UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Rodrigo de Paula da Silva

Curvas Elípticas

e o Teorema de Mordell

São José do Rio Preto
2019

Rodrigo de Paula da Silva

Curvas Elípticas

e o Teorema de Mordell

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática junto ao Programa de Pós-Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho" (IBILCE/UNESP), Câmpus de São José do Rio Preto.

Financiadora: CAPES

Orientador: Prof. Dr. Parham Salehyan

São José do Rio preto
2019

Silva, Rodrigo de Paula
S586c Curvas elípticas : e o teorema de Mordell. / Rodrigo de Paula da Silva. -- São José do Rio Preto, 2019
144 f. : il., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto
Orientador: Parham Salehyan

1. Curvas algébricas. 2. Geometria de curvas elípticas. 3. Curvas elípticas sobre corpos de números. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto.
Dados fornecidos pelo autor(a).
Essa ficha não pode ser modificada.

Rodrigo de Paula da Silva

Curvas Elípticas

e o Teorema de Mordell

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática junto ao Programa de Pós-Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho" (IBILCE/UNESP), Câmpus de São José do Rio Preto.

Financiadora: CAPES

Comissão Examinadora

Prof. Dr. Parham Salehyan
Unesp - Câmpus de São José do Rio Preto
Orientador

Prof. Dra. Michelle Ferreira Zanchetta Morgado
Unesp - Câmpus de São José do Rio Preto

Prof. Dr. Behrooz Mirzaii
Universidade de São Paulo, Instituto de Ciências Matemáticas e de Computação

São José do Rio Preto
07 de agosto de 2019

Àqueles que sempre acreditaram que eu seria capaz de atingir meus objetivos.

AGRADECIMENTOS

À Deus por me dar saúde.

À minha esposa por estar ao meu lado.

Aos meus pais pelo apoio.

Ao meu orientador pelo ensino.

À todas as pessoas que convivi na minha passagem pelo Ibilce.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, à qual agradeço.

RESUMO

Faremos neste trabalho um estudo das curvas elípticas. Do primeiro capítulo até o terceiro mostraremos as principais noções para o estudo desses objetos. Alguns resultados como o teorema de Riemann-Roch serão vistos em sequência. Veremos que curvas elípticas são dadas por equações de Weierstrass juntamente com uma estrutura de grupo nesse conjunto. O conteúdo dessa teoria servirá de base para o capítulo 4, onde demonstramos o teorema de Mordell-Weil. O procedimento de descida será mostrado, em seguida veremos o teorema de Mordell-Weil sobre o corpo dos números racionais. As funções altura serão definidas e então demonstraremos nosso principal resultado. Por fim, como um apêndice, veremos um pouco de pontos integrais sobre curvas elípticas. Apresentaremos a teoria de aproximação diofantina e alguns resultados de como as funções distância podem nos ajudar num estudo métrico ou topológico por meio dessas aproximações.

Palavras-chave: Geometria Algébrica. Curvas algébricas. Curvas elípticas. Mordell-Weil.

ABSTRACT

We will do in this work a study of the elliptic curves. From the first chapter to the third we will show the main notions for the study of these objects. Some results such as the Riemann-Roch theorem will be seen in sequence. We will see that elliptic curves are given by Weierstrass equations together with a group structure in that set. The content of this theory will serve as the basis for chapter 4, where we demonstrate Mordell-Weil's theorem. The descent procedure will be shown, then we will see Mordell-Weil's theorem on the field Q. The height functions will be defined and then we will demonstrate our main result. Finally, as an appendix, we will see some integral points on elliptic curves. We will present the theory of diophantine approximation and some results of how distance functions can help us in a metric or topological study through these approximations.

Keywords: Algebraic Geometry. Algebraic curves. Elliptic curves. Mordell-Weil.

