathbb{Z}[x]$ com $n = \partial p(x) \geq 2$. Então existe uma constante $c(\alpha)$ tal que $\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}$ para qualquer número racional $\frac{p}{q}$.*

Demonstração. Vamos escolher $c(\alpha) = \dfrac{1}{1 + \max\limits_{|t-\alpha|\leq 1} |P'(t)|}$ (Não se assuste! Alguém fez a conta de trás pra frente), onde $P'(t)$ denota a derivada de $P(x)$ no ponto t. A partir de agora separemos o problema em dois casos.

- Caso $\left|\alpha - \frac{p}{q}\right| > 1$. Como $q \in \mathbb{Z}^*$ então $|q^n| \geq 1$, além disso, $1 \geq c(\alpha)$ de modo que $1 \geq \frac{c(\alpha)}{q^n}$. Logo $\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}$.

- Caso $\left|\alpha - \frac{p}{q}\right| \leq 1$. Primeiramente, observe que segue do teorema 2.1 que o polinômio $P(x)$ é irredutível sobre $\mathbb{Q}[x]$, desse maneira, $P\left(\frac{p}{q}\right) \neq 0$ pois $\frac{p}{q} \in \mathbb{Q}[x]$. Além disso, $q^n \cdot P\left(\frac{p}{q}\right)$ é certamente um número inteiro pois $n = \partial P(x)$, portanto $\left|q^n \cdot P\left(\frac{p}{q}\right)\right| \geq 1$. Agora, o teorema do valor médio nos garante a existência de pelo menos um $t \in \mathbb{R}$, que esteja entre α e $\frac{p}{q}$ tal que: (Lembre que α é raíz do polinômio $P(x)$)

$$\left|P(\alpha) - P\left(\frac{p}{q}\right)\right| = \left|P\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \cdot |P'(t)|$$

  Multiplicando a equação acima por $|q^n|$ concluimos que $|q^n| \cdot \left|\alpha - \frac{p}{q}\right| \cdot |P'(t)| = \left|q^n \cdot P\left(\frac{p}{q}\right)\right| \geq 1$. Lembre também que estamos admitindo $\left|\alpha - \frac{p}{q}\right| \leq 1$ e assim $|t - \alpha| \leq 1$. Portanto temos:

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{|q^n|(1 + |P'(t)|)} \geq \frac{1}{q^n \cdot (1 + \max\limits_{|t-\alpha|\leq 1} |P'(t)|)} = \frac{c(\alpha)}{q^n}$$

  o que prova o teorema. ■

Observamos que, como visto acima, é muito valioso conciliarmos as visões de polinômios vindos da álgebra e do cálculo (como função contínua) pois assim ganhamos aquele "combo"(Anulamento de Bolzano, TVI, Weierstrass, TVM...).

Perceba que o teorema acima nos diz que números algébricos irracionais não podem ser tão "bem aproximados"por racionais, pois devem sempre respeitar a limitação imposta pelo teorema. O que podemos fazer em seguida, e parece razoável, é construirmos números que não respeitam o teorema de Liouville. Segue assim a próxima e fundamental definição.

Definição 4.1 (Números de Liouville)**.** *Um número α é chamado de* ***número de Liouville*** *se existir uma sequência de racionais $\left(\frac{p_j}{q_j}\right)_{j\in\mathbb{N}}$,distintos , com $q_j > 1\ \forall j \in \mathbb{N}$, tal que*

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j} \qquad \forall j \in \mathbb{N}$$

Exemplo 4.1 (Constante de Liouville)**.** . *O número $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ é um número de Liouville e é conhecido como a* ***constante de Liouville.***

Perceba primeiramente que série acima converge pelo teste da razão:

$$\lim_{k\to\infty} \frac{10^{k!}}{10^{(k+1)!}} = \lim_{k\to\infty} \frac{1}{10^{(k+1)}} = 0$$

Sabendo que $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$, defina $p_j = \sum_{k=1}^{j} 10^{j!-k!}$ e $q_j = 10^{j!}$. Assim

$$\left|\alpha - \frac{p_j}{q_j}\right| = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} - \sum_{k=1}^{j} \frac{1}{10^{k!}} = \sum_{k=j+1}^{\infty} \frac{1}{10^{k!}} = \frac{1}{10^{(j+1)!}}\left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \frac{1}{10^{(j+3)!-(j+1)!}} \dots\right)$$

Agora veja que

$$\frac{1}{10^{(j+1)!}}\left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \frac{1}{10^{(j+3)!-(j+1)!}} \dots\right) < \frac{1}{10^{(j+1)!}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} \dots\right)$$

como

$$\left(1 + \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} \dots\right) = \left(1 + \frac{1}{9}\right) = \frac{10}{9}$$

temos que

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{10^{(j+1)!}}\frac{10}{9} = \frac{10}{9 \cdot 10^{j!}(10^{j!})^j} < \frac{1}{(10^{j!})^j} = \frac{1}{(q_j)^j}$$

o que garante-nos que α é um número de Liouville.

