INTRODUÇÃO À TEORIA DE GALOIS DIFERENCIAL

GUILHERME CERQUEIRA
IME-USP

Resumo. Objetivo destas notas é criar um introdução simples para a Teoria de Galois Diferencial e ao fim demonstrar que a clássica função e^{x^2} não tem integral elementar. Para o mínimo de requisitos serem necessários há um breve apêndice sobre Álgebra Comutativa. As notas são majoritariamente baseadas em [1], pode-se considerar que foi feita uma tradução com correções do artigo. Alguns detalhes extras foram adicionados, além das correções, como: exemplos, intuições, demonstrações mais detalhadas e informações extras sobre a teoria.

Sumário

1. Introdução

Meu objetivo com as notas é criar uma introdução o mais elementar o possível, *em português*, para esta área intrigante, mas pouco difundida, e provar o resultado muito famoso de que e^{x^2} não possui integral em termos de funções elementares.

Esta teoria é uma "réplica"da Teoria de Galois em um contexto diferente, com uma construção que se assemelha à histórica feita inicialmente feita com polinômios simétricos. Maior parte da Teoria de Galois não é explicitamente utilizada, mas vários resultados e demonstrações são semelhantes se não análogos. Certamente um leitor familiarizado com Teoria de Galois ou simplesmente com resultados como *Teorema Fundamental dos Polinômios Simétricos* ou com o estudo de *Torres Radicais* terá uma facilidade extra ao passo que muita intuição é replicada nesta teoria. Apesar disso, considero que um bom curso de Anéis e Corpos é o único requisito para ler estas notas, para que isso seja verdade existem os dois apêndices sobre Álgebra Comutativa. Um primeiro curso em EDOs pode ajudar o leitor, mas não é necessário.

É pertinente citar que estas notas são majoritariamente baseadas em [1] que nos dá o caminho mais curto e elementar para resolver nosso problema de integrabilidade. Tal artigo é fortemente baseado em [2] que foi usado como suporte para estudo de certos detalhes da teoria. O livro [3] apesar de só citado como referência para a demonstração do *Teorema de Liouville* tem um introdução bem elementar e focada nos algoritmos de solução das EDOs, recomendável para o leitor interessado na parte mais analítico-computacional da teoria.

O leitor pode notar pelo sumário que muita teoria foi omitida, 3 fatores foram principais para esta escolha: o fato de que o objetivo central é entender o problema de integrabilidade de e^{x^2}, a tentativa de deixar as notas o mais elementares o possível e as limitações de tempo e

Date: September 2020.

conhecimento do próprio autor. Para um leitor interessado em ler mais sobre este assunto[1], sugiro estudar por [5] este livro tem uma exposição clara e rápida dos principais pontos da teoria com base teórica robusta, incluindo uma introdução à Geometria Algébrica Clássica que é essencial pois a topologia de Zariski é central no estudo dos *Grupos de Galois Diferenciais* assunto que infelizmente não coube nestas notas.

2. Teoria de Anéis com Derivação

Definiremos nesta sessão nossos objetos mais básicos, os Anéis (Corpos) com derivação, chamaremos eles de *Anéis (Corpos) Diferenciais*. Provaremos também alguns resultados básicos da teoria de Anéis e Corpos neste novo contexto. Considere que todos os anéis aqui tratados são comutativos com unidade e todos os corpos terão característica 0, a menos que seja explicitado o contrário.

Definição 2.1. Seja R um anel. Uma derivação em R é uma aplicação $D : R \longrightarrow R$ que é Aditiva (Ad) e respeita a Regra de Leibniz (RL). Ou seja, $\forall a; b \in R$:

(Ad) $D(a+b) = D(a) + D(b)$.
(RL) $D(ab) = aD(b) + D(a)b$.

Um anel com derivação chamaremos de *anel diferencial*, quando esse for também um corpo o chamaremos *corpo diferencial*. Para toda estrutura que se define é crucial ter algum exemplo base, sendo assim:

Exemplo 2.2. Nossos exemplos principais serão o anel de polinômios $\mathbb{C}[x]$ e o corpo $\mathbb{C}(x)$ com derivada usual. Nota-se também que sub-anéis de $C^\infty(\mathbb{R}, \mathbb{R})$, como $\mathbb{R}[x]$ serão possíveis exemplos, mas não focaremos nele pois futuramente termos um corpo algebricamente fechado será relevante.

Tais exemplos, em especial o *corpo diferencial* $\mathbb{C}(x)$, nos motivam a verificar se as propriedades conhecidas do Cálculo Diferencial são válidas no nosso contexto de Anéis Diferenciais e nossas próximas definições.

Proposição 2.3. [2]*Sejam $x, y \in R; y \neq 0$; elementos genéricos de um anel diferencial*[3]*. As seguintes propriedades são válidas:*

(1) $D(1) = 0$.
(2) $D(x^n) = nx^{n-1}D(x)$.
(3) $D(y^{-1}) = -\frac{D(y)}{y^2} := -D(y)y^{-2}$.
(4) $D(\frac{x}{y}) = \frac{yD(x) - xD(y)}{y^2}$.

Demonstração. Farei a conta somente de (4), tendo em vista que as outras são análogas e elementares.

$$D\left(\frac{x}{y}\right) = D(xy^{-1}) = xD(y^{-1}) + D(x)y^{-1} = -xD(y)y^{-2} + yD(x)y^{-2} = (yD(x) - xD(y))y^{-2}.$$

■

Definição 2.4. Uma *extensão diferencial de anéis* de R é um anel diferencial E tal que, $R \subset E$ e $D_E(a) = D_R(a), \forall a \in R$. Analogamente, um subanel diferencial de R é um anel S tal que, $S \subset R$ e $D_S(s) = D_R(s), \forall s \in S$.

Definição 2.5. O *conjunto de constantes* de R (denotado $const(R)$) é o kernel de D. Ou seja: $const(R) = \{a \in R \mid D(a) = 0\}$.

[1] O que eu pessoalmente recomendo, pois é uma teoria belíssima, digo isso mesmo sendo bem longe da área que estudo, no caso Geometria Diferencial.

[2] A não ser que dito o contrário R será um anel diferencial e K um corpo diferencial.

[3] Quando não houver possibilidade de confusão usar-se-a D para a derivação do anel (corpo) em questão, em outros casos o anel (corpo) estará explicitado como sub-índice, por exemplo: D_R.

Definição 2.6. Um *homomorfismo de anéis diferenciais* é um homomorfismo de anéis $\varphi : R \longrightarrow E$ tal que φ comuta com as derivações dos anéis, ou seja, o seguinte diagrama comuta:

$$\begin{array}{ccc} R & \xrightarrow{D_R} & R \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ E & \xrightarrow{D_E} & E \end{array}$$

Definição 2.7. Seja $I \subset R$ um ideal de R. I é um *ideal diferencial* se $D_R(I) \subset I$.

Note que se um ideal $I = \langle X \rangle$, ou seja é gerado por X e $D(X) \subset \langle X \rangle$, então I é ideal diferencial. Sendo assim, o anel quociente R/I pode ser visto como anel diferencial se equipado com a derivação $D_{R/I}(a + I) = D_R(a) + I$, que está bem definida pois $D_R(I) \subset I$.

Observação: Para o leitor não familiarizado com Localização de Anéis[4] recomendo pular para a definição 2.10 e retornar a esta parte quando for citada mais a frente, pois isto só será utilizado a partir do final da sessão 4.

Antes de mostrar como trabalhar com localização de anéis diferenciais, faremos uma definição:

Definição 2.8. Seja R um anel. O *anel de números duais sobre* R é o anel $R[\epsilon]/\left\langle \epsilon^2 \right\rangle = R \oplus R\epsilon$.

Proposição 2.9. *Defina a extensão da derivação de R para um de seus anéis de frações a seguinte forma: Seja Q um subconjunto multiplicativo de R tal que $1 \in Q; 0 \notin Q$. Define-se $D : Q^{-1}R \to Q^{-1}R$ extensão da derivação de R por $D(a/b) = \frac{bD(a)-aD(b)}{b^2}$. Então, a extensão $D(a/b)$ está bem definida.*

Demonstração. Usaremos o anel dos números duais sobre R para provar que a extensão da derivação está bem definida. Para isso me referirei a $R[\epsilon]$ como sendo o anel dos números duais sobre R, ou seja tendo em mente que $\epsilon^2 = 0$,[5] como ϵ é nilpotente, $x = a + b\epsilon$ é uma unidade em $R[\epsilon]$ se e somente se a e uma unidade em R. Uma verificação rápida mostra que o homomorfismo aditivo $D : R \to R$ é uma derivação em R se e somente se $\psi_D = (Id_R, D) : R \to R[\epsilon]$, ou seja $\forall r \in R; \psi_D(r) = r + D(r)\epsilon$, é um homomorfismo de anéis.

Seja ϕ a composição de ψ_D com o mapa de localização, que e um homomorfismo, $R[\epsilon] \to Q^{-1}R[\epsilon]$, então $\forall q \in Q\phi(q) = q/1 + (D(q)/1)\epsilon = y$. Como $q/1$ é unidade em $Q^{-1}R$, então y é unidade em $Q^{-1}R[\epsilon]$. Então ϕ se extende para um homomorfismo $\gamma : Q^{-1}R \to Q^{-1}R[\epsilon]$, então γ é da forma $(Id_{Q^{-1}R}, E)$, em que E extende D e $E(a/q) = \frac{qD(a)-aD(q)}{q^2}$, pela construção feita.

Logo, $D(a/b)$ está bem definido, como queríamos demonstrar.

■

Definiremos agora um dos conceitos centrais para o nosso tratamento, que você possivelmente viu sem muita formalização em um curso introdutório de EDO, os *Anéis de polinômios diferenciais.*

Definição 2.10. Dado R, o *anel de polinômios diferenciais sobre R na variável Y* é o seguinte anel de polinômios com quantidade **enumerável** de variáveis: $R\{Y\} := R[Y^{(i)} \mid i \in 0, 1, 2, ...]$. Sua derivação é definida como extensão da derivada em R tal que $D(Y^{(i)}) = Y^{(i+1)}$.

Mesmo que formalmente nosso anel tenha infinitas variáveis todas se relacionam pela derivação, sendo assim nossa intuição será de que temos uma só variável, como sugere a notação $R\{Y\}$, e suas derivações sucessivas e que esses são linearmente independentes.

A intuição para os elementos de $R\{Y\}$ vem do seguinte homomorfismo de anéis $R\{Y\} \longrightarrow End(R)$ que manda $Y^{(i)}$ *em* D^i e $a \in R$ na multiplicação pela esquerda por a.[6] Assim, nosso anel $R\{Y\}$ ajuda a formalizar e termos um melhor maquinário algébrico para tratar dos operadores diferenciais sobre R comumente vistos num curso inicial de EDO, no caso específico de $R = \mathbb{R}$ *ou* $\mathbb{C}$.

