Curvas Elípticas com Multiplicação Complexa

Adrian Alexander Ticona Delgado

Comissão Julgadora: Kostiantyn Iusenko – IME-USP (Orientador)
Iryna Kashuba – IME-USP
Aline Andrade – UFF

Monografia elaborada para a disciplina MAT–0148 — Introdução ao Trabalho Científico

Bacharelado em Matemática – Instituto de Matemática e Estatística – Universidade de São Paulo

2º Semestre de 2021

Agradecimentos

Inicio agradecendo a minha família pelo apoio ao longo dos intensos últimos meses de projeto. Agradeço aos professores que me guiaram de certa forma em direção a este tema. Mais especificamente aos Prof.s Vitor de Oliveira Ferreira e Lucia Satie Ikemoto Murakami pelo contato com a álgebra e teoria algébrica dos números e ao Prof. Eduardo Tengan por me ajudar na escolha do tema final. E por fim, ao meu orientador, Prof. Kostiantyn Iusenko, por todas discussões que foram feitas para que fosse possível a conclusão deste projeto.

Resumo

DELGADO, A. **Curvas Elípticas com Multiplicação Complexa**. ano. 76 p. Monografia – Bacharelado em Matemática – Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2º Semestre de 2021.
O tema central deste texto é curvas elípticas. A primeira parte, composta pelos Capítulos 1 e 2, trata da teoria de superfícies de Riemann e curvas algébricas que servirão como base para o Capítulo 3 que apresenta as duas perspectivas que podemos ter sobre as curvas elípticas. E por fim, no Capítulo 4, apresentamos algumas propriedades e resultados sobre curvas elípticas com multiplicação complexa. Em especial, a partir do j-invariante e de seus pontos de torção, obtemos extensões abelianas especiais de corpos quadráticos imaginários.
Palavras-chave: Teoria dos Números, Superfícies de Riemann, Curvas Algébricas, Curvas Elípticas.

Abstract

DELGADO, A. **Elliptic Curves with Complex Multiplication**. ano. 76 p. Monografia – Bacharelado em Matemática – Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2º Semestre de 2021.
The central theme of this text is elliptic curves. The first part, composed by the Chapters 1 and 2, deals with the theory of Riemann surfaces and algebraic curves which will be used in the Chapter 3 to show two perspectives about elliptic curves. And finally, in Chapter 4, we present some properties and results about elliptic curves with complex multiplication. In particular, we can construct special abelian extensions of imaginary quadratic fields from the j-invariant and torsion points of such curves.
Keywords: Number Theory, Riemann Surfaces, Algebraic Curves, Elliptic Curves

Sumário

Introdução

Um dos objetivos da chamada *teoria dos corpos de classe* é fornecer uma descrição (às vezes, explícita) das extensões abelianas de um certo corpo de números. Quando o corpo base é o corpo $\mathbb{Q}$ dos números racionais, o teorema de Kronecker-Weber diz que toda extensão abeliana finita está contida em uma extensão ciclotômica. Ou seja, ao adicionarmos certos valores da exponencial $e^{2\pi iz}$, conseguimos "cobrir" todas as extensões abelianas.

O 12º problema de Hilbert pergunta se isto ocorre para um corpo de números qualquer. Ou seja, se com o auxílio de funções analíticas, conseguimos uma classe de extensões abelianas que cobrem as demais. Antes do problema ser formulado, Kronecker obteve progresso no caso de corpos quadráticos imaginários, com o auxílio de funções elípticas e o seu sonho (*Kronecker's Jugendtraum*) consistia em mostrar que toda extensão abeliana finita está contida em uma que é construída dessa forma.

Com este objetivo em mente, o presente texto apresenta um estudo sistemático de curvas elípticas. Assim, os dois primeiros capítulos nos dão os pré-requisitos necessários. No Capítulo 1, tratamos das superfícies de Riemann na direção do Teorema de Riemann-Roch. No Capítulo 2, isto é feito no caso de curvas algébricas. Ao longo destes capítulos, buscamos destacar as semelhanças que este dois objetos possuem. Daí, no Capítulo 3 abordamos as curvas elípticas tendo como base os dois capítulos anteriores, destacando os seus aspectos analíticos e algébricos. E por fim, no Capítulo 4, enunciamos as propriedades especiais das chamadas curvas elípticas com multiplicação complexa. É este tipo de curva elíptica que nos permitirá construir extensões abelianas de um corpo de números quadrático imaginário.

Capítulo 1

Superfícies de Riemann

Neste capítulo, começamos tratando das chamadas *superfícies de Riemann*. Elas são certos tipos de espaços que se assemelham localmente com abertos de $\mathbb{C}$. Assim, podemos utilizar e estender resultados de análise complexa (de uma variável) para estes tipos de espaços. Além disso, faremos uso de uma ferramenta que será bastante útil, a *cohomologia de feixes*. A partir dela, obtemos resultados importantes como o Teorema de Riemann-Roch, essencial para o prosseguimento do texto. Como o foco do texto é curvas elípticas e suas propriedades aritméticas, certos resultados não serão provados com todo o rigor, mas serão fornecidas referências para o leitor interessado. Este capítulo teve [For81] como referência principal.

1.1 Definições e Teoria Local

Começamos com algumas definições preliminares.

Definição 1.1.1. Seja X um espaço topológico. Um **atlas euclidiano** (de dimensão n) sobre X é uma coleção $\mathcal{A} = \{(U_i, \varphi_i)\}_{i\in I}$ de pares (U_i, φ_i), chamados **cartas**, de abertos U_i e mapas contínuos $\varphi_i : U_i \to \mathbb{R}^n$ tais que

- $\bigcup_{i\in I} U_i = X$.
- φ_i é um homeomorfismo de U_i para um aberto de $\mathbb{R}^n$.

Definição 1.1.2. Um **espaço localmente euclidiano** é um espaço Hausdorff e 2º contável X no qual existe um atlas euclidiano $\{(U_i.\varphi_i)\}_{i\in I}$ de dimensão n para algum $n \geq 1$.

A partir destas, definimos o objeto de estudo deste capítulo.

Definição 1.1.3. Uma **superficie de Riemann** é um espaço Hausdorff, conexo e 2º contável X munido com um atlas euclidiano $\{(U_i.\varphi_i)\}_{i\in I}$ de dimensão 2 tais que para quaisquer $i, j \in I$ com $U_i \cap U_j \neq \varnothing$, a função de transição

$$\varphi_{ij} = \varphi_i \circ \varphi_j^{-1} : \varphi_j(U_i \cap U_j) \to \varphi_i(U_i \cap U_j)$$

é uma função holomorfa, após a identificação em $\mathbb{C}$ pelo mapa natural $(x, y) \mapsto x + yi$.

Observação 1.1.4. A definição acima pode ser resumida dizendo que uma superfície de Riemann é uma variedade complexa e conexa de dimensão um.

Se X admite dois atlas euclidianos $\{(U_i, \varphi_i)\}$ e $\{(V_j, \psi_j)\}$ cujas funções de transição são holomorfas, dizemos que eles são equivalentes se o mesmo ocorre com a união destes dois atlas. Isto define uma relação de equivalência e chamamos cada classe de equivalência de **estrutura complexa**.

Em uma superfície de Riemann, o que importa é a sua estrutura complexa. Assim, podemos tomar um atlas maximal que induz a mesma estrutura complexa. Basta adicionarmos "cartas compatíveis" ao atlas inicial. Em particular, as restrições das cartas antigas em abertos menores estão incluídos neste atlas maximal. É o que faremos daqui em diante.

Exemplo 1.1.5. O exemplo mais trivial de superfície de Riemann é o próprio $\mathbb{C}$. Podemos tomar como atlas o mapa identidade. O mesmo ocorre com abertos de $\mathbb{C}$.

Exemplo 1.1.6. Se X é uma superfície de Riemann e $U \subseteq X$ é aberto conexo, então U é uma superfície de Riemann cuja estrutura complexa é a induzida por X. Ou seja, tomamos as cartas cujo domínio está contido em U.

Exemplo 1.1.7. A esfera 2-dimensional S^2 admite a seguinte estrutura complexa. Tome as duas projeções $\pi_1 : S^2 \backslash \{(0,0,1)\} \to \mathbb{R}^2$ e $\pi_2 : S^2 \backslash \{(0,0,-1)\} \to \mathbb{R}^2$, cujas fórmulas são dadas abaixo.

$$\pi_1(x,y,z) = \left(\frac{x}{1-z}, \frac{y}{1-z}\right) \quad \text{e} \quad \pi_2(x,y,z) = \left(\frac{x}{1+z}, -\frac{y}{1+z}\right).$$

Então, a função de transição de π_1 para π_2 é

$$(\pi_2 \circ \pi_1^{-1})(u,v) = \left(\frac{u}{u^2+v^2}, -\frac{v}{u^2+v^2}\right)$$

que se identifica com a função $1/z$ que é holomorfa no domínio de definição $\mathbb{R}^2 \neq \{(0,0)\}$. De maneira análoga, a função de transição de π_2 para π_1 é holomorfa. Portanto, S^2 com esta estrutura complexa é uma superfície de Riemann, a chamada **esfera de Riemann**. O polo norte $(0,0,1)$ costuma ser chamado de *ponto no infinito* e denotado por ∞.

Exemplo 1.1.8. Seja $\mathbb{CP}^1$ o conjunto das classe de equivalência dos pontos de $\mathbb{C}^2 \backslash \{(0,0)\}$ onde a relação de equivalência $\sim$ é dada por

$$(z_1, z_2) \sim (w_1, w_2) \iff \exists \lambda \in \mathbb{C}^* \quad z_i = \lambda w_i, \quad i = 1, 2.$$

Tal conjunto é chamado de **reta projetiva complexa**. Munido com a topologia quociente, $\mathbb{CP}^1$ admite duas cartas

$$\begin{aligned} \sigma_1 : \mathbb{C} &\to \mathbb{CP}^1 \\ z &\mapsto [(z,1)] \end{aligned} \qquad \begin{aligned} \sigma_2 : \mathbb{C} &\to \mathbb{CP}^1 \\ z &\mapsto [(1,z)] \end{aligned}$$

cuja função de transição $\sigma_2^{-1} \circ \sigma_1 : \mathbb{C}^* \to \mathbb{C}^*$ é dada por $z \mapsto \frac{1}{z}$ que é holomorfa.

A partir da estrutura complexa, podemos dizer quando uma função contínua $f : X \to \mathbb{C}$ é holomorfa.

Definição 1.1.9. Seja X uma superfície de Riemann e seja $f : X \to \mathbb{C}$ uma função contínua. Dizemos que f é uma **função holomorfa** se em cada ponto $x \in X$, para toda carta $(U, \varphi : U \to \mathbb{C})$ com domínio em x, a função $f \circ \varphi^{-1} : \varphi(U) \to \mathbb{C}$ é holomorfa em $\varphi(x)$.

Se Y é outra superfície de Riemann e $F : X \to Y$ é uma contínua, F é dita uma **aplicação holomorfa** se para todo $x \in X$ e cartas (U, φ) e (V, ψ) de X e Y respectivamente, a "interpretação local" de F, dada por $\psi \circ F \circ \varphi^{-1}$ é holomorfa onde é definida.

Na verdade, basta verificar para apenas uma carta em torno de x, já que as funções de transição são holomorfas. Para $U \subseteq X$ aberto, denotamos por $\mathcal{O}_X(U)$ o conjunto das funções holomorfas $f : U \to \mathbb{C}$, no qual U tem a estrutura de superfície de Riemann induzida por X. O motivo para esta notação será dado na seção seguinte (ver Exemplo 1.2.7).

Os exemplos mais fáceis de funções holomorfas são as funções constantes. Pode ocorrer que estas sejam as únicas funções holomorfas em todo o espaço. Este é o caso das superficies de Riemann compactas.

Proposição 1.1.10. *Se X é uma superfície de Riemann compacta. Então, $\mathcal{O}_X(X) \cong \mathbb{C}$.*

Assim, se quisermos estudar este tipo de superfície, devemos permitir que as funções consideradas sejam "quase-holomorfas", admitindo singularidades. Isto nos leva à definição seguinte

Definição 1.1.11. Seja X uma superfície de Riemann. Uma **função meromorfa** em X é uma função holomorfa $f : X\backslash S \to \mathbb{C}$ que satisfaz as seguintes condições

- S é um subconjunto discreto de X.
- Para $s \in S$, temos $\lim_{z\to s} |f(z)| = +\infty$. Dizemos que s é um polo de f.

Denotamos por $\mathcal{M}(U)$ o conjunto das funções meromorfas em um aberto $U \subseteq X$. É claro que as funções holomorfas (em particular, as constantes) estão neste conjunto. Ou seja, temos $\mathcal{O}_X(U) \subseteq \mathcal{M}(U)$.

Se X é uma superfície de Riemann compacta e $f \in \mathcal{M}(X)$ é não-constante, em cada ponto $x \in X$, definimos a **ordem de anulamento** de f no ponto x da seguinte forma. Tomando uma carta (U, φ) em torno de x, f é interpretada como uma função holomorfa em uma vizinhança (perfurada) de zero. Assim, definimos

$$v_x(f) := \begin{cases} 0 & \text{se } f \text{ é holomorfa em } x \text{ e não se anula em } x, \\ k & \text{se } f \text{ é holomorfa em } x \text{ tem um zero de ordem } k \text{ em } x, \\ -k & \text{se } f \text{ tem um polo de ordem } k \text{ em } x. \end{cases}$$

Em outras palavras, $v_x(f) = m$ se em torno de x, f se escreve como $f = z^m h$ com h holomorfa em x e que não se anula em x.

As funções meromorfas globais admitem uma outra caracterização, fornecida pela proposição abaixo.

Proposição 1.1.12. *Seja X uma superfície de Riemann e $f \in \mathcal{M}(X)$ uma função meromorfa. Defina $\hat{f} : X \to \mathbb{CP}^1$ por*

$$\hat{f}(x) = \begin{cases} \infty := (1:0) & \text{se } f \text{ admite um polo em } x \\ (f(x):1) & \text{caso contrário.} \end{cases}$$

Então, $\hat{f}$ é uma aplicação holomorfa. Reciprocamente, se $F : X \to \mathbb{CP}^1$ é uma aplicação holomorfa não constante igual a ∞, então a sua restrição à $X\backslash F^{-1}(\infty)$ é uma função meromorfa f em X tal que $\hat{f} = F$.

Demonstração. Ver Teorema 1.15 em [For81]. □

Agora, queremos saber se no caso X compacto, temos funções meromorfas globais que não são constantes. A resposta é positiva e isto seguirá das ferramentas de cohomologia de feixes, que serão abordados na próxima seção.

Dadas X e Y superfícies de Riemann e uma aplicação holomorfa $f : X \to Y$, em cada ponto de x, a aplicação f pode ser expressa localmente de um certo tipo.

Proposição 1.1.13. *Seja $f : X \to Y$ uma aplicação holomorfa não-constante entre superfícies de Riemann X e Y. Se $x \in X$, então existem cartas $\varphi : U \to \mathbb{C}$, $\psi : V \to \mathbb{C}$ com $x \in U$ e $f(x) \in V$ tais que $(\psi \circ f \circ \varphi^{-1})(x) = x^d$, com $d \geq 1$.*

Dizemos que d é o **grau de ramificação** (ou **multiplicidade**) de f em x. Ele será denotado por $e_x(f)$. O motivo do nome "multiplicidade" é que para certas vizinhanças V, W de x e $f(x)$, temos que $f^{-1}(y) \cap V$ tem k pontos, para $y \in W$ diferente de $f(x)$.

1.2 Feixes e Cohomologia

Nesta seção, vamos introduzir um conceito importante para o estudo de superfícies de Riemann, principalmente as compactas. Vamos definir os grupos de cohomologia de feixes sobre espaços topológicos a fim de enunciar e demonstrar o teorema de Riemann-Roch.

Definição 1.2.1. Seja X um espaço topológico. Um **feixe** (de grupos abelianos) $\mathcal{F}$ sobre X consiste de

- Um grupo abeliano $\mathcal{F}(U)$ para cada aberto U de X. Seus elementos são as **seções de $\mathcal{F}$ sobre U**.
- Um homomorfismo de grupos $\rho_{U,V} : \mathcal{F}(U) \to \mathcal{F}(V)$ para um par de abertos U, V de X com $V \subseteq U$. Tais homomorfismos são também chamados de **restrições**.

que satisfaz $\rho_{U.W} = \rho_{V,W} \circ \rho_{U,V}$ para quaisquer $W \subseteq V \subseteq U$ abertos de X.

Além disso, $\mathcal{F}$ deve satisfazer mais duas condições adicionais

- (Identidade) Sejam $U \subseteq X$ aberto e $\{U_i\}_{i\in I}$ uma cobertura de U por abertos de U. Se $f, g \in \mathcal{F}(U)$ são tais que $\rho_{U,U_i}(f) = \rho_{U,U_i}(g)$ para todo $i \in I$, então $f = g$. Ou seja, seções sobre um aberto são determinadas por suas restrições.
- (Colagem) Sejam U e $\{U_i\}_{i\in I}$ como no item acima. Se para cada $i \in I$, escolhemos $f_i \in \mathcal{F}(U_i)$ de modo que $\rho_{U_i,U_i\cap U_j}(f_i) = \rho_{U_j,U_i\cap U_j}(f_j)$ para quaisquer $i, j \in I$, então existe $f \in \mathcal{F}(U)$ tal que $\rho_{U,U_i}(f) = f_i$. Podemos pensar em f como sendo a "colagem" das seções f_i.

Para não sobrecarregar a notação, vamos denotar $\rho_{U,V}(f)$ por $f|_V$ e dizer que é a **restrição de** f de U para V. Note que as condições de feixe implicam que $\mathcal{F}(\varnothing) = 0$.

Observação 1.2.2. Se $\mathcal{F}$ satisfaz apenas as duas primeiras condições da definição acima, dizemos que $\mathcal{F}$ é um **pré-feixe** sobre X. Na linguagem de categorias, $\mathcal{F}$ ser um pré-feixe é o mesmo que ser um funtor contravariante $\mathsf{Op}(X) \to \mathsf{Ab}$, onde $\mathsf{Op}(X)$ é a categoria dos abertos de X (os morfismos são as inclusões) e Ab é a categoria dos grupos abelianos.

Exemplo 1.2.3. Vamos dar um exemplo de um pré-feixe que não é feixe. Seja X a união de dois discos disjuntos D_1 e D_2 em $\mathbb{R}^2$ com a topologia induzida pela euclideana. Definimos $\mathbb{Z}$ o seguinte pré-feixe

$$\mathbb{Z}(U) = \begin{cases} \{f : U \to \mathbb{Z} \colon f \text{ constante}\} & U \neq \varnothing \\ 0 & U = \varnothing \end{cases}$$

Então, tomando $f_1 \equiv 0 \in \mathbb{Z}(D_1)$ e $f_2 \equiv 1 \in \mathbb{Z}(D_2)$, segue que f_1 e f_2 são iguais na interseção (que é vazia) mas não existe $f \in \mathbb{Z}(X)$ tal que $f|_{D_1} = f_1$ e $f|_{D_2} = f_2$.

Observação 1.2.4. Apesar da definição acima tratar apenas de feixes de grupos abelianos, pode-se definir de maneira similar feixes de anéis, k-espaços vetoriais ou k-álgebras, onde k é um corpo qualquer.

Os exemplos abaixo mostram que feixes aparecem naturalmente e, de certa forma, expressa a natureza local de alguns conceitos analíticos.

Exemplo 1.2.5. Para X um espaço topológico, temos o feixe $\mathcal{C}$ das funções contínuas com valores reais. Neste caso, $\mathcal{C}(U) = \{f : U \to \mathbb{R} \colon f \text{ contínua}\}$ e os homomorfismos de restrição são precisamente as restrições usuais. Note que $\mathcal{C}$ é um feixe de $\mathbb{R}$-álgebras.

Exemplo 1.2.6. Seja U um aberto de $\mathbb{R}^n$. Então, temos o feixe C^∞ das funções suaves com valores reais. Os grupos abelinos e homomorfismos são dados de maneira similar ao exemplo anterior.

Exemplo 1.2.7. Se X é uma superfície de Riemann, temos o feixe das funções holomorfas, denotado por $\mathcal{O}_X$. Ou seja, para $U \subseteq X$ aberto

$$\mathcal{O}_X(U) = \{f : U \to \mathbb{C} \colon f \text{ é holomorfa}\}$$

e as restrições são as restrições usuais. Note que $\mathcal{O}_X$ é um **subfeixe** do feixe C^∞ e também que $\mathcal{O}_X$ é um feixe de $\mathbb{C}$-álgebras. Se na definição acima, pedimos que f nunca se anule, então obtemos o feixe $\mathcal{O}_X^*$.

Exemplo 1.2.8. Se M é uma variedade suave, além do feixe C^∞ das funções suaves, podem-se obter outros feixes a partir de certas variedades que "se projetam" sobre X, os chamados fibrados diferenciáveis. Como exemplo, temos o feixe Ω^k das k-formas diferenciais com coeficientes suaves.

Ao longo deste capítulo, serão apresentados outros feixes que serão importantes posteriormente.

A próxima definição diz sobre como as seções de um feixe se comportam "ao redor" de um ponto.

Definição 1.2.9. Sejam X um espaço topológico e $\mathcal{F}$ um feixe de grupos abelianos. O **talo** de $\mathcal{F}$ em um ponto $x \in X$, denotado por $\mathcal{F}_x$ é definido como o seguinte colimite

$$\mathcal{F}_x := \varinjlim_{x \in U} \mathcal{F}(U).$$

Além do grupo abeliano, temos homomorfismos $\rho_{U,x} : \mathcal{F}(U) \to \mathcal{F}_x$ para cada aberto U que contém x tais que para $U \supseteq V$ abertos que contém x, o seguinte diagrama comuta:

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\rho_{U,V}} & \mathcal{F}(V) \\ & \searrow^{\rho_{U,x}} & \downarrow{\scriptstyle \rho_{V,x}} \\ & & \mathcal{F}_x \end{array}$$

A noção de colimite vem da teoria das categorias e satisfaz uma certa propriedade universal. Assim, dois colimites são isomorfos por um único isomorfismo (para mais detalhes, veja o Apêndice 3.A de [BT15] ou o Apêndice 3.3 de [Ten08], onde ela é abordada por meio dos chamados *sistemas diretos*). No caso da definição acima, a propriedade universal é descrita explicitamente a seguir.

Sejam A um grupo abeliano e para cada aberto U que contém x, um homomorfismo $\alpha_U : \mathcal{F}(U) \to A$. Suponha ainda que estes homomorfismos satisfazem $\alpha_V \circ \rho_{U,V} = \alpha_U$ para quaisquer abertos U e V que contém x e tais que $V \subseteq U$:

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\rho_{U,V}} & \mathcal{F}(V) \\ & \searrow^{\alpha_U} & \downarrow{\scriptstyle \alpha_V} \\ & & A \end{array}$$

Então, existe um *único* homomorfismo $\alpha : A \to \mathcal{F}_x$ tal que $\alpha_U = \rho_{U,x} \circ \alpha$:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & \mathcal{F}_x \\ & \searrow^{\alpha_U} & \downarrow{\scriptstyle \rho_{U,x}} \\ & & \mathcal{F}(U) \end{array}$$

A seguinte proposição exibe uma construção deste colimite, o que mostra que a definição anterior faz sentido.

Proposição 1.2.10. *Sejam $X, \mathcal{F}$ e x como na definição anterior. Definimos F_x como a seguinte união disjunta*

$$F_x = \bigsqcup_{x \in U} \mathcal{F}(U).$$

Definimos a seguinte relação entre os elementos de F_X: se $f \in \mathcal{F}(U)$ e $g \in \mathcal{F}(V)$, dizemos que

$$f \sim g \iff \exists W \text{ aberto que contém } x,\ W \subseteq U, V \text{ e tal que } f|_W = g|_W .$$

Então, $\sim$ é uma relação de equivalência e existe uma estrutura de grupo abeliano no quociente $F_x/\sim$ induzida pelos $\mathcal{F}(U_i)$. E mais, se definimos $\sigma_{U,x} : \mathcal{F}(U) \to F_x/\sim$ como sendo a composição da inclusão $\mathcal{F}(U) \to F_x$ com a projeção canônica, segue que $F_x/\sim$ junto com estes homomorfismos satisfazem a propriedade universal de colimite.

Esta construção nos diz que podemos pensar nos elementos de $\mathcal{F}_x$ como sendo seções de $\mathcal{F}$ sobre abertos que contém x levando em conta que identificamos seções que se tornam iguais em abertos menores.

Exemplo 1.2.11. Sejam X uma superfície de Riemann e x um ponto de X. O talo de $\mathcal{O}_X$ no ponto x será denotado por $\mathcal{O}_{X,x}$. Então, ele será isomorfo à $\mathbb{C}$-álgebra das séries de potências com raio de convergência positiva, pois duas funções holomorfas em volta de x são iguais se (em alguma carta coordenada) e só se admitem a mesma expansão em série de Taylor.

Exemplo 1.2.12. Sejam U um aberto de $\mathbb{R}^n$ e $x \in U$. Então, para cada $v \in \mathbb{R}^n$ existe um homomorfismo bem definido de $\mathbb{R}$-espaços vetoriais dado pela derivada direcional

$$\begin{aligned} \frac{\partial}{\partial v} : C^\infty_x &\to \mathbb{R} \\ f &\to \frac{\partial f}{\partial v}(x). \end{aligned}$$

De fato, se f e g são representantes de um mesmo elemento de C^∞_x, então suas derivadas direcionais serão iguais, pois ela depende apenas dos valores em uma vizinhança de x. Note que este homomorfismo ainda satisfaz a regra de Leibiniz

$$\frac{\partial}{\partial v}(fg) = f(x)\frac{\partial}{\partial v}(g) + g(x)\frac{\partial}{\partial v}(f).$$

Tais homomorfismos $C^\infty_x \to \mathbb{R}$ são ditos *derivações* em x. O espaço destas derivações costuma ser usado como definição de espaço tangente no contexto de variedades suaves.

Prosseguindo com os feixes, definimos abaixo mapas entre eles.

Definição 1.2.13. Sejam X um espaço topológico e $\mathcal{F}, \mathcal{G}$ feixes sobre X. Um **morfismo de feixes** $\varphi : \mathcal{F} \to \mathcal{G}$ consiste de uma coleção de homomorfismos $\{\varphi_U : \mathcal{F}(U) \to \mathcal{F}(U)\}$, um para cada aberto U de X tal que para quaisquer $V \subseteq U$ abertos, temos a seguinte condição de compatibilidade, expressa no diagrama abaixo

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\varphi_U} & \mathcal{G}(U) \\ {\scriptstyle \rho_{U,V}}\downarrow & & \downarrow{\scriptstyle \rho_{U,V}} \\ \mathcal{F}(V) & \xrightarrow{\varphi_V} & \mathcal{G}(V) \end{array}$$

Observação 1.2.14. Na linguagem de categorias, a definição acima é o equivalente a dizer que φ é uma transformação natural entre (os funtores) $\mathcal{F}$ e $\mathcal{G}$.

Se $\alpha : \mathcal{F} \to \mathcal{G}$ é um morfismo de feixes e $x \in X$, então temos um homomorfismo induzido entre os talos

$$\begin{aligned} \alpha_x : \mathcal{F}_x &\to \mathcal{G}_x \\ [f] &\to [\alpha_U(f)] \end{aligned}$$

onde U é algum aberto que contém x e $f \in \mathcal{F}(U)$.

A seguinte definição nos permite para mostrar a importância dos grupos de cohomologia, como pode ser visto no Teorema 1.2.26:

Definição 1.2.15. Sejam X um espaço topológico e $\mathcal{F}, \mathcal{G}, \mathcal{H}$ feixes sobre X. Sejam $\alpha : \mathcal{F} \to \mathcal{G}$ e $\beta : \mathcal{G} \to \mathcal{H}$ morfismos. Dizemos que

$$0 \longrightarrow \mathcal{F} \xrightarrow{\alpha} \mathcal{G} \xrightarrow{\beta} \mathcal{H} \longrightarrow 0$$

é uma **sequência exata (curta)** se para cada ponto x de X, temos a seguinte sequência exata de grupos abelianos

$$0 \longrightarrow \mathcal{F}_x \xrightarrow{\alpha_x} \mathcal{G}_x \xrightarrow{\beta_x} \mathcal{H}_x \longrightarrow 0 \, .$$

Observação 1.2.16. Usualmente, a definição de sequência exata curta não é feita como acima. Primeiro, se define o que seriam (os feixes) núcleo e imagem de um morfismo de feixes. Enquanto que no caso do núcleo a definição natural funciona, isto não ocorre com a imagem. Esta última necessita de uma etapa adicional, dada pelo processo de *feixificação* de um pré-feixe.

A ideia da feixificação é adicionar todas as colagens de seções em coberturas, de modo que seja satisfeita a propriedade de colagem. Assim, a propriedade que define estas seções se torna mais "local". Por exemplo, a feixificação do feixe $\mathbb{Z}$ do Exemplo 1.2.3, denotada por $\underline{\mathbb{Z}}$ é dada por

$$\underline{\mathbb{Z}}(U) = \begin{cases} \{f : U \to \mathbb{Z} : f \text{ localmente constante}\} & U \neq \varnothing \\ 0 & U = \varnothing \end{cases}$$

Pode-se verificar que $\underline{\mathbb{Z}}_x = \mathbb{Z}$ para todo $x \in X$.

Após definirmos o feixe núcleo e imagem, dizemos que

$$0 \longrightarrow \mathcal{F} \xrightarrow{\alpha} \mathcal{G} \xrightarrow{\beta} \mathcal{H} \longrightarrow 0$$

é uma sequência exata curta se α é injetor, β é sobrejetor e $\operatorname{im} \alpha = \ker \beta$ (como feixes!).

Exemplo 1.2.17. Seja X uma superfície de Riemann. Como $\underline{\mathbb{Z}}$ é um subfeixe de $\mathcal{O}_X$, temos um morfismo de inclusão $\underline{\mathbb{Z}} \to \mathcal{O}_X$. Agora, a função exponencial nos permite definir um morfismo $\exp : \mathcal{O}_X \to \mathcal{O}_X^*$ dado por

$$\begin{aligned} \exp_U : \mathcal{O}_X(U) &\to \mathcal{O}_X^*(X) \\ f : U \to \mathbb{C} &\mapsto (x \mapsto e^{2\pi i f(x)}). \end{aligned}$$

Tomando talos no ponto x, obtemos

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_{X,x} \xrightarrow{\exp_x} \mathcal{O}_{X,X}^* \longrightarrow 0$$

e verificamos que é uma sequência exata. Isto se deve aos seguintes fatos de análise complexa em uma variável

(i) Toda função holomorfa $f : U \to \mathbb{C}$ em $U \subseteq \mathbb{C}$ simplesmente conexo (por exemplo, um disco aberto) que não se anula pode ser expressa como e^g para alguma $g : U \to \mathbb{C}$ holomorfa (veja o Teorema 6.2 de [SS03]).

(ii) Um número complexo z é tal que $e^{2\pi i z} = 1$ se e só se $z \in \mathbb{Z}$.

Assim, concluímos que

$$0 \longrightarrow \underline{\mathbb{Z}} \longrightarrow \mathcal{O}_X \xrightarrow{\exp} \mathcal{O}_X^* \longrightarrow 0$$

é uma sequência exata, chamada **sequência exata exponencial**.

O que faremos a seguir é atribuir a um feixe $\mathcal{F}$ sobre um espaço topológico X (o nosso caso de interesse é quando X é uma superfície de Riemann), certos grupos abelianos. Para isso, introduzimos a seguinte definição

Definição 1.2.18. Um **complexo (de cocadeias)** é uma coleção de grupos abelianos C^k e homomorfismos $d^k : C_k \to C_{k+1}$ representado abaixo

$$\ldots \xrightarrow{d^{-1}} C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} \ldots$$

tais que $d^{k+1} \circ d^k = 0$ para todo k. Costuma-se denotar por $C^\bullet$. A partir de um complexo $C^\bullet$, definimos o **k-ésimo grupo de cohomologia** de $C^\bullet$ como

$$H^k(C^\bullet) := \frac{\ker d^k}{\operatorname{im} d^{k-1}}.$$

Costuma-se dizer que $\ker d^k \subseteq C^k$ é o **grupo dos k-cociclos** e que $\operatorname{im} d^{k-1} \subseteq C^k$ é o **grupo dos k-cobordos**.

Começamos construindo complexos de cocadeias para cada cobertura aberta de X. Se $\mathscr{U} = \{U_i\}_{i \in I}$ é uma cobertura aberta e $q \geq 0$ dizemos que um q-simplexo é uma $(q+1)$-upla de índices de I. Se $\sigma = (i_0, \ldots, i_{q+1})$ é um q-simplexo, denotamos $U_0 \cap \cdots \cap U_{q+1}$ por $|\sigma|$.

A partir daí, definimos o **grupo abeliano das q-cocadeias de $\mathscr{U}$** (com coeficientes em $\mathcal{F}$), denotado por $C^q(\mathscr{U}, \mathcal{F})$, como o conjunto das funções f cujo domínio é o conjunto dos q-simplexos e tal que $f(\sigma) \in \mathcal{F}(|\sigma|)$. Ou seja, é o seguinte produto direto

$$C^q(\mathscr{U}, \mathcal{F}) := \prod_{\sigma\ q\text{-simplexo}} \mathcal{F}(|\sigma|).$$

É imediato que $C^q(\mathscr{U}, \mathcal{F})$ tem uma estrutura natural de grupo, induzida pelos $\mathcal{F}(|\sigma|)$.