LISTA DE FIGURAS

LISTA DE SÍMBOLOS

C/K, quando C é definido sobre K.
$K(C),\ \bar{K}(C)$ o corpo de funções de C.
$\bar{K}[C]_P$ o anel local de C em P.
M_P o ideal maximal de $\bar{K}[C]_P$.
$\bar{K}[V]_P = \{F \in \bar{K}(V) \mid F = f/g,\ f,\ g \in \bar{K}[V],\ g(P) \neq 0\}$
K é um corpo de números.
M_K o conjunto completo de valores absolutos inequivalentes em K.
M_K^∞ o conjunto dos valores absolutos arquimedianos em M_K.
M_K^0 o conjunto dos valores absolutos não-arquimedianos em M_K.
$v(x) = -\log|x|_v$, para um valor absoluto $v \in M_K$ e $x \in K$.
ord_v é a valorização normalizada para $v \in M_K^0$, ou seja, satisfaz $\mathrm{ord}_v(K^*) = \mathbb{Z}$.
R é o anel dos inteiros de K que é igual a $\{x \in K : v(x) \geq 0, \forall v \in M_K^0\}$.
R^* é o grupo unidade de R, ou seja, $\{x \in K : v(x) = 0, \forall v \in M_K^0\}$.
K_v é o completamento de K em v, para $v \in M_K$.
R_v é o anel dos inteiros de K_v, para $v \in M_K^0$.
$\mathcal{M}_v$ é o ideal maximal de R_v, para $v \in M_K^0$.
k_v é o corpo residual de R_v, para $v \in M_K^0$.

SUMÁRIO

Introdução

O estudo das equações polinomiais em duas variáveis na forma mais simples, ou seja, sobre os números inteiros, surgiu antes da Grécia antiga. Atualmente as chamamos de equações diofantinas, estudo que combina técnicas da Teoria Algébrica dos Números e da Geometria Algébrica. Do ponto de vista da Teoria Algébrica dos Números, estaremos procurando soluções inteiras ou racionais nessas equações polinomiais. Já do ponto de vista da Geometria Algébrica, cada sistema de equações polinomiais descreve uma variedade, que é um objeto geométrico. É a junção dessas duas disciplinas a que chamamos Geometria Diofantina.

Como exemplo, considere a equação linear:

$$aX + bY = c, \qquad a, b, c \in \mathbb{Z}, \qquad a \text{ ou } b \neq 0.$$

Equações dessa forma sempre admitem solução racional. Em particular, suas soluções são inteiras se, e somente se, o maior divisor comum de a e b divide c.

Também podemos observar a equação quadrática:

$$aX^2 + bXY + cY^2 + dX + eY + f = 0, \qquad a, \ldots, f \in \mathbb{Z}, \quad a, b \text{ ou } c \neq 0.$$

Como já se sabe, essa equação descreve as seções cônicas, que por uma mudança de coordenadas com coeficientes racionais, pode ser transformada numa das seguintes formas:

$$\begin{aligned} AX^2 + BY^2 &= C, && \text{elipse,} \\ AX^2 - BY^2 &= C, && \text{hipérbole,} \\ AX + BY^2 &= 0, && \text{parábola.} \end{aligned}$$

O teorema de Hasse-Minkowski [16, IV Teorema 8] nos auxilia com as soluções de tais equações. Em resumo ele nos diz que um polinômio quadrático tem solução em $\mathbb{Q}$ se, e somente se, tem solução em todo completamento de $\mathbb{Q}$.

As equações quadráticas juntamente com as equações lineares em duas variáveis definem curvas de gênero zero. Existe muita teoria em relação a aritmética desses

objetos. Em seguida vem as curvas de gênero um, que são dadas por equações cúbicas em duas variáveis. A aritmética desses objetos, chamada curva elíptica, apresenta complexidades onde muitas pesquisas atuais estão centradas, com várias conjecturas e técnicas, tornando-a num ambiente muito frutífero. Curva elíptica é o principal objeto deste estudo. No início veremos seus principais conceitos e resultados, por exemplo, o teorema de Riemann-Roch será apresentado na primeira parte. Veremos que curvas elípticas são dadas por equações de Weierstrass juntamente com uma estrutura de grupo nesse conjunto. O conteúdo dessa teoria servirá de base para o capítulo 4. Estudaremos o procedimento de descida e definiremos a função altura, partindo assim para a demonstração do teorema de Mordell-Weil, o principal resultado deste trabalho. Por fim, veremos um pouco a respeito dos pontos integrais sobre curvas elípticas. Apresentaremos a teoria de aproximação diofantina e alguns resultados dos quais o teorema de Siegel, que não será demonstrado aqui, é a versão melhorada desses resultados.