[4]Ver apêndice A.

[5]Semelhante como é feito usualmente com $\mathbb{R}[i] = \mathbb{C}$, tendo em mente que $i^2 = -1$.

[6]Defina a notação D^i como sendo uma aplicação de $R \longrightarrow R$ que é a composição de D um número i de vezes.

Definição 2.11. Um *operador diferencial linear homogêneo sobre* R são os elementos $L \in R\{Y\}$ tal que o grau dos monômios de cada uma das variáveis $Y^{(i)}$ é no máximo 1.

Todo L pode ser escrito como:

$$L = \sum_{i \in \mathbb{N}} a_i Y^{(i)}; a_i \in R$$

Se $a_i = 0, \forall i > l$, diz-se que a *ordem de* L é l. Nesse mesmo caso, diz-se que L é *mônico* se $a_l = 1$.

Definição 2.12. Seja K um corpo diferencial e $K\{Y\}_1$ o conjunto dos elementos de grau 1 em $K\{Y\}$. Um ideal diferencial $I \subset K\{Y\}$ é dito *linear* se I é gerado por $I \cap K\{Y\}_1$. A *dimensão* de um ideal diferencial linear I é definida como a codimensão de $I \cap K\{Y\}_1$ em $K\{Y\}_1$. (Essa dimensão deve ser pensada como dimensão e codimensão dos espaços vetoriais dos anéis de polinômios sobre K.)

Vale notar que $K\{Y\}_1$ é um subespaço D-invariante de $K\{Y\}$. O próximo teorema servirá para elucidar algumas das definições e nomes usados.

Teorema 2.13. *Seja* $L \in K\{Y\}$ *um* operador diferencial linear homogêneo mônico de ordem l, *e seja* I *um ideal gerado por* $\{D^i L \mid i \in \{0, 1, 2, ...\}\}$. *Então,* I *é um* ideal diferencial linear de dimensão l.

Demonstração. Pela base de I nota-se que ele é um ideal diferencial. Então, precisamos garantir que o ideal é *linear* e que sua dimensão é l.

I é linear imediatamente do fato que L é homogêneo linear, suas derivações também o serão, sendo assim o conjunto $\{D^i L \mid i \in \{0, 1, 2, ...\}\}$ que gera I está contido em $K\{Y\}_1$.

Para analisar a dimensão olharemos para o quociente $K\{Y\}_1/(I \cap K\{Y\}_1)$ e provaremos que $\{\overline{Y}^{(0)}, ..., \overline{Y}^{(l-1)}\}$ é uma base, em que a barra em cima denota imagem módulo I.

A derivação se D age naturalmente no quociente, de acordo com a definição feita anteriormente, e como $L = Y^{(i)} + M$; em que M é uma combinação $K - linear$ de $Y^{(i)}$ de ordem menor que l, então $D^n L = Y^{(l+n)} + N$; em que N é combinação $K - linear$ de $Y^{(i)}$ com ordem menor que $l + n$. Dado que cada $D^i L, i \in \mathbb{N}$, pertence a I, então no quociente monômios com ordem maior ou igual a l serão todos representados por combinações $K - lineares$ de $\overline{Y}^{(0)}, ..., \overline{Y}^{(l-1)}$, então o mesmo conjunto gera $K\{Y\}_1/(I \cap K\{Y\}_1)$. Basta prová-lo linearmente independente.

Suponha por absurdo o contrário. Então, existe combinação $K - linear$ de $\overline{Y}^{(0)}, ..., \overline{Y}^{(l-1)}$ que dá $\overline{0}$. Então, essa mesma combinação linear fora no quociente; ou seja basta tirar as barras de cima dos $Y^{(i)}$; que pertence a I, obtendo-se então a equação:

$$\sum_{i=0}^{l-1} c_i Y^{(i)} = \sum_{j=0}^{n} b_j D^j L.$$

Como L é mônico, haverá algum fator $Y^{(i)}$ com $i > l - 1$ cujo coeficiente é não nulo no lado direito, mas no lado esquerdo todos os fatores de mesma ordem tem coeficiente nulo.Logo, Absurdo! ■

Esse teorema nos motiva a definir uma classe específica de ideais que serão importantes.

Definição 2.14. Seja $L \in K\{Y\}$ um operador diferencial linear homogêneo mônico de ordem l, e I um ideal de $K\{Y\}$ gerado por $\{D^i L \mid i \in \{0, 1, 2, ...\}\}$. Então, I é chamado *ideal diferencial linear gerado por* L.

Para finalizar a primeira parte desta introdução os próximos teoremas completam a caracterização da relação entre *ideais diferenciais lineares* e *operadores diferenciais lineares.*

Teorema 2.15. *Seja* $L = Y^{(l)} - \sum_{i=0}^{l-1} a_i Y^{(i)}$ *um operador diferencial linear homogêneo em* $K\{Y\}$ *de ordem* l. *Então* $\{Y^{(0)}, ..., Y^{(l-1)}, L, DL, D^2 L, ...\}$ *é uma base de* $K\{Y\}_1$. *Em particular, sendo*

I um ideal diferencial linear gerado por L, então $K\{Y\}/I$ é isomorfo (como anéis) ao anel de polinômios $K[\overline{Y}^{(0)}, ..., \overline{Y}^{(l-1)}]$. (note que esse último anel de polinômios é no sentido usual.)

Demonstração. Para demonstrar este resultado basta adaptar a segunda parte do Teorema 2.13, pois é demonstrado que $\{Y^{(0)}, ..., Y^{(l-1)}, L, DL, D^2L, ...\}$ gera $K\{Y\}_1$, mas a equação que prova $\{\overline{Y}^{(0)}, ..., \overline{Y}^{(l-1)}\}$ é um conjunto LI também prova que fora do quociente $\{Y^{(0)}, ..., Y^{(l-1)}, L, DL, D^2L, ...\}$ também é LI. Então é uma base, como queríamos demonstrar.

A segunda parte pode ser vista como uma aplicação do Teorema do Isomorfismo de anéis. Pode-se trocar a base, no caso as variáveis do polinômio, de $K\{Y\} = K[Y^{(0)}, Y^{(1)}, ...]$ para $\{Y^{(0)}, ..., Y^{(l-1)}, L, DL, ...\}$, agora tome a função que projeta $K\{Y\}$ em $K[Y^{(0)}, ..., Y^{(l-1)}]$, essa projeção é sobrejetora e seu kernel é I. Como anéis $K[Y^{(0)}, ..., Y^{(l-1)}]$ é isomorfo a $K[\overline{Y}^{(0)}, ..., \overline{Y}^{(l-1)}]$, então:

$$\begin{array}{ccc} K\{Y\} & \xrightarrow{\varphi} & K[\overline{Y}^{(0)}, ..., \overline{Y}^{(l-1)}] \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varphi}} & \\ K\{Y\}/I & & \end{array}$$

■

Como $K[\overline{Y}^{(0)}, ..., \overline{Y}^{(l-1)}]$ é domínio, temos como Corolário que todo I gerado por um operador diferencial linear homogêneo mônico é primo (pois o quociente é domínio) e o anel $K\{Y\}/I$ é Noetheriano, pois seus ideais são finitamente gerados.

Lembrando a definição da diferencial induzida no quociente nota-se que: (para $L = Y^{(l)} - \sum_{i=0}^{l-1} a_i Y^{(i)}$)

$$D(\overline{Y}^{(j)}) = \overline{D(Y^{(j)})} = \begin{cases} \overline{Y}^{(j+1)} & sej < l-1 \\ \sum_{i=0}^{l-1} a_i \overline{Y}^{(i)} & sej = l-1 \end{cases}$$

Teorema 2.16. *Seja $I \subset K\{Y\}$ um ideal diferencial linear de dimensão l. Então existe um único operador diferencial linear homogêneo mônico de ordem l tal que I é o ideal diferencial linear gerado por L. Consequentemente, todo operador diferencial linear homogêneo em I tem ordem pelo menos l. (Volta do teorema 2.13.)*

Demonstração. A notação de barra nesta demonstração está relacionada ao quociente $K\{Y\}_1/(I \cap K\{Y\}1)$. Seja k o inteiro maximal tal que $\overline{Y}^{(0)}, ..., \overline{Y}^{(k)}$ são linearmente independentes. Como a dimensão de I é l, então $k \leqslant l-1$. Então, existe um elemento $L \in I$ da forma:

$$L = Y^{(k+1)} - \sum_{i=0}^{k} a_i Y^{(i)}$$

Seja J o ideal diferencial linear gerado por L. Como $L \in I$, então $J \subset I$, consequentemente existe sobrejeção de $K\{Y\}_1/(J \cap K\{Y\}_1)$ em $K\{Y\}_1/(I \cap K\{Y\}_1)$. Pelo Teorema 2.13 a dimensão de $K\{Y\}_1/(J \cap K\{Y\}_1)$ é $k+1$ e pela sobrejetividade $k+1 \geqslant l$, como no início notamos que $k \leqslant l-1$, então $k+1 = l$, pela dimensão e o teorema anterior tem se que, $I \cap K\{Y\}_1 = J \cap K\{Y\}_1$. Como I e J são lineares ambos são gerados por suas respectivas intersecções com $K\{Y\}_1$, então $I = J$.

Para notar a minimalidade da ordem de L basta analisar o início do parágrafo acima em que se prova que $k+1 \geqslant l$ supondo k sendo ordem de um elemento genérico de I ao invés de ser o número construído no início.

A unicidade de L vem do fato que se M for outro operador diferencial linear homogêneo mônico em I, então $L - M \in I$ tem ordem menor que l, logo $L - M = 0$.

■

3. Resolvendo Equações Diferenciais

Nesta seção começaremos a analisar como encontrar soluções de EDOs, em particular achar soluções para $L = 0$ em que L é um operador diferencial linear homogêneo.

Definição 3.1. Seja $L = Y^{(l)} - \sum_{i=0}^{l-1} Y^{(i)}$ um operador diferencial linear homogêneo em $K\{Y\}$. O anel de polinômios $R = K[y_0, ..., y_l]$, com a derivação de K extendida para $y_0, ..., y_l$ definida como:

$$D_R(y_j) = \begin{cases} y_{j+1} & sej < l-1 \\ \sum_{i=0}^{l-1} a_i y_i & sej = l-1 \end{cases}$$

(R, D_R) descrito acima será chamada *Álgebra Universal de Soluções de L.* (Abreviaremos para AUS-L.)

A intensão desta definição é olhar tal conjunto como um espaço algébrico abstrato onde vamos procurar soluções de L e onde todas elas deveriam existir. Apesar da construção formal é imediato pela teoria construída ver que o AUS-L é $K\{Y\}/I$, em que I é o ideal diferencial linear gerado por L. O próximo teorema mostra que dada qualquer *K-álgebra* em que $L = 0$ tem uma solução y existe um único homomorfismo de *K-álgebras* de AUS-L para essa *K-álgebra* que leva y_0 em y.