Estes serão os grupos abelianos que irão compor o nosso complexo. Para os índices negativos, fazemos $C^q(\mathscr{U}, \mathcal{F}) = 0$. O homomorfismo d^i é definido como

$$\begin{aligned} d^k : C^k(\mathscr{U}, \mathcal{F}) &\to C^{k+1}(\mathscr{U}, \mathcal{F}) \\ f \mapsto d^k f : (i_0, \cdots, i_{q+1}) &\mapsto \sum_{j=0}^{q+1} (-1)^j f(U_{i_0}, \cdots, U_{i_{j-1}}, U_{i_{j+1}}, \cdots, U_{i_{q+1}})\Big|_{U_{i_0} \cap \cdots \cap U_{i_{q+1}}}. \end{aligned}$$

Fazendo as contas se verifica que $d^{k+1} \circ d^k$ para todo $k \geq 0$ (para mais detalhes, veja a Proposição 8.3 do [BT95] para um resultado similar). Assim, a partir do complexo

$$0 \longrightarrow C^0(\mathscr{U}, \mathcal{F}) \xrightarrow{d^0} C^1(\mathscr{U}, \mathcal{F}) \xrightarrow{d^1} C^2(\mathscr{U}, \mathcal{F}) \xrightarrow{d^2} \ldots$$

tomamos os grupos de cohomologia, que denotamos por $H^q(\mathscr{U}, \mathcal{F})$. Apesar de que estejam definidos para $q < 0$, só nos interessam os grupos com $q \geq 0$.

Para que possamos obter grupos de cohomologia independentes da cobertura aberta, tomamos coberturas cada vez mais finas. Se $\mathscr{V} = \{V_j\}_{j\in J}$ é uma outra cobertura aberta de X, dizemos que $\mathscr{V}$ é um **refinamento** de $\mathscr{U}$ via $\tau : J \to I$ se $V_j \subseteq U_{\tau(j)}$ para todo $j \in J$. Assim, temos um mapa induzido

$$\begin{aligned} t^q : C^q(\mathscr{U},\mathcal{F}) &\to C^q(\mathscr{V},\mathcal{F}) \\ f \mapsto t^q(f) : (j_0,\cdots,j_{q+1}) &\mapsto f(\tau(j_0),\cdots,\tau(j_{q+1}))\big|_{V_{j_0}\cap\cdots\cap V_{j_{q+1}}}. \end{aligned}$$

quando $q \geq 0$ e para $q < 0$, fazemos $t^q = 0$. Pode-se verificar que os mapas t^q se encaixam no seguinte diagrama comutativo:

$$\begin{array}{ccccccccc} \cdots & \xrightarrow{d^{q-2}} & C^{q-1}(\mathscr{U},\mathcal{F}) & \xrightarrow{d^{q-1}} & C^q(\mathscr{U},\mathcal{F}) & \xrightarrow{d^q} & C^{q+1}(\mathscr{U},\mathcal{F}) & \xrightarrow{t^{q+1}} & \cdots \\ & & \downarrow{\scriptstyle t^{q-1}} & & \downarrow{\scriptstyle t^q} & & \downarrow{\scriptstyle t^{q+1}} & & \\ \cdots & \xrightarrow{d^{q-2}} & C^{q-1}(\mathscr{V},\mathcal{F}) & \xrightarrow{d^{q-1}} & C^q(\mathscr{V},\mathcal{F}) & \xrightarrow{d^q} & C^{q+1}(\mathscr{V},\mathcal{F}) & \xrightarrow{d^{q+1}} & \cdots \end{array}$$

Então, dizemos que os mapas t^q definem um morfismo $t^\bullet$ entre os complexos $C^\bullet(\mathscr{U},\mathcal{F})$ e $C^\bullet(\mathscr{V},\mathcal{F})$. Daí, cada t^q leva cociclo em cociclo e cobordo em cobordo. Portanto, t^q induz um homomorfismo $\bar{t}^q : H^q(\mathscr{U},\mathcal{F}) \to H^q(\mathscr{V},\mathcal{F})$ entre os grupos de cohomologia.

Se temos outro mapa de refinamento $\tau' : J \to I$, ele induz um outro morfismo $t'^\bullet$ entre $C^\bullet(\mathscr{U},\mathcal{F})$ e $C^\bullet(\mathscr{V},\mathcal{F})$ que por sua vez induz homomorfismos $\bar{t}'^q : H^q(\mathscr{U},\mathcal{F}) \to H^q(\mathscr{V},\mathcal{F})$. Na verdade, estes homomorfismos são os mesmos que foram obtidos a partir dos mapas t^i. Isto é consequência da seguinte proposição

Proposição 1.2.19. *Sejam $\mathscr{V}$ e $\mathscr{U}$ duas coberturas abertas de X e suponha que $\mathscr{V}$ é mais fina que $\mathscr{U}$. Se $\tau,\tau' : J \to I$ são dois mapas de refinamento que induzem morfismos $t^\bullet$ e $t'^\bullet$ entre $C^\bullet(\mathscr{U},\mathcal{F})$ e $C^\bullet(\mathscr{V},\mathcal{F})$, então existem mapas $h^q : C^q(\mathscr{U},\mathcal{F}) \to C^{q-1}(\mathscr{V},\mathcal{F})$, tais que*

$$h^{q+1}\circ d^q + d^{q-1}\circ h^q = t^q - t'^q.$$

Demonstração: Para $q \leq 0$, faça $h^q = 0$. Se $q \geq 1$, definimos h^q como

$$\begin{aligned} h^q : C^q(\mathscr{U},\mathcal{F}) &\to C^{q-1}(\mathscr{V},\mathcal{F}) \\ f \mapsto h^q(f) : \sigma = (j_0,\cdots,j_{q-1}) &\mapsto \sum_{k=0}^{q-1}(-1)^k f(\tau'(j_0),\cdots,\tau'(j_k),\tau(j_k),\cdots,\tau(j_{q-1}))\big|_{|\sigma|}. \end{aligned}$$

E se verifica que cada h^q satisfaz a condição do enunciado (ver a demonstração do Lema 5 da Seção 3 de [Gun66] para detalhes). □

Observação 1.2.20. O que a proposição anterior está dizendo é precisamente que os mapas h^q formam uma *homotopia* entre os morfismos $t^\bullet$ e $t^\bullet$ e eles são ditos *homotópicos*. Morfismos homotópicos induzem os mesmos homomorfimos nos grupos de cohomologia.

De fato, se f_1 e f_2 são dois q-cociclos cuja diferença é um q-cobordo, então existe g tal que $f_1 - f_2 = d^{q-1}g$. Daí

$$\begin{aligned} (t^q - t'^q)(f_1 - f_2) &= h^{q+1}(d^q(f_1 - f_2)) + d^{q-1}(h^q(f_1 - f_2)) \\ &= h^{q+1}((d^q\circ d^{q-1})g) + d^{q-1}(h^q(f_1 - f_2)) \\ &= d^{q-1}(h^q(f_1 - f_2)). \end{aligned}$$

e segue que $\bar{t}^q([f_1]) = \bar{t}'^q([f_2])$.

Portanto, se $\mathscr{V}$ é uma cobertura mais fina que $\mathscr{U}$, temos homomorfismos bem-definidos

$$t^q_{\mathscr{V},\mathscr{U}} : H^q(\mathscr{U},\mathcal{F}) \to H^q(\mathscr{V},\mathcal{F}) \quad q \geq 0.$$

Se $\mathscr{W}$ é uma cobertura mais fina que $\mathscr{V}$, então temos a relação

$$t^q_{\mathscr{W},\mathscr{U}} = t^q_{\mathscr{W},\mathscr{V}} \circ t^q_{\mathscr{V},\mathscr{U}} \quad \forall q \geq 0.$$

Assim, temos um sistema direto de grupos abelianos e homomorfismos, pois dados duas coberturas abertas, pode-se tomar uma mais fina que elas. É o mesmo que vimos quando definimos o talo de um feixe. Daí, tomando o colimite nós finalmente obtemos os grupos de cohomologia desejados.

Definição 1.2.21. Seja X um espaço topológico e $\mathcal{F}$ um feixe de grupos abelianos sobre X. Então, os **grupos de cohomologia de** X (com coeficientes em $\mathcal{F}$) são definimos por

$$H^q(X,\mathcal{F}) := \varinjlim_{\mathscr{U}} H^q(X,\mathscr{U}).$$

Uma construção explícita pode ser fornecida seguindo a Proposição 1.2.10

Observação 1.2.22. Os grupos de cohomologia definidos acima são também chamados os *grupos de cohomologia de Čech*. Na verdade está é uma descrição mais explícita dos grupos de cohomologia definidos de maneira mais abstrata. Tais grupos são definidos da seguinte maneira:

- Começamos fornecendo uma resolução injetiva de $\mathcal{F}$, ou seja, uma sequência exata do tipo:

  $$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G}_0 \longrightarrow \mathcal{G}_1 \longrightarrow \dots$$

  com cada $\mathcal{G}_i$ um objeto injetivo na categoria $\mathsf{Sh}(X)$ dos feixes de grupos abelianos sobre X. Isto é sempre possível neste caso, pois $\mathsf{Sh}(X)$ é dito que possui *injetivos suficientes* (veja a discussão inicial da Seção 4.3 de [Voi03]).

- Daí, aplicamos o funtor $\Gamma : \mathcal{F} \mapsto \mathcal{F}(X)$ das seções globais e obtemos o complexo de grupos abelianos

  $$0 \longrightarrow \mathcal{G}_0(X) \longrightarrow \mathcal{G}_1(X) \longrightarrow \mathcal{G}_2(X) \longrightarrow \dots$$

- Sobre este complexo, tomamos os grupos de cohomologia e estes serão os grupos de cohomologia do feixe $\mathcal{F}$. A princípio, tais grupos dependem da resolução injetiva, mas pode-se mostrar que obtemos grupos abelianos isomorfos. E mais, se uma resolução injetiva é fixada para cada feixe, obtemos um funtor bem-definido $R\Gamma^i : \mathsf{Sh}(X) \to \mathsf{Ab}$ que costuma ser definido como o i-ésimo grupo de cohomologia.

Para mais detalhes sobre esta construção, veja o Capítulo 2 de [Wei94], em especial as seções 2.3 e 2.5, no contexto de categorias abelianas.

Começamos tratando do H^0. Se $\mathscr{U} = \{U\}_{i\in I}$ é uma cobertura aberta de X, então em $C^0(\mathscr{U},\mathcal{F})$ não temos cobordos, mas os cociclos são justamente as escolhas de seções $(f_i)_i$ que são compatíveis nas interseções. Como $\mathcal{F}$ é um feixe, isto significa que $H^0(\mathscr{U},\mathcal{F})$ é isomorfo ao grupo abeliano $\mathcal{F}(X)$ das seçoes globais sobre X. Assim, podemos dizer que $H^0(X,\mathcal{F})$ é $\mathcal{F}(X)$.

No caso do H^1, temos o seguinte lema

Lema 1.2.23. *Sejam $\mathscr{U}$, $\mathscr{V}$ coberturas de X com $\mathscr{V}$ mais fina que $\mathscr{U}$. Então, o homomorfismo*

$$t^1_{\mathscr{V},\mathscr{U}} : H^1(\mathscr{U},\mathcal{F}) \to H^1(\mathscr{V},\mathcal{F})$$

é injetor.

Demonstração. Ver Lema 12.4 de [For81]. □

Daí, segue da definição (explícita) de $H^1(X, \mathcal{F})$ que o homomorfismo

$$t^1_{\mathscr{U}} : H^1(\mathscr{U}, \mathcal{F}) \to H^1(X, \mathcal{F})$$

que vem junto com o colimite é injetor. Portanto, $H^1(X, \mathcal{F}) = 0$ se, e somente se, para toda cobertura aberta $\mathscr{U}$ de X, temos $H^1(\mathscr{U}, \mathcal{F}) = 0$.

No caso de superfícies de Riemann, só vamos nos interessar nos grupos H^0 e H^1. De fato, pode-se mostrar que neste caso, os grupos $H^k(X, \mathcal{F})$ com $k \geq 2$ se anulam para todo $\mathcal{F}$ feixe de grupos abelianos mas isto não será tratado aqui (veja a Seção 5.12 do Capítulo II do [God58]).

Por fim, finalizamos com dois resultados que serão importante para o cálculo dos grupos de cohomologia de feixes. Tais resultados não estão enunciados em suas versões gerais e estão adaptados para tratar apenas dos grupos H^0 e H^1.

O primeiro é o teorema de Leray, que diz que uma cobertura aberta adequada é suficiente para calcular os grupos de cohomologia.

Teorema 1.2.24 (Leray)**.** *Seja $\mathcal{F}$ um feixe de grupos abelianos sobre um espaço topológico X. Suponha que $\mathscr{U} = \{U_i\}_{i \in I}$ é uma cobertura aberta de X tal que $H^1(U_i, \mathcal{F}) = 0$ para todo $i \in I$. Então*

$$H^1(X, \mathcal{F}) \cong H^1(\mathscr{U}, \mathcal{F}).$$

Dizemos que $\mathscr{U}$ é uma cobertura de Leray (de primeira ordem) para o feixe $\mathcal{F}$.

Demonstração. Ver Teorema 12.8 de [For81]. □

Observação 1.2.25. Este resultado pode ser generalizado para coberturas de Leray de ordens superiores nos quais sobre as multi-interseções de até k abertos, o feixe tem cohomologia trivial (para um enunciado preciso, ver Teorema 4.41 de [Voi03] ou o Teorema 5 da Seção 3 de [Gun66]). A ideia principal é que para estas coberturas, a cohomologia de $\mathcal{F}$ é calculada com estas coberturas.

O segundo resultado envolve sequências exatas curtas de feixes. Notamos que dada uma sequência exata

$$0 \longrightarrow \mathcal{F} \xrightarrow{\alpha} \mathcal{G} \xrightarrow{\beta} \mathcal{H} \longrightarrow 0$$

de feixes de grupos abelianos sobre X, então temos uma sequência exata induzida de grupos abelianos

$$0 \longrightarrow \mathcal{F}(X) \xrightarrow{\alpha_X} \mathcal{G}(X) \xrightarrow{\beta_X} \mathcal{H}(X) \ .$$

Nem sempre o mapa β_X é sobrejetor. Porém, podemos "estender" esta sequência exata com os grupos de cohomologia.

Teorema 1.2.26. *Sejam X um espaço topológico e*

$$0 \longrightarrow \mathcal{F} \xrightarrow{\alpha} \mathcal{G} \xrightarrow{\beta} \mathcal{H} \longrightarrow 0$$

uma sequência exata de grupos abelianos. Então, existem homomorfismos δ, α^1 e β^1 tais que

$$0 \longrightarrow \mathcal{F}(X) \xrightarrow{\alpha^0} \mathcal{G}(X) \xrightarrow{\beta^0} \mathcal{H}(X) \xrightarrow{\delta} H^1(X, \mathcal{F}) \xrightarrow{\alpha^1} H^1(X, \mathcal{G}) \xrightarrow{\alpha^2} H^1(X, \mathcal{H})$$

é uma sequência exata de grupos abelianos, onde $\alpha^0 = \alpha_X$ e $\beta^0 = \beta_X$.

Demonstração. Ver Teorema 15.12 de [For81]. □

Observação 1.2.27. Voltando aos grupos de cohomologia abstratos, eles satisfazem uma generalização do Teorema 1.2.26: Se

$$0 \longrightarrow \mathcal{F} \xrightarrow{\alpha} \mathcal{G} \xrightarrow{\beta} \mathcal{H} \longrightarrow 0$$

é uma sequência exata de feixes de grupos abelianos sobre X, então temos uma sequência exata longa

$$0 \longrightarrow \Gamma(\mathcal{F}) \longrightarrow \Gamma(\mathcal{G}) \longrightarrow \Gamma(\mathcal{H}) \xrightarrow{\delta} R\Gamma^1(\mathcal{F}) \longrightarrow R\Gamma^1(\mathcal{G}) \longrightarrow R\Gamma^1(\mathcal{H}) \xrightarrow{\delta} \dots$$

Finalizamos enunciando alguns resultados sobre grupos de cohomologia de certos espaços topológicos. A seguir, X denota uma superfície de Riemann.

Proposição 1.2.28. *Valem os seguintes resultados*

(i) $H^1(X, C^\infty) = 0$, *onde* C^∞ *é o feixe das funções suaves com valores reais (ou complexos).*

(ii) Se X *é simplesmente conexo, então* $H^1(X, \underline{\mathbb{C}}) = H^1(X, \underline{\mathbb{Z}}) = 0$.

(iii) Se $X = X_R = \{z \in \mathbb{C} : |z| < R\}$ *com* $0 < R \leq \infty$, *então* $H^1(X, \mathcal{O}_X) = 0$.

(iv) $H^1(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}) = 0$.

Demonstração. Os itens são respectivamente os Teoremas 12.6, 12.7, 13.4 e 13.5 de [For81]. □

1.3 Superfícies de Riemann Compactas

O objetivo desta seção será aplicar os resultados de cohomologia de feixes para obter resultados sobre superfícies de Riemann compactos. Começamos enunciando alguns resultados preliminares. As demonstrações serão apenas esboçadas com referências para mais detalhes.

Seja X uma superfície de Riemann compacta. Como ela é também uma 2-variedade suave, temos os feixes Ω^1, Ω^2 de formas diferenciais sobre X. Elas podem ser descritas como funções $x \mapsto \omega_x$, $x \in X$ tais que $\omega_x \in \bigwedge^k (T_x X)^*$ ($k = 1$ ou 2) e que localmente são dadas por

$$\omega_x = f(x)dx + g(x)dy \qquad \text{ou} \qquad \omega_x = h(x)dx \wedge dy$$

onde f, g e h são funções suaves com valores reais. Também consideramos as suas complexificações $\Omega^1_{\mathbb{C}}$ e $\Omega^2_{\mathbb{C}}$ onde localmente temos as expressões acima com f, g e h funções suaves com valores complexos.

Vamos analisar o caso das 1-formas diferenciais complexas: No espaço tangente complexificado $(T_x X) \otimes \mathbb{C}$ no ponto $x \in X$, temos uma $\mathbb{C}$-base

$$\left\{ \frac{\partial}{\partial x} \otimes 1, \frac{\partial}{\partial y} \otimes 1 \right\}$$

induzida pelas coordenadas locais $\varphi : p \mapsto (x(p), y(p))$. Se elas são as partes real e imaginária de uma coordenada local holomorfa $\varphi : p \to z(p)$, pode-se mostrar que

$$\left\{ \frac{\partial}{\partial z} := \frac{1}{2}\left(\frac{\partial}{\partial x} \otimes 1 - \frac{\partial}{\partial y} \otimes i \right), \frac{\partial}{\partial \bar{z}} := \frac{1}{2}\left(\frac{\partial}{\partial x} \otimes 1 + \frac{\partial}{\partial y} \otimes i \right) \right\}$$

também é uma $\mathbb{C}$-base de $(T_x X) \otimes \mathbb{C}$ e que tal base independe da coordenada local holomorfa.

Daí, temos a base dual em $(T_x X)^* \otimes \mathbb{C}$ dada por

$$\{dz := dx \otimes 1 + dy \otimes i, d\bar{z} := dx \otimes 1 - dy \otimes i\}.$$

Assim, temos uma decomposição $(T_xX)^* = T^{1,0} \oplus T^{0,1}$ onde $T^{1,0} = \mathbb{C}dz$ e $T^{0,1} = \mathbb{C}d\bar{z}$. Isto nos dá uma decomposição $\Omega^1_{\mathbb{C}} = \Omega^{1,0} \oplus \Omega^{0,1}$ no nível das formas diferenciais.

O mapa de diferencial exterior $d : \Omega^0(X) \to \Omega^1(X)$ de formas diferenciais nos dá um mapa $d : \Omega^0_{\mathbb{C}}(X) \to \Omega^1_{\mathbb{C}}(X)$ entre as formas complexificadas. Ela é dada localmente (nas duas bases discutidas acima) por

$$df = \frac{\partial f}{\partial x}(dx \otimes 1) + \frac{\partial g}{\partial x}(dy \otimes 1) = \frac{\partial f}{\partial z}dz + \frac{\partial f}{\partial \bar{z}}d\bar{z},$$

onde

$$\frac{\partial f}{\partial z} := \frac{1}{2}\left(\frac{\partial f}{\partial x} - i\frac{\partial f}{\partial y}\right) \qquad \text{e} \qquad \frac{\partial f}{\partial \bar{z}} := \frac{1}{2}\left(\frac{\partial f}{\partial x} + i\frac{\partial f}{\partial y}\right).$$

Então, temos uma decomposição $d = \partial + \bar{\partial}$, onde ∂ e $\bar{\partial}$ são dados localmente por

$$\partial f = \frac{\partial f}{\partial z}dz \qquad \text{e} \qquad \bar{\partial} f = \frac{\partial f}{\partial \bar{z}}d\bar{z}.$$

Dentre as 1-formas diferenciais em X com valores complexos, temos o subespaço das **formas diferenciais holomorfas**. Eles são dados localmente por $\omega = fdz$, com f holomorfa. Tais subespaços nos fornecem um subfeixe Ω_X de $\Omega^1_{\mathbb{C}}$.

Observação 1.3.1. Em uma superfície de Riemann X temos a seguinte sequência exata curta de feixes

$$0 \longrightarrow \underline{\mathbb{C}} \longrightarrow \Omega^0_{\mathbb{C}} \xrightarrow{d} \mathcal{L} \longrightarrow 0,$$

onde $\mathcal{L}$ é o subfeixe de $\Omega^1_{\mathbb{C}}$ dado por $\mathcal{L}(U) = \ker(d : \Omega^1_{\mathbb{C}}(U) \to \Omega^2_{\mathbb{C}}(U))$. O motivo do mapa d ser sobrejetor nos talos segue essencialmente do lema de Poincaré (ver Corolário 4.1.1 de [BT95]), que tem como consequência o fato de que toda forma fechada é localmente uma forma exata.

A partir desta sequência exata curta obtemos a sequência exata longa

$$0 \longrightarrow \underline{\mathbb{C}}(X) \longrightarrow \Omega^0_{\mathbb{C}}(X) \xrightarrow{d} \mathcal{L}(X) \longrightarrow H^1(X, \underline{\mathbb{C}}) \longrightarrow H^1(X, \Omega^0_{\mathbb{C}}) \longrightarrow H^1(X, \mathcal{L}) \ .$$

Pela Proposição 1.2.28.i, $H^1(X, \Omega^0_{\mathbb{C}}) = 0$ e segue que

$$H^1(X, \underline{\mathbb{C}}) \cong \frac{\mathcal{L}(X)}{\operatorname{im}(d : \Omega^0_{\mathbb{C}}(X) \to \Omega^1_{\mathbb{C}}(X))} = \frac{\ker(d : \Omega^1_{\mathbb{C}}(X) \to \Omega^2_{\mathbb{C}}(X))}{\operatorname{im}(d : \Omega^0_{\mathbb{C}}(X) \to \Omega^1_{\mathbb{C}}(X))} = H^1_{dR}(X).$$

De fato, o teorema de Čech-De Rham (ver Teorema 8.9 em [BT95] para o caso do feixe $\underline{\mathbb{R}}$ com o auxílio da Obsevação 1.2.25) diz que os grupos de cohomologia de De Rham de X usando as formas diferenciais complexas coincidem com os grupos de cohomologia do feixe constante $\underline{\mathbb{C}}$.

O resultado cohomológico principal é o

Teorema 1.3.2. *Seja X uma superfície de Riemann compacta. Sejam $U \subset V$ abertos de X com $\overline{U} \subset V$. Então, o mapa natural*

$$H^1(V, \mathcal{O}_X) \to H^1(U, \mathcal{O}_X)$$

tem imagem de dimensão finita.

Demonstração: Esta é a versão para X compacto do Teorema 14.9 do [For81]. Ela depende de vários resultados técnicos da Seção 14 que envolvem técnicas de análise e portanto, sua demonstração não será feita aqui. □

A partir do teorema acima, temos o seguinte corolário

Corolário 1.3.3. *Se X é uma superfície de Riemann compacta, então $H^1(X, \mathcal{O}_X)$ tem dimensão finita.*

Os dois próximos corolários envolvem a existência de certas funções meromorfas não-constantes.

Corolário 1.3.4. *Seja X uma superfície de Riemann compacta. Então*

(a) Para $U \subset X$ aberto e $p \in U$, existe uma função meromorfa f que possui um polo em p e é holomorfa em $U\backslash\{p\}$.

(b) Dados $p_1, \ldots, p_n$ pontos distintos de X e $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ existe uma função meromorfa f em X tal que $f(p_i) = \alpha_i$ para $i = 1, \ldots, n$.

Demonstração: Ver os Teorema 14.12 e Corolário 14.13 do [For81], respectivamente. □

Assim, definimos o primeiro invariante de superfícies de Riemann compactas. Ele fará parte do Teorema de Riemann-Roch que será abordado na próxima seção.

Definição 1.3.5. O **gênero (aritmético)** de uma superfície de Riemann compacta é a dimensão de $H^1(X, \mathcal{O}_X)$ sobre $\mathbb{C}$. Denota-se por g_X.

Pela Proposição 1.2.28.iv, segue que $\mathbb{P}^1$ tem gênero zero.

Em relação às formas diferenciais, temos um outro feixe além de Ω_X, que é o feixe das **formas diferenciais meromorfas**, denotado por $\hat{\Omega}_X$. Elas essencialmente são dadas localmente por $f dz$, com f meromorfa. Mais especificamente, define-se da seguinte maneira

- Primeiro, definimos o polo de uma forma diferencial holomorfa em volta de ponto. Seja $U \subset X$ aberto e $x \in U$. Se $\omega \in \Omega_X(U\backslash\{x\})$, então em volta de x é dado por $f dz$. Tomando a expansão em série de Laurent de f em volta de x, caso existam finitos coeficientes não-nulos de ordem negativa, dizemos que ω tem um polo em x.

- Assim, para $U \subset X$ aberto, definimos $\hat{\Omega}_X(U)$ como sendo as formas diferenciais holomorfas em $U\backslash S$ tais que S é discreto e que têm um polo em cada ponto de S.

Se $\omega \in \hat{\Omega}_X(X)$ e $x \in X$, pode-se definir uma ordem de anulamento de ω em x por meio da representação local $\omega = f dz$ e usando a ordem de anulamento de funções meromorfas. Ela é denotada por $v_x(\omega)$. No caso de X compacto, os conjuntos de zeros e polos são finitos.

Encerramos esta seção fazendo alguns comentários sobre aplicações holomorfas. Sejam X, Y superfícies de Riemann compactas e $f : X \to Y$ uma aplicação holomorfa. Vamos assumir que f não é um mapa constante. Começamos com uma afirmação topológica.

Proposição 1.3.6. *Uma aplicação holomorfa $f : X \to Y$ não constante é um mapa aberto, fechado e próprio com fibras discretas.*

Demonstração: Dividimos em quatro partes, uma para cada propriedade a ser verificada:

- f é aberto: O fato de que f é aberto é uma afirmação local. Daí, o resultado segue da Proposição 1.1.13 pois o mapa $z \mapsto z^d$ leva uma vizinhança aberta de zero em uma outra vizinhança aberta de zero.

- f é própria: Se $K \subseteq Y$ é compacto, então $f^{-1}(K) \subseteq X$ é um fechado de um compacto e portanto, é um compacto.

- f possui fibras discretas: Note que se o conjunto $f^{-1}(y) \subseteq X$ não é discreto, então ele admite um ponto de acumulação em X. Daí, pelo teorema da identidade para aplicações holomorfas (ver Teorema 1.11 de [For81]) f seria constante igual a y e obtemos uma contradição.

- f é fechado: Seja $F \subset X$ fechado. Como Y é localmente compacto, é suficiente mostrar que $f(F) \cap K$ é compacto para todo $K \subseteq Y$ compacto. Como f é própria, $\tilde{K} = f^{-1}(K)$ é compacto e $F \cap \tilde{K}$ é compacto. Portanto, $f(F) \cap K = f(F \cap \tilde{K})$ é um compacto de Y.

□

Logo, $f(X)$ será aberto e fechado no conexo Y e obtemos

Corolário 1.3.7. *Toda aplicação holomorfa $f : X \to Y$ entre superfícies de Riemann compactas é constante ou sobrejetora.*

Agora, denotamos por S o conjunto dos pontos de X no qual f se ramifica. Ou seja $S := \{x \in X : e_x(f) > 1\}$. Sua imagem $f(S)$ é o chamado conjunto dos **valores críticos** de f. Notamos que S é um conjunto discreto e portanto, finito, pois X é compacto. Assim, $f(S)$ é um conjunto finito de pontos de Y. Além disso, S é justamente o conjunto dois pontos de X nos quais a restrição de f a uma vizinhança do ponto nunca é injetora.

O próximo lema diz que a restrição de f a $X\backslash S$ é uma aplicação bem comportada. De fato, costuma-se dizer que f é um **recobrimento ramificado**.

Proposição 1.3.8. *Seja $f : X \to Y$ uma aplicação holomorfa não-constante entre superfícies de Riemann compactas e seja $S \subseteq X$ definida como acima. Então, $\bar{f} := f|_{X\backslash S} : X\backslash S \to Y\backslash f(S)$ é um mapa de recobrimento próprio. Em particular, é um recobrimento de grau finito.*

Demonstração: Começamos mostrando que $\bar{f}$ é um homeomorfismo local. Isto segue essencialmente da proposição anterior, já que em uma vizinhança de cada ponto $\bar{f}$ é (em coordenadas locais adequadas) a função identidade e portanto, $\bar{f}$ é injetora. Como f também é aberta, temos um homeomorfismo com a imagem.

Então, $\bar{f}$ é um homeomorfismo local que ainda é um mapa próprio. Segue do Teorema 4.22 do [For81] que f é um mapa de recobrimento próprio. Daí, para $y \in Y\backslash f(S)$ a fibra é um compacto discreto de X e logo finito. Assim, $\bar{f}^{-1}$ consiste de d pontos. Como $Y\backslash f(S)$ é conexo por caminhos, toda fibra de $\bar{f}$ é finita com d pontos. □

Assim, todas as fibras de f sobre valores que não são críticos tem o mesmo número de pontos. Para tratarmos os valores críticos, precisamos levar em conta o índice de ramificação. A seguinte proposição nos permite unificar as duas situações de uma vez.

Proposição 1.3.9. *Seja $f : X \to Y$ uma aplicação holomorfa não-constante entre superfícies de Riemann compactas. Então, a quantidade*

$$n = \sum_{f(x)=y} e_f(x)$$

*independe do ponto $y \in Y$ e dizemos que n é o **grau** de f.*

Demonstração. Seja n o grau do recobrimento $\bar{f} : X\backslash S \to Y\backslash f(S)$. Então, sabemos que $\sum_{\phi(x)=y} = n$ se $y \notin f(S)$. Agora, suponha que $y \in f(S)$ e seja $f^{-1}(y) = \{p_1, \ldots, p_k\}$. Se fazemos $v_f(p_j) = m_j$, então segue da definição que existem vizinhanças U_j de p_j e V_j de y tais que $f^{-1}(y) \cap U_i$ tem m_j pontos com U_j's disjuntos dois a dois.

Como f é um mapa fechado, $F = f(X\backslash(U_1 \cup \cdots \cup U_k))$ também é fechado. Assim, $\tilde{V} = Y\backslash F$ é uma vizinhança de y com $f^{-1}(\tilde{V}) \subseteq U_1 \cup \cdots \cup U_k$. Assim, pode-se tomar $V \subseteq V_1 \cap \cdots \cap V_k$ vizinhança de y tal que $f^{-1}(V) \subseteq U_1 \cup \cdots \cup U_k$. Mas, se $y' \in V$ é diferente de y, então $f^{-1}(y) = \bar{f}^{-1}(y')$ e a fibra $f^{-1}(y')$ consiste de n pontos. Isto implica que

$$n = \#f^{-1}(y') = \sum_{j=1}^{k} \#(f^{-1}(y') \cap U_j) = \sum_{j=1}^{k} m_j.$$

□

Uma aplicação interessante é

Proposição 1.3.10 (Teorema Fundamental da Álgebra)**.** *Todo polinômio de grau n, $n \geq 1$ com coeficientes complexos possui n zeros contando multiplicidades.*

Demonstração. Todo polinômio nos dá uma função holomorfa $P : \mathbb{C} \to \mathbb{C}$. E mais, fazendo $P(\infty) = \infty$, ela pode ser estendida a uma aplicação holomorfa $\mathbb{CP}^1 \to \mathbb{CP}^1$ que também denotamos por P. Pode-se verificar que $e_P(\infty) = n$ e logo, P tem grau n. Assim, se $Z \subseteq \mathbb{C}$ é o conjunto dos zeros de P, temos $\sum_{x \in Z} e_P(x) = n$. O resultado segue pois se x é zero de P, $e_P(x)$ será igual a multiplicidade da raiz x em P. □

1.4 Teorema de Riemann-Roch

Vimos na seção anterior que em uma superfície de Riemann compacta, existem funções meromorfas não-constantes. Agora, estamos interessados em saber se existem e quantas funções meromorfas satisfazem certas condições sobre zeros e polos. Por exemplo, se $p, q \in X$ são pontos distintos, uma possível pergunta é saber se existem funções meromorfas que tem um zero em p de ordem pelo menos 2 e um polo em q de ordem no máximo 3.

Para expressar este tipo de condição, usamos os chamados divisores.