Capítulo 1

Variedades Algébricas

Neste capítulo introduziremos os conceitos e resultados que serão necessários ao longo dos próximos capítulos. Escrevemos a seguir algumas notações, que serão usadas ao longo do capítulo.

K é um corpo perfeito, ou seja, toda extensão algébrica de K é separável.
$\bar{K}$ o fecho algébrico de K.
$G_{\bar{K}/K}$ é o grupo de Galois de $\bar{K}/K$.

Considere também que m e n sejam inteiros positivos. Estamos assumindo que K é perfeito com o objetivo de simplificar o trabalho. Entretanto, como nosso trabalho final é fazer aritmética, nada impede que o corpo K seja eventualmente tomado como uma extensão algébrica de $\mathbb{Q}$, $\mathbb{Q}_p$, ou $\mathbb{F}_p$.

1.1 Variedades Afins

As variedades algébricas são os objetos fundamentais no estudo da Geometria Algébrica. Para estudá-las precisamos de algumas definições:

Definição 1.1. O espaço n-afim sobre $\bar{K}$ é definido pelo conjunto

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, \ldots, x_n) \mid x_i \in \bar{K}\}.$$

O conjunto dos pontos K-racionais é denotado por

$$\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n \mid x_i \in K\}.$$

Note que o grupo de Galois $G_{\bar{K}/K}$ age em $\mathbb{A}^n$. Para $\sigma \in G_{\bar{K}/K}$ e $P \in \mathbb{A}^n$,

$$P^\sigma = (x_1^\sigma, \ldots, x_n^\sigma).$$

Então $\mathbb{A}^n(K)$ pode ser caracterizado como

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : P^\sigma = P,\ \forall\ \sigma \in G_{\bar{K}/K}\}.$$

Seja $\bar{K}[X] = \bar{K}[X_1, \ldots, X_n]$ um anel de polinômios em n variáveis, e seja $I \subset \bar{K}[X]$ um ideal. Para cada I associamos um subconjunto de $\mathbb{A}^n$,

$$V_I = \{P \in \mathbb{A}^n\ : f(P) = 0,\ \forall\ f \in I\}.$$

Definição 1.2. Um conjunto algébrico afim é qualquer conjunto da forma V_I. Se V é um conjunto algébrico, o ideal de V é dado por

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0,\ \forall\ P \in V\}.$$

Diremos que um conjunto algébrico é definido sobre K se seu ideal $I(V)$ for gerado por polinômios em $K[X]$. Denotamos em geral, V/K como o conjunto dos pontos com coordenadas em K. Se V é definido sobre K, então o conjunto dos pontos K-racionais de V é

$$V(K) = V \cap \mathbb{A}^n(K).$$

Observação 1.1. Note que pelo Teorema da Base de Hilbert, todo ideal de $\bar{K}[X]$ e $K[X]$ são finitamente gerados.

Observação 1.2. Seja V um conjunto algébrico, e considere o ideal $I(V/K)$ definido por

$$I(V/K) = \{f \in K[X] : f(P) = 0,\ \forall\ P \in V\} = I(V) \cap K[X].$$

Então vemos que V é definido sobre K se, e somente se,

$$I(V) = I(V/K)\bar{K}[X].$$

Agora suponha que V é definido sobre K e seja $f_1, \ldots, f_m \in K[X]$ geradores para $I(V/K)$. Então $V(K)$ é o conjunto raízes $(x_1, \ldots, x_n)$ dos polinômios

$$f_1(X) = \cdots = f_m(X) = 0 \quad \text{com } x_1, \ldots, x_n \in K.$$

Assim um dos problemas fundamentais da Geometria Diofantina, chamado de soluções de equações polinomiais em números racionais, pode ser visto como o problema de descrever os conjuntos da forma $V(K)$ quando K for um corpo de números.