Teorema 3.2. *Seja $L \in K\{Y\}$ um operador diferencial linear homogêneo mônico e I o ideal diferencial linear gerado por L. Então, $K\{Y\}/I$ tem as seguintes propriedades:*

- $L(Y^{(0)} + I) = 0$.
- *Se S é uma* K-álgebra *diferencial e $y \in K$ satisfaz $L(y) = 0$, então existe um único homomorfismo diferencial de $K\{Y\} \longrightarrow S$, que leva $Y^{(0)} + I \mapsto y$.*

A demonstração é bem direta e não será feita, em compensação a real importância do teorema será vista nos exemplos a seguir.

Exemplo 3.3. Começando por um exemplo trivial, considere a equação $Y^{(1)} = 0$ sobre $\mathbb{C}$ com derivação trivial. (Ou seja, $D(z) = 0, \forall z \in \mathbb{C}$.) Neste caso a AUS é $\mathbb{C}[y]$ com derivação seguindo a extensão da definição inicial, que neste caso gerará a derivação trivial em $\mathbb{C}[y]$.

Exemplo 3.4. Considere agora um corpo genérico K com derivação trivial. A equação $Y^{(1)} = a$ não é homogênea, então a priori não estaria englobada na teoria que estamos construindo. Porém, solução z dessa equação respeita a seguinte relação: $D^2(z) = D(a) = 0$, então toda solução de $Y^{(1)} = a$ é solução de $Y^{(2)} = 0$, esta última tem AUS $K[y_0, y_1]$. (Aqui nossa derivação será, pela definição, trivial em K e $D(y_0) = y_1, D(y_1 = 0)$.) Note que o ideal I gerado por $y_1 - a$ é um ideal diferencial, dado que $y_1 - a \in const(K[y_0, y_1])$, e tem-se que $K[y_0, y_1]/I$ é isomorfo a $K[y]$ com $D_{K[y]}(y) = a$. (Note a semelhança com $K[y_0, y_1]/\langle y_1 - a\rangle \cong K[y_0, a] \cong K[y]$, pois $a \in K$, feito para anéis de polinômios usualmente.)

Exemplo 3.5. Uma leve variação do exemplo anterior é, seja K corpo diferencial arbitrário, considere a equação $Y^{(1)} = a$, em que $a \in K$ não é constante. (A diferença entre os exemplos é essencialmente que no anterior $const(K) = K$, pois derivada era trivial e aqui $a \notin const(K)$.) Seja $a_1 = D(a)/a \in K$ e considere a equação $Y^{(2)} - a_1 Y^{(1)} = 0$. A respectiva AUS é $K[y_0, y_1]$, por definição sua derivação é uma extensão da derivação de K tal que $D(y_0) = y_1, D(y_1) = a_1 y_1$. Seja $P = \langle y_1 - a\rangle$ um ideal em $K[y_0, y_1]$. Como $D(y_1 - a) = a_1(y_1 - a)$, então P é ideal diferencial. Como no exemplo anterior $K[y_0, y_1]/P$ é isomorfo a $K[y]$ com $D(y) = a$.

Seja K corpo diferencial arbitrário. Outra equação a ser analisada neste contexto é a: $Y^{(1)} - aY^{(0)} = 0, a \in K$. A AUS dessa equação é o anel de polinômios $K[y]$, em que $D(y) = ay$. Extensões desse tipo, ou seja uma extensão S de R em que $R(y) = S$ e $D(y)/y \in R$, são chamadas *adjunção de uma exponencial.*

Teorema 3.6. *Seja $E = K(z)$ uma extensão de corpo diferencial tal que $\frac{D(z)}{z} \in K$. Então z ou é* transcendental *sobre K, obtido por* adjunção de uma exponencial *a K, ou para algum $n \in \mathbb{Z}^+$ temos $z^n \in K$.*

Demonstração. Considere o anel de polinômios $K[y]$ com derivação $D(y) = ay, a = \frac{D(z)}{z}$, por hipótese $a \in K$. Esse anel é mapeado para E por um homomorfismo diferencial que leva $y \mapsto z$. O Kernel deste homomorfismo é um ideal diferencial primo, pois $K[y]$ é domínio e a derivada comuta com homomorfismos diferenciais. Semelhantemente também concluímos que $K[y]$ é um domínio de ideais principais, então temos dois casos para analisar. No primeiro, o Kernel em questão é gerado por um polinômio irredutível mônico p, no segundo é zero.

Analisando o primeiro: Como o Kernel é diferencial temos que $D(p)$ pertence ao Kernel e então é gerado por p, ou seja $p \mid D(p)$. Seja $p = y^n + p_{n-1}y^{n-1} + ... + p_0$, então:

$$D(p) = ny^{n-1}(D(y)) + \sum_{k=0}^{n-1}(D(p_k) + kp_k\frac{D(y)}{y})y^k = any^n + \sum_{k=0}^{n-1}(D(p_k) + akp_k)y^k$$

Como $p \mid D(p)$ e ambos tem grau n, $D(p) = anp$. Comparando termos de mesmo grau dos polinômios temos: $D(p_k) = (n-k)ap_k$ para $0 \leqslant k \leqslant n-1$. Note que, $D(\frac{z^{n-k}}{p_k}) = 0$, então $p_k = c_k z^{n-k}$ em que $c_k \in const(K)$. Em particular, temos que $z^n = \frac{p_0}{c_0}$.

No segundo caso: z é transcendente sobre L e é obtido por *adjunção de uma exponencial* a K. ■

Agora iniciaremos uma discussão sobre como fazer extensões diferenciais de corpos altera o sub-corpo de constantes de um dado corpo diferencial. Essa discussão será focada em extensões do tipo *adjunção de uma exponencial* e será detalhada na próxima sessão. Para finalizar esta sessão, alguns exemplos como prelúdio do que está por vir.

Exemplo 3.7. Seja $\mathbb{C}((z))$ o conjunto das séries de Laurent formais com coeficientes em $\mathbb{C}$. Note que, $\mathbb{C}(z)$ é um sub-anel diferencial de $\mathbb{C}((z))$, em que ambos tem a derivação usual: $D(z) = 1, D(z_0) = 0; z_0 \in \mathbb{C}$.

Exemplo 3.8. Seja f a série exponencial usual. Então $D(f) = f$. Considere o corpo $K = \mathbb{C}(f)$ e a equação $Y^{(1)} - Y^{(0)} = 0$. Como vimos antes, o AUS dessa equação é $K[y]$ em que $D(y) = y$. Porém, nota-se que K já possui uma solução para tal equação, então adicionar y para criar o AUS parece supérfluo. Note também que a seguinte equação é verdade em $K[y]$:

$$D(\frac{y}{f}) = \frac{fD(y) - yD(f)}{f^2} = \frac{fy - yf}{f^2} = 0$$

Então, adicionar essa possível solução supérflua gera uma nova constante: $\frac{y}{f}$. O objetivo da próxima sessão é investigar a estrutura por trás de adicionar novas constantes e as tais soluções supérfluas.

4. Dependência Linear de Constantes

Nesta sessão analisaremos o problema apresentado no final da última, para isso introduziremos mais algumas linguagens usuais de um curso de EDO no nosso contexto mais algébrico e criaremos uma extensão do AUS, formando um espaço ainda maior para obter soluções das nossas equações diferenciais.

Definição 4.1. Sejam $y_1, y_2..., y_s$ elementos de um corpo diferencial K. Então:

$$w = w(y_1, ..., y_s) = \begin{vmatrix} y_1^{(0)} & y_2^{(0)} & \cdots & y_s^{(0)} \\ y_1^{(1)} & y_2^{(1)} & \cdots & y_s^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(s-1)} & y_2^{(s-1)} & \cdots & y_s^{(s-1)} \end{vmatrix}$$

em que $y_i^{(j)} = D^j(y_i)$, é chamado *Determinante Wronskiano de $y_1, ..., y_s$* ou o *Wronskiano de $y_1, ..., y_s$*.

Alguns comentários sobre notação: elementos de K^n, para um dado corpo diferencial K serão escritos como $\mathbf{y} = (y_1, ..., y_n)$. Para todo $i \in \mathbb{N}$ definimos $\mathbf{y}^{(i)} = (D^i(y_1), ..., D^i(y_n))$. Assim escrevemos sinteticamente $w(\mathbf{y}) = det((\mathbf{y}^{(0)}, ..., \mathbf{y}^{(n-1)}))$.

Agora mostraremos como o Wronskiano se relaciona com a dependência linear de subconjunto do nosso corpo visto como vetores sobre o sub-corpo das constantes. Num curso de EDO costuma-se ver isso em situações específicas, com este nosso ponto de vista conseguiremos obter generalizações dos resultados usuais.

Teorema 4.2. *Seja K um corpo diferencial, e $y_1, ..., y_{n+1}$ elementos de K que satisfaça a equação: $Y^{(n)} - \sum_{i=0}^{n-1} a_i Y^{(i)} = 0, a_i \in K$. Então, $w(y_1, ..., y_{n+1}) = 0$.*

Demonstração. Seja $\mathbf{y} = (y_1, ..., y_{n+1})$. Então, $w(\mathbf{y}) = det(\mathbf{y}^{(0)}, ..., \mathbf{y}^{(n-1)})$, note que a última linha é combinação linear das anteriores, pela própria teoria de ideais diferenciais lineares é possível notar isso, então o determinante é 0.

■

Agora teremos uma condição necessária e suficiente para o Wronskiano zerar.

Teorema 4.3. *Seja K um corpo diferencial. Então $y_1, ..., y_n \in K$ são linearmente dependentes sobre $const(K)$ se e somente se $w(y_1, ..., y_n) = 0$.*

Demonstração. Começaremos pela ida, ou seja, suponha que os y_i são linearmente dependentes sobre $const(K)$. Então, existem $c_i \in const(K), 1 \leqslant i \leqslant n$, tal que $\sum_{i=1}^{n} c_i y_i$. aplicando o operador D^k na igualdade anterior temos: $\sum_{i=1}^{n} c_i D^k(y_i) = 0, \forall k$. Isso faz com que consigamos ver $c_1, ..., c_n$ como soluções não triviais do sistema linear nas variáveis x_i, que nos permitirá relacionar a afirmação com o Wronskiano:

$$\sum_{i=1}^{n} y_i^{(k)} x_i = 0; 0 \leqslant k \leqslant n-1$$

Note que a matriz dos coeficientes do sistema acima é o Wornskiano e dado que ele tem solução não trivial seu determinante tem que ser zero.