Definição 1.4.1. Seja X uma superfície de Riemann compacta. O **grupo dos divores** de X, denotado por $\mathrm{Div}(X)$, é o grupo abeliano livre gerado pelos pontos de X. Ou seja, os elementos D de x são combinações $\mathbb{Z}$-linares de pontos

$$D = \sum_{x \in X} a_x \cdot x, \quad a_x \in \mathbb{Z}$$

tais que finitos a_x são diferentes de zero.

O grau de um divisor D é definido como a soma de seus coeficientes a_x. Então, obtemos um homomorfismo $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ e temos o subgrupo $\mathrm{Div}^0(X)$ dos divisores de grau 0.

A partir da ordem de anulamento, podemos associar divisores a funções meromorfas.

Definição 1.4.2. Seja X uma superfície de Riemann compacta e $f \in \mathcal{M}(X) \backslash \{0\}$. Definimos o **divisor associado** a f como

$$\mathrm{div}(f) = \sum_{x \in X} v_x(f) \cdot x.$$

Um divisor é dito **principal** se ele é da forma $\mathrm{div}(f)$. Se D e D' são divisores, eles são ditos **linearmente equivalentes** se $D - D'$ é principal. Denotamos isto por $D \sim D'$. É simples verificar que os divisores principais formam um subgrupo de $\mathrm{Div}(X)$. O grupo quociente $\mathrm{Pic}(X)$ é o chamado **grupo de classes de divisores** ou **grupo de Picard** de X.

Uma propriedade que os divisores principais satisfazem é que

Proposição 1.4.3. *Todo divisor principal tem grau zero.*

Demonstração. Seja $f \neq 0$ uma função meromorfa sejam Z e P os conjuntos de zeros e polos de f, respectivamente. Então, temos

$$\mathrm{div}(f) = \sum_{x \in Z} v_x(f) \cdot x + \sum_{x \in P} v_x(f) \cdot x.$$

Mas, se $\hat{f} : X \to \mathbb{CP}^1$ é a aplicação meromorfa associada a f, pode-se mostrar que

$$e_x(f) = \begin{cases} v_x(f) & \text{se } x \in Z \\ -v_x(f) & \text{se } x \in P \end{cases}$$

Daí, segue do Teorema 1.3.9 que

$$\deg(\operatorname{div}(f)) = \left(\sum_{x\in Z} v_x(f)\right) + \left(\sum_{x\in P} v_x(f)\right) = \left(\sum_{\hat{f}(x)=0} e_x(\hat{f})\right) - \left(\sum_{\hat{f}(x)=\infty} e_x(\hat{f})\right) = 0.$$

□

Se $D = \sum_{x\in X} a_x \cdot x, D' = \sum_{x\in X} b_x \cdot x \in \operatorname{Div}(X)$, dizemos que $D \geq D'$ se $a_x \geq b_x$ para todo $x \in X$. É por meio desta relação de ordem parcial que podemos expressar condições sobre zeros e polos de funções meromorfas. Uma discussão mais detalhada está na Observação 2.4.2.

De maneira análoga, podemos associar divisores a formas diferenciais meromorfas.

Definição 1.4.4. Seja X uma superfície de Riemann compacta e $\omega \in \hat{\Omega}_X(X)$ uma forma diferencial meromorfa em X. O **divisor associado** a ω é definido por

$$\operatorname{div}(\omega) = \sum_{x\in X} v_x(\omega) \cdot x.$$

Assim, se $f \neq 0$ é uma função meromorfa não-constante, temos $\operatorname{div}(f\omega) = \operatorname{div}(f) + \operatorname{div}(\omega)$. Assim, se $\omega_1, \omega_2 \in \hat{\Omega}(X)$ são diferentes de zero, então existe $f \neq 0$ meromorfa tal que $\omega_1 = f\omega_2$. Daí, $\operatorname{div}(\omega_1) \sim \operatorname{div}(\omega_2)$ e temos a seguinte definição.

Definição 1.4.5. A **classe canônica** de uma superfície de Riemann compacta, denotada por K_X é a classe de um divisor associado a uma forma diferencial meromorfa ω não-nula. Um **divisor canônica** é um divisor D com $[D] = K_X \in \operatorname{Pic}(X)$.

Agora vamos definir para cada divisor, feixes de funções e formas diferenciais meromorfas sobre X.

Definição 1.4.6. Sejam X uma superfície de Riemann compacta e $D \in \operatorname{Div}(X)$. Definimos os feixes $\mathcal{O}_D$ e $\hat{\Omega}_D$ como

$$\begin{aligned}\mathcal{O}_D(U) &= \{0\} \cup \{f : U \to \mathbb{C} \colon f \neq 0 \text{ meromorfa com } \operatorname{div}(f) \geq -D\}\\ \hat{\Omega}_D(U) &= \{\omega \in \hat{\Omega}_X(U) \colon \operatorname{div}(f) \geq -D\}.\end{aligned}$$

Esclarecemos que nas desigualdades $\operatorname{div}(f)(\text{resp. } \operatorname{div}(\omega)) \geq -D$, $D \in \operatorname{Div}(X)$, queremos dizer que $e_x(f)(\text{resp. } e_x(\omega))$ é maior ou igual a $-a_x$ para todo $x \in U$.

Para $D = 0$, a definição acima nos dá os feixes $\mathcal{O}_X$ e Ω_X respectivamente. Se $D, D' \in \operatorname{Div}(X)$ são linearmente equivalentes, os feixes $\mathcal{O}_D$ e $\mathcal{O}_{D'}$ são isomorfos. De fato, se $\varphi \neq 0$ meromorfa é tal que $\operatorname{div}(\varphi) = D - D'$, então temos um isomorfismo $\alpha : \mathcal{O}_D \to \mathcal{O}_{D'}$ dado por

$$\begin{aligned}\alpha_U : \mathcal{O}_D(U) &\to \mathcal{O}_{D'}(U)\\ f &\mapsto f\varphi.\end{aligned}$$

De maneira análoga, temos um isomorfismo entre $\hat{\Omega}_D$ e $\hat{\Omega}_{D'}$.

Se $\omega \in \hat{\Omega}_X(X)\backslash\{0\}$ e $K = \operatorname{div}(\omega)$, então para todo $D \in \operatorname{Div}(X)$ temos um isomorfismo $\beta : \mathcal{O}_{D+K} \to \Omega_D$ dado por

$$\begin{aligned}\beta_U : \mathcal{O}_{D+K}(U) &\to \hat{\Omega}_D(U)\\ f &\mapsto f\omega.\end{aligned}$$

Em particular, temos $\mathcal{O}_K \cong \Omega_X$. Para a próxima proposição, definimos o seguinte feixe.

Definição 1.4.7. Seja X uma superfície de Riemann compacta. Para $P \in X$, definimos o **feixe arranha-céu**, denotado por $\mathbb{C}_P$, por

$$\mathbb{C}_P(U) = \begin{cases} \mathbb{C} & \text{se } P \in U \\ 0 & \text{se } P \notin U \end{cases}$$

e os mapas de restrição são o mapa trivial ou a identidade. É simples verificar que $(\mathbb{C}_P)_x = 0$ a menos que $x = P$ e neste caso temos $(\mathbb{C}_P)_P = \mathbb{C}$.

Ele tem cohomologia trivial no seguinte sentido

Proposição 1.4.8. *Se X é uma superfície de Riemann compacta, temos $H^0(X, \mathbb{C}_P) = \mathbb{C}$ e $H^1(X, \mathbb{C}_P) = 0$ para todo $P \in X$.*

Demonstração. Ver Seção 16.7 de [For81]. □

A proposição abaixo será importante para a demonstração do Riemann-Roch

Proposição 1.4.9. *Para X superfície de Riemann compacta, $D \in \mathrm{Div}(X)$ e $P \in X$, temos a sequência exata de feixes*

$$0 \longrightarrow \mathcal{O}_D \longrightarrow \mathcal{O}_{D+P} \xrightarrow{\beta} \mathbb{C}_P \longrightarrow 0$$

no qual o primeiro mapa é o mapa de inclusão $\mathcal{O}_D(U) \subseteq \mathcal{O}_{D+P}(U)$.

Demonstração: Primeiro, vamos descrever o mapa β. Para $U \subset X$ aberto:

- Se $P \notin U$, tome β_U o mapa trivial.
- Se $P \in U$, e $f \in \mathcal{O}_{D+P}(U)$, fixamos uma coordenada local z em volta de P tal que $z(P) = 0$. Então em torno de P, f admite uma série de Laurent da forma

  $$f(z) = \sum_{n=-k-1}^{\infty} c_n z^n$$

  onde $k = n_P$ é o coeficiente de P em D. Assim, fazemos $\beta(f) = c_{-k-1}$. Assim, $\beta(U)$ será um homomorfismo de grupos abelianos.

Pode-se verificar que β é um homomorfismo $\mathcal{O}_{D+P} \to \mathbb{C}_P$. E finalmente, a sequência será exata pelas seguintes observações

- Todo mapa de inclusão é injetor nos talos. E mais, para $x \notin P$ temos um isomorfismo $(\mathcal{O}_D)_x \to (\mathcal{O}_{D+P})_x$.
- Se $f \in (\mathcal{O}_{D+P})_P$ é tal que $\beta(f) = 0$, então a ordem de anulamento de f em P é no mínimo $-k$. Logo, f está em $(\mathcal{O}_D)_P$. A recíproca é claramente verdadeira.
- Para todo $a \in \mathbb{C}$, existe $f \in (\mathcal{O}_{D+P})_P$ com $\beta(f) = a$. Isto é claro se existe f com $\beta(f) \neq 0$. Se não for o caso, temos $(\mathcal{O}_D)_P = (\mathcal{O}_{D+P})_P$ e temos $\beta_P = 0$.

□

E finalmente, enunciamos o importantíssimo

Teorema 1.4.10 (Riemann-Roch)**.** *Seja X uma superfície de Riemann compacta. Então, para todo $D \in \mathrm{Div}(X)$, os grupos de cohomologia $H^0(X, \mathcal{O}_D)$ e $H^1(X, \mathcal{O}_D)$ têm dimensão finita sobre $\mathbb{C}$. Além disso, vale a seguinte fórmula*

$$\dim H^0(X, \mathcal{O}_D) - \dim H^1(X, \mathcal{O}_D) = 1 - g_X + \deg D.$$

Demonstração: Antes de começar, destacamos que como os feixes mencionados são também feixes de $\mathbb{C}$-espaços vetoriais, os grupos cohomologia têm uma estrutura de $\mathbb{C}$-espaço vetorial. Dividimos a demonstração em duas partes:

- Primeiro, notamos que o teorema é válido para $D = 0$. Isto segue da Proposição 1.1.10 e do Corolário 1.3.3.
- Depois, fixamos $P \in X$. Vamos mostrar que o teorema vale para D se e somente se vale para $D + P$. A partir da Proposição 1.4.9, temos a sequência exata longa

$$0 \longrightarrow H^0(X, \mathcal{O}_D) \longrightarrow H^0(X, \mathcal{O}_{D+P}) \xrightarrow{\beta_X} H^0(X, \mathbb{C}_P) \xrightarrow{\delta} \dots$$

$$\dots \xrightarrow{\delta} H^1(X, \mathcal{O}_D) \longrightarrow H^1(\mathcal{O}_{D+P}) \longrightarrow H^1(X, \mathbb{C}_P)$$

Como $H^1(X, \mathbb{C}_P) = 0$, temos a sequência acima se quebra em duas

$$0 \longrightarrow H^0(X, \mathcal{O}_D) \longrightarrow H^0(X, \mathcal{O}_{D+P}) \xrightarrow{\beta_X} \operatorname{im} \beta_X \longrightarrow 0$$

$$0 \longrightarrow \frac{H^0(X, \mathbb{C}_P)}{\operatorname{im} \beta_X} \xrightarrow{\delta} H^1(X, \mathcal{O}_D) \longrightarrow H^1(\mathcal{O}_{D+P}) \longrightarrow 0$$

Como $H^0(X, \mathbb{C}_P) = \mathbb{C}$, temos que $\operatorname{im} \beta_X$ e $\frac{H^0(X, \mathbb{C}_P)}{\operatorname{im} \beta_X}$ têm dimensão finita. Logo, $H^0(X, \mathcal{O}_D)$ e $H^1(X, \mathcal{O}_D)$ têm dimensão finita se e somente se $H^0(X, \mathcal{O}_{D+P})$ e $H^1(X, \mathcal{O}_{D+P})$ têm dimensão finita. Neste caso, a partir das identidades

$$\begin{aligned} \dim H^1(X, \mathcal{O}_{D+P}) &= \dim H^0(X, \mathcal{O}_D) + \dim \operatorname{im} \beta_X \\ \dim H^1(X, \mathcal{O}_D) &= (1 - \dim \operatorname{im} \beta_X) + \dim H^1(\mathcal{O}_{D+P}) \end{aligned}$$

obtemos $\dim H^0(X, \mathcal{O}_D) - \dim H^1(X, \mathcal{O}_D) + 1 = \dim H^0(X, \mathcal{O}_{D+P}) - \dim H^1(X, \mathcal{O}_{D+P})$ e concluímos que a fórmula vale para D se e somente se para $D + P$.

Assim, o teorema está demonstrado pois a partir de 0 chegamos a qualquer divisor D somando ou subtraindo uma quantidade finita de pontos. □

Algumas consequências diretas deste teorema são

Corolário 1.4.11. *Se $D \in \operatorname{Div}(X)$ é tal que $\deg D < 0$, temos $H^0(X, \mathcal{O}_D) = 0$ e $\dim H^1(X, \mathcal{O}_D) = 1 - g_X + \deg D$.*

Demonstração. Primeiro, provamos que $H^0(X, \mathcal{O}_D) = 0$. Isto segue a partir da contradição que se obtém ao tomar o grau da desigualdade $\operatorname{div}(f) \geq -D$ para uma suposta $f \neq 0$ em $H^0(X, \mathcal{O}_D)$. Assim, a fórmula para $\dim H^1(X, \mathcal{O}_D)$ segue do Teorema de Riemann-Roch. □

Corolário 1.4.12. *Se X é uma superfície de Riemann compacta, então existe uma aplicação holomorfa não-constante $X \to \mathbb{CP}^1$ com grau no máximo $g_X + 1$.*

Demonstração. Tomamos o divisor $D = (g_X + 1) \cdot P$ com $P \in X$ qualquer. Então, segue do Teorema de Riemann-Roch que

$$\dim H^0(X, \mathcal{O}_D) \geq 1 - g_X + \deg D = 1 - g_X + (g_X + 1) = 2.$$

Ou seja, existe $f \neq 0$ meromorfa não-constante que é holomorfa fora de P e que P é um polo de ordem no máximo $g_X + 1$. Assim, a aplicação induzida $\hat{f} : X \to \mathbb{CP}^1$ é não-constante e tem grau no máximo $g_X + 1$. □

Corolário 1.4.13. *Toda superfície de Riemann de gênero zero é isomorfa a* $\mathbb{CP}^1$.

Demonstração. Pelo corolário anterior, existe $\varphi : X \to \mathbb{CP}^1$ holomorfa não-constante de grau no máximo 1. Então, φ tem grau exatamente um. Isto mostra que φ não se ramifica e é um recobrimento de grau 1. Em particular φ é uma bijeção e será um isomorfismo pois em cada ponto de X, e tomando cartas como na Proposição 1.1.13, f é a função $z \mapsto z$ que é um biholomorfismo. □

Então, o corolário acima nos diz que existe (a menos de isomorfismo) apenas uma superfície de Riemann de gênero zero. Registramos abaixo o seguinte fato que foi demonstrado acima.

Proposição 1.4.14. *Seja $F : X \to Y$ uma aplicação holomorfa não-constante entre superfícies de Riemann compactas. Se F tem grau um, então F é um isomorfismo.*

Uma maneira alternativa de enunciar a fórmula do teorema de Riemann-Roch é por meio da dualidade de Serre. Vamos ser bem breves aqui e apenas enunciaremos o resultado.

Teorema 1.4.15 (Dualidade de Serre)**.** *Seja X uma supefície de Riemann compacta. Então para todo $D \in \mathrm{Div}(X)$, existe um pareamento $\mathbb{C}$-bilinear perfeito*

$$\langle \cdot, \cdot \rangle_D : H^0(X, \Omega_{-D}) \times H^1(X, \mathcal{O}_D) \to \mathbb{C}.$$

Em particular, temos um isomorfismo $H^0(X, \Omega_{-D}) \cong H^1(X, \mathcal{O}_D)^*$.

Demonstração. Este é o resultado da Seção 17.9 do [For81]. Para ver a demonstração completa, veja os resultados da Seção 17. □

Obtemos imediatamente que $H^0(X, \Omega_X)$ tem dimensão g_X. Costuma-se chamar esta dimensão de **gênero (geométrico)** de X. Então, a dualidade de Serre nos diz que os gêneros aritmético e geométrico coincidem.

Observação 1.4.16. De um ponto de vista topológico, uma superfície de Riemann compacta X é uma superfície orientada e fechada. Então, pelo teorema da classificação das superfícies, segue que X é homeomorfa a um g-toro, i.e., uma soma conexa de g toros. Assim, pode-se dizer que X tem g buracos e dizemos que g é o **gênero (topológico)** de X, que vamos denotá-lo por g_X.

Esta quantidade está presente na cohomologia singular de X pois temos $H^1(X, \mathbb{Z}) = \mathbb{Z}^{2\mathrm{g}_X}$. Logo, conclui-se que $b_1 := \dim_{\mathbb{C}} H^1_{dR}(X) = 2\mathrm{g}_X$. Vamos dar uma ideia de como provar que $\mathrm{g}_X = g_X$.

Primeiro, usamos que X é projetivo, ou seja, existe um mergulho holomorfo $X \hookrightarrow \mathbb{CP}^n$ para algum n (o resultado-chave para mostrar isto é o Teorema 17.22 de [For81]). Logo, X satisfaz a chamada *decomposição de Hodge* (ver Corolário 3.2.12 de [Huy04]):

$$H^1_{dR}(X) \cong H^{1,0}(X) \oplus H^{0,1}(X)$$

onde os grupos $H^{1,0}(X)$ e $H^{0,1}(X)$ são grupos de cohomologia de certos complexos de cocadeias (os chamados *grupos de cohomologia de Dolbeault*). Por exemplo:

$$H^{1,0}(X) = \ker(\bar{\partial} : \Omega^{1,0}_{\mathbb{C}}(X) \to \Omega^{1,1}_{\mathbb{C}}(X)) \cong H^0(X, \Omega_X).$$

Mas, os grupos $H^{1,0}(X)$ e $H^{0,1}(X)$ têm a mesma dimensão sobre $\mathbb{C}$ (veja o Corolário já mencionado). Portanto, tomando dimensões, obtemos $2\mathrm{g}_X = 2g_X$ e concluímos o que queríamos.

A partir da dualidade de Serre, temos uma fórmula alternativa do Teorema de Riemann-Roch. É desta maneira que será enunciada a versão para curvas algébricas. No enunciado, $l(D)$ denota a dimensão de $H^0(X, \mathcal{O}_D)$ para $D \in \mathrm{Div}(X)$.

Proposição 1.4.17. *Seja X uma superfície de Riemann compacta. Então, para $D \in \mathrm{Div}(X)$ vale a seginte fórmula*

$$l(D) - l(K - D) = 1 - g_X + \deg D,$$

onde K é um divisor canônico de X.

Demonstração: Sabemos que temos um isomorfismo $\mathcal{O}_{K-D} \cong \Omega_{-D}$. Então, junto com a dualidade de Serre obtemos

$$\begin{aligned} l(D) - l(K - D) &= \dim H^0(X, \mathcal{O}_D) - \dim H^0(X, \mathcal{O}_{K-D}) \\ &= \dim H^0(X, \mathcal{O}_D) - \dim H^1(X, \Omega_{-D}) \\ &= \dim H^0(X, \mathcal{O}_D) - \dim H^1(X, \mathcal{O}_D) \end{aligned}$$

e o resultado segue do Teorema de Riemann-Roch. □

Corolário 1.4.18. *Em uma superfície de Riemann compacta X, todo divisor canônico tem grau $2g_X - 2$.*

Demonstração. Tomando $D = K$ na fórmula acima obtemos

$$\begin{aligned} \deg K &= g_X - 1 + l(K) - l(0) \\ &= g_X - 1 + \dim H^0(X, \mathcal{O}_K) - H^0(X, \mathcal{O}_X) \\ &= g_x - 1 + \dim H^1(X, \Omega_X) - \dim H^0(X, \mathcal{O}_X) \\ &= 2g_x - 2. \end{aligned}$$

□

Corolário 1.4.19. *Seja X uma superfície de Riemann compacta. Se $D \in \mathrm{Div}(X)$ é tal que $\deg D > 2g_X - 2$, então $H^1(X, \mathcal{O}_D) = 0$.*

Demonstração. De fato, se K é um divisor canônico, temos pela dualidade de Serre $H^1(X, \mathcal{O}_D)^* \cong H^0(X, \mathcal{O}_{-D})$. Como $\Omega_{-D} \cong \mathcal{O}_{K-D}$, temos também $H^0(X, \Omega_{-D}) \cong H^0(X, \mathcal{O}_{K-D})$. Pelo corolário anterior, temos $\deg(K - D) < 0$ e o resultado segue do Corolário 1.4.11. □

Além do grau de uma aplicação holomorfa, definimos o seguinte.

Definição 1.4.20. Sejam X, Y supefícies de Riemann compactas e $f : X \to Y$ aplicação holomorfa não-constante. Definimos a **ramificação total** de f, denotado por b_f como a soma

$$b_f = \sum_{x \in X} (e_x(f) - 1).$$

Esta soma está bem-definida pois sabemos que o conjunto $S = \{x \in X : e_x(f) > 0\}$ é finito. Assim, f é não-ramificada se e somente se $b_f = 0$. Assim, concluímos o capítulo enunciando o

Teorema 1.4.21 (Riemann-Hurwitz)**.** *Seja $f : X \to Y$ uma aplicação holomorfa não-constante entre superfícies de Riemann compactas. Temos a seguinte fórmula*

$$\chi_X = n \cdot \chi_Y - b_f$$

onde $\chi_X = 2 - 2g_X$, $\chi_Y = 2 - 2g_Y$ são as características de Euler de X e Y, respectivamente.[1]

Demonstração. Ver o teorema da Seção 17.14 de [For81]. □

[1] Pela Observação 1.4.16, estas quantidades são de fato, as características de Euler no sentido topológico.

Capítulo 2

Curvas Algébricas

Neste capítulo, faremos um estudo introdutório de curvas algébricas. Os resultados aqui obtidos serão utilizados quando estudarmos a descrição algébrica de curvas elípticas. Várias das definições e conceitos apresentados são motivados pela teoria de superfícies de Riemann. Assim como no capítulo anterior, alguns dos resultados serão apenas enunciados mas citamos referências para o leitor interessado.

2.1 Definições Preliminares

Começamos revisando o conceito clássico de variedade algébrica afim. A partir desta seção, faremos a seguinte convenção.

k denota um corpo que será **algebricamente fechado**!

Definição 2.1.1. O **espaço afim n-dimensional sobre** k, denotado por $\mathbb{A}^n_k$ ou $\mathbb{A}^n$ (caso o corpo k esteja implícito), consiste no conjunto das n-uplas $(a_1, \ldots, a_n)$, onde cada a_i está em k.

Definição 2.1.2. Um **conjunto algébrico afim** é um subconjunto de um espaço afim $\mathbb{A}^n$ dado por uma coleção S de polinômios em $k[X_1, \ldots, X_n]$. Tal conjunto será denotado por $V(S)$.

Exemplo 2.1.3. Se $f \in k[X_1, \ldots, X_n]$ é não-constante, então $X = V(f)$ é um conjunto algébrico afim. Se $n = 1$, então X é um conjunto finito de pontos. Porém, se $n \geq 2$, usando o fato de que k é infinito, pode-se mostrar que X é um conjunto infinito.

Se I é o ideal gerado pelo conjunto S, então temos $V(S) = V(I)$. Assim, podemos supor que S é um ideal. E mais, como o anel de polinômios $k[X_1, \ldots, X_n]$ é um anel noetheriano, o conjunto algébrico $V(I)$ pode ser definido por uma quantidade *finita* de polinômios.

Observação 2.1.4. O conjunto $\mathbb{A}^n$, ao contrário de k^n, não terá uma estrutura de k-espaço vetorial, apesar de ter os mesmos elementos. Assim, não temos uma definição precisa de *dimensão* neste contexto. Mas veremos adiante uma maneira de atribuir uma dimensão a um dado conjunto algébrico afim. Com esta definição, $\mathbb{A}^n$ terá, de fato, dimensão n.

Neste capítulo iremos estudar estes objetos, só que de um ponto de vista geométrico. E como todo espaço que merece o nome de *geométrico*, precisamos definir uma certa topologia sobre ele. Para isso, basta definir para os espaços afins $\mathbb{A}^n$.

Proposição 2.1.5. *Os conjuntos algébricos afins, formam os fechados de uma topologia em $\mathbb{A}^n$, chamada de* ***topologia de Zariski****.*

Demonstração: Basta mostrar que os conjuntos da forma $V(I)$, com I ideal satisfazem as propriedades dos fechados. Por exemplo, se $(I_\alpha)_\alpha$ é uma família de ideais, então se verifica facilmente que

$$\bigcap_\alpha V(I_\alpha) = V\left(\sum_\alpha I_\alpha\right).$$

□

Assim, para cada conjunto algébrico afim, atribuímos a topologia de subespaço induzida pelo espaço afim ambiente.

Exemplo 2.1.6. Considere o conjunto algébrico afim $X = V(Y - X^2) \subseteq \mathbb{A}^2$ que pode ser interpretado como uma "parábola". Então, como o ponto $(-1, 1) \in X$ é um fechado de A^2, segue que $U = X\backslash\{(-1, 1)\}$ é um aberto de X. Em geral, os abertos de um conjunto algébrico afim costumam ser muito grandes. Isto abre possibilidade para os chamados *espaços irredutíveis* como será visto adiante.

No contexto de superfícies de Riemann, além dos espaços, estudamos funções cujo domínio é (um aberto do) espaço. Neste caso, as nossas funções serão definidas por polinômios

Definição 2.1.7. Seja $X = V(I) \subseteq \mathbb{A}^n$ um conjunto algébrico afim. Uma **função regular (global) sobre** X é uma função $f : X \to k$ que coincide com uma função polinômial. Ou seja, existe $p \in k[X_1, \ldots, X_n]$ tal que $f(a_1, \ldots, a_n) = p(x_1, \ldots, x_n)$ para todo $(a_1, \ldots, a_n) \in X$. Denotamos o conjunto de tais funções por $k[X]$.

Notamos que este polinômio nem sempre é unicamente determinado. Considere por exemplo, a parábola $X = V(Y - X^2)$. Então, os polinômios Y e X^2 definem a mesma função regular $f : X \to k$. Assim, a partir do mapa natural

$$k[X_1, \ldots, X_k] \twoheadrightarrow k[X]$$

obtemos o seguinte resultado.

Proposição 2.1.8. *Dado um conjunto algébrico afim $X \subseteq \mathbb{A}^n$, temos o seguinte isomorfismo de k-álgebras.*

$$k[X] \cong \frac{k[X_1, \ldots, X_n]}{I(X)},$$

onde $I(X)$ é o ideal dos polinômios que se anulam identicamente em X, também chamado ***ideal de*** *X.*

Dizemos que $k[X]$ é o **anel das coordenadas** de X. O nome se deve ao fato de que ele é gerado como k-álgebra pelas funções coordenadas $x_1, \ldots, x_n$. A seguinte proposição nos diz que o anel de coordenadas $k[X]$ é reduzido.

Proposição 2.1.9. *Se $f \in k[X]$ é tal que existe $n \geq 1$ tal que $f^n = 0$, então $f = 0$.*

Demonstração: Isto segue simplesmente do fato de que como k não possui divisores de zero, $f(x)^n = 0$ se e somente se $f(x) = 0$. □

Isto implica que o ideal $I(X)$ é sempre um ideal radical. Além disso, é fácil verificar que $V(I(X)) = X$. Assim, $X = V(I) = V(I(X))$, o que mostra que podemos ter dois ideais que definem um mesmo conjunto algébrico. Porém, quando k é algebricamente fechado, uma das consequências do Nullstellensatz (ver Teorema 9.3.4 de [BT15]) é que existe um único ideal I tal que I é radical e $V(I) = X$, que será precisamente $I(X)$.

Observação 2.1.10. Se o corpo base k não fosse algebricamente fechado, então tal resultado não seria verdadeiro. Por exemplo, para $k = \mathbb{Q}$, os ideais radicais (de fato, primos) $\langle x^2 + y^2 + 1\rangle$ e $\langle x^4 + y^4 + 1\rangle$ geram o conjunto vazio como conjunto algébrico.

De agora em diante, vamos assumir que o ideal $I(X)$ é primo. Faremos isso por dois motivos: um é que o anel de coordenadas $k[X]$ será um domínio de integridade, no qual podemos tomar o corpo de frações e também por conta de X consistir apenas de um "pedaço" como diz a seguinte

Proposição 2.1.11. *Seja $X \subseteq \mathbb{A}^n$ um conjunto algébrico afim. Então $I(X)$ é primo se e somente se X é **irredutível**, ou seja, não pode ser escrito como $X = X_1 \cup X_2$, onde X_1 e X_2 são conjuntos algébricos propriamente contidos em X.*

Demonstração: Ver Proposição 2.3.18 de [BT15]. □

Em um conjunto algébrico afim irredutível X, todo aberto é denso. De fato, se $U, V \subseteq X$ são abertos não-vazios, então não podemos ter $(X\backslash U) \cup (X\backslash V) = X$. Daí, tomando complementares, concluímos que $U \cap V \neq \varnothing$. Assim, os abertos de um conjunto algébrico afim, que sabemos que são grandes, têm a possibilidade de serem densos.

Exemplo 2.1.12. Seja $X = V(XY) \subseteq \mathbb{A}^2$ o conjunto algébrico formado pelos eixos. Então, X *não* é irredutível, pois temos os fechados próprios $V(X)$ e $V(Y)$ cuja união é todo o X. Isto também é visto no anel de coordenadas, pois como $I(X) = \langle XY \rangle$, segue do Teorema Chinês dos Restos (ver Teorema 1.5.1 do [BT15]) que

$$k[X] \cong \frac{k[X,Y]}{\langle XY \rangle} = \frac{k[X,Y]}{\langle X \rangle} \times \frac{k[X,Y]}{\langle Y \rangle} \cong k[X] \times k[X]$$

que não é domínio.

Com isso, introduzimos mais uma definição

Definição 2.1.13. Uma **variedade algébrica afim** é um conjunto algébrico afim $X \subseteq \mathbb{A}^n$ irredutível, ou equivalentemente, tal que $I(X)$ é um ideal primo.

Além do anel de coordenadas $k[X]$, em uma variedade algébrica afim temos o seu **corpo de funções**, que definimos como sendo o corpo de frações de $k[X]$. Ele é denotado por $k(X)$. Podemos interpretá-los como funções da seguinte forma: seja f um elemento não-nulo de $k(X)$ e seja x_0 um ponto de X. Se existem $p, q \in k[X]$ tais que $f = \frac{p}{q}$ e $q(x_0) \neq 0$, então dizemos f é **regular em** x_0 e definimos $f(x_0)$ como sendo $\frac{p(x_0)}{q(x_0)}$. Isto independe da fração escolhida, desde que o denominador não se anule em x_0.

Exemplo 2.1.14. Como $k[X] \subseteq k(X)$, toda função polinomial $X \to k$ está no corpo de funções e é regular em todo ponto de X.

Exemplo 2.1.15. Sobre a reta afim $V = \mathbb{A}^1$, temos $k(V) = k(X)$, o corpo das funções racionais em uma variável X, e temos os seguintes exemplos:

- O elemento $\frac{1}{X}$ nos dá uma função regular sobre o aberto $\mathbb{A}^1\backslash\{0\}$.
- O elemento $\frac{1}{(X-1)(X-2)}$ nos dá uma função regular sobre o aberto $\mathbb{A}^1\backslash\{1,2\}$.

Observação 2.1.16. Assim, podemos ver cada $f \in k(X)$ como uma função $U \to k$, onde U é um aberto de X. Nem sempre a função f é regular em todo o X. Além disso, se $f \in k(X)$ é regular em todos os pontos de um aberto U de X, isto não significa que temos uma fração "global" de modo que $f = \frac{p}{q}$ com $q(x_0) \neq 0$ para todo $x_0 \in U$ como mostra o seguinte exemplo.

Exemplo 2.1.17. Seja $X = V(XY - ZW) \subseteq \mathbb{A}^4$ e considere o elemento $f_0 = \frac{X}{W}$. Então $f_0 = \frac{Z}{Y}$ e segue que f_0 define uma função regular sobre o aberto $U = X\backslash V(Y, W)$ mas que admite duas representações.

Para definir a dimensão de uma variedade algébrica afim, utilizamos o conceito de grau de transcendência de uma extensão de corpos K/k.

Definição 2.1.18. Seja X uma variedade algébrica afim. Então, a **dimensão de** X, denotada por $\dim X$, é definida como o grau de transcendência da extensão $k(X)/k$.