Exemplo 4.2. *A constante de Liouville é um caso especial de alguns números de Liouville que possuem certo padrão. Considere os números da forma $\alpha = \sum_{n=1}^{\infty} \frac{a_n}{b^{n!}}$ com $b \geq 2$ e $a_n \in \{1, 2, 3 \dots, b-1\}$. Novamente, perceba que a série converge pelo teste da razão. Em todos esses casos podemos concluir que α é um número de Liouville, conforme atesta o desenvolvimento a seguir.*

Escolhendo $q_j = b^{j!}$ *e* $p_j = \sum_{n=1}^{j} a_n b^{j!-n!}$ *temos que:*

$$\left|\alpha - \frac{p_j}{q_j}\right| = \sum_{n=j+1}^{\infty} \frac{a_n}{b^{n!}} \leq (b-1) \sum_{n=j+1}^{\infty} \frac{1}{b^{n!}} < (b-1) \sum_{n=(j+1)!}^{\infty} \frac{1}{b^n} = \frac{(b-1)b}{b^{(j+1)!}(b-1)} < \frac{1}{(b^{j!})^j}.$$

Onde usamos soma de PG e a primeira desigualdade restrita é justificada pela desigualdade a seguir que é obtida comparando termo a termo.

$$\frac{1}{b^{(j+1)!}} + \frac{1}{b^{(j+2)!}} + \frac{1}{b^{(j+3)!}} \ldots < \frac{1}{b^{(j+1)!}} + \frac{1}{b^{(j+1)!+1}} + \frac{1}{b^{(j+1)!+2}} \ldots$$

Logo

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j}$$

.

Observamos que denotaremos o conjunto de todos os números de Liouville por $\mathbb{L}$. Existe também, um ponto de vista ligeiramente diferente, que se expressa no próximo teorema, para reconhecer um número de Liouville.

Teorema 4.2. *α é um número de Liouville, se e somente se, para todo $n \geq 1$ existe um racional $\frac{p}{q}$, com $q > 1$, tal que:*

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}$$

.

Demonstração. ($\Rightarrow$) Se α é um número de Liouville, existe uma sequência de racionais $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$, tal que $0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^n}$. Basta agora tomar, para cada n, $p = p_n$ e $q = q_n$.

($\Leftarrow$) Sabemos que para cada n existe $\frac{p_n}{q_n}$, dependendo de n, tal que a desigualdade do enunciado é válida e $q_n > 1$. Defina portanto, $X = \bigcup_{n\in\mathbb{N}} \left\{\frac{p_n}{q_n}\right\}$. Perceba agora que X não pode ser finito pois se fosse, existiria $\frac{P}{Q} \in A$ tal que $\left|\alpha - \frac{P}{Q}\right| < \frac{1}{Q^n}$ para todo $n \in N^{\#} \subset N$, onde $N^{\#}$ é infinito. Ora, dessa maneira teríamos obrigatoriamente a igualdade $\frac{P}{Q} = \alpha$. Um absurdo, pois $0 < \left|\alpha - \frac{P}{Q}\right|$. Assim, A é infinito e o resultado segue. ■

Iremos agora provar um teorema que servirá como uma ponte para o os resultados que vem em seguida.

Teorema 4.3 (O grande lema)**.** *A sequência $(\ q_j)_{\ j\in\mathbb{N}}$ da definição* 4.1 *é ilimitada.*

Demonstração. Suponha, por absurdo, que não seja assim. Portanto $\exists M > 0$ tal que $q_j \leq M$ para todo $j \in \mathbb{N}$. Como $\left|\alpha - \frac{p_j}{q_j}\right| \leq \frac{1}{q_j^j} < 1$ temos $q_j\left|\alpha - \frac{p_j}{q_j}\right| = |q_j\alpha - p_j| < q_j$. Além disso, como $|p_j| - |q_j\alpha| < |q_j\alpha - p_j|$ segue que $|p_j| < |q_j\alpha| + q_j < M(\ |\alpha| + 1)$. Logo $(\ p_j)_{\ j\in\mathbb{N}}$ é limitada.