Reciprocamente, suponha $w(y_1, ..., y_n) = 0$, então analogamente ao caso anterior existem soluções não triviais $b_1, ..., b_n \in K$, para o sistema:

$$\sum_{i=1}^{n} y_i^{(k)} x_i = 0; 0 \leqslant k \leqslant n-1$$

Queremos provar que esta solução está em $const(K)$. Como ela é não trivial, então existe algum b_i não nulo e pode ser rearranjado os índices para que $b_1 \neq 0$ e depois dividir todos os números da solução por b_1. Ou seja, podemos supor sem perda de generalidade $b_1 = 1$. Como $D(1) = 0$ para qualquer anel diferencial, então sabemos já que $b_1 \in const(K)$. Agora note que, para cada $k, 0 \leqslant k \leqslant n-1$, temos:

$$\sum_{i=1}^{n} y_i^{(k)} b_i = 0;$$

Aplicando D na equação para $0 \leqslant k \leqslant n-2$, temos que:

$$\sum_{i=1}^{n} y_i^{(k+1)} b_i + \sum_{i=1}^{n} y_i^{(k)} D(b_i) = 0;$$

Nas equações anteriores o primeiro somatório é zero. O segundo tem o primeiro termo zero pois $b_1 \in const(K)$, então $D(b_2), ..., D(b_n)$ é solução pro sistema linear:

$$\sum_{i=1}^{n} y_i^{(k)} x_i = 0; 0 \leqslant k \leqslant n-2$$

Note que a matriz dos coeficientes deste novo sistema é o Wronskiano $w(y_2, ..., y_n)$. Seja esse Wronskiano é diferente de zero então a solução que encontramos é trivial, logo $D(b_i) = 0$ e então $b_i \in const(K); \forall i \in \{1, ..., n\}$ como queríamos demonstrar. Caso contrário, é possível repetir o mesmo processo da demonstração para $y_2, ..., y_n$ como a dimensão é finita o processo eventualmente acaba e em cada passo prova-se que o elemento de menor índice é uma constante, sendo assim a demonstração está terminada.

■

Veremos agora um teorema sobre a estrutura do espaço de soluções de uma equação diferencial linear e isso motivará nossas próximas definições.

Teorema 4.4. *Seja L um operador diferencial homogêneo linear mônico de ordem l sobre o corpo diferencial K. Seja E uma extensão diferencial do corpo K e seja S o conjunto de soluções de $L = 0$ em E. Então S é um espaço vetorial sobre o corpo de constantes $const(E)$[7] de dimensão no máximo l.*

Demonstração. A aplicação que leva $y \mapsto L(y)$ em E é uma transformação $const(E) - linear$, então o seu kernel é um $const(E)$ espaço vetorial, tal kernel é S por definição. Pelo teorema 4.2 qualquer conjunto de $l + 1$ elementos de S tem Wornskiano zero e então por teorema 4.3 são linearmente dependentes sobre $const(E)$. Então a dimensão de S é no máximo l sobre $const(E)$.

■

Apesar de simples, o teorema anterior nos mostra que dado um operador bem comportado sobre um corpo diferencial a dimensão do espaço de soluções da equação diferencial associada a esse operador é limitado e carrega informações da extensão do corpo, mais especificamente de suas constantes, e da ordem do operador, que motiva nossa próxima definição, que caminha na direção de conseguirmos definir um espaço grande o suficiente para abarcar qualquer solução da equação diferencial, considerando as extensões de corpo que serão necessárias nesse processo.

Definição 4.5. Seja L um operador diferencial linear mônico de ordem l sobre K. Dizemos que $L = 0$ tem um *conjunto de soluções completo na extensão diferencial de corpos E* de K se o conjunto de soluções em E tem dimensão l sobre o corpo de constantes de E. Ou seja, existem elementos $y_1, ..., y_l \in E$ tal que $L(y_i) = 0$ e o Wronskiano $w(y_1, ..., y_l) \neq 0$.

Nosso próximo teorema mostra a força dos resultados anteriores que geram uma correspondência entre um operador bem comportado e o seu conjunto de soluções completo.

Teorema 4.6. *Sejam L_1 e L_2 operadores diferenciais lineares homogêneos mônicos de ordem l sobre um corpo K, e suponha que há elementos $y_1, ..., y_l \in K$ linearmente independentes sobre $const(K)$ tal que $L_1(y_i) = L_2(y_i) = 0$ para cada i, ou seja, $y_1, ..., y_l$ é um conjunto de soluções completo de L_1 e L_2. Então, $L_1 = L_2$, mais precisamente $L_1 = L_2 = \frac{w(Y, y_1, ..., y_l)}{w(y_1, ..., y_l)}$.*[8]

Demonstração. Suponha que $L_1 = \sum_{i=0}^{l} a_i Y^{(i)}$ e $L_2 = \sum_{i=0}^{l} b_i Y^{(i)}$, por hipótese tem-se que $a_l = b_l = 1$. Seja j o maior índice tal que $a_j \neq b_j$. Considere $L = (a_j - b_j)^{-1}(L_1 - L_2)$, apesar de ser natural estudar a diferença entre os operadores dado que queremos mostrar a unicidade queremos também que ele seja mônico, por isso escolhemos tal j e dividimos por tal constante. Agora nota-se que L é um operador diferencial linear homogêneo mônico de ordem $j < l$, porém o espaço de soluções $L = 0$ contém $y_1, ..., y_l$ então tem dimensão sobre o corpo das constantes maior ou igual a l, o que contradiz o teorema 4.4, logo não existe tal j. Então, $a_i = b_i$ para cada i, ou seja $L_1 = L_2$.

Para a segunda afirmação do teorema, usaremos essa unicidade para provar que o operador escrito da forma que o teorema pressupõe é o operador inicial. Seja $L_3 = \frac{w(Y, y_1, ..., y_l)}{w(y_1, ..., y_l)}$. Note que

[7] Este é um dos erros mais drásticos em [1], se olhar em [2] notará que a versão apresentada aqui é a correta, ou basta verificar a demonstração.

[8] Na notação usada no final do teorema o Y é para indicar a coordenada livre que será preenchida pelo vetor que o operador em questão será aplicado, isso ficará bem claro na demonstração do teorema.

L_3 é mônico, além disso por vir de um Wronskiano, no caso um determinante, ele é também um operador diferencial linear homogêneo sobre K e pela dimensão do determinante tem ordem l. Note que $L_3(y_i) = 0$, pelas propriedades básicas do determinante. Então, pela unicidade $L_3 = L_1 = L_2$.

■

Os resultados acima nos encaminham no sentido de que para um operador diferencial bem comportado de ordem l, só é possível adicionar ao espaço de soluções da Equação Diferencial associada ao operador de no máximo l soluções linearmente independentes sobre o corpo de constantes. Para fechar esta sessão definiremos como fazer isso de modo abstrato e geral, ou seja adicionar um conjunto de soluções completo. Para algumas das construções e demonstrações a seguir serão necessárias algumas ferramentas de Álgebra Comutativa que serão brevemente recordadas num apêndice.

Definição 4.7. Seja $L = Y^{(l)} - \sum_{i=0}^{l-1} Y^{(i)}$ um operador diferencial homogêneo linear mônico em $K\{Y\}$. Seja $S = K[y_{ij} \mid 0 \leqslant i \leqslant l-1, 1 \leqslant j \leqslant l][w^{-1}]$ a localização[9] do anel de polinômios $R = K[y_{ij}]$ de l^2 variáveis em $w = det(y_{ij})$. Defina a derivação D_R em R por:

$$D_R(y_{ij}) = y_{i+1,j}; i < l-1 D_R(y_{l-1,j}) = \sum_{i=0}^{l-1} a_i y_{ij}$$

Basta extender essa derivação para S.[10] Chamaremos S de *álgebra universal de soluções completa de* $L = 0$, abreviaremos para AUSC-L.

Esta definição vem de uma construção análoga a feita anteriormente para adicionar uma única solução, porém neste caso invertemos w. Isso é feito para formalmente garantir que as soluções adicionadas são linearmente independentes sobre o sub-corpo das constantes. Isso é feito, pois os resultados desta sessão tiveram justamente o objetivo de relacionar a inversibilidade de w, ou condições de o Wronskiano zerar, com a independência linear de soluções sobre o corpo das constante e a Localização de Anéis aparece naturalmente pois essa ferramenta cria inversos para os elementos desejados de um anel, mas há um preço a se pagar por adicionar essa propriedade ao seu anel.

Até agora nossa construção permitiu a partir de um operador bem comportado L sobre um corpo diferencial K criar um extensão de K em que L tem conjunto de soluções completo, nosso agora objetivo é refinar esse processo. Assim como na Teoria de Corpos usual para se obter soluções para uma equação polinomial sobre um dado corpo é possível extensões de corpos adicionando muito mais elementos até chegar em um espaço grande o suficiente. Parte da Teoria de Galois usual ajuda a refinar esse processo tentando localizar mais precisamente até onde precisamos extender e quem é o "espaço de soluções optimal". Seguiremos com uma filosofia semelhante, foi visto que no exemplo de adicionar uma exponencial em um anel que tem exponencial que isso gerava novas constantes. Na próxima sessão mostraremos que dado L é possível construir uma única extensão diferencial E de K tal que L tem conjunto de soluções completo e E não possui novas constantes em relação a K. Essa extensão será chamada *Extensões de Picard-Vessiot.*

5. Extensões de Picard-Vessiot

Esta sessão se resume a discutir as extensões de Picard-Vessiot, iniciaremos com a definição e depois provaremos sua existência e unicidade, mas naturalmente alguns lemas técnicos serão necessários nesse processo.

Definição 5.1. Seja L um operador diferencial linear homogêneo mônico de ordem l sobre o corpo diferencial K. O extensão diferencial de corpo $E \supset K$ é chamada *extensão de Picard-Vessiot de K por L* se:

[9]Olhar no apêndice A.

[10]Para o leitor que pulou a parte sobre Localização de Anéis Diferenciais na seção 2 basta retornar a Proposição 2.9.

- E é gerado sobre K pelo conjunto V de soluções de $L = 0$ em E.($E = K\langle V\rangle$.)
- E contém o conjunto de soluções completo de $L = 0$, ou seja, existem $y_1, ..., y_l \in V$ tal que $w(y_1, ..., y_l) \neq 0$.
- Toda constante em E também está em K.

Iniciaremos com algumas propriedades da extensão de Picard-Vessiot, como o próximo teorema que garante a sua minimalidade em relação a todas as extensões que possuem o conjunto de soluções completo de $L = 0$ mostrando que se essa extensão existir ela é o refinamento ou "conjunto de soluções optimal"que procuramos, depois será discutida a existência da extensão quando o corpo de constantes é algebricamente fechado, que será nossa suposição extra sobre o corpo diferencial inicial K para realizar nosso estudo.