Observação 2.1.19. Existe uma definição mais geral de dimensão para espaços topológicos. Ela é definida como o tamanho máximo de uma cadeia de fechados irredutíveis:

$$\dim X := \sup\{n \geq 0 : \exists X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \subseteq X \text{ com } X_i \text{ fechado irredutível}\}.$$

Também temos o conceito de dimensão para anéis (comutativos), a chamada **dimensão de Krull**. Ela é dada por

$$\dim R := \sup\{n \geq 0 : \exists \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subseteq R \text{ com } \mathfrak{p}_i \text{ ideal primo}\}.$$

No caso de X ser uma conjunto algébrico afim, pelo Nullstellenstaz e pela Proposição 2.1.11, concluímos que $\dim X = \dim k[X]$. E mais, caso X seja uma variedade afim, segue do Teorema 9.2.1 de [BT15] que $\dim k[X]$ é o grau de transcendência de $\operatorname{Frac} k[X] = k(X)$ sobre k.

Exemplo 2.1.20. Se $X = \mathbb{A}^n$, temos $k(X) = k(X_1, \ldots, X_n)$ e segue que X tem dimensão n.

Exemplo 2.1.21. Pode-se mostrar que $X \subseteq \mathbb{A}^n$ é uma variedade afim de dimensão $n-1$ se e somente se $X = V(f)$ para f irredutível e não-constante. Para mais detalhes, veja a Proposição I.1.13 do [Har77].

A seguir, definimos o conceito de ponto singular. Intuitivamente, é esperado que um ponto seja suave se seu espaço tangente tem a mesma dimensão da variedade. Assim, o ponto $(0,0)$ da variedade afim $C : y^2 = x^3 + x^2$ não seria suave, pois ele possui duas retas tangentes, a saber $y = x$ e $y = -x$.

Primeiro, definimos o anel local de um ponto.

Definição 2.1.22. Seja $X \subseteq \mathbb{A}^n$ uma variedade afim. Então, o **anel local de** X **em** x, denotado por $\mathcal{O}_{X,x}$ é definido como

$$\mathcal{O}_{X,x} = \{f \in k(X) : f \text{ é regular em } x\}.$$

Pode-se mostrar que $\mathcal{O}_{X,x}$ é a localização de $k[X]$ em relação ao ideal maximal $\mathfrak{m}_x$ das funções que se anulam em x e também que $\dim \mathcal{O}_{X,x} = \dim X$ (veja o Teorema 3.2.c do Capítulo I de [Har77]). Assim, $\mathcal{O}_{X,x}$ é de fato um anel local, cujo corpo de frações é $k(X)$.

Definição 2.1.23. O **espaço tangente a** x de uma variedade afim $X \subseteq \mathbb{A}^n$ é definido como o dual do k-espaço vetorial $\mathfrak{m}_x/\mathfrak{m}_x^2$. Ele é denotado por $T_x X$.

Assim, x é dito **não-singular** ou **liso** se $\dim_k T_x X = \dim X$. Isto é o mesmo que dizer que $\mathcal{O}_{X,x}$ é um *anel local regular*[1].

Exemplo 2.1.24. Considere as seguintes variedades afins

$$X = V(Y^2 - X^3 - X) \quad \text{e} \quad Y = V(Y^2 - X^3 - X^2)$$

Pelo Exemplo 2.1.21, ambas têm dimensão um. Seja $P = (0,0)$. Daí, temos que para X e Y, o ideal maximal $\mathfrak{m}_P$ é gerado por X e Y. Assim, $\mathfrak{m}_P^2$ é gerado por X^2, XY e Y^2. No caso do X, temos $X = Y^2 - X^3 \equiv 0 \pmod{\mathfrak{m}_P^2}$, o que implica que $\mathfrak{m}_P/\mathfrak{m}_P^2 = \langle Y \rangle$. Portanto, P é um ponto liso de X. Porém, no caso de Y, sua equação não nos dá uma relação entre X e Y modulo $\mathfrak{m}_P^2$. Assim, $\mathfrak{m}_P/\mathfrak{m}_P^2$ é gerado por X e Y e segue que $\dim T_P Y = 2$. Neste caso, P é um ponto singular de Y.

[1] Dizemos que um anel local $(A, \mathfrak{m}, k)$ é *regular* se $\dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2$.

Existe uma outra caracterização, mais concreta, dos pontos não-singulares. Ela é motivada pelo critério jacobiano utilizado para decidir se um ponto de um conjunto de zeros de funções suaves é regular.

Proposição 2.1.25. *Sejam $X \subseteq \mathbb{A}^n$ uma variedade afim, x um ponto de X e $f_1, \ldots, f_m$ geradores de $I(X)$. Então, x é não-singular se e somente se a "matriz jacobiana"*

$$\left[\frac{\partial f_i}{\partial x_j}(x)\right]_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$$

tem posto $n - \dim X$.

Demonstração: Ver Teorema 5.1 do Capítulo I de [Har77]. □

Exemplo 2.1.26. Seja $X = V(f) \subseteq \mathbb{A}^n$, onde $f \in k[X_1, \ldots, X_n]$ é um polinômio irredutível não-constante. Então, pelo Exemplo 2.1.21, X tem dimensão $n-1$. Daí, para $P \in X$, segue da proposição acima que P é um ponto liso se e somente se o seu "vetor gradiente"

$$\left[\frac{\partial f}{\partial X_1}(P) \quad \frac{\partial f}{\partial X_2}(P) \quad \cdots \quad \frac{\partial f}{\partial X_n}(P)\right]$$

é não-nulo. Podemos aplicar isto às variedades do Exemplo 2.1.24 para concluir novamente que $P = (0,0)$ é um ponto liso de $X = V(Y^2 - X^3 - X)$ e P é um ponto singular de $Y = V(Y^2 - X^3 - X^2)$.

2.2 Variedades Projetivas

Agora, introduzimos outra classe de espaço ambiente para as variedades algébricas

Definição 2.2.1. O **espaço projetivo n-dimensional sobre** k, denotado por $\mathbb{P}^n_k$ ou $\mathbb{P}^n$, consiste no conjunto das $(n+1)$-uplas $(a_0, \ldots, a_n)$ com $a_i \in k$, diferentes de $(0, \ldots, 0)$, onde identificamos duas delas quando elas são múltiplas uma da outra por um elemento não-nulo de k. Assim,

$$\mathbb{P}^n_k = (k^{n+1}\backslash\{0\})/\sim,$$

onde $a \sim b \iff a = \lambda b$, $\lambda \in k^*$. A classe de equivalência de $(a_0, \ldots, a_n)$ é denotada por $(a_0 : \cdots : a_n]$.

Se queremos definir subconjuntos de $\mathbb{P}^k$ dados por zeros de polinômios, vamos considerar apenas polinômios homogêneos.

Definição 2.2.2. Um **conjunto algébrico projetivo** é um subconjunto de um espaço projetivo $\mathbb{P}^n$ dado por uma coleção S de polinômios homogêneos em $k[X_0, \ldots, X_n]$. Tal conjunto será denotado por $Z(S)$.

Pode-se mostrar de maneira similar ao caso afim que os conjuntos algébricos projetivos de $\mathbb{P}^n$ formam os fechados de uma topologia, também chamada **topologia de Zariski**. Assim, cada conjunto algébrico projetivo possui a topologia de subespaço de $\mathbb{P}^n$.

Se I é o ideal gerado por S, então I é o que é chamado de *ideal homogêneo*. Além disso, se definirmos para J ideal homogêneo

$$Z(J) = \bigcap_{f\in J \text{ homogêneo}} Z(f),$$

então temos $Z(S) = Z(I)$ e logo, podemos assumir que S é um ideal homogêneo. E novamente, usando o fato de que $k[X_0, \ldots, X_n]$ é noetheriano, temos que $Z(J)$ pode ser definido por uma quantidade finita de polinômios homogêneos.

Definimos o **ideal de** X, denotado por $I(X)$, como sendo o ideal homogêneo gerado pelos polinômios homogêneos $f \in k[X_0, \ldots, X_n]$ tais que f se anula identicamente em X. Ele é um ideal radical de $I(X)$ com $X = Z(I(X))$. Logo, todo conjunto algébrico projetivo é definido por um ideal radical.

Imitando a Proposição 2.1.8, definimos o **anel de coordenadas de** X como sendo a seguinte k-álgebra

$$k[X] \cong \frac{k[X_0, \ldots, X_n]}{I(X)}.$$

Ao contrário do caso afim, esta álgebra não possui uma interpretação como funções $X \to k$.

Observação 2.2.3. Destacamos que o espaço projetivo $\mathbb{P}^n$ pode ser visto como a colagem de $n+1$ espaços afins. De fato, para cada $0 \leq i \leq n$, temos a seguinte bijeção

$$\begin{aligned} \varphi_i : \mathbb{A}^n &\to U_i \\ (a_1, \ldots, a_n) &\mapsto (a_1 : \cdots : a_{i-1} : 1 : a_i : \cdots : a_n) \end{aligned}$$

onde $U_i = \{(a_0 : \cdots : a_n) \in \mathbb{P}^n : a_i \neq 0\}$ e temos $\mathbb{P}^n = U_0 \cup \cdots \cup U_n$. Isto acaba passando para os conjuntos algébricos projetivos, de modo que podemos pensar que o conjunto $X = Z(I)$, para I ideal homogêneo, é uma colagem de $n+1$ conjuntos algébricos afins.

Por exemplo, seja $X = Z(zy - x^2) \subseteq \mathbb{P}^2$. Então, temos bijeções

$$\varphi_0 : V(zy - 1) \to X \cap U_0, \quad \varphi_1 : V(z - x^2) \to X \cap U_1, \quad \varphi_2 : V(y - x^2) \to X \cap U_2.$$

E mais, como cada U_i é um aberto de $\mathbb{P}^2$, podemos dizer que cada $X \cap U_i$ é um "aberto afim" de X. Isto também ocorre em geral e é razoável pensar em estender conceitos de variedades afins para projetivas tomando "vizinhanças afins".

Aqui temos uma definição análoga de variedade afim

Definição 2.2.4. Um conjunto algébrico $X \subseteq \mathbb{P}^n$ é dito uma **variedade projetiva** se ela é irredutível.

Existe um resultado análogo à Proposição 2.1.11, ou seja, que X é irredutível se e somente se ideal homogêneo $I(X)$ é primo (veja o Exercício 2.4.b do [Har77]).

Exemplo 2.2.5. Vamos chamar de **reta** um conjunto algébrico X definido por uma equação $F = 0$, onde $F \in k[X_0, \ldots, X_n]$ é não-constante e da forma $a_0X_0 + \cdots + a_nX_n$. Se $p \in k[X_0, \ldots, X_n]$ se anula em X, então por uma versão projetiva do Nullstellensatz, temos que p está no radical do ideal $\langle F \rangle$. Como F é irredutível, $\langle F \rangle$ é primo e portanto, radical. Logo, $p \in \langle F \rangle$ e segue que $I(X) = \langle F \rangle$. Assim, X é uma variedade projetiva.

Exemplo 2.2.6. Usando o mesmo raciocínio, se $F \in k[X_0, \ldots, X_n]$ é um polinômio homogêneo e irredutível, $Z(F)$ é uma variedade projetiva chamada de *hipersuperfície*.

Seja $X \subseteq \mathbb{A}^n$ uma variedade afim. Podemos injetá-lo em $\mathbb{P}^n$ por algum dos mapas φ_i. Por conveniência, escolhemos o mapa φ_0. Definimos o **fecho projetivo** de X, denotado por $\bar{X}$, como sendo o conjunto algébrico $\bar{X} = Z(S)$, onde

$$S = \{f_h : f \in I(X)\}$$

e p_h é a homogenização do polinômio $p \in k[X_1, \ldots, X_n]$ em relação a uma nova variável X_0.

Observação 2.2.7. Se tivéssemos escolhido outro φ_i precisaríamos renumerar as variáveis como

$$(X_1, \ldots, X_n) \to (X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n).$$

Daí, homogenizamos em relação a uma nova variável X_i.

A proposição abaixo diz algumas de suas propriedades.

Proposição 2.2.8. *Se $X \subseteq \mathbb{A}^n$ é uma variedade afim, então $\bar{X}$ é uma variedade projetiva e é o fecho de $\varphi_i(X)$ na topologia de Zariski. Além disso, se $Y \subseteq \mathbb{P}^n$ é uma variedade projetiva e $0 \leq i \leq n$ é tal que $Y \cap U_i \neq \varnothing$, então $Y \cap U_i$ é uma variedade afim com fecho projetivo Y.*

Demonstração: Para a primeira afirmação, isto segue do Exercício 2.9 do [Har77]. Para a segunda afirmação, basta provar que as bijeções $\varphi_i : \mathbb{A}^n \to U_i$ na Observação 2.2.3 sao homeomorfismos (para uma demonstração veja a Proposição 2.2 do Capítulo I de [Har77]). Daí, o resultado segue do fato que um aberto não-vazio de um irredutível Y é irredutível e denso em Y. □

Costuma-se dizer, para $X \subseteq \mathbb{P}^n$ variedade projetiva, que os pontos de $X \cap \{X_0 = 0\}$ são chamados **pontos no infinito** de X.

Exemplo 2.2.9. No caso de cônicas, isto é, variedades projetivas contidas em $\mathbb{P}^2$ definidas por polinômios homogêneos de grau dois, os pontos no infinito podem ser interpretados como direções assintóticas:

- Para a parábola afim $V(Y - X^2)$, o seu fecho projetivo é dado por $V(YZ - X^2)$ e tem como único ponto no infinito o ponto $(0 : 1 : 0)$. Tal ponto corresponde ao vetor $(0, 1)$ que nos dá a reta vertical $X = 0$.
- Para a hipérbole afim $V(XY - 1)$, o seu fecho projetivo é dado por $V(XY - Z^2)$. Neste caso, temos dois pontos no infinito, que são $(0 : 1 : 0)$ e $(1 : 0 : 0)$. Tais pontos correspondem aos vetores $(0, 1)$ e $(1, 0)$, que nos dão as retas $Y - X = 0$ e $Y + X = 0$.

Para estender as definições dadas na seção anterior, somos guiados pela Observação 2.2.3 e pela proposição acima.

Definição 2.2.10. Seja $X \subseteq \mathbb{P}^n$ uma variedade projetiva. A **dimensão de** X, denotada por $\dim X$, é definida como sendo a dimensão de algum $X \cap U_i$.

Definição 2.2.11. O **corpo de funções** de uma variedade projetiva $X \subseteq \mathbb{P}^n$ é o corpo de funções de algum $X \cap U_i$. Ele será denotado por $k(X)$.

Definição 2.2.12. Seja $X \subseteq \mathbb{P}^n$ uma variedade projetiva e seja $x_0 \in X$. Dizemos que x_0 é um **ponto liso** de X se ele é ponto liso de $X \cap U_i$ para algum $0 \leq i \leq n$.

Definição 2.2.13. Seja $X \subseteq \mathbb{P}^n$ uma variedade projetiva e seja x_0 um ponto de X. O **anel local de** X **em** x_0, denotado por $\mathcal{O}_{X,x_0}$, é o anel local de $X \cap U_i$ em x_0 para algum i.

Mais adiante, forneceremos outras descrições de alguns dos objetos definidos acima.

Observação 2.2.14. Se k é um corpo perfeito, é possível que uma variedade algébrica (afim ou projetiva) X é tal que $I(X)$ é gerado por polinômios com coeficientes em k. Neste caso, dizemos que X é **definido sobre** k e denotamos isto por X/k. No caso afim, temos outro anel de coordenadas

$$k[X] := \frac{k[X_1, \ldots, X_n]}{I(X) \cap k[X_1, \ldots, X_n]}$$

que será um domínio, cujo corpo de frações denotamos por $k(X)$.

Como k é perfeito, a extensão infinita $\bar{k}/k$ é galoisiana, pois $\bar{k}$ coincide com o fecho separável, com grupo de Galois G_k. Assim, para X/k, o grupo G_k age em $\bar{k}[X]$ e $\bar{k}(X)$ e pode-se mostrar que os conjuntos dos G_k-invariantes são identificados com $k[X]$ e $k(X)$, respectivamente. Estas afirmações também se estendem para variedades projetivas pois são definidos a partir de variedades afins.

2.3 Curvas e seus Morfismos

Nesta seção, vamos focar em uma classe de variedades projetivas, que são as curvas. Desta vez, k irá denotar um corpo perfeito[2]. Recordamos que uma variedade projetiva $X \subseteq \mathbb{P}^n_{\bar{k}}$ é **definida sobre** k se o ideal $I(X)$ pode ser gerado por polinômios homogêneos com coeficientes em k.

Definição 2.3.1. Uma **curva (projetiva)** é uma variedade projetiva $X \subseteq \mathbb{P}^n_{\bar{k}}$ de dimensão um.

Em um ponto liso de X, o anel local de X neste ponto é bem comportado no seguinte sentido.

Proposição 2.3.2. *Sejam X uma curva e $x \in X$ um ponto liso. Então, $\mathcal{O}_{X,x}$ é um anel de valorização discreta.*

Demonstração: Segue das hipóteses do enunciado que $\mathcal{O}_{X,x}$ é um anel local regular de dimensão um. Daí, segue da Proposição 9.2 de [AM18] que $\mathcal{O}_{X,x}$ é um anel de valorização discreta. □

Assim, para cada $f \in \bar{k}(X)$ regular em x_0, ou seja, um elemento de $\mathcal{O}_{X,x}$, podemos atribuir um "peso", dado pela valorização de $\mathcal{O}_{X,x}$

$$\begin{aligned} v_x : \mathcal{O}_{X,x}\backslash\{0\} &\to \mathbb{Z}_{\geq 0} \\ f &\mapsto \max\{j \geq 1 \colon f \in \mathfrak{m}_x^j\}. \end{aligned}$$

Recordamos que por ser uma valorização, ela satisfaz as seguintes propriedades:

- $v_x(fg) = v_x(f) + v_x(g)$ para quaisquer $f, g \in \mathcal{O}_{X,x}$.
- $v_x(f+g) \geq \min\{v_x(f), v_x(g)\}$ para quaisquer $f, g \in \mathcal{O}_{X,x}$.

Aqui, fazemos $v_x(0) = \infty$ e $\infty \geq a$ para todo $a \in \mathbb{Z}_{\geq 0}$. Segue da segunda propriedade que $v_x(f+g) = \min\{v_x(f), v_x(g)\}$ se $v_x(f) \neq v_x(g)$.

Tal valorização se estende naturalmente aos elementos não-nulos do corpo de frações $\bar{k}(X)$. Um elemento $t \in \mathcal{O}_{X,x}\backslash\{0\}$ é dito um **uniformizador** para X em x se $v_x(t) = 1$. Ele pode ser interpretado como o análogo da coordenada local z em uma superfície de Riemann. O uniformizador satisfaz a seguinte propriedade

Proposição 2.3.3. *Seja X/k uma curva, e seja $t \in k(X)$ um uniformizador em algum ponto liso $x \in X(k)$. Então, $k(X)$ é uma extensão finita e separável de $k(t)$.*

Demonstração: Ver Proposição II.1.4 de [Sil09]. □

A partir da valorização em um ponto liso, temos a seguinte definição.

Definição 2.3.4. Sejam X uma curva, $x \in X(\bar{k})$ um ponto liso e $f \in \bar{k}(X)$. Dizemos que

- x é um **zero de ordem** d de f se $v_x(f) \geq d$, com $d \geq 1$.
- x é um **polo de ordem** d de f se $-d \leq v_x(f) < 0$ com $d \geq 1$.

Assim, temos algo semelhante com superfícies de Riemann, onde cada função meromorfa $f \in \mathcal{M}(X)$ possui uma "ordem de anulamento" em cada ponto de X, podendo ser negativa.

Exemplo 2.3.5. Considere a curva $X = V(Y^2 - X^3 - X)$. Então, sabemos pelo Exemplo 2.1.24 que $P = (0,0)$ é um ponto liso de X e que $\mathfrak{m}_P = \langle X, Y\rangle$, com $\mathfrak{m}_P/\mathfrak{m}_P^2 = \langle \overline{Y}\rangle$. A partir dessas informações, obtemos os seguintes exemplos:

- A função $Y \in \mathcal{O}_{X,P}$ tem ordem de anulamento igual a 1, pois $Y \notin \mathfrak{m}_P^2$.

[2] Se o leitor desejar, k denota um corpo de característica zero ou um corpo finito.

- A função $X \in \mathcal{O}_{X,P}$ pertence a $\mathfrak{m}_P^2$ pois $X = Y^2 - X^3 \equiv 0 \pmod{\mathfrak{m}_P^2}$ e temos $v_P(X) \geq 2$. Como X satisfaz $X^3 + X = Y^2$ ao tomarmos a ordem de anulamento, segue que

$$2v_P(Y) = v_P(Y^2) = v_P(X^3 + X) = \min\{v_P(X^3), v_P(X)\} = v_P(X).$$

  Assim, segue do item anterior que $v_P(X) = 2$.

Também temos o seguinte resultado.

Proposição 2.3.6. *Sejam X uma curva lisa e $f \in \bar{k}(X)$ não-nulo. Então, f possui finitos zeros e polos em X. E mais, se f não possui polos, então $f \in \bar{k}^*$.*

Demonstração: O fato de que $v_x(f)$ é diferente de zero em finitos $x \in X$ pode ser visto ou na página 149 do [Sha13] ou no Lema I.6.5 do [Har77] no contexto de curvas abstratas.

Se f não possui polos em X, então ela é uma função regular em todo o X. Assim, o resultado segue ou do Teorema I.3.4.a do [Har77] ou do Corolário 1.1 na Seção 1.5.2 do [Sha13] onde f é interpretado como um mapa $X \to \mathbb{P}^1$. □

Agora, vamos tratar de morfismos entre curvas. Primeiro, definimos morfismos entre variedades projetivas.

Definição 2.3.7. Sejam $X \subseteq \mathbb{P}^n$ e $Y \subseteq \mathbb{P}^m$ variedades projetivas. Um **mapa racional** $\phi : X \to Y$ é dado por

$$\phi(x) = (f_0(x) : \cdots : f_m(x))$$

para certos $f_0, \ldots, f_m \in \bar{k}(X)$, de modo que se os f_i's são regulares e nem todos se anulam em algum $x \in X(\bar{k})$, temos $\phi(x) \in Y(\bar{k})$.

Pode ser o caso que troquemos cada f_i por gf_i, para um certo $g \in \bar{k}(X)^*$. Note que isto não altera os valores de ϕ. Se $x \in X(\bar{k})$ é tal que exista $g \in \bar{k}(X)^*$ de modo que cada f_i é regular em x e nem todos os f_i's se anulam em x, dizemos que ϕ é **regular** ou **bem definida** em x. Um mapa racional é dito um **morfismo** se ele é regular em todos os pontos de $X(\bar{k})$.

Se X/k e Y/k, ϕ é dito **definido sobre** k se (a menos de uma multiplicação por um elemento de $\bar{k}(X)^*$) $f_0, \ldots, f_m \in k(X)$.

Observação 2.3.8. Uma maneira alternativa de descrever mapas racionais é por polinômios homogêneos. De fato, pelo Teorema I.3.4.c do [Har77], temos o seguinte isomorfismo

$$\bar{k}(X) \cong \bar{k}[X]_{(\langle 0 \rangle)} := \left\{ \frac{f}{g} := f, g \in \bar{k}[X] \text{ homogêneos de mesmo grau, } g \neq 0 \right\} \subseteq \operatorname{Frac} k[X].$$

Então, após "limparmos os denominadores", um mapa racional pode ser descrito como $\phi = [p_0, \ldots, p_n]$ tais que

- Cada $p_i \in \bar{k}[X_0, \ldots, X_n]$ é homogêneo, todos de mesmo grau e nem todos em $I(X)$.
- Para todo $f \in I(Y)$, $f(p_0, \ldots, p_n) \in I(X)$.

e dizemos que ϕ é regular em $x \in X(\bar{k})$ se existem $\psi_0, \ldots, \psi_n \in \bar{k}[X_0, \ldots, X_n]$ homogêneos de mesmo grau tais que $\phi_i \psi_j = \phi_j \psi_i$ em $k[X]$ para todos $0 \leq i, j \leq n$ e $\psi_i \neq 0$ em $k[X]$ para algum i.

Exemplo 2.3.9. O mapa racional

$$\begin{aligned} \phi : \mathbb{P}^2 &\to \mathbb{P}^2 \\ (x : y : z) &\mapsto (x^2 : xy : z^2) \end{aligned}$$

é regular em todo ponto de $\mathbb{P}^2$, exceto em $(0 : 1 : 0)$.

Uma característica interessante de curvas lisas é que um mapa racional é regular em todo ponto. Isto é consequência da seguinte proposição

Proposição 2.3.10. *Sejam X uma curva, $Y \subseteq \mathbb{P}^n$ uma variedade projetiva e $x \in X(\bar{k})$ um ponto liso. Se $\phi : X \to Y$ é um mapa racional, então ϕ é regular em x. Em particular, se X é lisa, então ϕ é um morfismo.*

Demonstração: Suponha que ϕ é dada por $\phi = (f_0 : \cdots : f_n)$. Então, se $t \in \bar{k}(X)$ é um uniformizador para X em x, multiplicando cada f_i por t^r, com $r = \min v_x(f_i)$, segue que ϕ será regular em x. □

Exemplo 2.3.11. Se $\operatorname{char} k \neq 2$, temos que $X = V(X^2 + Y^2 - Z^2) \subseteq \mathbb{P}^2$ é isomorfo a $\mathbb{P}^1$. De fato, como X e $\mathbb{P}^1$ são curvas lisas, temos os seguintes mapas racionais que são morfismos

$$\begin{aligned} \phi : X &\to \mathbb{P}^1 & \psi : \mathbb{P}^1 &\to X \\ (a : b : c) &\mapsto (a + c : b) & (s : t) &\mapsto (s^2 - t^2 : 2st : s^2 + t^2) \end{aligned}$$

e se verifica que ϕ e ψ são inversos um do outro.

O seguinte teorema nos diz que mapas entre curvas lisas têm um caráter "mais rígido". Compare com a Proposição 1.3.7.

Teorema 2.3.12. *Seja $\phi : X \to Y$ um morfismo entre curvas lisas. Então, ϕ é constante ou sobrejetor.*

Demonstração: Suponha que ϕ não seja constante. Então, podemos concluir de duas maneiras

- Provar que ϕ é um mapa finito, usando o Teorema 1.16 na Seção 1.5.3 de [Sha13] e usar o Teorema 1.12 na Seção 1.5.3 do [Sha13] que diz que todo mapa finito é sobrejetor.
- Mostrar que $\phi(X)$ é um fechado irredutível de X e portanto, as únicas possibilidades são um ponto ou todo o X. É o que é feito na Proposição II.6.8 do [Har77].

□

Seja X/k uma curva lisa e seja $f \in k(X)$. Então, o mapa racional

$$\begin{aligned} \phi_f : X &\to \mathbb{P}^1 \\ x &\mapsto (f(x) : 1) \end{aligned}$$

é um morfismo pela Proposição 2.3.10, que é definido sobre k. De fato, temos

$$f(x) = \begin{cases} (f(x) : 1) & \text{se } v_x(f) \geq 0 \\ (1 : 0) & \text{caso contrário.} \end{cases}$$

Reciprocamente, se $\phi : X \to \mathbb{P}^1$ é um morfismo definido sobre k, então se ϕ é dado por $(f : g)$, temos duas possibilidades.

- $g = 0$. Isto implica que $\phi \equiv (1 : 0)$, ou seja, ϕ é constante igual a $(1 : 0)$, que denotamos por ∞.
- $g \neq 0$. Daí, temos $\phi = \phi_{f/g}$, com $f/g \in k(X)$.

Assim, temos uma bijeção entre morfismos $\phi : X \to \mathbb{P}^1$ (diferentes de ∞) definidos sobre k e elementos de $k(X)$. Um resultado análogo vale para $k = \bar{k}$.

Agora, sejam X/k e Y/k curvas lisas e $\phi : X \to Y$ um mapa racional não-constante que é definido sobre k. Então, temos um homomorfismo induzido entre os corpos de funções

$$\begin{aligned} \phi^* : k(Y) &\to k(X) \\ f &\mapsto f \circ \phi. \end{aligned}$$

Note que estamos identificando cada $f \in k(Y)$ com um morfismo $Y \to \mathbb{P}^1$ por conta da bijeção que descrevemos acima. Como ϕ^* é uma mapa entre corpos, ele é injetor e além disso, ele fixa o corpo base k.

Também temos uma mapa $\phi_* : k(X) \to k(Y)$ que é dado essencialmente tomando o mapa de norma associado à extensão $k(X)/\phi^* k(Y)$:

$$\begin{aligned} \phi_* : k(X) &\to k(Y) \\ f &\mapsto (\phi^*)^{-1}(N_{k(X)/\phi^* k(Y)}(f)). \end{aligned}$$

O seguinte teorema nos diz que estudar curvas suaves definidas sobre k é o mesmo que estudar mapas entre os seus corpos de funções. O mesmo teorema será válido se consideramos curvas lisas quaisquer, trocando k por $\bar{k}$.

Teorema 2.3.13. *Sejam X e Y curvas lisas definidas sobre k.*

(a) Seja $\phi : X \to Y$ um morfismo não constante definido sobre k. Então, $k(X)$ é uma extensão finita de $\phi^*(k(Y))$.

(b) Seja $\iota : k(Y) \to k(X)$ um homomorfismo de k-álgebras. Então, existe um único morfismo não constante $\phi : X \to Y$ definido sobre k tal que $\phi^* = \iota$.

(c) Seja K um corpo tal que $k \subseteq K \subseteq k(X)$ com $k(X)/K$ de grau finito. Então, existe uma curva lisa $\mathfrak{X}/k$, única a menos de k-isomorfismo, e existe $\phi : X \to \mathfrak{X}$ não-constante e definido sobre k tal que $\phi^* k(\mathfrak{X}) = K$.

Demonstração: (a) Ver o Teorema II.6.8 do [Har77]. O resultado essencialmente segue do fato de que $k(X)$ e $k(Y)$ são corpos finitamente gerados com grau de transcendência um sobre k.

(b) Vamos assumir que $Y \subseteq \mathbb{P}^n$ e $Y \not\subseteq \{X_0 = 0\}$. Então, em Y temos as funções coordenadas

$$g_i :- \frac{X_i}{X_0} \in k(Y).$$

Daí, $\phi : X \to Y$ dado por $\phi = (1 : \iota(g_1) : \cdots : \iota(g_n))$ é tal que $\phi^* = \iota$ e ϕ é não-constante. Além disso, se $\psi = (\psi_0 : \cdots : \psi_n)$ é outro mapa racional com $\psi^* = \iota$, então para cada i

$$\frac{f_i}{f_0} = \psi^* g_i = \phi^* g_i = i(g_i).$$

Logo, $\psi = \phi$.

(c) Primeiro, tratamos o caso em que k é algebricamente fechado. A ideia é construir a partir do corpo K uma "curva singular abstrata". Daí, o Teorema I.6.9 do [Har77] diz que tal curva se identifica com uma curva projetiva lisa. É por meio desta linguagem que se prova o Corolário I.6.12 do [Har77] que afirma que existe uma equivalência entre as categorias

- corpos finitamente gerados K com grau de transcendência um sobre k e mapas de k-álgebras.
- curvas projetivas lisas e mapas dominantes (que será o mesmo que não-constantes).

Para o caso geral, se obtém a partir do caso algebricamente fechado tomando G_k-invariantes. □

A partir do item (a) do teorema acima, temos a seguinte definição

Definição 2.3.14. Seja $\phi : X \to Y$ um mapa entre curvas lisas e definidas sobre k. Definimos o **grau** de ϕ, denotado por $\deg \phi$, da seguinte maneira:

- Se ϕ é constante, definimos $\deg \phi = 0$.
- Caso contrário, ϕ é dito **finito** e definimos $\deg \phi = [k(X) : \phi^*(k(Y))]$. Dependendo de como é a extensão finita $\bar{k}(X)/\phi^*\bar{k}(Y)$ dizemos que ϕ é **separável, inseparável** ou **puramente inseparável**.

No caso geral, definimos o grau de ϕ como sendo $[\bar{k}(X) : \phi^*(\bar{k}(Y))]$. No caso de X, Y e ϕ serem definidos sobre k, os dois graus coincidem.

Observação 2.3.15. Em uma extensão finita L/K de corpos, se definem os chamados **grau separável** e **grau inseparável** como sendo $[L : K']$ e $[K' : K]$ respectivamente, onde K' é o fecho separável de K em L. Passamos estas definições para mapas não-constantes $\phi : X \to Y$ assim como fizemos na definição acima e serão denotados por $\deg_s \phi$ e $\deg_i \phi$ respectivamente.

Temos o seguinte resultado similar à Proposição 1.4.14 no caso de superfícies de Riemann compactas.

Corolário 2.3.16. *Sejam X e Y curvas suaves e seja $\phi : X \to Y$ um morfismo de grau um. Então, ϕ é um isomorfismo.*

Demonstração: Ver Corolário II.2.4.1 do [Sil09]. □

A próxima definição busca interpretar o comportamento de um mapa entre curvas lisas na "vizinhança" de um ponto, da mesma forma que vimos no caso de superfícies de Riemann.

Definição 2.3.17. Seja $\phi : X \to Y$ um mapa não constante entre curvas lisas e seja $x \in X(\bar{k})$. O **índice de ramificação de ϕ em x**, denotado por $e_\phi(x)$, é dado por $e_\phi(x) = v_x(\phi^*(t))$, onde $t \in \bar{k}(Y)$ é um uniformizador em $\phi(x)$.