Portanto $(\ q_j\ )_{\ j\in\mathbb{N}}$ e $(\ p_j\ )_{\ j\in\mathbb{N}}$ são sequências de números inteiros limitadas e portanto com apenas finitos termos distintos. Desse modo, $\left(\ \frac{p_j}{q_j}\right)_{\ j\in\mathbb{N}}$ é uma sequência de números racionais com finitos termos distintos, o que contraria o fato de tal sequência possuir infinitos termos distintos. ■

Utilizando o teorema acima podemos também obter a seguinte proposição que é uma condição necessária para estarmos no caminho certo.

Proposição 4.1. *Todo número de Liouville é irracional ($\alpha \in \mathbb{L} \Rightarrow \alpha \in \mathbb{R} - \mathbb{Q}$)*

Demonstração. Suponha $\alpha \in \mathbb{L}$, tal que $\alpha = \frac{p}{q} \in \mathbb{Q}$. Por hipótese, existe uma sequência $\left(\ \frac{p_j}{q_j}\right)_{\ j\in\mathbb{N}}$ de racionais distintos tais que $\left|\frac{p}{q} - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j}$, ou seja, $\left|\frac{pq_j - p_jq}{qq_j}\right| < \frac{1}{q_j^j}$. Além disso, como pq_j e p_jq são números inteiros distintos, a sua diferença em módulo é maior ou igual a 1 e assim obtemos:

$$|pq_j - qp_j| \geq 1 \Rightarrow \frac{1}{|qq_j|} \leq \left|\frac{pq_j - p_jq}{qq_j}\right| < \frac{1}{q_j^j}$$

Isso nos diz que $|q|q_j > q_j^j$ e portanto $|q| > q_j^{j-1}$, um absurdo pois pelo grande lema a sequência $(\ q_j)_{\ j\in\mathbb{N}}$ é ilimitada. Logo todo número de Liouville é irracional. ■

Por fim, conseguiremos agora provar o resultado que consolidou o trabalho feito por Liouville na busca por números transcendentes. Apresentamos o

Teorema 4.4. *Todo número de Liouville é transcendente ($\alpha \in \mathbb{L} \Rightarrow \alpha \in \mathbb{T}$)*

Demonstração. Pela Proposição 4.1, se α for um número de Liouville então α é irracional. Suponha agora que α é algébrico e é raiz de $P(x)$ onde $\partial P(x) = n \geq 2$, então pelo teorema de Liouville (Teorema 4.1) temos que que vale a seguinte desigualdade para qualquer racional $\frac{p}{q}$.

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}$$

Em especial essa desigualdade é válida para os números da sequência $\left(\ \frac{p_j}{q_j}\right)_{\ j\in\mathbb{N}}$ da definição de número de Liouville. Dessa forma temos que:

$$\frac{c(\alpha)}{q_j^n} < \left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j} \qquad \Rightarrow \qquad \frac{q_j^n}{c(\alpha)} > q_j^j$$

Da desigualdade acima segue que $q_j^{j-n} < \frac{1}{c(\alpha)}$, o que contradiz novamente o grande lema, pois assim teríamos a limitação de $(\ q_j)_{\ j\in\mathbb{N}}$. Portanto todo número de Liouville é transcendente. ■

Como consequência do teorema podemos afirmar que o número do exemplo 4.1 e todos os números do exemplo 4.2 são, de fato, transcendentes. Desse modo, agora sabemos mais do que apenas a existência de números transcendentes, podemos ,de fato, exibi-los.

Observamos, por fim, que a recíproca do teorema 4.4 não é válida. Na verdade, é possível provar que quase nenhum número transcendente é número de Liouville. Citando um exemplo, provou-se, com a ajuda de resultados merecedores (e ganhadores) da medalha Fields (veja [2]) que a constante de Champernowne dada por $M = 0,1234567891011121314...$ é um número transcendente. Apesar disso não M é um número de Liouville. Os números e e π também não são números de Liouville, apesar de serem transcendentes.

Referências

[1] FIGUEIREDO, D. G. Números Irracionais e Transcendentes. 3. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2002.

[2] MARQUES, D. Teoria dos números transcendentes 1. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2013.

[3] LIMA, E. L. Curso de análise vol.1 .14. ed. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2016.

[4] TENGAN, E. SALDANHA, N. MOREIRA, C. G. MARTINEZ, F. B. Teoria dos Números. 3. ed. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2015.

[5] MARTIM, P. A. Grupos, Corpos e Teoria de Galois. 1. ed. São Paulo: Livraria da Física, 2010.

[6] JANESCH, O. R. Álgebra II Florianópolis. UFSC/EAD/ CED/CFM, 2008.