Teorema 5.2. *Seja $E \supset K$ uma extensão de Picard-Vessiot de K pelo operador L. Se existe $E \supset C \supset K$ tal que C é extensão intermediária que contenho o conjunto de soluções completo de $L = 0$, então $E = C$.*

Demonstração. Pela definição da extensão de Picard-Vessiot $const(E) = const(K)$, consequentemente $const(E) = const(C)$. Seja V_E o conjunto de soluções de $L = 0$ em E e análogo para V_C. Pela definição, $E = K\langle V_E\rangle$ e $C = K\langle V_C\rangle$. Como ambos conjuntos de solução são o conjunto de soluções completo, V_C gera V_E sobre $const(E)$, porém sabemos que $const(E) = const(C)$, então $V_C = V_E$, logo $E = K\langle V_E\rangle = K\langle V_C\rangle = C$.

■

A próxima propriedade será importante para demonstrar a unicidade da extensão, mostra que ela se comporta bem com homomorfismos. Em particular, nos mostra que a extensão de Picard-Vessiot é o análogo nesta teoria do *Corpo de Decomposição* na Teoria de Galois clássica.

Teorema 5.3. *Seja $E_1, E_2 \supset K$ extensões de Picard-Vessiot de ordem l pelo operador L sobre K, seja $E \supset K$ uma extensão sem novas constantes. Assuma que $\sigma_i : E_i \longrightarrow E$ é um $K-$ mergulho $diferencial$,$i \in \{1, 2\}$. Então, $\sigma_1(E_1) = \sigma_2(E_2)$.*

Demonstração. Seja $V_i = L^{-1}(0)$ em E_i e $V = L^{-1}(0)$ em E. Então, cada V_i é um espaço vetorial de dimensão l sobre $const(K)$ e V um espaço vetorial sobre o mesmo corpo de dimensão no máximo l. Isso acontece pois $const(E_1) = const(E_2) = const(E)$ pela definição da extensão de Picard-Vessiot e pois E não tem novas constantes, aliado com o fato que o ordem de L limita superiormente a dimensão de $L^{-1}(0)$. Por conta do mergulho tem-se que $\sigma_i(V_i) \subset V$, então $\sigma_1(V_1) = V = \sigma_2(V_2)$. Como $E_i = K\langle V_i\rangle$, então $\sigma_1(E_1) = \sigma_2(E_2)$.

■

Provaremos agora a existência da extensão de Picard-Vessiot, depois sua unicidade a menos de isomorfismos diferenciais, primeiro provaremos alguns resultados auxiliares. O primeiro dos resultados auxiliares é um teorema de Álgebra Comutativa cuja demonstração foge do escopo deste trabalho, para sua demonstração é possível olhar a página 10 de [2].

Teorema 5.4. *Seja R uma* K-álgebra *finitamente gerada, e $d \in R$ um elemento qualquer. Uma das duas situações acontece: ou d é algébrico sobre K ou então existe $c \in K$ tal que $d - c$ é não é uma unidade de R.*

Agora vamos aos Lemas que vamos provar.

Lema 5.5. *Seja R um domínio de integridade diferencial, finitamente gerado sobre K. Seja F o corpo de frações de R. Suponha que F possua uma constante $d \notin K$. Se d não é algébrico sobre $const(K)$, então R possui um ideal próprio diferencial.*

Demonstração. Seja $I = \{h \in R \mid hd \in R\}$. Note que I é um ideal de R; tal ideal é não vazio pois d é por definição formado por uma fração de elementos de R. Por hipótese, d é uma constante e isso faz com que o ideal I seja um ideal diferencial, pois: $D(hd) = D(h)d$ que pertence a R se hd pertence. Se $I \neq R$, então é o ideal próprio procurado no teorema. Caso contrário, como $1 \in R$, então $d \in R$ pela própria definição de I. Olharemos agora para os ideais da forma $(d - c)R$ em que $c \in const(K)$, note que todos esses são ideais diferenciais.

Se algum for propriamente contido em R, então a demonstração termina pois é o ideal que queremos. Caso contrário d é algébrico sobre K pelo Teorema 5.4, porém desejamos provar que ele é algébrico sobre $const(K)$. Para provar o que falta considere o polinômio minimal de d em $K[x]$, escreveremos ele como $p(x) = x^n + p_{n-1}x^{n-1} + ... + p_0$. Pela definição desse polinômio temos que: $0 = D(p(d)) = D(p_{n-1})d^{n-1} + ... + D(p_0)$, então d também é raiz do seguinte polinômio: $q(x) = D(p_{n-1})x^{n-1} + ... + D(p_0)$, que possui grau menor que $p(x)$. Pela definição polinômio minimal tem-se que $q(x) \cong 0$, logo $D(p_i) = 0$ para cada i. Então, $p(x) \in const(K)[x]$, logo d é algébrico sobre $const(K)$.

■

Corolário 5.6. *Seja R um domínio de integridade diferencial, finitamente gerado sobre o corpo diferencial K. Seja F o corpo de frações de R. Se R não possui ideais diferenciais próprios e $const(K)$ é algebricamente fechado, então $const(F) = const(K)$.*

O corolário anterior nos mostra que o corpo de constante ser algebricamente fechado e algumas outras características são interessantes para obtermos a propriedade de não criar novas constantes.

Lema 5.7. *Seja R um anel diferencial e I um ideal diferencial maximal de R tal que o quociente R/I tem característica zero. Então I é primo.*

Demonstração. Nesta demonstração olharemos tudo no quociente, pois é possível traduzir todas nossas informações para o quociente: a informação de I ser maximal se traduz em R/I não ter ideais diferenciais próprios, a informação que queremos provar se traduzirá como o quociente ser domínio de integridade e nossa outra hipótese é sobre o quociente. Por isso denotarei $A = R/I$ e farei todas as contas em A como se fosse uma anel não específico com essas propriedades e não usarei notação de classe de equivalência. Desejamos provar que A é domínio de integridade.

Tome $a, b \in A; a \neq 0; b \neq 0$, tal que $ab = 0$. Nosso primeiro passo é provar que se $ab = 0$ então $D^k(a)b^{k+1} = 0$ para $k > 0$. Faremos uma indução em k;

- Caso base $[1 \mapsto k] : 0 = D(0) = D(ab) = aD(b) + D(a)b$, multiplicando por b, tem-se: $D(a)b^2 = 0$.

- Passo indutivo $[n \mapsto k \Rightarrow n+1 \mapsto k]$: por hipótese de indução temos que $D^n(a)b^{n+1} = 0$, derivando e depois multiplicando por b, tem-se: $0 = D^{n+1}(a)b^{n+2} + (n+1)D^n(a)b^{n+1}D(b)$, por hipótese de indução o segundo termo da soma é zero, então $D^{n+1}(a)b^{n+2} = 0$.

Terminando a indução.

■

Seja J um ideal diferencial gerado por a, ou seja, $J = \sum_{i=0}^{\infty} RD^i(a)$. Suponha que b não é nilpotente. Dado um elemento arbitrário de J, $\sum_{i=0}^{n} r_i D^i(a)$ e multiplicando ele por b^{n+1} nosso resultado anterior, demonstrado por indução, garante que $(\sum_{i=0}^{n} r_i D^i(a))b^{n+1} = 0$, logo todo elemento de J é divisor de zero. Em particular, isso implica que é impossível que $1 \in J$ e como J é não trivial dado que $0 \neq a \in J$. Então, J é um ideal diferencial próprio de A o que contradiz nossas hipóteses. Como b é um divisor de zero arbitrário, isso implica que todo divisor de zero em A é nilpotente. Em particular, existe um $n \in \mathbb{Z}^+$ minimal tal que $a^n = 0$. Então $0 = D(a^n) = na^{n-1}$ e como, por hipótese, A tem característica zero temos que $na^{n-1} \neq 0$, logo $D(a)$ é divisor de zero. Repetindo o processo obtemos que todo $D^k(a)$ é divisor de zero, então nilpotente. Por conseguinte J tem que todos seus elementos são nilpotentes, logo obtemos novamente que $1 \notin J$ e de forma análoga contradizendo nossa hipótese. Dessa contradição segue que não podem existir a, b não nulos tais que $ab = 0$, ou seja A é domínio de integridade, ou seja, I é primo. Agora provaremos a existência da extensão de Picard-Vessiot.

Teorema 5.8. *Seja K um corpo diferencial com seu corpo de constantes algebricamente fechado. Seja L um operador diferencial linear homogêneo mônico sobre K e S a AUSC-L sobre K, por*

fim seja P um ideal diferencial maximal de S. Então P é primo e o corpo de frações F do domínio de integridade S/P é a extensão de Picard-Vessiot de K por L.

Demonstração. Note que S é gerada diferencialmente sobre K pelas soluções de $L = 0$ e o inverso do Wronskiano (por causa da Localização), então o mesmo é verdade para S/P. Pelo Lema 5.7, P é primo e pelo fato de P ser maximal então S/P não tem ideais diferenciais próprios. Pelo corolário 5.6 os corpos de constantes coincidem, ou seja, $const(F) = const(K)$. Além disso, F é gerado diferencialmente sobre K pelas soluções de $L = 0$ e como o inverso do Wronskiano é unidade em S é unidade em S/P e então deve ser não nulo em F, logo $L = 0$ tem um conjunto de soluções completo em F. Assim verificasse que F possui todas as propriedades da definição **??**, logo F é a extensão de Picard-Vessiot de K para L.

■

Na construção anterior toma-se um P ideal diferencial maximal, mas S poderia ter mais de um desses. Então, nosso próximo resultado responde justamente a pergunta de se é única a construção do Teorema anterior. Veremos a extensão de Picard-Vessiot é única a menos de isomorfismo diferencial. Para o leitor interessado em quão canônica esta construção é, no livro [2] essa discussão é respondida, mas requer um pouco mais de teoria do que é apresentada aqui e foge ao escopo destas notas.

Teorema 5.9. *Sejam E_1, E_2 extensões de Picard-Vessiot de K para o operador L de ordem l. Suponha que $const(K)$ é algebricamente fechado. Então, existe um $K-isomorfismos\ diferenciais$ de $E_1 \to E_2$.*

Nesta demonstração usaremos algumas construções com produtos tensoriais[11], pro leitor não familiarizado pode olhar as breves notas no apêndice ou livros na bibliografia, porém só um conhecimento básico do assunto é suficiente para entender a demonstração.

Demonstração. Considere que E_1 é a extensão de Picard-Vessiot construída no teorema anterior e importaremos a notação daquele teorema para este.