Dizemos que ϕ é **não ramificado em** x se $e_\phi(x) = 1$ e que ϕ é **não-ramificado** se ele é não ramificado em todo ponto de X. A próxima proposição exibe algumas propriedades dos índices de ramificação.

Proposição 2.3.18. *Seja $\phi : X \to Y$ um mapa não constante de curvas lisas. Então:*

(a) Para todo $y \in Y(\bar{k})$

$$\sum_{\phi(x)=y} e_\phi(x) = \deg \phi.$$

(b) Para todo ponto $y \in Y(\bar{k})$, exceto finitos, temos $\#\phi^{-1}(y) = \deg_s \phi$ (o grau separável de ϕ).

(c) Se $\psi : Y \to Z$ é outro mapa não constante de curvas lisas, então para todo $x \in X(\bar{k})$

$$e_{\psi\circ\phi}(x) = e_\phi(x) \cdot e_\psi(\phi(x)).$$

Demonstração: (a) Existem duas maneiras de demonstrar este fato

- Deduzir a partir de um fato sobre pullback de divisores que está enunciado como a Proposiçao II.6.9 do [Har77] ou o Teorema 3.5 na Seção 3.2.1 do [Sha13]. Também iremos ver tal resultado como o item (a) da Proposição 2.4.9.

- Interpretamos como um resultado sobre a ramificação de ideais primos em extensões de domínios de Dedekind. Isto é feito a partir da Proposição I.8.2 do [Neu99] ou a Proposição 10 do Capítulo I de [Ser79].

(b) Façamos o caso em que ϕ é separável. Então, considerando a extensão de domínios de Dedekind $\phi^*\bar{k}[Y] \subseteq \bar{k}[X]$ a partir da Proposição I.8.4 do [Neu99], concluímos que finitos pontos de X têm índice de ramificação maior que um. Assim, o resultado segue.

(c) Sejam $t \in \bar{k}(Y), s \in \bar{k}(Z)$ uniformizadores em $\phi(x)$ e $\psi(\phi(x))$, respectivamente. Então, por definição $t^{e_\psi(\phi(x))}$ e $\psi^* s$ tem o mesmo $v_{\phi(x)}$. Logo

$$e_\psi(\phi(x)) \cdot e_\phi(x) = v_x(\phi^*(t^{e_\psi(\phi(x))})) = v_x((\psi \circ \phi)^* s) = e_{\psi\circ\phi}(x).$$

□

Corolário 2.3.19. *Um mapa $\phi : X \to Y$ é não-ramificado se e somente se $\#\phi^{-1}(y) = \deg \phi$ para todo $y \in Y(\bar{k})$.*

Demonstração: De fato, dado $y \in Y(\bar{k})$, temos pelo item (a) da proposição anterior que

$$\deg \phi = \sum_{\phi(x)=y} e_\phi(x) \geq \#\phi^{-1}(y).$$

Assim, $e_\phi(f) = 1$ para todo $x \in X(\bar{k})$ na fibra sobre y se e somente se $\#\phi^{-1}(y) = \deg \phi$. □

Observação 2.3.20. Faremos alguns comentários rápidos sobre curvas X/k com $\operatorname{char} k = p > 0$. Neste caso, para $q = p^f$, definimos a curva $X^{(q)}$ como sendo tal que

$$I(X^{(q)}) = \langle \{ f^{(q)} := f \in I(X) \cap k[X_0, \ldots, X_n] \text{ homogêneo} \} \rangle$$

onde para $f \in k[X_0, \ldots, X_n]$, $f^{(q)}$ é obtido a partir de f elevando todos os coeficientes de f a potência q. Assim, obtemos outra curva $X^{(q)}/k$ e temos um mapa natural

$$\begin{aligned} \mathsf{F}^q : X &\to X^{(q)} \\ (a_0 : \cdots : a_n) &\mapsto (a_0^q : \cdots : a_n^q), \end{aligned}$$

chamado **morfismo de Frobenius (de ordem q)**. Algumas propriedades que este mapa satisfaz são

- $(\mathsf{F}^q)^* k(X^{(q)}) = k(X)^q := \{f^q : f \in k(X)\}$.
- F^q é um mapa puramente separável.
- $\deg \mathsf{F}^q = q$.

Para uma prova destas três afirmações, veja a Proposição II.2.11 de [Sil09]. E por conta do Teorema 2.3.13, pode-se concluir que para $X/k, Y/k$ curvas lisas e $\psi : X \to Y$ definida sobre k, então ψ se decompõe como

$$X \xrightarrow{\mathsf{F}^q} X^{(q)} \xrightarrow{\varphi} Y$$

com $q = \deg_i \phi$ e φ separável (ver Corolário II.2.12 de [Sil09]).

2.4 Teorema de Riemann-Roch

Um teorema importante sobre curvas algébricas é o teorema de Riemann-Roch. Ele está relacionado ao conceito de gênero de uma curva algébrica. Antes de enunciá-lo, vamos desenvolver alguns conceitos preliminares.

Começamos com a definição de divisor. agora no contexto de curvas algébricas.

Definição 2.4.1. O **grupo de divisores** de uma curva X, denotado por $\mathrm{Div}(X)$, é o grupo abeliano gerado pelos pontos $x \in X(\bar{k})$.

Assim, um divisor $D \in \mathrm{Div}(X)$ é uma soma formal finita de pontos com coeficientes inteiros.

$$D = \sum_{x \in X} a_x \cdot x \quad a_x \in \mathbb{Z}.$$

O **grau** de um divisor $D \in \mathrm{Div}(X)$ é definido como a soma de seus coeficientes a_x. Logo, os divisores de grau zero formam um subgrupo denotado por $\mathrm{Div}^0(X)$.

No grupo dos divisores, definimos a seguinte relação de ordem. Para $D_1 = \sum_{x \in X} a_x \cdot x$ e $D_2 = \sum_{x \in X} b_x \cdot x$:

$$D_1 \geq D_2 \iff a_x \geq b_x \quad \forall x \in X.$$

Em particular, quando $D_2 = 0$ dizemos que D_1 é **efetivo**.

Se X é uma curva lisa e $f \in \bar{k}(X)^*$, então podemos atribuir a f um divisor $\mathrm{div}(f)$ dado por

$$\mathrm{div}(f) := \sum_{x \in X} v_x(f) \cdot x.$$

Segue da Proposição 2.3.6 que isto está bem definido. Como cada v_x é um homomorfismo, segue que temos um homomorfismo de grupos

$$\mathrm{div} : \bar{k}(X)^* \to \mathrm{Div}(X).$$

Observação 2.4.2. Assim como no caso de superfícies de Riemann, nós podemos expressar condições sobre zeros e polos de funções regulares usando divisores. Mais especificamente, sejam $f \in \bar{k}(X)^*$ e $x_1, \ldots, x_m, y_1, \ldots, y_n$ pontos distintos de X. Então, se $a_1, \ldots, a_m, b_1, \ldots, b_n$ são inteiros positivos, temos que

$$\mathrm{div}(f) \geq \sum_{j=1}^{m} a_j \cdot x_j - \sum_{j=1}^{n} b_j \cdot y_j$$

se e somente se

- f tem um zero em x_j de ordem pelo menos a_j, $1 \leq i \leq m$.
- f tem (no máximo) um polo em y_j de ordem no máximo b_j, $1 \leq j \leq n$.

Por exemplo, podemos expressar o fato de que uma função $f \in \bar{k}(X)^*$ apenas se anula em $x \in X$ com ordem pelo menos 2, escrevendo $\mathrm{div}(f) \geq 2 \cdot x$. Note que f não possui polos em X.

Definição 2.4.3. Dizemos que $D \in \mathrm{Div}(X)$ é um **divisor principal** se ele é da forma $\mathrm{div}(f)$ para algum $f \in \bar{k}(X)^*$. Dois divisores D_1 e D_2 são ditos **linearmente equivalentes** se $D_1 - D_2$ é principal. Denotamos isto por $D_1 \sim D_2$.

Note que os divisores principais formam um subgrupo de $\mathrm{Div}(X)$, pois temos

- $\mathrm{div}(f) = 0$ se $f \in \bar{k}^*$.
- $\mathrm{div}(f) - \mathrm{div}(g) = \mathrm{div}(fg^{-1})$ para quaisquer $f, g \in \bar{k}(X)^*$.

Assim, podemos tomar o grupo quociente, o chamado **grupo de classes de divisores** ou **grupo de Picard** de X. Ele é denotado por $\mathrm{Pic}(X)$.

A Proposição 1.4.3 no capítulo anterior também é válida para curvas algébricas.

Proposição 2.4.4. *Seja X uma curva lisa e seja $f \in \bar{k}(X)^*$. Então:*

(a) $\mathrm{div}(f) = 0$ *se e somente se* $f \in \bar{k}^*$.

(b) $\deg(\mathrm{div}(f)) = 0$.

Demonstração: (a) Como $\mathrm{div}(f) = 0$, em particular, f é regular em X o que implica, pela Proposição 2.3.6, que $f \in \bar{k}^*$. A recíproca é claramente verdadeira.

(b) Isto novamente segue da Proposição II.6.9 do [Har77] ou do Teorema 3.5 da Seção 3.2.1 do [Sha13]. Tal resultado será visto como o item (a) da Proposição 2.4.9.

□

Exemplo 2.4.5. Em $\mathbb{P}^1$, todo divisor de grau zero é principal. De fato, se $D = \sum n_x \cdot x$ com $\sum n_x = 0$, temos

$$D = \mathrm{div}\left(\prod_{x \in \mathbb{P}^1} (\beta_x X - \alpha_x Y)^{n_x}\right),$$

onde para $x \in \mathbb{P}^1$, $\alpha_x, \beta_x \in \bar{k}$ são tais que $x = (\alpha_x : \beta_x)$. Notamos que como $\sum n_x = 0$, $\prod_{x \in \mathbb{P}^1} (\beta_x X - \alpha_x Y)^{n_x}$ será um quociente de dois polinômios homogêneos de mesmo grau. Assim, o mapa $\deg : \mathrm{Div}(\mathbb{P}^1) \to \mathbb{Z}$ nos dá um isomorfismo $\mathrm{Pic}(\mathbb{P}^1) \cong \mathbb{Z}$.

Exemplo 2.4.6. Suponha que $\mathrm{char}\, k \neq 2$ e sejam $\alpha_1, \alpha_2, \alpha_3 \in \bar{k}$ distintos. Considere a curva dada pelo fecho projetivo de

$$X : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Então, segue do Exemplo 2.1.26 que X é uma curva lisa e $O = (0 : 1 : 0)$ é o único ponto no infinito. Se definimos $P_i := (\alpha_i : 0 : 1)$ para $i = 1, 2, 3$, temos

$$\mathrm{div}(x - \alpha_i) = 2 \cdot P_i - 2 \cdot O \quad \text{e} \quad \mathrm{div}(y) = 1 \cdot P_1 + 1 \cdot P_2 + 1 \cdot P_3 - 3 \cdot O,$$

onde $x = \frac{X}{Z}, y = \frac{Y}{Z} \in \bar{k}(X)$.

Pela proposição anterior, o subgrupo dos divisores principais está contido em $\mathrm{Div}^0(X)$. O grupo quociente será denotado por $\mathrm{Pic}^0(X)$. Ele será importante para a Seção 3.2, quando tratarmos da lei de grupo sobre os pontos de uma curva elíptica.

Observação 2.4.7. Algo interessante que destacamos aqui é que temos a seguinte sequência exata

$$1 \longrightarrow \bar{k}^* \longrightarrow \bar{k}(X)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(X) \longrightarrow \mathrm{Pic}^0(X) \longrightarrow 0$$

que se assemelha bastante com uma que se obtém na teoria algébrica dos números

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow \bar{K}^* \longrightarrow \text{ideais fracionários de } K \longrightarrow \text{grupo de classe de ideais} \longrightarrow 1\,.$$

Aqui, $K/\mathbb{Q}$ é um corpo de números e $\mathcal{O}_K$ é o seu anel de inteiros.

Seja $\phi : X \to Y$ um mapa não-constante entre curvas lisas. Como vimos, ϕ induz os seguintes mapas entre os corpos de funções

$$\phi^* : \bar{k}(Y) \to \bar{k}(X) \quad \phi_* : \bar{k}(X) \to \bar{k}(Y).$$

De maneira análoga, definimos os seguintes mapas entre os grupos de divisores

$$\begin{aligned} \phi^* : \mathrm{Div}(Y) &\to \mathrm{Div}(X) & \qquad \phi_* : \mathrm{Div}(X) &\to \mathrm{Div}(Y) \\ y &\mapsto \sum_{\phi(x)=y} e_\phi(x) \cdot x & \qquad x &\mapsto \phi(x). \end{aligned}$$

Exemplo 2.4.8. Reinterpretando a ordem de anulamento de $f \in \bar{k}(X)^* \backslash k^*$ através do índice de ramificação do morfismo não-constante $\phi_f : X \to \mathbb{P}^1$ associado, segue que

$$\operatorname{div}(f) = \phi_f^*(1 \cdot (0:1) - 1 \cdot (1:0)).$$

A seguinte proposição enuncia algumas propriedades destes dois mapas

Proposição 2.4.9. *Seja $\phi : X \to Y$ um mapa não-constante entre curvas lisas. Então:*

(a) $\deg \phi^*(D) = (\deg \phi) \cdot (\deg D) \quad \forall D \in \operatorname{Div}(Y)$.

(b) $\phi^*(\operatorname{div}(f)) = \operatorname{div}(\phi^* f) \quad \forall f \in \bar{k}(Y)^*$.

(c) $\deg \phi_*(D) = \deg D \quad \forall D \in \operatorname{Div}(X)$.

(d) $\phi_*(\operatorname{div}(f)) = \operatorname{div}(\phi_* f) \quad \forall f \in \bar{k}(X)^*$.

(e) $\phi_* \circ \phi^* : \operatorname{Div}(Y) \to \operatorname{Div}(Y)$ *é a multiplicação por* $\deg \phi$.

(f) Se $\psi : Y \to Z$ é outro mapa não-constante entre curvas lisas, temos

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \quad e \quad (\psi \circ \phi)_* = \psi_* \circ \phi_*.$$

Demonstração: Ver a Proposição II.3.6 do [Sil09]. □

Uma consequência da proposição acima é uma outra demonstração do item b) da Proposição 2.4.4. Para X curva lisa e $f \in \bar{k}(X)^*$ não-constante, segue do Exemplo 2.4.8 que

$$\deg(\operatorname{div}(f)) = \deg(\phi_f^*(1 \cdot (0:1) - 1 \cdot (1:0))) = \deg \phi_f \cdot \deg(1 \cdot (0:1) - 1 \cdot (1:0)) = 0.$$

Observação 2.4.10. Segue dos itens (a)-(d) da proposição acima que os mapas ϕ^* e ϕ_* levam divisores de grau zero (resp. principais) em divisores de grau zero (resp. principais). Assim, obtemos mapas

$$\phi^* : \operatorname{Pic}^0(Y) \to \operatorname{Pic}^0(X) \qquad \text{e} \qquad \phi_* : \operatorname{Pic}^0(X) \to \operatorname{Pic}^0(Y).$$

Tais mapas serão importantes para a Seção 3.2 quando tratarmos de isogenias entre curvas elípticas e da definição de isogenia dual.

O próximo conceito relacionado ao teorema de Riemann-Roch é o de forma diferencial. Primeiro, definimos o que são derivações.

Definição 2.4.11. Sejam F um corpo, A uma F-álgebra e M um A-módulo. Uma **F-derivação de A para M** é um mapa F-linear $d : A \to M$ que satisfaz a regra de Leibniz

$$d(a_1 a_2) = a_1 d(a_2) + a_2 d(a_1).$$

Uma consequência disso é que $d(a) = 0$ se $a \in F$, ou seja, os elementos de F são considerados "constantes".

Exemplo 2.4.12. Sejam $A = M = F[x, y]$. Então, a derivada parcial (formal) em relação a x, $\partial_x : F[x, y] \to F[x, y]$ é uma F-derivação.

Exemplo 2.4.13. Seja X uma superfície de Riemann e tome $F = \mathbb{C}$. Daí, considere $A = \mathcal{O}_X(X)$ o anel das funções holomorfas e $M = \Omega^1(X)$ o $\mathcal{O}_X(X)$-módulo das formas diferenciais holomorfas sobre X. Então, a diferencial

$$\begin{aligned} d : \mathcal{O}_X(X) &\to \Omega^1(X) \\ f &\mapsto \frac{\partial f}{\partial z}\, dz \end{aligned}$$

é um exemplo de uma $\mathbb{C}$-derivação.

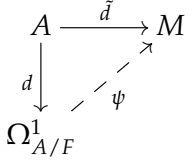
A seguinte definição nos dá uma maneira de interpretar derivações como mapas lineares.

Definição 2.4.14. Seja F um corpo e A uma F-álgebra. O módulo das **formas diferenciais de** A **sobre** F consiste de:

- Um A-módulo denotado por $\Omega^1_{A/F}$.
- Uma "F-derivação universal" $d : A \to \Omega^1_{A/F}$.

tal que o par $(\Omega^1_{A/F}, d)$ satisfaz a seguinte propriedade universal:

Toda F-derivação $\tilde{d} : A \to M$ se fatora como $\psi \circ d$ para um único $\psi : \Omega^1_{A/F} \to M$ homomorfismo de A-módulos.



Denotamos a imagem de $a \in A$ sob d por da.

Assim, este objeto é definido por uma propriedade universal e portanto, se existe ele é único a menos de um (único) isomorfismo compatível de A-módulos.

Para que a definição acima faça sentido, temos a seguinte construção

Proposição 2.4.15. *Para F corpo e A uma F-álgebra, o A-módulo Ω definido abaixo satisfaz as condições da definição acima.*

- *Considere o A-módulo livre T gerado pelo conjunto $\{da : a \in A\}$.*
- *Seja I o A-submódulo gerado por da para $a \in F$, $d(a+b) - da - db$ para qualquer $(a,b) \in A \times A$ e por elementos da forma $d(ab) - ad(b) - bd(a)$ para qualquer $(a,b) \in A \times A$.*
- *Faça $\Omega = T/I$ e considere a F-derivação $d : A \to \Omega$ dada por $d(a) = da + I$.*

Demonstração. Ver a Proposição 6.1.3 do [Liu06] □

Agora, aplicamos esta definição para curvas e temos um análogo de $\hat{\Omega}_X(X)$ (para X superfície de Riemann).

Definição 2.4.16. Seja X uma curva. O **espaço das formas diferenciais (meromorfas) sobre** X, denotado por Ω_X é definido como sendo $\Omega^1_{\bar{k}(X)/\bar{k}}$, o $\bar{k}(X)$-espaço vetorial das formas diferenciais de $\bar{k}(X)$ sobre $\bar{k}$.

Seja $\phi : X \to Y$ uma mapa não-constante entre curvas. Então, o mapa entre os corpos de funções $\phi^* : \bar{k}(Y) \to \bar{k}(X)$ induz uma $\bar{k}$-derivação

$$\begin{aligned} d : \bar{k}(Y) &\to \Omega_X \\ f &\mapsto d(\phi^* f). \end{aligned}$$

onde Ω_X é um $\bar{k}(Y)$-espaço vetorial via o mapa ϕ^*. Assim, temos um mapa $\bar{k}(Y)$-linear, o **pull-back** de formas diferenciais

$$\begin{aligned} \phi^* : \Omega_Y &\to \Omega_X \\ f dg &\mapsto (\phi^* f) d(\phi^* g). \end{aligned}$$

Este mapa nos dá um critério útil para determinar quando ϕ é um mapa separável

Proposição 2.4.17. *Seja X uma curva lisa. Então:*

(a) Ω_X é um $\bar{k}(X)$-espaço vetorial de dimensão um.

(b) Seja $f \in \bar{k}(X)$. Se $\bar{k}(X)/\bar{k}(f)$ é uma extensão finita e separável, então df é uma $\bar{k}(X)$-base de Ω_X.

(c) Seja $\phi : X \to Y$ um mapa não-constante entre curvas lisas. Então, ϕ é separável se e só se o mapa $\phi^* : \Omega_Y \to \Omega_X$ é injetor.

Demonstração: (a) Veja o Teorema 3.19 na Seção 3.5.4 do [Sha13] no contexto mais geral de p-formas diferenciais racionais/meromorfas. Uma prova mais algébrica é obtida a partir do Teorema 59.iii) da Seção 27.B do [Mat80], onde usamos o fato de que $\bar{k}(X)/\bar{k}(t)$ é finita e separável quando t é um uniformizador em algum ponto de X.

(b) Veja o Teorema 59.iii) da Seção 27.B do [Mat80].

(c) Ver o item (c) da Proposição II.4.2 do [Sil09].

□

A próxima proposição exibe mais algumas propriedades do espaço Ω_X. Destacamos que assim como fizemos para funções regulares $f \in \bar{k}(X)$, a partir desta proposição, também definiremos em cada ponto de x, uma valorização $v_x(\cdot)$ no espaço das formas diferenciais.

Proposição 2.4.18. *Sejam X uma curva, $x \in X(\bar{k})$ um ponto liso e $t \in \bar{k}(X)$ um uniformizador em x. Então:*

(a) Para cada $\omega \in \Omega_X$ existe uma única função $g \in \bar{k}(X)$, que depende de ω e t que satisfaz

$$\omega = g\,dt.$$

Denotamos g por ω/dt.

(b) Seja $f \in \bar{k}(X)$ regular em x. Então df/dt também é regular em x.

*(c) Seja $\omega \in \Omega_X$ não-nulo. A quantidade $v_x(\omega/dt)$ depende apenas de ω e x e independe do uniformizador t. Esta quantidade é a chamada **ordem de** ω **em** P e denotamos por $v_x(\omega)$.*

(d) Se X é uma curva lisa e $\omega \in \Omega_X$ é não-nulo, então $v_x(\omega) = 0$ para todos os pontos $x \in X$, exceto finitos.

Demonstração: Ver Proposição II.4.3 do [Sil09]. □

Dizemos que $\omega \in \Omega_X \backslash \{0\}$ é **regular** se temos $\mathrm{ord}_x(\omega) \geq 0$ para todo $x \in X(\bar{k})$. De maneira similar, dizemos que ω **não se anula** em X se temos $\mathrm{ord}_x(\omega) \leq 0$ para todo $x \in X(\bar{k})$.

Com essa definição de ordem de anulamento, fica natural definirmos divisores associados a formas diferenciais.

Definição 2.4.19. Seja X uma curva lisa e $\omega \in \Omega_X$ não-nulo. O **divisor associado a** ω é dado por

$$\mathrm{div}(\omega) := \sum_{x \in X(\bar{k})} v_x(\omega) \cdot x.$$

Sejam ω_1 e ω_2 dois elementos não-nulos de Ω_X. Então, como Ω_X é um $\bar{k}(X)$-espaço vetorial de dimensão um (item (a) da Proposição 2.4.17), existe $f \in \bar{k}(X)^*$ tal que $\omega_1 = f\omega_2$. Daí, para $t \in \bar{k}(X)$ um uniformizador, temos

$$\omega_1 = g\,dt \quad \text{e} \quad \omega_2 = fg\,dt$$

para algum $g \in \bar{k}(X)^*$. Assim, segue da definição de ordem que $\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$. Ou seja, $[\mathrm{div}(\omega)] \in \mathrm{Pic}(X)$ independe de ω. Com isso, temos a seguinte definição

Definição 2.4.20. A **classe (de divisores) canônica** de uma curva lisa X é dada pela imagem em $\mathrm{Pic}(X)$ de algum $\omega \in \Omega_X$ não-nulo. Qualquer divisor na mesma classe é chamado de **divisor canônico**.

Agora que todos os conceitos preliminares foram apresentados e discutidos, partimos para o resultado principal. O teorema de Riemann-Roch é um resultado relacionado a certos espaços de funções que serão definidos a seguir.

Definição 2.4.21. Seja X uma curva lisa e $D \in \mathrm{Div}(X)$. Definimos o seguinte $\bar{k}$-subespaço de $\bar{k}(X)$:

$$\mathcal{L}(D) := \{f \in \bar{k}(X)^* : \ \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Denotamos a dimensão deste espaço por $\ell(D)$. Notamos que se $D_1 \leq D_2$ temos $\mathcal{L}(D_1) \subseteq \mathcal{L}(D_2)$. Algumas propriedades destes espaços estão enunciadas abaixo

Proposição 2.4.22. *Seja X uma curva lisa e $D \in \mathrm{Div}(X)$. Então:*

(a) Se $\deg D < 0$, então $\mathcal{L}(D) = \{0\}$ e portanto $\ell(D) = 0$.

(b) $\mathcal{L}(D)$ tem dimensão finita sobre $\bar{k}$.

(c) Se $D' \sim D$, então $\mathcal{L}(D')$ é isomorfo a $\mathcal{L}(D)$ e portanto $\ell(D') = \ell(D)$.

Demonstração: (a) É a mesma ideia na prova da Proposição 1.4.11.

(b) Isto é obtido a partir da Proposição II.5.19 do [Har77] que diz que em certas condições, o espaço das seções globais de certos feixes sobre um esquema X/A é um A-módulo finitamente gerado.

(c) O mesmo raciocínio usado no caso de superfícies de Riemann (ver discussão após a Definição 1.4.6).

□

Observação 2.4.23. Para uma curva lisa X, seja $K_X \in \mathrm{Div}(X)$ um divisor canônico. Ou seja, $K_X = \mathrm{div}(\omega)$ para algum $\omega \in \Omega_X$ não-nulo. Então, se $f \in \mathcal{L}(K_X)$ é não-nulo, temos $\mathrm{div}(f) \geq -\mathrm{div}(\omega)$. Daí, temos $\mathrm{div}(f\omega) \geq 0$ e concluímos que $f\omega$ é regular. Reciprocamente, se $\alpha \in \Omega_X$ é regular e não-nulo, então $\alpha = g\omega$ com $g \in \bar{k}(X)^*$ tal que $\mathrm{div}(g) \geq -\mathrm{div}(\omega)$. Assim, temos um isomorfismo

$$\begin{aligned} \mathcal{L}(K_X) &\to \Omega(X) \\ f &\to f\omega. \end{aligned}$$

onde $\Omega(X)$ é o $\bar{k}$-subespaço de Ω_X das formas diferencias regulares.

Motivado pela teoria das superfícies de Riemann, definimos o **gênero** de uma curva lisa X como sendo a dimensão sobre $\bar{k}$ de $\Omega(X)$. Ele será denotado por g_X ou g se a curva X estiver implícita.

Exemplo 2.4.24. Vamos mostrar que $\Omega(\mathbb{P}^1) = 0$, o que nos permite concluir que $g_{\mathbb{P}^1} = 0$, assim como no caso analítico. Seja $t \in \bar{k}(\mathbb{P}^1)$ a coordenada $\frac{X}{Y}$. Então, temos

$$\mathrm{div}(dt) = -2 \cdot \infty.$$

onde $\infty = (1:0)$. De fato, no ponto $P_\alpha = (\alpha : 1)$, $\alpha \in \bar{k}$, a função $t - \alpha$ é um uniformizador e

$$v_{P_\alpha}(dt) = v_{P_\alpha}(d(t-\alpha)) = 0.$$

E no ponto ∞, a função $\frac{1}{t}$ é um uniformizador e

$$v_\infty(dt) = v_\infty\left(-t^2 d\left(\frac{1}{t}\right)\right) = -2.$$

Logo, $dt \notin \Omega(\mathbb{P}^1)$. E mais, se $\omega \in \Omega_{\mathbb{P}^1}$ é não-nulo, então $\omega = f\,dt$ e

$$\deg(\operatorname{div}(\omega)) = \deg(\operatorname{div}(f)) + \deg(\operatorname{div}(dt)) = -2.$$

E portanto, $\omega \notin \Omega(\mathbb{P}^1)$.

Exemplo 2.4.25. Vamos usar a notação do Exemplo 2.4.6. Então, temos

$$\operatorname{div}(dx) = 1 \cdot P_1 + 1 \cdot P_2 + 1 \cdot P_3 - 3 \cdot O$$

e segue que $\operatorname{div}\left(\frac{dx}{y}\right) = 0$. Daí, $\frac{dx}{y} \in \Omega(X)\backslash\{0\}$. Depois, veremos que X tem gênero um, o que implica que $\frac{dx}{y}$ gera $\Omega(X)$.

E finalmente, enunciamos abaixo o

Teorema 2.4.26 (Riemann-Roch)**.** *Seja X uma curva lisa e seja $K_X \in \operatorname{Div}(X)$ um divisor canônico. Então, para todo $D \in \operatorname{Div}(X)$, temos*

$$\ell(D) - \ell(K_X - D) = \deg D - g + 1.$$

Demonstração: Uma demonstração sofisticada deste teorema é dada no Teorema IV.1.3 do [Har77]. Ela usa um análogo da dualidade de Serre para mostrar que o teorema equivale a

$$\chi(\mathcal{L}(D)) := \dim H^0(X, \mathcal{L}(D)) - \dim H^1(X, \mathcal{L}(D)) = 1 - g + \deg D,$$

onde $\mathcal{L}(D)$ é o análogo algébrico do feixe $\mathcal{O}_D$ na Definição 1.4.6. Assim, o resultado segue essencialmente pelos mesmos passos da demonstração do Teorema 1.4.10.

Uma alternativa é ver os resultados do Capitulo I do [Lan82] no qual se trabalha sobre o corpo de funções $\bar{k}(X)$. □

Corolário 2.4.27. *Para X curva lisa, temos*

(a) $\ell(K_X) = g$.

(b) $\deg K_X = 2g - 2$.

(c) Se $\deg D > 2g - 2$, *então* $\ell(D) = \deg D - g + 1$.

Demonstração: (a) Faça $D = 0$ no teorema acima.

(b) Faça $D = K_X$ e use o item anterior.

(c) Se $\deg D > 2g - 2$, pelo item anterior e o item (a) da Proposição 2.4.22, $\ell(K_X - D) = 0$. Daí, o resultado segue.

□

Exemplo 2.4.28. Já vimos no Exemplo 2.4.24 que $\Omega(\mathbb{P}^1) = 0$, o que implica que $\ell(K_{\mathbb{P}^1}) = g_{\mathbb{P}^1} = 0$. Daí, por Riemann-Roch

$$\ell(D) - \ell(K_{\mathbb{P}^1} - D) = \deg D + 1.$$

Como $K_{\mathbb{P}^1} = -2 \cdot O$, segue que para $\deg D \geq -1$, temos $\deg(K_{\mathbb{P}^1} - D) = 0$ e $\ell(D) = \deg D + 1$.

Exemplo 2.4.29. Continuando o Exemplo 2.4.25, como $\operatorname{div}\left(\frac{dx}{y}\right) = 0$, segue que 0 é um divisor canônico. Daí, $g_X = \ell(K_X) = \ell(0) = 1$. Portanto, $\ell(D) = \deg D$ se $\deg D \geq 1$ e também que $\frac{dx}{y}$ é um gerador de $\Omega(X)$.

Também temos no caso das curvas algébricas um análogo do Teorema 1.4.21:

Teorema 2.4.30 (Riemann-Hurwitz)**.** *Seja $\phi : X \to Y$ uma mapa separável não-constante entre curvas lisas. Então*

$$\chi_X \leq (\deg \phi)\chi_Y - b$$

onde $\chi_X = 2 - 2g_X$ (análogo para Y) e $b = \sum_{x \in X(\bar{k})}(e_\phi(x) - 1)$ é a ramificação total de ϕ. Além disso, a igualdade vale se e somente se

- $\operatorname{char} k = 0$ *ou*
- $\operatorname{char} k = p > 0$ *e* $p \nmid e_\phi(x)$ *para todo* $x \in X(\bar{k})$.

Demonstração: Ver Teorema II.5.9 do [Sil09]. □

Observação 2.4.31. No caso X/k, o grupo G_k age em $\operatorname{Div}(X)$ de maneira natural. O conjunto dos G_k-invariantes é denotado por $\operatorname{Div}_k(X)$. Isto não necessariamente é igual ao subgrupo $\operatorname{Div}(X/k)$ dos divisores que são somas formais de pontos k-racionais. Para tais divisores, pode-se mostrar que $\mathcal{L}(D)$ admite uma $\bar{k}$-base formado por elementos de $k(X)$ (ver Proposição II.5.8 do [Sil09]).

Capítulo 3

Curvas Elípticas

3.1 Perspectiva Analítica

Nesta seção, iniciamos o estudo de curvas elípticas começando do ponto vista analítico. Nesta abordagem, nossos objetos são os toros complexos e vamos estudá-los usando as ferramentas desenvolvidas no Capítulo 1.

3.1.1 Definições Iniciais

Definição 3.1.1. Um **reticulado** em $\mathbb{C}$ é um grupo abeliano livre $\Lambda \subseteq \mathbb{C}$ de posto 2 que gera $\mathbb{C}$ sobre $\mathbb{R}$, ou seja, tal que $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{C}$. Um **paralelogramo fundamental** para Λ é um subconjunto $\Gamma \subseteq \mathbb{C}$ da forma

$$\Gamma = \{\alpha_0 + s\lambda_1 + t\lambda_2 := 0 \leq s, t < 1\}$$

onde $\alpha_0 \in \mathbb{C}$ e (λ_1, λ_2) é uma $\mathbb{Z}$-base de Λ.

Exemplo 3.1.2. Alguns exemplos de reticulados são

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \quad \text{e} \quad \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

onde $\omega = e^{\frac{2\pi}{3}}$. Em geral, anéis de inteiros algébricos $\mathcal{O}_K$ de corpos quadráticos imaginários $K/\mathbb{Q}$ nos fornecem exemplos de reticulados.