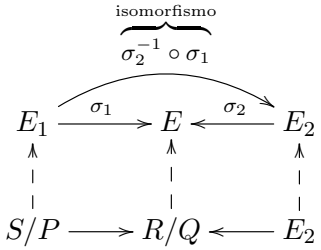
Considere o anel $R = S/P \otimes_K E_2$. R é gerado diferencialmente como uma álgebra sobre E_2 pelos geradores de S/P. Como S/P é, por construção, gerado sobre K soluções linearmente independentes $y_1, ..., y_n$ de L, R é finitamente gerado sobre E_2. Tome Q um ideal diferencial próprio maximal de R e considere sua imagem inversa I pela inclusão $S/P \hookrightarrow S/P \otimes_K E_2$, ou seja, $I = \{a \in S/P \mid a \otimes_K 1 \in Q\}$. Note que, I é um ideal diferencial de S/P, pois Q é ideal diferencial no produto tensorial e a inclusão preserva a estrutura diferencial, mas por construção S/P não possui ideais diferenciais próprios, logo $I = S/P$ ou I é o ideal trivial.

Se $I = S/P$, então $1 \otimes_K 1 \in Q$, o que é absurdo já que $Q \neq R$; então I é trivial. Consequentemente, S/P se injeta em R/Q pela inclusão passada pro quociente, ou seja, a aplicação que leva $a \mapsto (a \otimes_K 1) + Q$.[12] A aplicação $E_2 \to R/Q$ que leva $b \mapsto (1 \otimes_K b) + Q$ também é injetor. Pelo Lema 5.7, Q é primo, então R/Q é domínio de integridade. Seja F o corpo de frações de R/Q. Como o domínio de integridade diferencial R/Q não tem ideias diferenciais próprios, é finitamente gerado como álgebra sobre o corpo diferencial E_2, e $const(E_2) = const(K)$ que são algebricamente fechados. Então, pelo Lema 5.6 as constantes de F coincidem com as de E_2 e K.

O mergulho de S/P para R/Q se extende a um mergulho σ_1 de E_1 para F, e o mergulho de E_2 para R/Q se extende para um mergulho σ_2 de E_2 para F. Note que ambos mergulhos são identidade em K. Como temos dois mergulhos, um de cada extensão de Picard-Vessiot em questão, em F e as extensões não tem novas constantes em relação a K. Pelo Teorema 5.3, esses mergulhos tem a mesma imagem, logo a aplicação $\sigma_2^{-1} \circ \sigma_1$ é o $K - isomorfismo$ desejado de E_1 para E_2. A construção do isomorfismo pode ser visualizado pelo diagrama abaixo:

[11] Ver apêndice B.

[12] Intuitivamente o quociente por Q só colapsa a parte direita do produto tensorial, a relativa a E_2, já que projetar Q em S/P é somente o zero.



■

Isso encerra, em essência, os assuntos teóricos a serem tratados antes de irmos para nossa aplicação desejada. Porém, *enunciarei* um teorema e um corolário que encaminham o leitor para a direção que a discussão teórica tomaria se fosse continuada. Para os familiarizados com Teoria de Galois já é natural imaginar que iniciaríamos uma análise dos grupos de automorfismos da extensão de Picard-Vessiot, infelizmente um tratamento em mais detalhes desses objetos não só foge ao escopo do livro como requer mais requisitos do leitor. Para o interessado nos detalhes pode seguir [2].

Teorema 5.10. *Seja K um corpo diferencial com const(K) algebricamente fechado. Seja L um operador diferencial linear homogêneo mônico sobre K, e $E \supset K$ a extensão de Picard-Vessiot de K por L. Seja $a \in E - K$. Então exite um K-automorfismo diferencial τ de E tal que $\tau(a) \neq a$.*

Seja G um grupo de automorfismos diferenciais do corpo diferencial E. O conjunto de pontos fixos $E^G = \{a \in E \mid \sigma(a) = a; \forall \sigma \in G\}$ é um subcorpo diferencial de E.

Corolário 5.11. *Seja K um corpo diferencial com const(K) algebricamente fechado. Seja E a extensão de Picard-Vessiot de K e seja G o grupo de todos os automorfismos diferenciais de E fixando K. Então $E^G = K$.*

Com isso terminamos nossa discussão sobre a extensão de Picard-Vessiot e caminharemos em direção a nossa aplicação desejada. Para isso teremos uma breve introdução de alguns novos importantes conceitos para termos a linguagem certa para falar de integrável por funções elementares.

6. Teorema de Liouville

Nesta sessão resolveremos o problema inicial de provar que e^{x^2} não possui integral elementar, nossa principal ferramenta para isso será o *Teorema de Liouville*, mas antes de enunciar o teorema e resolver o problema, precisamos criar a linguagem certa para atacar o problema, por exemplo qual o significado de ser integrável em termos de funções elementares?

Definição 6.1. Seja K um corpo diferencial, E uma extensão de corpos diferencial. Chamaremos $t \in E$ uma *primitiva sobre* K se $D(t) \in K$. Além disso, dizemos que $t \in E, t \neq 0$, é *hiper-exponencial* sobre K se $\frac{D(t)}{t} \in K$.

Definição 6.2. Seja K um corpo diferencial, E uma extensão de corpos diferencial.Dizemos que $t \in E$ é *Liouvilliano sobre* K se t é uma das 3 opções: *algébrico, ou uma primitiva, ou hiper-exponencial sobre* K. Analogamente, dizemos que L é uma *extensão Liouvilliana* de K se existem $t_1, ..., t_n \in E$ tal que $E = K(t_1, ..., t_n)$ e cada t_i é Liouvilliano sobre $K(t_1, ..., t_{i-1})$ para $1 \leqslant i \leqslant n$.

Agora teremos definições relativas a extensões Liouvillianas especificas para o problema que queremos resolver.

Definição 6.3. Sejam K e E como definidos anteriormente. Dizemos que $t \in E$ é um *logaritmo sobre* K se $D(t) = \frac{D(b)}{b}$ para algum $b \in K, b \neq 0$. Dizemos que $t \in E, t \neq 0$ é uma *exponencial sobre* K se $\frac{D(t)}{t} = D(b)$ para algum $b \in K$.

Definição 6.4. Seja K um corpo diferencial, E uma extensão de corpo diferencial. Dizemos que $t \in E$ é *elementar sobre* K se é uma das 3 opções: *algébrico, um logaritmo, ou uma exponencial sobre* K. Dizemos que $t \in E$ é *monômio elementar* sobre K se t é *transcendente e elementar* sobre K e também $const(K(t)) = const(E)$. Analogamente, dizemos que E é uma *extensão elementar* de K se existem $t_1, ..., t_n \in E$ tal que $E = K(t_1, ..., t_n)$ e t_i é elementar sobre $K(t_1, ..., t_{i-1})$ para $1 \leqslant i \leqslant n$. Por fim, dizemos que $f \in K$ *tem integral elementar sobre* K se existe extensão elementar E de K e $g \in E$ tal que $D(g) = f$.

Definição 6.5. Uma *função elementar* é qualquer elemento de qualquer extensão elementar do corpo diferencial $\mathbb{C}(x)$ com derivada usual.

Note que, as funções usuais de Cálculo são elementares sobre $\mathbb{C}(x)$ pela nossa definição, ou seja $ln(x), e^x$ e funções trigonométricas. Indicando que nossa definição é coerente.

Agora enunciamos o principal teorema da sessão, este nos dará as condições necessárias e suficientes para uma função ser integrável em termos de funções elementares, o Teorema de Liouville.

Teorema 6.6. *(Teorema de Liouville) Seja K um corpo diferencial e $f \in K$. Se existe uma extensão elementar E de K com $const(K) = const(E)$, e $g \in E$ tal que $D(g) = f$, então existem $v \in K$; $u_1, ..., u_m \in K$ não nulos; e $c_1, ..., c_m \in const(K)$ tal que:*

$$f = D(v) + \sum_{i=1}^{m} c_i \frac{D(u_i)}{u_i}$$

Corolário 6.7. *Seja K um corpo diferencial e E uma extensão de corpos diferencial de K que não adiciona novas constantes gerada por adjunção de uma exponencial, ou seja, $E = K(e^g); g \in E$. Suponha que e^g é transcendental sobre K. Para qualquer $f \in K$, $fe^g \in E$ tem primitiva elementar em alguma extensão de corpos diferencial sem novas constantes de E, ou seja, fe^g tem integral elementar, isso ocorre se e somente se existe algum elemento $a \in K$ tal que: $f = D(a) + aD(g)$.*

Note que a equação para f no Corolário é um caso específico do Teorema de Liouville e será Corolário que usaremos para demonstrar que e^{x^2} não é integrável em termos de funções elementares.

As demonstrações desses resultados será omitida por motivos de tamanho das notas, mas o leitor interessado pode acompanhar a demonstração feita no livro [3].

Teorema 6.8. *A função e^{x^2} não é integrável em termos de funções elementares sobre $\mathbb{C}(x)$.*[13]

Demonstração. Pelo corolário 6.7 temos que $e^{x^2} = 1.e^{x^2}$ tem integral elementar se e somente se existe $a \in \mathbb{C}(x)$ tal que: $1 = D(a) + 2ax$. Provaremos por absurdo que não existe tal função. Suponha que $a = \frac{p}{q} \in \mathbb{C}(x)$ satisfaz a equação e $mdc(p, q) = 1$, então:

$$1 = \frac{D(p)q - pD(q)}{q^2} + \frac{2px}{q} \Longleftrightarrow \frac{pD(q)}{q} = D(p) + 2px - q$$

Isso implica que q divide $pD(q)$, mas como $mdc(p, q) = 1$, então q divide $D(q)$, como esses são polinômios, então q é uma constante. Então sem perda de generalidade pode-se assumir $a = \frac{p}{q} = p$.

Agora que temos polinômios dos dois lados da equação $1 = D(a) + 2ax$ podemos comparar os graus em relação a x e notar que o lado esquerdo tem grau zero e o direito tem grau pelo menos 1, logo não pode existir tal a. Que gera nosso absurdo, então concluímos que e^{x^2} não tem integral elementar, como queríamos.

■

[13] A demonstração aqui apresentada segue um caminho elementar, feito em [1], porém [2] resolve o problema de não integrabilidade de e^{-x^2}, que é análogo, usando uma abordagem diferente e mais teórica, que foge do escopo das notas, no seu capítulo 6.

O apêndice é uma breve lista de definições, resultados e exemplos para o leitor não familiarizado com um curso Álgebra Comutativa[14]. Como estas notas necessitam de bem pouco muitas propriedades importantes das estruturas aqui apresentadas serão deixadas de lado para favorecer a brevidade da revisão. Para mais detalhes recomendo o livro [4] do Eduardo Tengan neste assunto.

Apêndice A. Localização

Localização é uma ferramente muito importante para estudo de anéis comutativos e geometria algébrica. Ela nos permite generalizar a construção do corpo de frações de um domínio de integridade. Mais precisamente, ela nos permite escolher quais elementos do nosso anel (**que pode até não ser um domínio**) adicionaremos inversos. Esse processo de acrescentar unidades a priori pode parecer complicar o estudo do anel, mas ele reduz a quantidade de ideias primos do anel de modo bem específico e permite estudar propriedades do anel original nessa sua versão local.