Definição 3.1.3. Um **toro complexo (1-dimensional)** é um quociente $\mathbb{C}/\Lambda$ por um reticulado Λ.

A definição de curva elíptica que vamos utilizar será a seguinte

Definição 3.1.4. Uma **curva elíptica** é um toro complexo 1-dimensional $E = \mathbb{C}/\Lambda$. Denotamos por 0_E a classe de equivalência do zero.

Observação 3.1.5. Notamos que toda curva elíptica $E = \mathbb{C}/\Lambda$ possui as seguintes propriedades:

- Existe uma estrutura de grupo abeliano natural em E, induzida por $\mathbb{C}$. Mais explicitamente, temos a operação
$$(z + \Lambda) + (w + \Lambda) = (z + w) + \Lambda$$
e o elemento neutro deste grupo é 0_E.
- Com a topologia quociente, E é um espaço topológico conexo e compacto. Mais ainda, vamos ver que ele é uma *superfície de Riemann*, ou seja, é como se fosse uma curva complexa.

Estas duas observações serão a "essência" do que seria uma curva elíptica. Isto se repetirá quando definirmos curvas elípticas como curvas algébricas.

3.1.2 Funções Duplamente Periódicas

Agora, estamos interessados em estudar funções cujo domínio é uma curva elíptica $\mathbb{C}/\Lambda$. Assim, propomos a seguinte definição

Definição 3.1.6. Seja $\Lambda \subseteq \mathbb{C}$ um reticulado. Uma função holomorfa/meromorfa $f : \mathbb{C} \to \mathbb{C}$ é dita **Λ-periódica** se $f(z+\lambda) = f(z)$ para todo $(z, \lambda) \in \mathbb{C} \times \Lambda$.

Observação 3.1.7. Costuma-se também dar o nome de função **duplamente periódica**. A razão é que ao tomarmos uma $\mathbb{Z}$-base (α, β) de Λ, temos que f é Λ-periódica se, e somente se $f(z+\alpha) = f(z+\beta) = f(z)$ para todo $z \in \mathbb{C}$. Assim, f possui dois períodos, que são dados por α e β.

Poderíamos começar nosso estudo de funções Λ-periódicas começando pelas funções holomorfas. Este caso é bastante simples, por conta dos seguinte resultado

Proposição 3.1.8. *Se $f : \mathbb{C} \to \mathbb{C}$ é holomorfa e Λ-periódica, então f é constante.*

Demonstração: Se $\Gamma \subseteq \mathbb{C}$ é um paralelogramo fundamental para Λ, então como f é Λ-periódica, os valores de f são os mesmos de sua restrição $f|_\Gamma$. Por conta de Γ ser compacto, segue que f é limitada e, portanto, pelo teorema de Liouville, é constante. □

Assim, se estamos procurando por funções Λ-periódicas interessantes, devemos permitir singularidades. A proposição abaixo coleta algumas propriedades deste tipo de função no caso meromorfo

Proposição 3.1.9. *Seja $f : \mathbb{C} \to \mathbb{C}$ uma função meromorfa e Λ-periódica. Então*

i) $\sum_{z \in \mathbb{C}/\Lambda} Res_z(f) = 0$.

ii) $\sum_{z \in \mathbb{C}/\Lambda} ord_z(f) = 0$.

iii) $\sum_{z \in \mathbb{C}/\Lambda} ord_z(f) \cdot z \in \Lambda$.

Aqui, o somatório $\sum_{z \in \mathbb{C}/\Lambda}$ significa que a soma é tomada sobre um paralelogramo fundamental. Tais somas serão finitas por conta de $\mathbb{C}/\Lambda$ ser compacta.

Demonstração: Os itens i) e ii) são essencialmente aplicações adequadas do teorema do resíduo para funções de uma variável complexa. O item iii) além do teorema do resíduo, usa-se o fato de que para $g : U\backslash\{0\} \to \mathbb{C}$ holomorfa, a integral

$$\frac{1}{2\pi i} \int_\gamma g(z)\, dz$$

ao longo de uma curva fechada $\gamma : [0,1] \to U\backslash\{0\}$ é um inteiro. Para mais detalhes, ver o Teorema VI.2.2 do [Sil09]. □

Seja $f : \mathbb{C} \to \mathbb{C}$ uma função meromorfa e Λ-periódica. Então, pela Proposição 1.1.12 podemos vê-la como um mapa holomorfo $f : \mathbb{C} \to \mathbb{P}^1$. Veremos mais tarde que isto induz um mapa holomorfo $\tilde{f} : \mathbb{C}/\Lambda \to \mathbb{P}^1$. Pelo item i) da proposição anterior, segue que se $\tilde{f}$ possui um único polo em $\mathbb{C}/\Lambda$, então ele é de ordem pelo menos 2.

Agora, vamos mostrar de maneira explícita que existem funções Λ-periódicas não-constantes. Começamos com a definição abaixo

Definição 3.1.10. Seja Λ um reticulado. Definimos a **função $\wp$ de Weierstraß** por

$$\wp(z, \Lambda) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda\backslash\{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Quando o reticulado Λ é implícito, costuma-se denotar também por Λ.

Proposição 3.1.11. *Se Λ é um reticulado, então a série que define $\wp(z,\Lambda)$ define uma função meromorfa em $\mathbb{C}$ que será Λ-periódica. Ela satisfaz as seguintes propriedades:*

(i) $\wp(z,\Lambda)$ *é par.*

(ii) $\wp(z,\Lambda)$ *admite um polo em cada ponto de Λ com resíduo zero.*

Demonstração: Vamos mostrar que a série que define $\wp$ é absolutamente convergente e nos dá uma função holomorfa em $\mathbb{C}\backslash\Lambda$.

Fixe $r>0$. Se $z\in\mathbb{C}\backslash\Lambda$ com $|z|<r$, para $|\lambda|>2r$, temos pela desigualdade triangular

$$\left|\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right|=\left|\frac{z(2\lambda-z)}{\lambda^2(z-\lambda)^2}\right|\leq\frac{|z|(2|\lambda|+|z|)}{|\lambda|^2(|\lambda|-|z|)^2}\leq\frac{10|z|}{|\lambda|^3}\leq\frac{10r}{|\lambda|^3}.$$

Então, como $|\lambda|<2r$ para finitos $\lambda\in\Lambda$, se K é um compacto de $\mathbb{C}\backslash\{0\}$ contido no disco $|z|<r$, temos que

$$|\wp(z,\Lambda)|\leq C+\sum_{\lambda\in\Lambda\backslash\{0\}}\frac{1}{|\lambda|^3},$$

para alguma constante C. Mas, a série $\sum_{\lambda\in\Lambda\backslash\{0\}}\frac{1}{|\lambda|^3}$ converge (ver Lema III.2.3 do [Mil06]). Assim, segue do teste de Weiestraß que $\wp(z,\Lambda)$ converge absolutamente e uniformemente em K. Portanto, $\wp(z,\Lambda)$ define uma função holomorfa em $\mathbb{C}\backslash\Lambda$. Assim, o item i) é imediato ao substituirmos z por $-z$.

Para o item ii), tome $\lambda\in\Lambda$. Vemos a partir da série que define Λ que

$$\wp(z,\Lambda)=\frac{1}{(z-\lambda)^2}+g(z)$$

com g holomorfa em uma vizinhança de λ. Logo, $\wp(z,\Lambda)$ é meromorfa em $\mathbb{C}$ com um polo de ordem dois e resíduo zero e cada ponto de Λ.

Para mostrar que $\wp(z,\Lambda)$ é Λ-periódica, temos duas possibilidades:

- Trocar z por $z+\lambda$, $\lambda\in\Lambda$, e mostrar que a série não se altera, ou
- Provar que $\wp'(z,\Lambda)$ é dada pela série

$$\sum_{\lambda\in\Lambda}\frac{-2}{(z-\lambda)^3}.$$

No segundo caso, a série converge absolutamente e uniformemente em compactos de $\mathbb{C}\backslash\Lambda$ seguindo um raciocínio similar ao que fizemos acima. Daí, como a série $\sum_{\lambda\in\Lambda}\frac{-2}{(z-\lambda)^3}$ é obtida derivando termo a termo a série que define $\wp(z,\Lambda)$, o resultado segue.

Se para $\lambda\in\lambda$, definimos $F(z)=\wp(z+\lambda,\Lambda)-\wp(z,\Lambda)$, obtemos $F'(z)=\wp'(z+\lambda)-\wp'(z)$. Como $\wp'(z,\Lambda)$ é claramente Λ-periódica, segue que $F'(z)=0$ e segue que $\wp(z,\Lambda)$ é Λ-periódica. □

Esta função Λ-periódica será útil quando mostrarmos que toda curva elíptica pode ser dada por uma equação cúbica (ver Proposição 3.1.18). Além disso, pode-se mostrar que $\wp$ e $\wp'$ geram todas as funções Λ-periódicas (ver Teorema VI.3.2 do [Sil09]).

3.1.3 Curvas Elípticas como Superfícies de Riemann

Começamos enunciando de maneira mais precisa a afirmação que fizemos na Observação 3.1.5

Proposição 3.1.12. *Seja $\Lambda \subseteq \mathbb{C}$ um reticulado. Então, a curva elíptica $E = \mathbb{C}/\Lambda$ admite uma estrutura natural de superfície de Riemann, que será induzida por $\mathbb{C}$, de modo que*

- *O mapa de projeção $\pi : \mathbb{C} \to E$ é holomorfo.*
- *Um mapa contínuo $f : E \to Y$ é holomorfo se e somente se $f \circ \pi$ é holomorfo, onde Y é outra superfície de Riemann.*

Demonstração: O fato de E ser Hausdorff segue do seguinte fato de Topologia Geral

- Se $\sim$ é uma relação de equivalência em X de modo que o mapa de projeção canônica $X \to X/\sim$ é aberto e $R = \{(x_1, x_2) \in X \times X \colon x_1 \sim x_2\}$ é fechado em $X \times X$, então $X/\sim$, com a topologia quociente, é Hausdorff.

Como podemos tomar uma base enumerável de $\mathbb{C}$ por abertos U tais que $\pi|_U$ é injetor, pode-se mostrar que as imagens destes abertos por π formam uma base enumerável de E. A conexidade de E segue da conexidade de $\mathbb{C}$.

Resta mostrar que existe um atlas euclidiano com funções de transição holomorfas.

Para cada ponto $p \in E$, tome um aberto de E da forma $V_p = \pi(U_p)$, onde $U_p \subseteq \mathbb{C}$ é uma vizinhança aberta de q (com $\pi(q) = p$) suficientemente pequena de modo que $\pi|_{U_p}$ é injetor. Assim, temos um homeomorfismo dado pela "inversa local" $\varphi_p : V_p \to U_p$ e obtemos um atlas euclidiano $\{(V_p, \varphi_p)\}_{p \in H}$. É simples verificar que as funções de transição serão translações o que implica que são holomorfas.

As duas afirmações listadas seguem da construção da estrutura complexa sobre E. □

Assim, concluímos que para cada reticulado $\Lambda \subseteq \mathbb{C}$, a curva elíptica $E_\Lambda := \mathbb{C}/\Lambda$ é uma superfície de Riemann que também é compacta. Daí, as funções Λ-periódicas $\wp(z, \Lambda)$ e $\wp'(z, \Lambda)$ obtidas na Proposição 3.1.11 definem funções meromorfas em E_Λ que denotamos por $\wp_\Lambda$ e $\wp'_\Lambda$, omitindo o índice Λ quando o reticulado estiver implícito.

Outra propriedade que curvas elípticas complexas possuem é que todas tem o mesmo gênero:

Proposição 3.1.13. *Para todo reticulado $\Lambda \subseteq \mathbb{C}$, a curva elíptica complexa E_Λ é uma superfície de Riemann compacta de gênero um.*

Demonstração: De acordo com a discussão acima, basta mostrar que $X = E_\Lambda$ têm gênero um. Uma possibilidade, que pode ser feita de imediato, é usar que E_Λ é homeomorfa a um toro que possui gênero topológico um. Porém, usamos aqui a equivalência entre os gêneros topológico e geométrico feita na Observação 1.4.16, que utiliza fatos sofisticados de Geometria Complexa.

Assim, mostramos de outra maneira utilizando o teorema de Riemann-Hurwitz. A função $\wp(z, \Lambda)$ é uma função meromorfa em $\mathbb{C}$. Logo, temos uma aplicação holomorfa $\wp : \mathbb{C} \to \mathbb{P}^1$. Mas a partir da Proposição 3.1.13, $\wp$ induz uma aplicação holomorfa $E_\Lambda \to \mathbb{P}^1$ que também denotamos por $\wp$.

Agora, como o único "polo" de $\wp$ em E_Λ é $0 + \Lambda$ e tem ordem dois, segue que o grau de $\wp$ é dois e que $\wp$ se ramifica neste ponto. Os outros pontos de ramificação serão dados por $z + \Lambda$, $z \notin \Lambda$, onde $\wp'(z, \Lambda) = 0$, pois neste pontos, não temos uma vizinhança no qual $\wp$ é injetor (ver Proposição 1.1.13 do [Huy04]).

Na demonstração da Proposição 3.1.11, vimos como é a série que define $\wp'(z, \Lambda)$. A partir dela, concluímos que $0 + \Lambda$ é o único "polo" de $\wp'$ em E_Λ com ordem três. Mas, pelo item ii) da Proposição 3.1.9 (ou mesmo a Proposição 1.4.3), $\wp'$ possui, contando multiplicidades, três zeros em E_Λ.

Como $\wp(z,\Lambda)$ é par, segue que $\wp'(z,\Lambda)$ é ímpar. Daí, se $\alpha \in \mathbb{C}$ é tal que $2\alpha \in \Lambda$, temos

$$\wp'(\alpha,\Lambda) = \wp'(2\alpha-\alpha,\Lambda) = \wp'(-\alpha,\Lambda) = -\wp'(\alpha,\Lambda) \Rightarrow \wp'(\alpha) = 0.$$

Assim, se (λ_1,λ_2) é uma $\mathbb{Z}$-base de Λ, concluímos que

$$\frac{\lambda_1}{2}+\Lambda, \quad \frac{\lambda_2}{2}+\Lambda, \quad \frac{\lambda_1+\lambda_2}{2}+\Lambda$$

junto com $0+\Lambda$ são os pontos de ramificação de $\wp$, todos com índice de ramificação dois. Portanto, pelo Teorema 1.4.21, segue que

$$2-2g_{E_\Lambda} = 2-2g_{\mathbb{P}^1}-4(2-1) = -2 \Rightarrow g_{E_\Lambda} = 1.$$

□

Concluímos que toda curva elíptica complexa é uma superfície de Riemann compacta de gênero um com um ponto destacado. Vamos ver que vale a recíproca: a ideia é definir o seguinte "mapa" de integração:

$$p \mapsto \int_{p_X}^{p} \omega$$

onde $\omega \in H^0(X,\Omega_X)$ é um gerador (veja a Seção 1.10 do [For81] para a definição de integração de formas diferenciais). O problema é que ele depende de uma escolha de um caminho de p_X a p e logo, não está bem-definido. Mas, para duas escolhas diferentes de caminhos, as integrais diferem por um quantidade do tipo $\int_\gamma \omega$, onde γ é um caminho fechado em X. Assim, se mostrarmos que o conjunto

$$P = \left\{ \int_\gamma \omega \colon \gamma \text{ caminho fechado} \right\} \subseteq \mathbb{C}$$

é um reticulado, obtemos um mapa bem-definido $X \to \mathbb{C}/P$. Daí, restaria mostrar que tal mapa é um isomorfismo.

Como estamos tratando de caminhos fechados em X, vamos considerar o grupo de homologia $H_1(X,\mathbb{Z})$. Nele, pode-se definir um mapa de integração

$$[\delta] \to \int_\delta \omega.$$

Dessa forma, o conjunto P pode ser reescrito como

$$P = \left\{ \int_\delta \omega \colon [\delta] \in H_1(X,\mathbb{Z}) \right\}.$$

que pode ser interpretado como os **períodos** de ω. Registramos abaixo a

Proposição 3.1.14. *O conjunto P é um reticulado de $\mathbb{C}$.*

Demonstração: Ver Teorema 21.4 do [For81] no caso geral. □

Assim, definimos o **mapa de Abel-Jacobi** como

$$\begin{aligned} j : X &\to \mathbb{C}/P \\ p &\mapsto \int_{p_X}^{p} \omega \pmod{P}. \end{aligned}$$

e dizemos que $\mathbb{C}/P$ é a **jacobiana** de X. Queremos mostrar que j é um isomorfismo. Por $\mathbb{Z}$-linearidade, j se estende a $\mathrm{Div}(X)$, que também denotamos por j. Sobre este mapa, temos o seguinte teorema

Teorema 3.1.15 (Abel). *Se $D \in \mathrm{Div}^0(X)$, então $j(D) = 0 \pmod P$ se e somente se D é principal.*

Demonstração: Isto segue do Teorema 20.7 do [For81]. □

Assim, concluímos com o

Teorema 3.1.16. *Seja X uma superfície de Riemann compacta de gênero um com um ponto destacado p_X. Então, existe um reticulado $\Lambda \subseteq \mathbb{C}$ tal que $X \cong \mathbb{C}/\Lambda$ onde o isomorfismo pode ser tomado de modo que p_X é levado para $0 + \Lambda$.*

Demonstração: Como X tem gênero um, tome $\omega \in \Omega_X(X)$ uma forma diferencial holomorfa que gera $H^0(X, \Omega_X)$. Considere o mapa de Abel-Jacobi

$$\begin{aligned} j : X &\to \mathbb{C}/P \\ p &\mapsto \int_{p_X}^{p} \omega \pmod P. \end{aligned}$$

Primeiro, vamos mostrar que j é uma aplicação holomorfa. Se $p \in X$ e (U, z) é uma carta holomorfa com $z(p) = 0$, segue que j é descrito localmente por

$$j(z) = \int_0^z \eta \pmod P.$$

onde ω é localmente dado por $\omega = \eta\, dz$ em volta de p.

Em seguida, vamos provar que j é injetor. Suponha que $p, q \in X$ são distintos tais que $j(p) = j(q)$. Então, $D = 1 \cdot p - 1 \cdot q \in \mathrm{Div}^0(X)$ é tal que $j(D) = 0 \pmod P$. Pelo Teorema 3.1.15, existe $f \in \mathcal{M}(X)$ com $\mathrm{div}(f) = D$. Assim, a aplicação

$$\hat{f} : X \to \mathbb{P}^1$$

obtida pela Proposição 1.1.12 é tal que $\hat{f}^{-1}(\infty) = \{q\}$ e $e_{\hat{f}}(q) = 1$. Logo, pela Proposição 1.3.9, $\hat{f}$ tem grau um e portanto, um isomorfismo. Mas isto não pode ocorrer pois os gêneros de X e $\mathbb{P}^1$ são distintos.

Daí, j será uma aplicação holomorfa de grau um entre X e $\mathbb{C}/P$ que são superfícies de Riemann compactas. Assim, tomando $\Lambda = P$, j será um isomorfismo $X \to \mathbb{C}/\Lambda$ que leva p_X em $0 + \Lambda$. □

3.1.4 Algebrização

A príncipio, curvas elípticas complexas são superfícies de Riemann compactas. Ou seja, são objetos de caráter analítico. Nesta seção, vamos mostrar que estes objetos podem ser vistos como curvas algébricas projetivas.

Em primeiro lugar, recordamos que dado um reticulado $\Lambda \subseteq \mathbb{C}$, construímos uma função meromorfa Λ-periódica especial, a função $\wp$ de Weierstraß, definida como

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Pela Proposição 3.1.11, $\wp$ define uma função meromorfa na superfície de Riemann $E_\Lambda = \mathbb{C}/\Lambda$. Em torno de $z = 0 + \Lambda$, a expansão em série de Laurent pode ser obtida da seguinte maneira:

O termo geral no somatório pode ser reescrito como

$$\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} = \frac{1}{\lambda^2} \left(\frac{1}{(1 - z/\lambda)^2} - 1 \right).$$

Recordamos que para $|w| < 1$, vale que

$$\frac{1}{(1-w)^2} = 1 + 2w + 3w^2 + \dots$$

Assim, para $|z|$ suficientemente pequeno, para todo $\lambda \in \Lambda\backslash\{0\}$ vale que

$$\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} = \frac{1}{\lambda^2}\left(2\left(\frac{z}{\lambda}\right) + 3\left(\frac{z}{\lambda}\right)^2 + \dots\right) = \sum_{k=1}^{\infty} \frac{(k+1)}{\lambda^{k+2}} z^k.$$

Portanto, a expansão de $\wp$ em torno de $z = 0$ é dada por

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}$$

onde G_{2k} é a **série de Eisenstein (de peso $2k$)**, dada por

$$G_{2k}(\Lambda) := \sum_{\lambda \in \Lambda\backslash\{0\}} \frac{1}{\lambda^{2k}}.$$

Assim, derivando termo a termo, obtemos a expansão em série de Laurent de $\wp'$ em torno de $z = 0 + \Lambda$:

$$\wp'(z, \Lambda) = -\frac{2}{z^3} + \sum_{k=1}^{\infty} 2k(2k+1) G_{2k+2} z^{2k-1}.$$

A partir destas expressões, podemos obter uma relação algébrica entre $\wp$ e $\wp'$.

Proposição 3.1.17. *Dado um reticulado $\Lambda \subseteq \mathbb{C}$, as funções $\wp$ e $\wp'$ são algebricamente dependentes. Mais precisamente,*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4(\Lambda)\wp(z) - 140G_6(\Lambda).$$

Demonstração: Perto de $z = 0 + \Lambda$, temos as seguintes expansões em série de Laurent

$$\begin{aligned}
\wp'(z)^2 &= \left(-\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 - \dots\right)^2 \\
&= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 \dots \\
\wp(z)^3 &= \left(\frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 \dots\right)^3 \\
&= \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + \dots
\end{aligned}$$

Então, $\wp'(z)^2 - 4\wp(z)^3$ não tem o termo com $\frac{1}{z^6}$ e a sua expansão em série de Laurent em torno de $0 + \Lambda$ é

$$\wp'(z)^2 - 4\wp(z)^3 = -\frac{60G_4}{z^2} - 140G_6 + \dots$$

Assim, $\wp'(z)^2 - 4\wp(z)^3 + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda)$ é uma função holomorfa em E_Λ que se anula em $0 + \Lambda$. Portanto, ela é identicamente nula e o resultado segue. □

A partir desta relação algébrica, obtemos uma maneira de reinterpretar E_Λ como uma *curva algébrica projetiva complexa*. Isto está mais detalhado abaixo. Aqui, denotamos $60G_4(\Lambda)$ e $140G_6(\Lambda)$ por $g_4(\Lambda)$ e $g_6(\Lambda)$ respectivamente.

Proposição 3.1.18. *Seja $\Lambda \subseteq \mathbb{C}$ um reticulado. Então:*

(i) *O polinômio* $f(x) = 4x^3 - g_4(\Lambda)x - g_6(\Lambda)$ *possui raízes distintas.*

(ii) *O polinômio homogêneo*

$$F(X, Y, Z) = Y^2Z - 4X^3 + g_4(\Lambda)XZ^2 + g_6(\Lambda)Z^3$$

define um conjunto de zeros $\mathcal{E}_\Lambda$ *em* $\mathbb{CP}^2$ *que admite uma estrutura natural de superfície de Riemann.*

(iii) *Se definimos* $\Psi_\Lambda : E_\Lambda \to \mathbb{CP}^2$ *como*

$$\Psi_\Lambda(z + \Lambda) = \begin{cases} (\wp(z) : \wp'(z) : 1) & \text{se } z \notin \Lambda \\ (0 : 0 : 1) & \text{caso contrário.} \end{cases}$$

Então, Ψ_Λ *define um isomorfismo (de superfícies de Riemann) entre* E_Λ *e* $\mathcal{E}_\Lambda$.

Demonstração: (i) Vimos na demonstração da Proposição 3.1.13 que se (λ_1, λ_2) é uma $\mathbb{Z}$-base de Λ, então

$$\alpha_1 = \frac{\lambda_1}{2}, \quad \alpha_2 = \frac{\lambda_2}{2}, \quad \alpha_3 = \frac{\lambda_1 + \lambda_2}{2}$$

são raízes de $\wp'(z, \Lambda)$. Logo, $\wp(\alpha_1, \Lambda), \wp(\alpha_2, \Lambda), \wp(\alpha_3, \Lambda)$ são raízes de f. Resta mostrar que os valores acima são distintos.

Vamos mostrar que $\wp : E_\Lambda \to \mathbb{C}$ assume o valor $\wp(\alpha_1, \Lambda)$ apenas uma vez (para os outros valores, temos um raciocínio análogo). Considere a função

$$g(z) := \wp(z, \Lambda) - \wp(\alpha_1, \Lambda).$$

Então, α_1 é um zero de g, com ordem pelo menos dois, pois $g'(\alpha_1) = \wp'(\alpha_1, \Lambda) = 0$. Mas, se considerarmos a função meromorfa induzida $g : E_\Lambda \to \mathbb{C}$, temos $v_g(0 + \Lambda) = -2$ e $v_g(\alpha_1 + \Lambda) \geq 2$. Como $0 + \Lambda$ é o único polo de g, segue do item ii) da Proposição 3.1.9 que $\alpha_1 + \Lambda$ é o único zero de g e provamos o que queríamos.

Assim, como os pontos $\alpha_i + \Lambda \in E_\Lambda$, $i = 1, 2, 3$ são distintos, concluímos que α_1, α_2, α_3 são distintos.

(ii) Isto segue essencialmente do item anterior e do critério das derivadas parciais.

(iii) Ver Proposição 3.7 do [Mil06].

□

3.1.5 Isogenias e Torção

Nesta seção, vamos tratar da noção de *isogenia*. De maneira vaga, isto seria o análogo correto de morfismos entre curvas elípticas. Segue abaixo a definição no caso complexo

Definição 3.1.19. Sejam E e E' curvas elípticas complexas. Uma **isogenia** é uma aplicação holomorfa não-constante $\phi : E \to E'$ tal que $\phi(0_E) = 0_{E'}$. Denotamos o conjunto de tais mapas, junto com o mapa constante igual a $0_{E'}$, por $\mathrm{Hom}(E, E')$.

Temos a seguinte caracterização:

Proposição 3.1.20. *Toda isogenia entre curvas elípticas complexas é um homomorfismo de grupos. Mais especificamente, sejam* $\Lambda, \Lambda' \subseteq \mathbb{C}$ *reticulados. Então,* $\phi : E_\Lambda \to E_{\Lambda'} \in \mathrm{Hom}(E, E')$ *se e somente se é da forma* $\phi(z + \Lambda) = \alpha z + \Lambda'$ *com* $\alpha \in \mathbb{C}$ *tal que* $\alpha\Lambda \subseteq \Lambda'$.

Demonstração: Ver Proposição 3.3 do [Mil06]. □

Segue da proposição acima que toda isogenia não-constante é **não-ramificada**, ou seja, o índice de ramificação de ϕ em todo ponto é igual a 1. Assim, pela Proposição 1.3.8 tal mapa é um mapa de recobrimento finito. Daí, dizemos que o **grau** da isogenia ϕ é o número de pontos em uma fibra qualquer de ϕ, ou seja, o grau da aplicação holomorfa. No caso da isogenia constante $\phi \equiv 0_{E'}$, dizemos por convenção que o grau é zero.

Se E é uma curva elíptica complexa, as isogenias de E nela mesma são ditos **endomorfismos** e o seu conjunto é denotado por $\mathrm{End}(E)$. Assim, temos as seguintes interpretações.

$$\mathrm{Hom}(E_\Lambda, E_{\Lambda'}) = \{\alpha \in \mathbb{C} \colon \alpha\Lambda \subseteq \Lambda'\} \qquad \text{e} \qquad \mathrm{End}(E_\Lambda) = \mathrm{End}(\Lambda) \coloneqq \{\alpha \in \mathbb{C} \colon \alpha\Lambda \subseteq \Lambda\}.$$

Corolário 3.1.21. *Duas curvas elípticas E_Λ e $E_{\Lambda'}$ são isomorfas se e somente se existe $\alpha \in \mathbb{C}^*$ tal que $\alpha\Lambda = \Lambda'$.*

Segue que temos uma bijeção

$$\left\{\begin{array}{c}\text{classes de homotetia de} \\ \text{reticulados } \Lambda \subseteq \mathbb{C}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{classes de isomorfismo de} \\ \text{curvas elípticas complexas}\end{array}\right\}$$
$$\Lambda \mapsto E_\Lambda$$

Dada uma curva elíptica complexa E_Λ, uma classe importante de isogenias é fornecida pela multiplicação por m, com $m \in \mathbb{Z}$ e denotada por $[m]$. Isto nos dá um homomorfismo injetor $\mathbb{Z} \to \mathrm{End}(E)$. Mas para certos reticulados Λ, tal homomorfismo não é sobrejetor e temos mais endomorfismos que, como vimos, são induzidos pela multiplicação por um complexo. Neste caso, dizemos que E_Λ, ou Λ, admite *multiplicação complexa*.

Exemplo 3.1.22. Um exemplo de reticulado com multiplicação complexa é $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ com $\tau \notin \mathbb{R}$ inteiro algébrico de grau dois. De fato, como τ satisfaz uma equação do tipo

$$\tau^2 + a\tau + b = 0,$$

com $a, b \in \mathbb{Z}$, segue que $\tau \cdot \Lambda = \tau(\mathbb{Z} + \tau\mathbb{Z}) \subseteq \mathbb{Z} + \tau\mathbb{Z}$ e concluímos que $\tau \in \mathrm{End}(E)$. Em particular, os reticulados do Exemplo 3.1.2 admitem multiplicação complexa.

Os pontos do núcleo de $[n]$, $n \geq 1$, denotado por $E[n]$, são chamados de **pontos de n-torção** de E. Sobre este conjunto, temos.

Proposição 3.1.23. *Para $m \geq 1$ e E curva elíptica complexa, temos $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ como grupos abelianos. Em particular, temos que $[m]$ tem grau m^2.*

Demonstração. Se $E = E_\Lambda$, com $\Lambda \subseteq \mathbb{C}$ reticulado. Então, é simples verificar que para (λ_1, λ_2) uma $\mathbb{Z}$-base de Λ, temos

$$E[m] = \left\{\left(i \cdot \frac{\lambda_1}{n} + j \cdot \frac{\lambda_2}{n}\right) + \Lambda \colon 0 \leq i, j < n\right\}.$$

□

3.2 Perspectiva Algébrica

Desta vez, vamos estudar as curvas elípticas como curvas algébricas. A seguinte definição imita alguns aspectos do caso complexo

Definição 3.2.1. Seja k um corpo perfeito. Uma **curva elíptica sobre** k é uma curva algébrica projetiva definida sobre k que é lisa de gênero um. Ela também será munida de um ponto k-racional, que será denotado por 0_E. Quando o corpo base não for mencionado, assume-se que esta definido sobre o seu fecho algébrico $\bar{k}$.

3.2.1 Equação de Weierstraß

Nosso objetivo é obter uma descrição mais simples de curvas elípticas. Veremos que toda curva elíptica sobre um corpo k é isomorfa a uma curva projetiva plana dada por uma equação cúbica de um certo tipo. Tal equação é chamada **equação de Weierstraß**.

Teorema 3.2.2. *Seja X/k uma curva elíptica. Então, existem $a_1, a_2, a_3, a_4, a_6 \in k$ tais que X é isomorfa a curva projetiva E definida pela equação*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

E mais, podemos escolher um isomorfismo que leva 0_E ao ponto $[0, 1, 0]$.

Tal teorema é consequência direta da seguinte

Proposição 3.2.3. *Seja X/k uma curva elíptica com ponto base O_X. Então:*

(i) Existem $x, y \in k(X)$ tais que o morfismo

$$\phi : X \to \mathbb{P}^2$$

dado por $\phi = (x : y : 1)$ nos dá um k-isomorfismo entre X e uma curva em $\mathbb{P}^2$ dada por

$$E : T^2 + a_1ST + a_3T = S^3 + a_2S^2 + a_4S + a_6, \qquad (*)$$

*com $a_1, a_2, a_3, a_4, a_6 \in k$ e $\phi(O_X) = (0 : 1 : 0)$. Tais funções x e y são ditas **coordenadas de Weierstraß** para X.*

(ii) Se duas equações de Weierstraß são obtidas como acima, então uma é obtida a partir da outra por uma mudança de variável do tipo

$$S = u^2S' + r$$
$$T = u^3T' + su^2S' + t$$

com $u \in k^*$ e $r, s, t \in k$.

(iii) Se $E \subseteq \mathbb{P}^2$ é dado por uma equação do tipo $(*)$, então E/k é uma curva elíptica, onde o ponto base pode ser tomado como sendo o ponto $(0 : 1 : 0)$.

Demonstração. (i) Como X tem gênero um, pelo item (c) do Corolário 2.4.27, $\ell(D) = \deg D$ se $\deg D \geq 0$. Em particular, $\ell(n \cdot O_X) = n$ para $n \geq 0$.

Em $\mathcal{L}(1 \cdot O_x)$ temos as funções constantes e segue que não existe $f \in \bar{k}(X)^*$ com um polo de ordem um em O_X. Em $\mathcal{L}(2 \cdot O_X)$, além das funções constantes, existe $x \in \bar{k}(X)^*$ que possui um polo de ordem dois em O_X. Assim, $(1, x)$ é uma $\bar{k}$-base de $\mathcal{L}(2 \cdot O_X)$. Por um raciocínio similar, existe $y \in \bar{k}(X)^*$ com polo de ordem três em O_X tal que $(1, x, y)$ é uma $\bar{k}$-base de $\mathcal{L}(3 \cdot O_X)$. A partir da Observação 2.4.31, pode-se obter uma $\bar{k}$-base $(1, x, y)$ de $\mathcal{L}(3 \cdot O_X)$ com $x, y \in k(X)$.

Com isso, temos que $v_{O_X}(x^2) = -4$, $v_{O_X}(xy) = -5$ e segue que $(1, x, y, x^2, xy)$ é uma $\bar{k}$-base de $\mathcal{L}(5 \cdot O_X)$. Porém, em $\mathcal{L}(6 \cdot O_X)$ também temos y^2 e x^3, completando o conjunto

$$W = \{1, x, y, x^2, xy, y^2, x^3\}$$

de sete funções em $\mathcal{L}(6 \cdot O_X)$ que é linearmente dependente sobre $\bar{k}$. Mas, por conta da igualdade $\dim_k \operatorname{span}_k W = \dim_{\bar{k}} \operatorname{span}_{\bar{k}} W$, segue que W também é linearmente dependente sobre k. Assim, existem $\alpha_1, \ldots, \alpha_7 \in k$ tais que

$$\alpha_1 + \alpha_2x + \alpha_3y + \alpha_4x^2 + \alpha_5xy + \alpha_6y^2 + \alpha_7x^3 = 0.$$

Temos que $a_6, a_7 \neq 0$ pois caso contrário, teríamos uma contradição em relação à ordem do polo em O_X ou ao fato de que $(1, x, y, x^2, xy)$ é linearmente independente sobre k.

Assim, através da substituição $(x, y) \mapsto (-a_6a_7x, a_6a_7^2y)$, os coeficientes de x^2 e y^3 serão iguais a um. Dai, para tais x e y, o morfismo

$$\phi : X \to \mathbb{P}^2$$

dado por $\phi = (x : y : 1)$ tem imagem em uma curva E dada por uma equação do tipo $(*)$ e satisfaz $\phi(O_X) = (0 : 1 : 0)$ por conta das ordem de anulamento de x e y em O_X.

Resta mostrar que ϕ induz um isomorfismo entre curvas lisas. Começamos provando que ϕ é um mapa racional de grau um, ou seja, que $[k(X) : \phi^*k(E)] = 1$. Como $k(E) = k(s, t)$, onde $s = X/Z$ e $t = Y/Z$, segue que $\phi^*k(E) = k(x, y)$. Assim, queremos mostrar que $k(E) = k(x, y)$.

A partir dos mapas

$$\begin{aligned} \phi_x : X &\to \mathbb{P}^1 & \qquad \phi_y : X &\to \mathbb{P}^1 \\ p &\mapsto (x(p) : 1) & \qquad p &\mapsto (y(p) : 1) \end{aligned}$$

e do item (a) da Proposição 2.3.18 concluímos que

$$\deg \phi_x = [k(X) : k(x)] = 2 \quad \text{e} \quad \deg \phi_y = [k(X) : k(y)] = 3,$$

e concluímos que $k(X) = k(x, y)$.

Agora, vamos provar que E é de fato lisa. Se E fosse singular, pela Proposição X, existiria um mapa racional $\psi : E \to \mathbb{P}^1$ de grau um, Dai, $\psi \circ \phi : X \to \mathbb{P}^1$ seria um mapa entre curvas lisa de grau um e, portanto, um isomorfismo. Mas isto contradiz o fato de que $g_X = 1$ e $g_{\mathbb{P}^1} = 0$.

Juntando as conclusões acima, concluímos que $\phi : X \to E$ é um (k-)isomorfismo entre curvas lisas.

(ii) Se (x, y) e (x', y') são coordenadas de Weierstraß, então através dos isomorfismos ϕ, as funções x, x' correspondem a $s = X/Z$, enquanto que y, y' correspondem a $t = Y/Z$. Após algumas contas, vemos que para $P = (0 : 1 : 0) \in E$, $v_P(s) = -2$ e $v_P(t) = -3$. Assim, concluímos que $v_{O_X}(x) = v_{O_X}(x') = -2$ e $v_{O_X}(y) = v_{O_X}(y') = -3$ e segue que $(1, x, y)$ e $(1, x', y')$ são k-bases de $\mathcal{L}(3 \cdot O_X) \cap k(X)$.

Então, levando em contas as ordens de anulamento em O_X, temos a seguinte identidade

$$\begin{pmatrix} 1 & x & y \end{pmatrix} = \begin{pmatrix} 1 & x' & y' \end{pmatrix} \begin{bmatrix} 1 & r & t \\ & \alpha_1 & \beta_2 \\ & & \alpha_2 \end{bmatrix}$$

para $\alpha_1, \alpha_2 \in k^*$ e $\beta_2, r, t \in k$. Substituindo as expressões de x e y' na equação de Weierstraß obtida a partir de (x', y'), conclui-se que devemos ter $\alpha_1^3 = \alpha_2^2$. Usando a parametrização $u \mapsto (u^2, u^3)$ da cúspide $y^2 = x^3$, segue que existe $u \in k^*$ tal que $\alpha_1 = u^2$ e $\alpha_2 = u^3$. Assim, fazendo $s = \beta_2/u^2$, obtemos

$$\begin{pmatrix} 1 & x & y \end{pmatrix} = \begin{pmatrix} 1 & x' & y' \end{pmatrix} \begin{bmatrix} 1 & r & t \\ & u^2 & su^2 \\ & & u^3 \end{bmatrix}$$

e o resultado segue.

(iii) Seja $E \subseteq \mathbb{P}^2$ lisa, dada por uma equação de Weierstraß

$$T^2 + a_1ST + a_3T = S^3 + a_2S^2 + a_4S + a_6.$$

Note que $(0:1:0)$ é um ponto k-racional de E. Assim, resta mostrar que E tem gênero um. Temos duas maneiras

- Verificar que a forma diferencial

$$\omega = \frac{1}{2y + a_1x + a_3}dx \in \Omega_E$$

satisfaz $\mathrm{div}(\omega) = 0$ (ver Proposição III.1.5 do [Sil09]). Assim, $K_E = 0$ e sgue do item (b) do Corolário 2.4.27 que $g_E = 1$.

- Usar o Teorema de Riemann-Hurwitz 2.4.30 para deduzir o seguinte resultado (ver Exercício 2.7 do [Sil09]):

Se $X \subseteq \mathbb{P}^2$ é uma curva lisa definida por um polinômio homogêneo de grau d, então

$$g_X = \frac{(d-1)(d-2)}{2}.$$

□

Assim, toda curva elíptica pode ser "mergulhada" no plano projetivo e a equação que a define pode ser escolhida como sendo a do tipo descrito no teorema acima. Portanto, na maior parte das vezes, definimos curvas elípticas como curvas planas definidas por polinômios (homogêneos) de grau 3. Em muitos casos, damos apenas uma equação afim (em duas variáveis) que define uma curva afim em $\mathbb{A}^2$ mas na verdade, nos referimos ao *fecho projetivo* (ver Definição 2.2.8).

Prosseguimos discutindo um pouco mais sobre curvas cúbicas planas definidas por uma equação do tipo

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

com $a_1, a_2, a_3, a_4, a_6 \in \bar{k}$. Vamos nos referir a elas como **(curvas) cúbicas de Weierstraß**. Destacamos que elas não necessariamente definem curvas lisas.

Em uma cúbica de Weierstraß E, temos sempre o ponto $O = (0:1:0)$ e, de fato, é o único ponto na reta no infinito $Z = 0$. Em volta deste ponto, ou seja, no aberto afim $E \cap \{Y \neq 0\}$, Z é o ponto $(0,0)$ da curva afim

$$z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Expandindo o polinômio $g(x,y) = z + a_1xz + a_3z^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$ em volta de $(0,0)$, obtemos

$$g(x,z) = z + (a_1xz + a_3z^2) - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3)$$

e segue que $z = 0$, que corresponde a reta $Z = 0$ em $\mathbb{P}^2$ é a reta tangente a E no ponto O.

E mais, substituindo $z = 0$ na equação acima obtemos $x^3 = 0$ e concluímos que O é um *ponto de inflexão* de E, ou seja, cuja reta tangente intersecta E com multiplicidade pelo menos 3 (veja o Problema 3.12 do [Ful08]).

A menos do ponto O, toda cúbica de Weierstraß pode ser considerada como o aberto afim

$$E_{\text{afim}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

O motivo da numeração dos coeficientes a_i é que através da mudança de variável $(x,y) \mapsto (u^2x', u^3y')$, obtemos $a_i = u^ia_i'$ para $i = 1,2,3,4,6$.

Se $\mathrm{char}\, k \neq 2,3$ podemos simplificar a equação que define E para uma da forma

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

Neste caso, definimos as seguintes quantidades

- coeficiente $c_4 = -48A$
- discriminante: $\Delta = -16(4A^3 + 27B^2)$
- j-invariante: $j = -1728\frac{(4A)^3}{\Delta}$

Elas também podem ser definidas para uma cúbica de Weiestraß qualquer cujas expressões estão na Seção III.1 do [Sil09].

As únicas mudanças de variável descritas no item (ii) da Proposição 3.2.3 que preservam a forma simplificada são da forma

$$x = u^2 x'$$
$$y = u^3 y'$$

com $u \in \bar{k}^*$. Após uma tal substituição, temos as fórmulas de transformação

$$A' = \frac{A}{u^4}, \quad B' = \frac{B}{u^6}, \quad \Delta' = \frac{\Delta}{u^{12}}.$$

e segue que $j' = j$.

Sobre os possíveis pontos singulares, começamos com

Proposição 3.2.4. *Para toda cúbica de Weierstraß, o ponto $O = (0 : 1 : 0)$ é sempre um ponto liso.*

Demonstração. Segue do critério das derivadas parciais na curva afim $E \cap U_1$, onde $U_1 \subseteq \mathbb{P}^2$ é o aberto afim dos pontos $(x : y : z)$ com $y \neq 0$. □

Assim, suponha que $(\alpha : \beta : 1)$ é um ponto singular de uma cúbica de Weierstraß E. Então, (α, β) será um ponto singular de E_{afim} e segue que

$$\frac{\partial f}{\partial x}(\alpha, \beta) = \frac{\partial f}{\partial y}(\alpha, \beta) = 0, \quad \text{onde } f = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6.$$

Assim, expandindo $f(x, y)$ em volta de (α, β), segue que

$$f(x,y) = \frac{1}{2}\frac{\partial^2 f}{\partial x^2}(\alpha,\beta)(x-\alpha)^2 + \frac{\partial^2 f}{\partial x \partial y}(\alpha,\beta)(x-\alpha)(y-\beta) + \underbrace{\frac{1}{2}\frac{\partial^2 f}{\partial y^2}(\alpha,\beta)}_{=1}(y-\beta)^2 + -(x-\alpha)^3.$$

O termo quadrático pode ser fatorado em $\bar{k}$ em dois termos lineares em $x - \alpha$ e $y - \beta$, resultando em

$$f(x,y) = ((y-\beta) - \lambda(x-\alpha))((y-\beta) - \lambda'(x-\alpha)) - (x-\alpha)^3$$

para certos $\lambda, \lambda' \in \bar{k}$. Estes dois fatores lineares podem ser interpretados com as **retas tangentes** a E_{afim} no ponto (α, β) (veja a Seção 3.1 do [Ful08]).

Então, existem dois tipos de pontos singulares

- **nó**: quando $\lambda \neq \lambda'$, ou seja, quando existem duas retas tangentes em (α, β). Um exemplo clássico é a cúbica $y^2 = x^3 + x^2$.
- **cúspide**: quando $\lambda = \lambda'$, ou seja, temos uma reta tangente "dupla" em (α, β). Um exemplo clássico é a cúbica $y^2 = x^3$.

A seguinte proposição mostra alguns resultados envolvendo cúbicas de Weierstraß

Proposição 3.2.5. *Sejam $E, E' \subseteq \mathbb{P}^2$ cúbicas de Weierstraß. Então:*

(i) (Critério de Singularidade)

- *E é lisa se, e somente se, $\Delta \neq 0$.*
- *E possui nó se, e somente se, $\Delta = 0$ e $c_4 \neq 0$.*
- *E possui cúspide se, e somente se, $\Delta = 0$ e $c_4 = 0$.*

(ii) O j-invariante parametriza as classes de isomorfismo de curvas elípticas no seguinte sentido:

- *Se E e E' são lisas, então elas são isomorfas (sobre $\bar{k}$ apenas) se, e somente se, $j = j'$.*
- *Para todo $j_0 \in \bar{k}$, existe uma cúbica de Weierstraß lisa $E/k(j_0)$ tal que $j = j_0$.*

Demonstração. Ver Proposição III.1.4 do [Sil09]. □

3.2.2 A Lei de Grupo

Nesta seção, vamos mostrar essencialmente que toda curva elíptica X com ponto base O_X é um grupo algébrico no qual o ponto O_X é o elemento netro. Vamos ver duas maneiras de fornecer uma estrutura de grupo no conjunto dos pontos $X(\bar{k})$.

Começamos assumindo que $X = E \subseteq \mathbb{P}^2$ é uma cúbica de Weierstraß lisa com ponto base $O_X = O = (0 : 1 : 0)$. Se P e Q são pontos de E, denotamos a reta que passa por P e Q por ℓ_{PQ}[1]. Pelo teorema de Bézout (ver Seção 5.3 do [Ful08]) ou de maneira mais elementar olhando no sistema de equações que define os pontos de interseção de ℓ_{PQ} com E, existem três pontos de interseção com multiplicidade.

Se ℓ_{PQ} é dado por uma equação linear $aX + bY + cZ = 0$, pode-se mostrar que se P, Q, R são os pontos de interseção, então temos

$$\operatorname{div}(as + bt + c) = 1 \cdot P + 1 \cdot Q + 1 \cdot R - 3 \cdot O,$$

onde $s = X/Z, t = Y/Z \in k(E)$.

A partir de $P, Q \in E(\bar{k})$, definimos $P +_W Q$ como o terceiro ponto de interseção de E com a reta ℓ_{OR}, onde R é o terceiro ponto de interseção de E com a reta ℓ_{PQ}. Esta operação possui as seguintes propriedades:

Proposição 3.2.6. *Seja $E \subseteq \mathbb{P}^2$ uma cúbica de Weierstaß lisa e $P, Q \in E(\bar{k})$. Se $R \in E(\bar{k})$ é definido como acima, então:*

(i) $(P +_W Q) +_W R = O$.

(ii) $P +_W Q = Q +_W P$.

(iii) $P +_W O = P$.

(iv) Para todo $P \in E(\bar{k})$, existe $P' \in E(\bar{k})$ tal que $P +_W P' = O$.

Ou seja, O se comporta como elemento neutro e todo ponto admite uma inverso.

Demonstração. Os três primeiros itens seguem diretamente da definição de $+_W$ e usando o fato de que a reta tangente a E no ponto O intersecta E com multiplicidade três em O. No caso do item (iv), tome P' como sendo o terceiro ponto de interseção de E com a reta ℓ_{OP} e o resultado segue do item (i). □

[1] Se $P = Q$, definimos ℓ_{PQ} como a reta tangente a E no ponto P.

A proposição acima mostra que $(E(\bar{k}), +_W)$ satisfaz os axiomas de grupo, exceto a associatividade. Existem provas elementares deste fato, ou por meio de fórmulas explicitas, ou utilizando um truque de álgebra linear envolvendo o espaço das curvas cúbicas. Ambas apesar de serem simples, nos levam a analisar vários casos, são trabalhosas e não nos dão um motivo desta operação definir um grupo.

O que faremos é provar indiretamente por meio de uma outra estrutura de grupo em $E(\bar{k})$, que utiliza principalmente o teorema de Riemann-Roch. Assumindo a associatividade, concluímos que $(E(\bar{k}), +_W)$ é um **grupo abeliano**. Notamos que a operação $+_W$ pode ser descrita de maneira mais geométrica, afirmando que *pontos colineares somam zero* de acordo com o item (i) da proposição acima. Se E/k, então o conjunto dos pontos k-racionais $E(k)$ é um subgrupo de $E(\bar{k})$.

Se E é uma cúbica de Weierstraß singular, ainda podemos definir uma estrutura de grupo, agora sobre os conjunto $E_{\text{lisa}}(\bar{k})$ dos pontos lisos de E. Neste caso, é possível descrever este grupo:

Proposição 3.2.7. *Se $E \subseteq \mathbb{P}^2$ é uma cúbica de Weierstraß singular, então $(E_{lisa}(\bar{k}), +_W$ é um grupo abeliano. Além disso*

- *Se E possui um nó, temos um isomorfismo $(E_{lisa}(\bar{k}), +_W) \cong (\bar{k}^*.\times)$.*
- *Se E possui uma cúspide, temos um isomorfismo $(E_{lisa}(\bar{k}), +_W) \cong (\bar{k}, +)$.*

Demonstração. Ver Proposição III.2.5 do [Sil09]. □

A seguir, vamos definir uma estrutura de grupo em $X(\bar{k})$, onde X é uma curva elíptica com ponto base O_X. O nosso objetivo é construir uma bijeção de $X(\bar{k})$ com o grupo abeliano $\text{Pic}^0(X)$. Começamos com um lema simples

Lema 3.2.8. *Seja (X, O_X) uma curva elíptica. Então para todo $D \in \text{Div}^0(X)$, existe um único $P = P_D \in X(\bar{k})$ tal que $D \sim 1 \cdot P - 1 \cdot O_X$.*

Demonstração. Ver Proposição III.3.4.a do [Sil09]. □

Assim, obtemos um mapa

$$\begin{aligned} \sigma : \text{Div}^0(X) &\to X(\bar{k}) \\ D &\mapsto P_D. \end{aligned}$$

Se $D \sim D'$, então pelo Lema 3.2.8, $P_D = P'_D$. Reciprocamente, se $\sigma(D) = \sigma(D')$, devemos ter $D \sim D'$. Assim, σ passa ao quociente e induz o mapa

$$\begin{aligned} \overline{\sigma} : \text{Pic}^0(X) &\to X(\bar{k}) \\ [D] &\mapsto P_D \end{aligned}$$

que será injetor. Como σ é claramente sobrejetor, segue que $\overline{\sigma}$ é uma bijeção. A sua inversa, denotada por κ, é dada por

$$\begin{aligned} \kappa : X(\bar{k}) &\to \text{Pic}^0(X) \\ P &\mapsto [1 \cdot P - 1 \cdot O_X]. \end{aligned}$$

Assim, a operação de grupo de $X(\bar{k})$ é a induzida de $\text{Pic}^0(X)$ por meio da bijeção κ e denotamos esta operação por $+_\kappa$. Por meio desta operação temos o seguinte

Corolário 3.2.9. *Sejam (X, O_X) uma curva elíptica e $D = \sum n_x \cdot x \in \text{Div}^0(X)$. Então:*

$$D \text{ é principal} \iff \sum_{x \in X(\bar{k})} [n_x](x) = O_X,$$

onde para $m \in \mathbb{Z}$, $[m] : X(\bar{k}) \to X(\bar{k})$ é o mapa de multiplicação por m.

Demonstração. Para $D \in \mathrm{Div}^0(X)$, temos as seguintes equivalências

$$\begin{aligned} D \sim 0 &\iff [D] = 0 \\ &\iff \overline{\sigma}([D]) = O_X \\ &\iff \sum_{x \in X(\bar{k})} [n_x](\overline{\sigma}([1 \cdot x])) = O_X \\ &\iff \sum_{x \in X(\bar{k})} [n_x](\overline{\sigma}([1 \cdot x])) - \sum_{x \in X(\bar{k})} [n_x](\overline{\sigma}([1 \cdot O_X])) = O_X \\ &\iff \sum_{x \in X(\bar{k})} [n_x](\overline{\sigma}(\underbrace{[1 \cdot x - 1 \cdot O_X]}_{\kappa(x)})) = O_X \\ &\iff \sum_{x \in X(\bar{k})} [n_x](x) = O_X. \end{aligned}$$

□

Assim, se definimos $S : \mathrm{Div}^0(X) \to X(\bar{k})$ é definido como $S\left(\sum n_x \cdot x\right) = \sum [n_x](x)$, temos a seguinte sequência exata de grupos abelianos

$$1 \longrightarrow \bar{k}^* \longrightarrow \bar{k}(X)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(X) \xrightarrow{S} X(\bar{k}) \longrightarrow 0\,.$$

Notamos que o mapa induzido $\bar{S} : \mathrm{Pic}^0(X) \to X(\bar{k})$ é precisamente $\overline{\sigma}$. De fato, temos para $D = \sum n_x \cdot x \in \mathrm{Div}^0(X)$

$$\kappa(\bar{S}([D])) = \kappa\Big(\sum [n_x](x)\Big) = \sum [n_x \cdot P - n_x \cdot O_X] = [D] = \kappa(\overline{\sigma}([D])).$$

Se $X = E \subseteq \mathbb{P}^2$ é uma cúbica de Weierstraß lisa, vamos mostrar que as operações $+_W$ e $+_\kappa$ coincidem. Para isso, é suficiente provarmos que $\kappa : E(\bar{k}) \to \mathrm{Pic}^0(E)$ satisfaz

$$\kappa(P +_W Q) = \kappa(P) + \kappa(Q) = \kappa(P +_\kappa Q)$$

para quaisquer $P, Q \in E(\bar{k})$. Seja R o terceiro ponto de interseção de ℓ_{PQ} com E e sejam $F, G \in \bar{k}[X, Y, Z]$ as polinômios homogêneos que definem as retas ℓ_{PQ} e ℓ_{OR} respectivamente. Então, sabemos que

$$\mathrm{div}(F/Z) = 1 \cdot P + 1 \cdot Q + 1 \cdot R - 3 \cdot O \quad \text{e} \quad \mathrm{div}(G/Z) = 1 \cdot O + 1 \cdot R + 1 \cdot (P +_W Q) - 3 \cdot O$$

o que implica que $[1 \cdot P + 1 \cdot Q] = [1 \cdot (P +_W Q) + 1 \cdot O]$ em $\mathrm{Pic}(X)$. Daí:

$$\kappa(P) + \kappa(Q) = [1 \cdot P + 1 \cdot Q - 2 \cdot O] = [1 \cdot (P +_W Q) - 1 \cdot O] = \kappa(P +_W Q).$$

A operação $+_W$ (ou $+_\kappa$) definem os mapas de adição $a : E \times E \to E$ e inversão $i : E \to E$. O conjunto $E \times E \subseteq \mathbb{P}^2 \times \mathbb{P}^2$ pode ser visto como uma variedade algébrica (de dimensão dois) de várias maneiras. Uma é considerando $E \times E$ como um conjunto algébrico definido por polinômios bihomogêneos ou pelo chamado *mergulho de Segre* $\sigma_{2,2} : \mathbb{P}^2 \times \mathbb{P}^2 \to \mathbb{P}^8$ que identifica $E \times E$ com uma subvariedade de $\mathbb{P}^8$ no sentido clássico. De qualquer modo, temos o seguinte resultado.

Teorema 3.2.10 (Curvas Elípticas são Grupos Algébricos)**.** *Os mapas de adição e inversão*

$$\begin{aligned} a : E \times E &\to E \\ (P, Q) &\mapsto P +_W Q \end{aligned} \qquad\qquad \begin{aligned} i : E &\to E \\ P &\mapsto -P \end{aligned}$$

são morfismos entre variedades projetivas.

Demonstração. Ver o Teorema III.3.6 do [Sil09]. □

3.2.3 Isogenias e Torção

No caso algébrico, temos um análogo da definição de isogenia

Definição 3.2.11. Sejam $(E, O_E), (E', O_{E'})$ curvas elípticas. Uma **isogenia** $\phi : E \to E'$ é um mapa não constante tal que $\phi(O_E) = O_{E'}$.

Às vezes, também consideremos o mapa constante $\phi \equiv O_{E'}$ como uma isogenia, apesar de não estar de acordo com a definição mais geral para variedades abelianas.

Recordamos que, se $\phi : X \to Y$ e $\psi : Y \to Z$ são mapas não-constantes entre curvas lisas, vale a fórmula

$$\deg(\psi \circ \phi) = (\deg \phi)(\deg \psi).$$

Tal fórmula pode ser estendida para ϕ e ψ constantes.

Se $\phi, \psi : E \to E'$ são morfismos, segue do Teorema 3.2.10 que $\phi + \psi : E \to E'$ dado por $(\phi + \psi)(x) = \phi(x) + \psi(x)$ também é um morfismo. Dessa forma, definimos os seguintes grupos abelianos

- $\mathrm{Hom}(E, E') := \{O_{E'}\} \cup \{\phi : E \to E' \mid \phi \text{ isogenia}\}$.
- $\mathrm{End}(E) := \mathrm{Hom}(E, E)$ (endomorfismos de E).
- $\mathrm{Aut}(E) := \mathrm{End}(E)^*$ (automorfismos de E).

O grupo $\mathrm{End}(E)$ também tem a estrutura de anel (não necessariamente comutativo) se considerarmos a multiplicação como sendo a composição. Isto pode ser facilmente verificado, exceto a distributividade

$$\phi \circ (\psi + \psi') \stackrel{?}{=} (\phi \circ \psi) + (\phi + \psi').$$

Isto será estabelecido após mostrarmos que toda isogenia é um homomorfismos de grupos abelianos.

Se (E, O_E) é uma curva elíptica, para todo $m \in \mathbb{Z}$, temos o morfismo $[m] : E \to E$ de multiplicação por m. Sobre tais mapas, temos a seguinte proposição

Proposição 3.2.12. *O mapa de multiplicação por $m \in \mathbb{Z}$, $[m] : E \to E$ é uma isogenia se $m \neq 0$.*

Demonstração. Ver Proposição III.4.2.a do [Sil09]. □

Definição 3.2.13. Seja (E, O_E) uma curva elíptica. Para $m \geq 1$, definimos o conjunto dos **pontos de m-torção**, denotado por $E[m]$, como sendo

$$E[m] := \{P \in E(\bar{k}) : [m](P) = O_E\}.$$

O **subgrupo de torção** de E, denotado por E_{tors}, é definido como $E_{\mathrm{tors}} = \bigcup_m E[m]$.

Sobre os grupos $\mathrm{Hom}(E, E')$ e $\mathrm{End}(E)$ temos o seguinte resultado. Mais tarde, vamos descrever com mais detalhes a estrutura do anel $\mathrm{End}(E)$.

Proposição 3.2.14. *Sejam E, E' curvas elípticas. Então:*

(i) $\mathrm{Hom}(E, E')$ *é um grupo abeliano sem elementos de torção, ou seja, se $m \cdot \phi = 0$, então $m = 0$ ou $\phi = 0$.*

(ii) $\mathrm{End}(E)$ *é um anel de característica zero sem divisores de zero.*

Demonstração: Os dois itens são essencialmente aplicações da fórmula do grau da composição de dois mapas discutido no começo desta subseção. Mais detalhes nos itens (b) e (c) da Proposição III.4.2 do [Sil09]. □

Observação 3.2.15. Como $\mathrm{End}(E)$ tem característica zero, temos um mapa injetor

$$\begin{aligned}[\cdot] : \mathbb{Z} &\to \mathrm{End}(E)\\ m &\mapsto [m].\end{aligned}$$

Se este mapa *não* é sobrejetor, e isto é caso bastante especial quando o corpo base tem característica zero, dizemos que E possui **multiplicação complexa**.

Abaixo estão alguns exemplos de isogenias

Exemplo 3.2.16 (Multiplicação Complexa)**.** Considere a curva elíptica $E/\mathbb{Q}$ com equação

$$E_{\text{afim}} : y^2 = x^3 - x.$$

Nela temos o seguinte endomorfismo

$$\begin{aligned}[i] : E &\to E\\ (a:b:c) &\mapsto \begin{cases}(-a/c : i\cdot b/c : 1) \text{ se } c \neq 0\\ O = (0:1:0) \text{ caso contrário.}\end{cases}\end{aligned}$$

Pode-se verificar que $[i]$ satisfaz $[i]^2 = [-1]$, o que mostra que $[i]$ não está na imagem de $\mathbb{Z}$ pelo mapa $[\cdot] : \mathbb{Z} \to \mathrm{End}(E)$, e portanto, E admite multiplicação complexa. Na verdade, $\mathrm{End}(E)$ é isomorfo a $\mathbb{Z}[i]$ pelo mapa

$$\begin{aligned}\mathbb{Z}[i] &\to \mathrm{End}(E)\\ m + ni &\mapsto [m] + [n] \circ [i].\end{aligned}$$

Em particular, temos $\mathrm{Aut}(E)$ finito e isomorfo a $\mathbb{Z}/4\mathbb{Z}$.

Exemplo 3.2.17 (Frobenius)**.** Sejam k um corpo de característica positiva p, $q = p^r$ e E/k uma cúbica de Weierstraß lisa. Recordamos que pela Observação 2.3.20, temos a curva $E^{(q)}$ e o mapa de Frobenius

$$\mathsf{F}^q : E \to E^{(q)}$$

dado por $F^q = (s^q : t^q : 1)$. Como temos o homomorfismo $\sigma : k \to k$ dado por $\sigma(a) = a^p$, a partir das equações que definem Δ e j, segue que $\Delta(E^{(q)}) = \Delta(E)^q$ e $j(E^{(q)}) = j(E)^q$. Em particular, concluímos que $E^{(q)}/k$ é uma cúbica de Weierstraß lisa e portanto, uma curva elíptica. Assim, F^q é uma isogenia (não-constante) entre E e $E^{(q)}$.

No caso $k = \mathbb{F}_q$, temos $\sigma = \mathrm{id}$ e $E^{(q)} = E$. Daí, F^q é um endomorfismo de E cujo conjunto dos pontos fixos é o conjunto dos pontos $\mathbb{F}_q$-racionais $E(\mathbb{F}_q)$.

O seguinte teorema mostra que toda isogenia é um homomorfismo de grupos abelianos. Note que será importante a descrição de $E(\bar{k})$ por $\mathrm{Pic}^0(E)$.

Teorema 3.2.18. *Sejam E, E' curvas elípticas. Então, para $\phi \in \mathrm{Hom}(E, E')$, temos*

$$\phi(P + Q) = \phi(P) + \phi(Q) \quad \forall P, Q \in E.$$

Demonstração: Isto é imediato se $\phi \equiv O_{E'}$. Caso contrário, ϕ é não-constante e podemos definir o homomorfismo

$$\phi_* : \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(E')$$

induzido pelo pushforward de divisores descrito na Observação 2.4.10. Então, temos o seguinte diagrama comutativo

$$\begin{array}{ccc} E(\bar{k}) & \xrightarrow{\phi} & E'(\bar{k}) \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa'} \\ \mathrm{Pic}^0(E) & \xrightarrow[\phi_*]{} & \mathrm{Pic}^0(E') \end{array}$$

De fato, temos

$$(\kappa' \circ \phi)(P) = \kappa'(\phi(P)) = [1 \cdot \phi(P) - 1 \cdot O_{E'}] = \phi_*([1 \cdot P - 1 \cdot O_E]) = (\phi_* \circ \kappa)(P).$$

Como κ e κ' são, por definição, isomorfismos de grupos, segue que ϕ é um homomorfismo. □

Corolário 3.2.19. *Se $\phi : E \to E'$ é uma isogenia, então $\ker \phi = \phi^{-1}(O_{E'})$ é um subgrupo finito de $E(\bar{k})$.*

Demonstração: Como ϕ é um homomorfismo de grupos, é claro que $\ker \phi$ é um subgrupo de $E(\bar{k})$. Além disso, pelo item (a) da Proposição 2.3.18, temos

$$\#\ker \phi \leq \# \sum_{\phi(x)=O_{E'}} e_\phi(x) = \deg \phi$$

o que implica que $\ker \phi$ é finito. □

Registramos abaixo os seguintes resultados que mostram como curvas elípticas se comportam de maneira semelhante a grupos abelianos.

Proposição 3.2.20 (Teorema do Isomorfismo)**.** *(i) Sejam X, Y, Z curvas elípticas e $\phi : X \to Y$, $\psi : X \to Z$ isogenias e suponha que ϕ é separável. Se $\ker \phi \subseteq \ker \psi$, então existe uma única isogenia $\lambda : Y \to Z$ tal que $\psi = \lambda \circ \phi$.*

$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ & \searrow^{\psi} & \downarrow{\scriptstyle \exists \lambda} \\ & & Z \end{array}$$

(ii) Seja X uma curva elíptica e $H \subseteq E(\bar{k})$ um subgrupo finito. Então, existe uma única curva elíptica $\hat{X}$ (ou X/H) e uma isogenia separável $\pi : X \to \hat{X}$ tal que $\ker \pi = H$.