Começaremos com uma breve discussão da construção, que como essencialmente tudo nestes apêndices, é feito em mais detalhes em [4]. Antes, uma definição necessária.

Definição A.1. Seja A um anel. Um *conjunto multiplicativo* $S \subset A$ é um subconjunto fechado por produto, ou seja $s, t \in S \Longrightarrow st \in S$, e tal que $1 \in S$.

A construção replica a construção usual do corpo de frações, porém feita para um conjunto multiplicativo $S \subset A$ e nossa relação de equivalência será levemente diferente para contornar o problema de divisores de zero.

(Construção): Dado anel A e $S \subset A$ conjunto multiplicativo, a *localização de A com respeito a S* é o anel $S^{-1}A$. Como esperado $S^{-1}A := A \times S/\sim$ com a relação de equivalência dada por:

$$\frac{a_1}{s_1} = \frac{a_2}{s_2} \in S^{-1}A \Longleftrightarrow \exists t \in S \mid t(s_2a_1 - s_1a_2) = 0, em\ A.$$

Na conta acima as "frações"representam as classes de equivalência e não propriamente a multiplicação pelo inverso do número no denominador. Ou seja, a classe de $(a, s) \in A \times S$ é $\frac{a}{s} \in S^{-1}A$. Soma e produto no nosso novo anel seguem o esperado:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2a_1 + s_1a_2}{s_1s_2} \qquad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1a_2}{s_1s_2}$$

Com isso, o novo anel $S^{-1}A$ é também comutativo, com zero sendo $\frac{0}{1}$ e unidade $\frac{1}{1}$. Também há um morfismo natural de anéis, o *mapa de localização:*

$$\begin{array}{rccc} \rho: & A & \longrightarrow & S^{-1}A \\ & a & \longmapsto & \frac{a}{1} \end{array}$$

Observação: Pode-se rapidamente notar pela relação de equivalência que gera a localização que localizar por conjuntos multiplicativos que possuam o zero não é uma ideia muito interessante a priori[15]. Além disso, e mais importante, se A *é domínio* e $0 \notin S$, então $\frac{a_1}{s_1} = \frac{a_2}{s_2} \Longleftrightarrow a_1s_2 = s_1a_2$, então as localizações são subanéis do *corpo de frações* de A e o mapa de localização é a inclusão $A \hookrightarrow S^{-1}A$. Porém, veremos em exemplos futuros que o mapa de localização não só nem sempre é injetivo, no caso de um anel geral, como também se houverem divisores de zero no seu conjunto multiplicativo eles podem "encolher"o anel, isso se tornará mais preciso em breve.

Observação: Uma noção importante para localização, mas que não será muito importante para nosso estudo é a localização de módulos e álgebras, essa localização no Anel base do módulo ou álgebra, ou seja, se M é um A-módulo (ou A-álgebra) então a localização $S^{-1}M$ de M com relação

[14]Para um leitor não familiarizado com o estudo de módulos, pode supor que os módulos tratados ao longo do apêndice são Espaços Vetoriais, porém essas ferramentas brilham realmente no contexto de módulos, então é recomendável tentar ver por esse ponto de vista.

[15]Porém, é possível mostrar que $S^{-1}A = 0 \Longleftrightarrow 0 \in S$ e esse resultado tem aplicações úteis

a S é o $S^{-1}A$-módulo (ou $S^{-1}A$-álgebra) cujos elementos são frações $\frac{m}{s}$ em que $m \in M; s \in S$ com a identificação:

$$\frac{m_1}{s_1} = \frac{m_2}{s_2} \in S^{-1}A \Longleftrightarrow \exists t \in S \mid t(s_2 m_1 - s_1 m_2) = 0, em\ M.$$

As suas operações de soma e multiplicação por escalar são, como esperado:

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2} \qquad \frac{a}{s_1} \cdot \frac{m}{s_2} = \frac{am}{s_1 s_2}$$

para todo $a \in A, s_i \in S; m_i \in M$.

Definiremos agora os principais exemplos que, o primeiro é exatamente o que aparecerá na nossa teoria. Depois apresentaremos a *Propriedade Universal da Localização.*

Definição A.2. Seja A um anel e M um A-módulo. Denotaremos por:

- $A_h = A[h^{-1}]$ e M_h as localizações dos respectivos conjuntos pelo conjunto multiplicativo $S = \{h^n \mid n \geqslant 0\}$ das potências de um elemento $h \in A$;
- A_P *e* M_P as localizações de A e M com relação ao conjunto multiplicativo $S = A \backslash P$ em que P é um ideal primo de A.

Teorema A.3. ***(Propriedade Universal da Localização)*** *Seja A e B anéis, seja $S \subset A$ um conjunto multiplicativo e seja $\rho : A \to S^{-1}A$. Denote por:*

$$Hom_S(A, B) := \{\phi \in Hom(A, B) \mid \phi(S) \subset B^\times\}^{16}$$

A localização nos dá uma bijeção natural

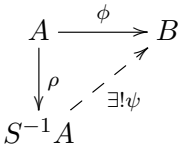
$$Hom(S^{-1}A, B) \xrightarrow{\approx} Hom_S(A, B)$$

$$\psi \longmapsto \psi \circ \rho$$

cujo inverso leva $\phi \in Hom_S(A, B)$ em $\psi \in Hom(S^{-1}A, B)$ definido por

$$\psi\left(\frac{a}{s}\right) = \phi(s)^{-1} \cdot \phi(a) \qquad (a \in A, s \in S)$$

Assim, para todo $\phi \in Hom_S(A, B)$, existe um único $\psi \in Hom(S^{-1}A, B)$ que faz o diagrama abaixo comutar:



Veremos agora brevemente nossos exemplos[17].

Exemplo A.4. Seja $A\,\mathbb{Z}/12\,\mathbb{Z}$ e considero e ideal gerado por $\overline{2}$, que é primo, $P = \langle\overline{2}\rangle$, analisaremos brevemente "quem é"A_P. Seja $\rho : A \to A_P$ o mapa de localização; note que $\overline{3} \notin P$ então será uma unidade, então:

$$0 = \rho(\overline{12}) = \rho(\overline{3})\rho(\overline{4})\rho(\overline{4}) = 0 \in A_P$$

Como todo elemento ímpar é inversível módulo 4 e todo elemento que vem de um impar na nossa localização será uma unidade além de $\overline{4}$ ser levado em 0, então é razoável intuir que $A_P = \mathbb{Z}/4\,\mathbb{Z}$, o que é verdade! Para mais detalhes olhe o livro.

Vale ressaltar que o mapa de localização não é injetor neste caso e que o nosso anel "encolheu"por conta dos divisores de zero como $\overline{2}, \overline{4}, \overline{8}$.[18]

[16] $Hom(A, B)$ é o conjunto de homomorfimos de $A \to B$ e $B^\times$ é o conjunto das unidades.

[17] Para mais detalhes o leitor pode olhar em [4]

[18] Para mais detalhes e um entendimento preciso e formal disto leia o capítulo 4 e [4]

Exemplo A.5. Seja A um anel qualquer e $h \in A$. É possível mostrar que:

$$A_h = \frac{A[x]}{(1-hx)}$$

Então a notação $A[h^{-1}]$ faz sentido intuitivo.

Apêndice B. Produto Tensorial

O Produto Tensorial é uma construção que permeia diferentes áreas da matemática. Este tópico não é tão importante para estas notas, mas é imprescindível para leituras posteriores na área e entender como trabalhar com álgebras vai ser implicitamente importante ao longo das notas. Ainda que o produto tensorial apareça explicitamente nestas notas só na demonstração do Teorema 5.9.

Nossa necessidade dessa construção é bem superficial, então este apêndice também será, entender a definição do produto tensorial de álgebras é, na prática tudo que precisamos. Uma característica importante do Produto Tensorial é formalizar a mudança de base do seu módulo, espaço vetorial, álgebra,... um exemplo específico que o leitor com um bom curso de Álgebra Linear pode conhecer é a Complexificação de um Espaço Vetorial.

Para mais detalhes o leitor é sempre convidado a olhar no livro [4]. Este apêndice é retirado majoritariamente de lá.

Definição B.1. Seja A um anel e sejam M, N e T A-módulos. Um mapa bilinear é uma função

$$\phi : M \times N \to T$$

que é A-linear em cada entrada separadamente, ou seja,

(i) $\phi(a_1 m_1 + a_2 m_2, n) = a_1 \phi(m_1, n) + a_2 \phi(m_2, n)$
(ii) $\phi(m, a_1 n_1 + a_2 n_2) = a_1 \phi(m, n_1) + a_2 \phi(m, n_2)$

para todo $m, m_i \in M, n, n_i \in N$ e $a_i \in A$. O conjunto de todos os mapas bilineares entre $M \times N$ e T será denotado por $\mathrm{Bil}_A(M \times N, T)$.

Veremos primeiro a propriedade universal do Produto Tensorial, depois a construção. A ideia é que teremos dois A-módulos M, N e construiremos um novo A-módulo $M \otimes_A N$, chamado *Produto Tensorial de M e N sobre A*, juntamente com uma aplicação bilinear:

$$\otimes : M \times N \to M \otimes_A N$$

Para o leitor familiarizado com Categorias, representam o funtor $Bil_A(M \times N, -)$.