Demonstração. Ver o Corolário III.4.11 e a Proposição III.4.12 do [Sil09], respectivamente. □

Se $\phi : E \to E'$ é uma isogenia entre curvas elípticas E e E', sabemos que o seguinte diagrama comuta:

$$\begin{array}{ccc} E(\bar{k}) & \xrightarrow{\phi} & E'(\bar{k}) \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa'} \\ \mathrm{Pic}^0(E) & \xrightarrow[\phi_*]{} & \mathrm{Pic}^0(E') \end{array}$$

Agora, desejamos obter uma isogenia no sentido contrário $\hat{\phi} : E' \to E$ a partir de ϕ. No nível dos grupos Pic^0, existe um outro mapa

$$\begin{aligned} \phi^* : \mathrm{Pic}^0(E') &\to \mathrm{Pic}^0(E) \\ [Q] &\mapsto \sum_{\phi(P)=Q} [e_\phi(P) \cdot P] \end{aligned}$$

induzido pelo pullback de divisores. Então, temos um homomorfismo $\hat{\phi} : E'(\bar{k}) \to E(\bar{k})$ tal que o seguinte diagrama é comutativo

$$\begin{array}{ccc} E(\bar{k}) & \xleftarrow{\hat{\phi}} & E'(\bar{k}) \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa'} \\ \mathrm{Pic}^0(E) & \xleftarrow[\phi^*]{} & \mathrm{Pic}^0(E') \end{array} .$$

O que faremos a seguir é mostrar que tal mapa é de fato uma isogenia e dizemos que é a **isogenia dual** de ϕ, denotada por $\hat{\phi}$. A sua caracterização segue da seguinte proposição

Proposição 3.2.21. *Seja $\phi : E \to E'$ uma isogenia de grau m. Então:*

(i) Existe uma única isogenia $\hat{\phi} : E' \to E$ tal que $\hat{\phi} \circ \phi = [m]$.

(ii) Como homomorfismo de grupos abelianos, $\hat{\phi}$ é igual a $\kappa^{-1} \circ \phi^* \circ \kappa'$.

Demonstração. Ver Teorema III.6.1 do [Sil09]. □

Assim, definimos para $\phi \in \mathrm{Hom}(E, E')$ o seu dual $\hat{\phi}$ como:

$$\hat{\phi} = \begin{cases} \kappa^{-1} \circ \phi^* \circ \kappa' & \text{se } \phi \not\equiv O_{E'} \\ O_{E'} & \text{caso contrário} \end{cases}.$$

Abaixo estão listadas algumas propriedades da isogenia dual.

Proposição 3.2.22. *Sejam X, Y, Z curvas elípticas, $\phi, \psi \in \mathrm{Hom}(X, Y)$ e $\lambda \in \mathrm{Hom}(Y, Z)$. Então:*

(i) Se $\deg \phi = m$, então $\hat{\phi} \circ \phi = [m]_E$ e $\phi \circ \hat{\phi} = [m]_{E'}$.

(ii) $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.

(iii) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.

(iv) $\widehat{[m]}_E = [m]_{E'}$ e $\deg[m] = m^2$ para todo $m \in \mathbb{Z}$.

(v) $\deg \hat{\phi} = \deg \phi$.

(vi) $\hat{\hat{\phi}} = \phi$.

Demonstração. Ver o Teorema III.6.2 do [Sil09]. □

Corolário 3.2.23. *Sejam X, Y curvas elípticas. Então, o mapa*

$$\deg : \mathrm{Hom}(X, Y) \to \mathbb{Z}$$

é uma forma quadrática positiva definida sobre $\mathbb{Z}$, ou seja, satisfaz

- $\deg(\phi) \geq 0$ *com igualdade se e só se* $\phi = 0$.
- $\deg(-\phi) = \deg(\phi)$.
- *O mapa* $(\phi, \psi) \mapsto \deg(\phi + \psi) - \deg \phi - \deg \psi$ *é $\mathbb{Z}$-bilinear.*

Demonstração: A única condição não-trivial a ser verificada é a última. Usamos a notação

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg \phi - \deg \psi.$$

Por meio da injeção $[\cdot] : \mathbb{Z} \to \mathrm{End}(X)$ temos em $\mathrm{End}(E)$

$$\begin{aligned} [\langle \phi, \psi \rangle] &= [\deg(\phi + \psi)] - [\deg \phi] - [\deg \psi] \\ &= (\widehat{\phi + \psi}) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi \quad \text{(segue dos itens (i),(ii) da Proposição 3.2.22)} \end{aligned}$$

Como esta última expressão é $\mathbb{Z}$-bilinear em ϕ e ψ, o resultado segue. □

Corolário 3.2.24. *Seja E uma curva elíptica e $m \in \mathbb{Z}$ não-nulo. Então*

(i) Se $m \neq 0$ em $\bar{k}$, então $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ como grupos abelianos.

(ii) Se $\mathrm{char}\, \bar{k} = p > 0$, então

$$E[p^e] = \{O_E\} \quad \forall e \geq 1 \qquad \text{ou} \qquad E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \quad \forall e \geq 1.$$

Demonstração. Ver o Corolário III.6.4 do [Sil09]. □

3.2.4 O diferencial invariante

Aqui vamos discutir algumas propriedades de um tipo especial de forma diferencial que existe em um curva elíptica (E, O_E). Se $E \subseteq \mathbb{P}^2$ é uma cúbica de Weierstraß lisa dada pela equação

$$E_{\text{afim}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

definimos a forma diferencial

$$\omega_E := \frac{1}{2y + a_1x + a_3}dx \in \Omega_E.$$

onde $x = X/Z, y = Y/Z \in \bar{k}(E)$, que como foi comentado na demonstração da Proposição 3.2.3 satisfaz $\text{div}(\omega_E) = 0$. Ele é chamado de **diferencial invariante** de E por conta da seguinte

Proposição 3.2.25. *Para todo $P \in E(\bar{k})$, temos $\tau_P^*\omega_E = \omega_E$ onde $\tau_P : E \to E$ é a translação por P.*

Demonstração. Ver a Proposição III.5.1 do [Sil09]. □

O próximo resultado nos permite "linearizar" mapas entre cúbicas de Weierstraß.

Proposição 3.2.26. *Sejam $E, E' \subseteq \mathbb{P}^2$ cúbicas de Weierstraß lisas e $\omega_{E'} \in \Omega_{E'}$ o diferencial invariante. Se $\phi, \psi \in \text{Hom}(E, E')$, então*

$$(\phi + \psi)^*\omega_{E'} = \phi^*\omega_{E'} + \psi^*\omega_{E'}.$$

Logo, temos o seguinte homomorfismo

$$\begin{aligned}\Psi : \text{Hom}(E, E') &\to \Omega_{E'} \\ \phi &\mapsto \phi^*\omega_{E'}.\end{aligned}$$

Demonstração. Ver a Proposição III.5.3 do [Sil09]. □

Se (X, O_X) é uma curva elíptica não temos uma escolha canônica de diferencial invariante e dizemos que $\omega \in \Omega_X$ é *um* diferencial invariante se satisfaz a condição da Proposição 3.2.25. Um exemplo é obtido ao tomarmos $x, y \in \bar{k}(X)$ coordenadas de Weierstraß e tomarmos o pullback pelo isomorfismo $X \to E \subseteq \mathbb{P}^2$ da diferencial invariante ω_E de cúbica de Weierstraß lisa E associada de acordo com a Proposição 3.2.3. Ela é explicitamente dada por

$$\frac{1}{2y + a_1x + a_3}dx \in \Omega_X.$$

Se tomamos outras coordenadas de Weierstraß $x', y' \in \bar{k}(X)$, sabemos pelo item (b) da Proposição 3.2.3 que a cúbica de Weierstraß lisa E' associada é obtida a partir de E através da mudança de variável

$$\begin{cases} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{cases} \qquad u, r, s, t \in \bar{k}, u \neq 0.$$

Como se verifica que temos $\omega_{E'} = u\omega_E$, segue que os diferenciais invariantes de X obtidos a partir de E e E' são múltiplos um do outro por uma constante.

3.2.5 O Módulo de Tate

Seja $(E/k, O_E)$ uma curva elíptica. Então, para $m \neq 0$ primo com a característica, sabemos pela Proposição 3.2.24 que

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Além disso, como E está definida sobre k, pode-se mostrar que $[m]$ também está definida sobre k. Isto implica que $[m]$ comuta com a ação de G_k em $E(\bar{k})$:

$$\sigma \cdot [m](P) = [m] \cdot (\sigma \cdot P) \quad \forall P \in E(\bar{k}).$$

Assim, G_k se restringe a uma ação em $E[m]$ e isto nos dá uma representação

$$\rho : G_k \to \mathrm{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$$

onde o último isomorfismo é obtido ao tomarmos uma $\mathbb{Z}/m\mathbb{Z}$-base de $\mathrm{Aut}(E[m])$. O que faremos a seguir é juntar estas representações para $m = \ell^n$, com ℓ primo diferente de $\mathrm{char}\, k$. Isto é feito por meio da seguinte definição

Definição 3.2.27. Sejam E uma curva elíptica e $\ell \neq \mathrm{char}\, k$ primo. Definimos o **módulo de Tate (ℓ-ádico) de** E como sendo o seguinte limite projetivo

$$T_\ell(E) \coloneqq \varprojlim E[\ell^n]$$

onde os mapas $E[\ell^{n+1}] \to E[\ell^n]$ são os mapas de multiplicação por ℓ.

Para mais detalhes sobre a definição de limite projetivo ou a noção mais geral de limite na teoria de categorias veja o Apêndice A.3 de [BT15] ou o Apêndice 3.3 de [Ten08].

Como consequência da Proposição 3.2.24, cada $E[\ell^n]$ é um $\mathbb{Z}/\ell^n\mathbb{Z}$-módulo e, portanto, nos dá uma estrutura de $\mathbb{Z}_\ell$-módulo sobre $T_\ell(E)$ (veja o Capítulo 4 sobre a construção do anel $\mathbb{Z}_\ell$ dos inteiros ℓ-ádicos). Além disso, temos que como $\mathbb{Z}_\ell$(ou $\mathbb{Z}_p$)-módulos:

- $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ se $\ell \neq 0$ em k.
- $T_p(E) \cong 0$ ou $\mathbb{Z}_p$ se $\mathrm{char}\, k = p > 0$.

Assim, se $\ell \neq \mathrm{char}\, k$ é primo, e E é definida sobre k, então as ações de G_k em cada $E[\ell^n]$ nos dão uma ação de G_k em $T_\ell(E)$ e isto nos dá uma representação

$$\rho_\ell : G_k \to \mathrm{Aut}(T_\ell(E)) \cong GL_2(\mathbb{Z}_\ell).$$

Se E, E' são curvas elípticas e $\phi : E \to E'$ é uma isogenia, então ϕ leva cada $E[\ell^n]$ em $E'[\ell^n]$ e obtemos um mapa $\mathbb{Z}_\ell$-linear

$$\phi_\ell : T_\ell(E) \to T_\ell(E').$$

Assim, obtemos um homomorfismo de grupos abelianos

$$\begin{aligned} \mathrm{Hom}(E, E') &\to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(E), T_\ell(E')) \\ \phi &\mapsto \phi_\ell \end{aligned}$$

que induz um mapa $\mathbb{Z}_\ell$-linear

$$\mathrm{Hom}(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(E), T_\ell(E')).$$

Sobre este mapa, temos a seguinte proposição

Proposição 3.2.28. *Se ℓ é um primo diferente de* $\mathrm{char}\, k$*, o mapa $\mathbb{Z}_\ell$-linear natural*

$$\mathrm{Hom}(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(E), T_\ell(E'))$$

é injetor

Demonstração. Ver o Teorema III.7.4 do [Sil09]. □

Corolário 3.2.29. *Para E, E' curvas elípticas, o grupo abeliano* $\mathrm{Hom}(E, E')$ *tem posto no máximo* 4.

Demonstração. Pela Proposição 3.2.14, $\mathrm{Hom}(E, E')$ é livre de torção. Então, temos a igualdade

$$\mathrm{rank}_{\mathbb{Z}} \mathrm{Hom}(E, E') = \mathrm{rank}_{\mathbb{Z}_\ell} \mathrm{Hom}(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$$

no sentido de que o lado esquerdo é finito se e somente se o lado direto é finito e neste caso, os dois são iguais. Porém, pela Proposição 3.2.28, segue que para $\ell \neq \mathrm{char}\, k$

$$\mathrm{rank}_{\mathbb{Z}_\ell} \mathrm{Hom}(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \leq \mathrm{rank}_{\mathbb{Z}_\ell} M_2(\mathbb{Z}_\ell) = 4$$

e o resultado segue. □

3.2.6 Endomorfismos e Automorfismos

Concluímos este capítulo descrevendo a estrutura do anel de endomorfismos e do grupo de automorfismos de uma curva elíptica E. O que sabemos até agora sobre $\mathrm{End}(E)$ é que

- É um anel de característica zero, não possui divisores de zero e é um grupo abeliano de posto no máximo 4 (Proposição 3.2.14 e Corolário 3.2.29).
- Possui uma anti-involução dado por $\phi \mapsto \hat{\phi}$ que fixa $\mathbb{Z}$ (itens (ii), (iii), (iv) e (vi) da Proposição 3.2.22).
- Vale que $\phi \circ \hat{\phi} \in \mathbb{Z}_{\geq 0}$ e $\phi \circ \hat{\phi} = 0 \iff \phi = 0$ (item (i) da Proposição 3.2.22).

Acontece que é possível classificar os anéis que possuem estas propriedades:

Proposição 3.2.30. *Se R é um anel que satisfaz as três propriedades acima, então R é um dos seguintes tipos:*

- $R \cong \mathbb{Z}$.
- *R é uma ordem em um corpo quadrático imaginário $K = \mathbb{Q}(\alpha)$.*
- *R é uma ordem em uma ordem em uma álgebra de quatérnions $A = \mathbb{Q}\langle \alpha, \beta \rangle$.*

Demonstração. Veja o Teorema III.9.3 do [Sil09]. □

Corolário 3.2.31. *Se E é uma curva elíptica, então* $\mathrm{End}(E)$ *é um dos três tipos mencionados na proposição anterior.*

Em relação ao grupo de automorfismos $\mathrm{Aut}(E)$, temos o seguinte resultado

Proposição 3.2.32. *Para E curva elíptica,* $\mathrm{Aut}(E)$ *é finito de ordem dividindo* 24. *Mais especificamente:*

$$\#\,\mathrm{Aut}(E) = \begin{cases} 2 \text{ se } j(E) \neq 0, 1728 & \\ 4 \text{ se } j(E) = 1728 & e \quad \mathrm{char}\, k \neq 2, 3 \\ 6 \text{ se } j(E) = 0 & e \quad \mathrm{char}\, k \neq 2, 3 \\ 12 \text{ se } j(E) = 0 = 1728 & e \quad \mathrm{char}\, k = 3 \\ 24 \text{ se } j(E) = 0 = 1728 & e \quad \mathrm{char}\, k = 2 \end{cases}$$

Demonstração. Ver o Teorema III.10.1 do [Sil09]. □

Capítulo 4

Multiplicação Complexa

Neste capítulo, tratamos das curvas elípticas com multiplicação completa. Começamos tratando de curvas elípticas sobre $\mathbb{C}$ e depois discutimos sobre os possíveis corpos de definição. Por Fim, enunciamos alguns resultados interessantes sobre tais curvas. Em especial, os fato de que o j-invariante é um inteiro algébrico e que a partir dos pontos de torção se pode construir extensões abelianas de corpos quadráticos imaginários. Destacamos que não fornecemos demonstrações completas dos resultados enunciados e apenas damos a referência correspondente na referência principal que é o [Sil94].

4.1 Propriedades Gerais

Seja $E/\mathbb{C}$ uma curva elíptica com multiplicação complexa, ou seja, com $\mathrm{End}(E) \supsetneq \mathbb{Z}$. Então, de acordo com o Teorema VI.5.5 de [Sil09], é isomorfo a $\mathbb{Z}$ ou a uma ordem R em corpo quadrático imaginário. Uma outra maneira é usar a caracterização do Corolário 3.2.31 e o Corolário III.5.6.c do [Sil09]. De agora em diante, vamos tratar de curvas elípticas $E/\mathbb{C}$ cujo anel de endomorfismos é isomorfo a $\mathcal{O}_K$, onde K é um corpo quadrático imaginário.

Exemplo 4.1.1. Para K corpo quadrático imaginário, o seu anel de inteiros $\Lambda = \mathcal{O}_K$ é um reticulado da forma $\mathbb{Z} + \tau\mathbb{Z}$. Pela Proposição 3.1.18, temos um isomorfismo entre a curva elíptica complexa $E_\Lambda = \mathbb{C}/\Lambda$ com a seguinte curva algébrica projetiva

$$\mathcal{E}_\Lambda : Y^2Z = 4X^3 - g_4(\Lambda)XZ^2 - g_6(\Lambda)Z^3,$$

que será uma curva elíptica, com ponto base $O = (0 : 1 : 0)$. E mais, temos um isomorfismo entre o anel de endomorfismos (analíticos) de E_Λ e o anel de endomorfismos (algébricos) de $\mathcal{E}_\Lambda$ (veja o Teorema VI.4.1 do [Sil09]). Assim, temos $\mathrm{End}(\mathcal{E}_\Lambda) \cong \mathrm{End}(E_\Lambda) = \mathcal{O}_K$.

Enunciamos abaixo que temos um isomorfismo $\mathcal{O}_K \cong \mathrm{End}(E)$ especial.

Proposição 4.1.2. *Seja $E/\mathbb{C}$ uma curva elíptica com multiplicação complexa por $\mathcal{O}_K \subseteq \mathbb{C}$. Então, existe um único isomorfismo*

$$[\cdot] : \mathcal{O}_K \to \mathrm{End}(E)$$

tal que para qualquer diferencial invariante $\omega \in \Omega_E$

$$[\alpha]^*\omega = \alpha\omega \quad \forall \alpha \in \mathcal{O}_K.$$

*Neste caso, dizemos que o par $(E, [\cdot])$ é **normalizado**.*

Demonstração. ver a Proposição II.1.1 de [Sil94]. □

Definimos abaixo o conjunto das classes de $\mathbb{C}$-isomorfismo de curvas elípticas com multiplicação complexa por $\mathcal{O}_K$ como

$$\mathsf{Ell}(\mathcal{O}_K) := \frac{\{\text{curvas elipticas } E/\mathbb{C} \text{ com } \mathrm{End}(E) \subseteq \mathcal{O}_K\}}{\mathbb{C}\text{-isomorfismo}} = \frac{\{\text{reticulados } \Lambda \subseteq \mathbb{C} \text{ com } \mathrm{End}(\Lambda) = \mathcal{O}_K\}}{\text{homotetia}}.$$

Este conjunto é será não-vazio. De fato, se $\mathfrak{a} \subseteq K$ é uma ideal fracionário não-nulo, então $\mathfrak{a} \subseteq \mathbb{C}$ é um reticulado e a curva elíptica $E_{\mathfrak{a}}/\mathbb{C}$ associada satisfaz $\mathrm{End}(E_{\mathfrak{a}}) \cong \mathcal{O}_K$ (veja a seção 1 do Capítulo 2 do [Sil94]). Além disso, se $c \in K^*$, então $E_{\mathfrak{a}}$ e $E_{c\mathfrak{a}}$ são $\mathbb{C}$-isomorfas. Assim, suspeitamos que exista uma relação entre $\mathsf{Ell}(\mathcal{O}_K)$ e o grupo $\mathsf{Cl}(\mathcal{O}_K)$ das classes de ideais de $\mathcal{O}_K$. Por exemplo, temos um mapa

$$\begin{aligned} \mathsf{Cl}(\mathcal{O}_K) &\to \mathsf{Ell}(\mathcal{O}_K) \\ [\mathfrak{a}] &\mapsto E_{\mathfrak{a}}. \end{aligned}$$

Definimos para $\Lambda \subseteq \mathbb{C}$ reticulado e $\mathfrak{a} \subseteq K$ ideal fracionário não-nulo, o conjunto

$$\mathfrak{a} \cdot \Lambda := \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r := \alpha_i \in \mathfrak{a}_i, \lambda_i \in \Lambda\}.$$

A relação entre $\mathsf{Ell}(\mathcal{O}_K)$ e $\mathsf{Cl}(\mathcal{O}_K)$ é estabelecida na seguinte proposição

Proposição 4.1.3. *Seja K um corpo quadrático imaginário. Então, valem as seguintes afirmações:*

(a) Seja $\lambda \subseteq \mathbb{C}$ um reticulado com $E_\Lambda \in \mathsf{Ell}(\mathcal{O}_K)$ e sejam $\mathfrak{a}, \mathfrak{b}$ ideais fracionários não-nulos de K, Então:

(i) $\mathfrak{a} \cdot \Lambda \subseteq \mathbb{C}$ é um reticulado.

(ii) A curva elíptica $E_{\mathfrak{a}\cdot\Lambda}/\mathbb{C}$ satisfaz $\mathrm{End}(E_{\mathfrak{a}\cdot\Lambda}) \cong \mathcal{O}_K$.

(iii) $E_{\mathfrak{a}\cdot\Lambda} \cong E_{\mathfrak{b}\cdot\Lambda}$ se e somente se $[\mathfrak{a}] = [\mathfrak{b}]$ em $\mathsf{Cl}(\mathcal{O}_K)$.

A partir dos três itens acima, obtemos uma ação de $\mathsf{Cl}(\mathcal{O}_K)$ em $\mathsf{Ell}(\mathcal{O}_k)$ dada por $[\mathfrak{a}] \cdot E_\Lambda = E_{\mathfrak{a}^{-1}\cdot\Lambda}$.

(b) A ação de $\mathsf{Cl}(\mathcal{O}_K)$ em $\mathsf{Ell}(\mathcal{O}_K)$ definida no item anterior é livre e transitiva. Em particular, $\mathsf{Ell}(\mathcal{O}_K)$ é finito com $\#\mathsf{Ell}(\mathcal{O}_K) = \#\mathsf{Cl}(\mathcal{O}_K)$.

Demonstração. Ver a Proposição II.1.2 do [Sil94]. □

Definição 4.1.4. Para $(E, [\cdot]) \in \mathsf{Ell}(\mathcal{O}_K)$ normalizado e $\mathfrak{a}$ ideal não-nulo de $\mathcal{O}_K$, definimos o conjunto dos **pontos de $\mathfrak{a}$-torção** de E como

$$E[\mathfrak{a}] = \{P \in E \colon [\alpha](P) = O_E \quad \forall \alpha \in \mathfrak{a}\}.$$

Em particular, para $\mathfrak{a} = m\mathcal{O}_K$, temos $E[\mathfrak{a}] = E[m]$.

Seja $E \in \mathsf{Ell}(\mathcal{O}_K)$. Então, $E \cong E_\Lambda$ com $\Lambda \subseteq \mathbb{C}$ reticulado tal que $\mathrm{End}(\Lambda) = \mathbb{C}$. Como $\Lambda \subseteq \mathfrak{a}^{-1}\Lambda$, temos um mapa analítico natural

$$\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1} \cdot \Lambda$$

entre curvas elípticas complexas que corresponde a uma isogenia

$$\phi_{\mathfrak{a}} : E_\Lambda \to [\mathfrak{a}] \cdot E_\Lambda.$$

A próxima proposição nos dá uma descrição precisa desta isogenia e do conjunto $E[\mathfrak{a}]$.

Proposição 4.1.5. *Seja $E \in \mathsf{Ell}(\mathcal{O}_K)$ e $\mathfrak{a}$ ideal não-nulo de $\mathcal{O}_K$. Então:*

(a) $E[\mathfrak{a}]$ é o núcleo da isogenia $\phi_{\mathfrak{a}} : E \to [\mathfrak{a}] \cdot E_\Lambda$.

(b) $E[\mathfrak{a}]$ *é um* $\mathcal{O}_K/\mathfrak{a}$*-módulo livre de posto um.*

Demonstração. Ver a Proposição II.1.4 do [Sil94]. □

Corolário 4.1.6. *Seguindo a notação da proposição acima, temos:*

(a) A isogenia $\phi_{\mathfrak{a}} : E \to [\mathfrak{a}] \cdot E$ *tem grau* $N_{K/\mathbb{Q}}(\mathfrak{a})$.

(b) Para todo $\alpha \in \mathcal{O}_K$*, o endomorfismo* $[\alpha] : E \to E$ *tem grau* $|N_{K/\mathbb{Q}}|(\alpha)$.

Demonstração. Veja o Corolário II.1.5 do [Sil94]. □

Em relação ao corpo de definição de curvas elípticas em $\text{Ell}(\mathcal{O}_K)$, o resultado-chave é a seguinte proposição

Proposição 4.1.7. *Seja K um corpo quadrático imaginário. Então*

(a) Para $E \in \text{Ell}(\mathcal{O}_K)$*, temos* $j(E) \in \bar{\mathbb{Q}}$.

(b) O mapa natural

$$\text{Ell}_{\bar{\mathbb{Q}}}(\mathcal{O}_K) = \frac{\{\textit{curvas elítpicas } E/\bar{\mathbb{Q}} \textit{ com } \text{End}(E) \cong \mathcal{O}_K\}}{\bar{\mathbb{Q}}\textit{-isomorfismo}} \leftrightarrow \text{Ell}(\mathcal{O}_K)$$

é uma bijeção,

Demonstração. Ver a Proposição II.2.1 do [Sil94]. □

Assim, se $E/\mathbb{C}$ é uma curva elíptica com $\text{End}(E) \cong \mathcal{O}_K$, então pelo item (b) da proposição acima ela é $\mathbb{C}$-isomorfa a uma curva elíptica $E_1/\bar{\mathbb{Q}}$. Agora, pelo item (ii) da Proposição 3.2.5, existe uma curva elíptica $E_2/\mathbb{Q}(j(E_1))$ que é $\bar{\mathbb{Q}}$-isomorfa a E_1 e temos $j(E) = j(E_1) = j(E_2)$. Portanto, E é $\mathbb{C}$-isomorfa a uma curva elíptica $E'/\mathbb{Q}(j(E))$.

4.2 Integralidade e Extensões Abelianas

Vimos na seção anterior que se $E/\mathbb{C}$ é uma curva elíptica que representa um elemento de $\text{Ell}(\mathcal{O}_K)$. Mas pode-se afirmar algo mais forte

Teorema 4.2.1. *Seja* $E/\mathbb{C} \in \text{Ell}(\mathcal{O}_K)$*. Então,* $j(E)$ *é um inteiro algébrico.*

Demonstração. Ver o Teorema II.6.1 do [Sil94]. Na Seção 6 do Capítulo II deste mesmo livro, existem duas demonstrações. Uma de natureza analítica e outra que utiliza resultados de teoria de corpos de classe local (ver o Capitulo 2 de [Ten08]) juntamente com o chamado Critério de Néron-Ogg-Shafarevich descrito na Seção VII.7 do [Sil09]. □

Os próximos resultados descrevem como construir extensões abelianas de K a partir do j-invariante e dos pontos de torção de curvas elípticas em $\text{Ell}(\mathcal{O}_K)$. Este fenômeno é semelhante ao que ocorre quando o corpo base é $\mathbb{Q}$. De fato, o chamado *Teorema de Kronecker-Weber* diz que toda extensão abeliana $L/\mathbb{Q}$ está contida em uma extensão ciclotômica $\mathbb{Q}(\mu_n)/\mathbb{Q}$, onde $\mu_n = e^{\frac{2\pi i}{n}}$ é uma raiz n-ésima primitiva da unidade. Notamos que as raízes da unidade são os pontos de torção do círculo unitário S^1 que pode ser visto como uma curva algébrica (real).

A teoria de corpos de classe para um corpo de números K nos fornece um resultado análogo: toda extensão finita e abeliana L/K está contida em um **ray class field** $K(\mathfrak{a})$, onde $\mathfrak{a}$ é um modulus (este é o Corolário VI.6.3 do [Neu99]). No caso de K quadrático imaginário, um modulus equivale a um ideal não-nulo de $\mathcal{O}_K$. Em particular, para $\mathfrak{a} = \mathcal{O}_K$, o ray class field $H = K(\mathfrak{a})$ é o chamado **corpo de classe de Hilbert** de K. Ele também é caracterizado como a extensão abeliana maximal no qual nenhum primo de K se ramifica em H (Proposição VI.6.8 do [Neu99]). Sobre este corpo, temos o seguinte resultado:

Teorema 4.2.2. *Se $E/\mathbb{C}$ é uma curva elíptica que representa um elemento de $\text{Ell}(\mathcal{O}_K)$, então $K(j(E))$ é o corpo de classe de Hilbert de K.*

Demonstração. Ver o Teorema II.4.3 do [Sil94]. □

Por fim, a partir de $E \in \text{Ell}(\mathcal{O}_K)$, podemos obter todos os ray class field $K(\mathfrak{a})$. Para isto, precisamos de uma função auxiliar, chamada uma **função de Weber** $h : E \to \mathbb{P}^1$ que é definida sobre H. Se $E \in \text{Ell}(\mathcal{O}_K)$, sabemos que podemos tomar E'/H que é $\mathbb{C}$-isomorfa a E. Se ela é dada por uma equação de Weierstraß

$$E'_{\text{afm}} : y^2 = x^3 + Ax + B \quad A, B \in H,$$

um exemplo de função de Weber é

$$h(x,y) = \begin{cases} x & \text{se } AB \neq 0 \\ x^2 & \text{se } B = 0 \\ x^3 & \text{se } A = 0 \end{cases}$$

Feito isso, enunciamos o

Teorema 4.2.3. *Seja $E/H \in \text{Ell}(\mathcal{O}_K)$ e $h : E \to \mathbb{P}^1$ uma função de Weber. Então para todo $\mathfrak{a}$ ideal de $\mathcal{O}_K$, o corpo $K(j(E), h(E[\mathfrak{a}]))$ é o ray class field $K(\mathfrak{a})$. Como consequência, a extensão abeliana maximal de K é dada por $K^{ab} = K(j(E), h(E_{tors}))$.*

Demonstração. Ver o Teorema II.5.6 e o Corolário II.5.7 do [Sil94]. □

Assim, se $E \in \text{Ell}(\mathcal{O}_K)$ é dada por uma equação de Weiestraß

$$E_{\text{afim}} : y^2 = x^3 + Ax + B \quad A, B \in H,$$

então quando $AB \neq 0$, os ray class fields de K são obtidos a partir de K acrescentando $j(E)$ e as coordenadas x dos pontos de $\mathfrak{a}$-torção. Em particular, se $E \cong E_\Lambda$ com $\Lambda = \mathcal{O}_K = \mathbb{Z} + \tau\mathbb{Z}$, tanto j quanto a função de Weber podem ser consideradas como funções analíticas de τ (ver a Seção I.4 do [Sil94] e o Exemplo II.5.5.2 do [Sil09]). Isto significa que os ray class fields de K são obtidos acrescentando valores especiais de algumas funções analíticas algo que também ocorre no caso do corpo base $\mathbb{Q}$ pois as raízes da unidades são justamente os valores da exponencial $e^{2\pi iz}$ nos números racionais.

Bibliografia

[God58] Roger Godement. *Topologie algébrique et théorie des faisceaux*. Actualités scientifiques et industrielles 1252. Hermann, 1958.

[Gun66] Robert C. Gunning. *Lectures on Riemann Surfaces*. Princeton Mathematical Notes. Princeton University Press, 1966.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1977.

[Ser79] Jean-Pierre Serre. *Local Fields*. 1ª ed. Graduate Texts in Mathematics 67. Springer-Verlag New York, 1979.

[Mat80] Hideyuki Matsumura. *Commutative Algebra*. 2ª ed. Mathematics Lecture Note Series 56. Benjamin/Cummings Pub. Co, 1980.

[For81] Otto Forster. *Lectures on Riemann Surfaces*. 1ª ed. Graduate Texts in Mathematics 81. Springer-Verlag New York, 1981.

[Lan82] Serge Lang. *Introduction to Algebraic and Abelian Functions*. 2ª ed. Graduate Texts in Mathematics 89. Springer-Verlag New York, 1982.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. 1ª ed. Graduate Texts in Mathematics 151. Springer-Verlag New York, 1994.

[Wei94] Charles A. Weibel. *An Introduction to Homological Algebra*. Cambridge Studies in Advanced Mathematics 38. Cambridge University Press, 1994.

[BT95] Raoul Bott e Loring W. Tu. *Differential Forms in Algebraic Topology*. Graduate Texts in Mathematics 82. Springer, 1995.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. 1ª ed. Grundlehren der mathematischen Wissenschaften. Springer-Verlag Berlin Heidelberg, 1999.

[SS03] Elias M. Stein e Rami Shakarchi. *Complex Analysis*. Vol. 2. Princeton Lectures in Analysis. Princeton University Press, 2003.

[Voi03] Claire Voisin. *Hodge Theory and Complex Algebraic Geometry I*. 1ª ed. Vol. 1. Cambridge Studies in Advanced Mathematics 76. Cambridge University Press, 2003.

[Huy04] Daniel Huybrechts. *Complex Geometry: An Introduction*. Universitext. Springer, 2004.

[Liu06] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics, 6. Oxford University Press, 2006.

[Mil06] J.S. Milne. *Elliptic Curves*. 1ª ed. BookSurge Publishers, 2006.

[Ful08] William Fulton. *Algebraic Curves - An Introduction to Algebraic Geometry*. 2008. URL: http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf.

[Ten08] Eduardo Tengan. *An Invitation to Local Fields*. 2008. URL: http://www.mtm.ufsc.br/xja/arquivos/tengan_prerequisitos.pdf.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2ª ed. Graduate Texts in Mathematics 106. Springer-Verlag New York, 2009.

[Sha13] Igor R. Shafarevich. *Basic Algebraic Geometry 1: Varieties in Projective Space*. 3ª ed. Springer, 2013.

[BT15] Herivelto Borges e Eduardo Tengan. *Álgebra Comutativa em Quatro Movimentos*. 1ª ed. Projeto Euclides. IMPA, 2015.

[Str17] Benoît Stroh. *Courbes Elliptiques*. 2017. URL: https://webusers.imj-prg.fr/~benoit.stroh/elliptique.pdf. Notas de aula.

[AM18] M. F. Atiyah e I. G. Macdonald. *Introduction To Commutative Algebra*. CRC Press, 2018.