(Propriedade Universal): Para qualquer A-módulo "de teste"T, a aplicação:

$$\begin{array}{rccc} : & Hom_A(M \otimes N, T) & \longrightarrow & Bil_A(M \times N, T) \\ & f & \longmapsto & f \circ \otimes \end{array}$$

é uma bijeção. Ou seja, dado uma aplicação bilinear $\phi \in Bil_A(M \times N, T)$, queremos que exista um *único morgismo de A-módulos* $f : M \otimes_A N \to T$ que faz o seguinte diagrama comutar:

$$\begin{array}{ccc} M \times N & \xrightarrow{\phi} & T \\ {\scriptstyle \otimes}\downarrow & \nearrow_{\exists! f} & \\ M \otimes N & & \end{array}$$

(Construção): Considere o A-modulo livre com base $\{e_{m,n} \mid (m,n) \in M \times N\}$, ou seja:

$$\bigoplus_{(m,n \in M \times N)} A \cdot e_{m,n}$$

e seja R o submódulo gerado pelos elementos da forma:

(i) $e_{am,n} - a \cdot e_{m,n}, e_{m,an} - a \cdot e_{m,n}$

(ii) $e_{m_1+m_2,n} - e_{m_1,n} - e_{m_2,n}$
(iii) $e_{m,n_1+n_2} - e_{m,n_1} - e_{m,n_2}$

em que $m, m_i \in M; n, n_i \in N$ e $a \in A$. Definimos:

$$M \otimes_A N := \frac{\bigoplus_{(m,n)\in M\times N} A \cdot e_{m,n}}{R}$$

Denotamos a imagem de $e_{m,n}$ em $M \otimes_A N$ por $m \otimes n$, que chamaremos de *tensor elementar*. Assim, os tensores elementares geram $M \otimes_A N$ e satisfazem as relações:

(i) $(am) \otimes n = a(m \otimes n) = m \otimes (an)$
(ii) $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$
(iii) $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$

para todo $m, m_i \in M; n, n_i \in N$ e $a \in A$, de modo que temos um mapa bilinear:

$$\begin{array}{rccc} \otimes : & M \times N & \longrightarrow & M \otimes_A N \\ & (m, n) & \longmapsto & m \otimes n \end{array}$$

Para mais detalhes sobre a construção consultar o livro. Vale notar que todo elemento e $M \otimes_A N$ é gerado como soma de tensores elementares, logo para tratar de morfismos basta definir neles. Veremos alguns isomorfismos importantes para a teoria e que nos dão uma noção de como a estrutura funciona:

Teorema B.2. ***(Isomorfismos Básicos)*** *Seja A um anel. Temos os seguintes isomorfismos canônicos:*

(i) *(Associatividade)*

$$\begin{array}{rccc} : & (M \otimes_A N) \otimes_A P & \longrightarrow & M \otimes_A (N \otimes_A P) \\ & (m \otimes n) \otimes p & \longmapsto & m \otimes (n \otimes p) \end{array}$$

(ii) *(Elemento Neutro)*

$$\begin{array}{rccc} : & A \otimes_A M & \longrightarrow & M \\ & a \otimes m & \longmapsto & am \end{array}$$

(iii) *(Comutatividade)*

$$\begin{array}{rccc} : & M \otimes_A N & \longrightarrow & N \otimes_A M \\ & m \otimes n & \longmapsto & n \otimes m \end{array}$$

(iv) *(Distributividade com relação à Soma Direta)*

$$\begin{array}{rccc} : & M \otimes_A (\bigoplus_{i\in I} N_i) & \longrightarrow & \bigoplus_{i\in I}(M \otimes_A N_i) \\ & m \otimes (n_i)_{i\in I} & \longmapsto & (m \otimes n_i)_{i\in I} \end{array}$$

(v) *(Quociente) Para qualquer ideal $I \subset A$,*

$$\begin{array}{rccc} : & M \otimes_A (A/I) & \longrightarrow & M/IM \\ & m \otimes \overline{a} & \longmapsto & \overline{am} \end{array}$$

(vi) *(Localização) Para qualquer conjunto multiplicativo $S \subset A$*

$$\begin{array}{rccc} : & (S^{-1}A) \otimes_A M & \longrightarrow & S^{-1}M \\ & \frac{a}{s} \otimes m & \longmapsto & \frac{am}{s} \end{array}$$

Veremos agora alguns exemplos para entender um pouco a versatilidade dessa construção.

Exemplo B.3. Seja K um corpo de V, W espaços vetoriais de dimensão finita sobre K. Sejam $v_1, ..., v_n$ e $w_1, ..., w_m$ bases de V e W respectivamente. Pela distributividade, temos o seguinte isomorfismo:

$$V \otimes_K W = (\bigoplus_{1\leqslant i\leqslant n} K \cdot v_i) \otimes_K (\bigoplus_{1\leqslant i\leqslant m} K \cdot w_i) = \bigoplus_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}} K \cdot v_i \otimes w_j$$

Logo, $V \otimes_K W$ é um espaço vetorial com base $\{v_i \otimes w_j \mid 1 \leqslant i \leqslant n; 1 \leqslant j \leqslant m\}$ e portanto:

$$dim_K(V \otimes_K W) = (dim_K(V)) \cdot (dim_K W)$$

Exemplo B.4. Sejam $m, n \in \mathbb{Z}$ e $d = mdc(m, n)$. Temos um isomorfismo:

$$\frac{\mathbb{Z}}{\langle m \rangle} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{\langle n \rangle} = \frac{\mathbb{Z}/\langle m \rangle}{\langle n \rangle \cdot (\mathbb{Z}/\langle m \rangle)} = \frac{\mathbb{Z}/\langle m \rangle}{(\langle m \rangle + \langle n \rangle)/\langle m \rangle)} = \frac{\mathbb{Z}}{\langle m, n \rangle} = \frac{\mathbb{Z}}{\langle d \rangle}$$

Antes e estudarmos o Produto Tensorial de Álgebras que é nosso real objetivo, veremos a interpretação de como o produto tensorial pode ser vista como uma mudança de base, ou mais intuitivamente uma "troca de coeficientes"como descrito no livro [4]. Nosso estudo será muito mais raso direto que o do livro, principalmente para evitar a linguagem de categorias e aplicações que fogem ao escopo das notas.[19] A teoria para álgebras será análoga em muitos aspectos e então esta primeira visão em módulos da uma intuição e naturalidade maior aos objetos.

(Mudança de Base): O produto tensorial de módulos é particularmente interessante quando temos uma A-álgebra B para "multiplicar"nosso A-módulo M. Neste caso, o produto tensorial $M \otimes AB$ ppode ser visto como B-módulo: para cada $b_0 \in B$ fixado, a multiplicação por b_0

$$B \xrightarrow{b_0} B$$

define um morfismo de A-módulos

$$\begin{array}{rccc} Id \otimes b_0 : & M \otimes_A B & \longrightarrow & M \otimes_A B \\ & m \otimes b & \longmapsto & m \otimes b_0 b \end{array}$$

Assim, $M \otimes_A B$ adquire uma estrutura e B-módulo via multiplicação na segunda coordenada. Essa estrutura se extende para os morfismos, então se $f : M \to M'$ é um morfismo e A-módulos, então temos que $f \otimes Id : M \otimes_A B \to M' \otimes_A B$ é um morfismo de B-módulos.[20] Uma notação para simplificar é denotar o B-módulo $M \otimes_A B$ como M_B e o morfismo $f \otimes Id$ por f_B quando não gerar ambiguidade. Essa estrutura ficará mais clara com um exemplo.

Exemplo B.5. Seja $L \supset K$ uma exensão de corpos e V um K-espaço vetorial de dimensão n. Se $v_1, ..., v_n$ é uma base de V sobre K, então

$$V_L = V \otimes_K L = (\bigoplus_{1 \leqslant i \leqslant n} K \cdot v_i) \otimes_K L = \bigoplus_{1 \leqslant i \leqslant n} (K \cdot v_i \otimes_K L) = \bigoplus_{1 \leqslant i \leqslant n} L \cdot (v_i \otimes 1)$$

é um L-espaço vetorial de dimensão n, sendo $v_1 \otimes 1, ..., v_n \otimes 1$ uma base sobre L. Assim, temos:

$$dim_L(V_L) = dim_L(V \otimes_K L) = dim_K(V)$$

Apesar de existirem outras propriedades interessantes, vamos estudar logo exemplos de produtos tensoriais de álgebras. E seremos breves, mas re-itero que mais detalhes sobre essa teoria rica e demonstrações das afirmações aqui feitas podem ser encontrados em [4].

Definição B.6. Dadas duas A-álgebras B e C, o produto tensorial $B \otimes_A C$ admite uma estrutura de A-álgebra: como a aplicação

$$\begin{array}{rccc} : & B \times C \times B \times C & \longrightarrow & B \otimes_A C \\ & b \otimes c \otimes b' \otimes c' & \longmapsto & (bb') \otimes (cc') \end{array}$$

é A-multilinear, define um morfismo de A-módulos

$$\begin{array}{rccc} : & (B \otimes_A C) \otimes_A (B \otimes_A C) & \longrightarrow & B \otimes_A C \\ & b \otimes c \otimes b' \otimes c' & \longmapsto & (bb') \otimes (cc') \end{array}$$

[19] Como enter a mudança de base como um funtor e o produto tensorial de álgebras como um coproduto. Ideias detalhadas no livro.

[20] Por isso, $- \otimes_A B$ é chamado funtor mudança de base.

ou seja, uma operação de produto em $B \otimes_A C$, fazendo deste um anel cuja unidade é $1 \otimes 1$. Este anel é uma A-álgebra: multiplicação por $a \in A$ é dada por $a(b \otimes c) = (ab) \otimes c = b \otimes (ac)$.

Veremos agora nossos últimos exemplos para contextualizar como essas estruturas aparecem e são entendidas aos olhos das nossas discussões anteriores.

Exemplo B.7. Para qualquer A-álgebra B, temos um isomorfismo de B-álgebras:

$$\begin{array}{rccc} : & A[x] \otimes_A B & \longrightarrow & B[x] \\ & p(x) \otimes b & \longmapsto & b \cdot p(x) \end{array}$$

Em particular temos que: $A[x] \otimes_A A[y] = A[x, y]$.

Veremos agora que nossa mudança de base se comporta bem com quocientes.

Exemplo B.8. Seja B um A-módulo e seja $f(x) \in A[x]$. Então temos um isomorfismo de B-álgebras

$$\begin{array}{rccc} \phi : & \frac{A[x]}{\langle f(x) \rangle} \otimes_A B & \longrightarrow & \frac{B[x]}{\langle f(x) \rangle} \\ & \overline{p(x)} \otimes b & \longmapsto & \overline{b \cdot p(x)} \end{array}$$

Por fim, um exemplo especial na própria Teoria de Galois Clássica.

Exemplo B.9. Seja $L \supset K$ um extensão de Galois finita com grupo de Galois $G = Gal(L/K)$. Então temos um isomorfismo de L-álgebras

$$\begin{array}{rccc} : & L \otimes_K L & \longrightarrow & Maps(G, L) \\ & a \otimes b & \longmapsto & (a \cdot (b))_{\sigma \in G} \end{array}$$

Aqui, $L \otimes_K L$ é visto como L-álgebra via multiplicação pela esquerda e $Maps(G, L) \cong L^{|G|}$ é o L-espaço vetorial de todas as funções de G em L, ou seja, o L-espaço vetorial de todas as tupla indexadas por elementos $\sigma \in G$ e entradas em L.

Referências

[1] James Murphy *Differential Galois Theory*, 2010 REU: PARTICIPANT PAPER. (http://www.math.uchicago.edu/ may/VIGRE/VIGRE2010/REUPapers/Murphy.pdf)

[2] Andy R. Magid, *Lectures on Differential Galois Theory*, University Lecture Series Volume: 7; AMS (1994)

[3] Manuel Bronstein. Symbolic Integration I: Transcendental Functions. Springer-Verlag (2005)

[4] Herivelto Borges e Eduardo Tengan, *Álgebra Comutativa em Quatro Movimentos*. IMPA (2015)

[5] Teresa Crespo e Zbigniew Hajto, *Algebraic Groups and Differential Galois Theory*. Graduate Studies in Mathematics Volume: 122; AMS (2011)