Note que se $f(X) \in K[X]$ e $P \in \mathbb{A}^n$, então para qualquer $\sigma \in G_{\bar{K}/K}$,

$$f(P^\sigma) = f(P)^\sigma.$$

Consequentemente se V é definido sobre K, então a ação $G_{\bar{K}/K}$ em $\mathbb{A}^n$ induz uma ação em V, e assim

$$V(K) = \{P \in V : P^\sigma = P,\ \forall\ \sigma \in G_{\bar{K}/K}\}.$$

Exemplo 1.1. Seja V um conjunto algébrico em $\mathbb{A}^2$ dado pela equação única

$$X^2 - Y^2 = 1.$$

O conjunto V é definido sobre K, para qualquer corpo K. Assuma que $\mathrm{char}(K) \neq 2$. Então o conjunto $V(K)$ está em correspondência biunívoca com $\mathbb{A}^1(K)\backslash\{0\}$ através do mapa

$$\begin{aligned} \mathbb{A}^1(K)\backslash\{0\} &\longrightarrow V(K), \\ t &\longmapsto \left(\frac{t^2+1}{2t}, \frac{t^2-1}{2t}\right). \end{aligned}$$

Exemplo 1.2. O conjunto algébrico

$$V : X^n + Y^n = 1$$

é definido sobre $\mathbb{Q}$. O último teorema de Fermat, provado em 1995 por Andrew Wiles, diz que para todo $n \geq 3$,

$$V(\mathbb{Q}) = \begin{cases} \{(1,0),(0,1)\} & \text{se } n \text{ é ímpar,} \\ \{(\pm 1,0),(0,\pm 1)\} & \text{se } n \text{ é par.} \end{cases}$$

Exemplo 1.3. O conjunto algébrico

$$V : Y^2 = X^3 + 17$$

tem muitos pontos $\mathbb{Q}$-racionais, por exemplo

$$(-2,3) \qquad (5234, 378661) \qquad \left(\frac{137}{64}, \frac{2651}{512}\right).$$

De fato, $V(\mathbb{Q})$ é infinito.

Definição 1.3. Um conjunto algébrico V é chamado uma variedade afim se $I(V)$ é um ideal primo em $\bar{K}[X]$.

Note que se V é definido sobre K, é suficiente checar que $I(V/K)$ é primo em $K[X]$.

Por exemplo, considere o ideal $(X_1^2 - 2X_2^2)$ em $\mathbb{Q}[X_1, X_2]$.

Seja V/K uma variedade. Então o anel de coordenadas afins de V/K é definido por

$$K[V] = \frac{K[X]}{I(V)}.$$

Como $K[X]$ é um domínio, seu corpo de frações é o conjunto $K(V)$, chamado corpo de funções de V/K. O mesmo vale para $\bar{K}$ ao invés de K.

Definição 1.4. Seja V uma variedade algébrica. A dimensão de V, denotada por $\dim(V)$, é o grau de transcendência de $\bar{K}(V)$ sobre $\bar{K}$, ou seja, o número de elementos de uma base de transcendência para a extensão finita do corpo.

Exemplo 1.4. A dimensão de $\mathbb{A}^n$ é n, pois $\bar{K}(\mathbb{A}^n) = \bar{K}(X_1, \ldots, X_n)$. Similarmente, se $V \subset \mathbb{A}^n$ é dado por uma única equação polinomial

$$f(X_1, \ldots, X_n) = 0,$$

então $\dim(V) = n - 1$.

No estudo de objetos geométricos, estaremos interessados em coisas que são ou não "suaves". A definição a seguir formalizará esta noção em termos do critério Jacobiano para existência de plano tangente ao ponto na curva.

Definição 1.5. Seja V uma variedade, $P \in V$, e $f_1, \ldots, f_m \in \bar{K}[X]$ um conjunto de geradores para $I(V)$. Então V é *não-singular* (ou *suave*) *em* P se a matrix $m \times n$

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

tem rank $n - \dim(V)$. Se V é não-singular em todo ponto, então diremos simplesmente que V é *não-singular* (ou *suave*).

Exemplo 1.5. Seja V dado por uma única equação polinômial

$$f(X_1, \ldots, X_n) = 0.$$

Então o exemplo anterior nos diz que $\dim(V) = n - 1$, e então $P \in V$ é um ponto singular se, e somente se,

$$\frac{\partial f}{\partial X_1}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0.$$

Como P também satisfaz $f(P) = 0$, isto dá $n + 1$ equações para n coordenadas de qualquer ponto singular. Assim para uma escolha qualquer de um polinômio f, esperamos que V seja não singular.

Exemplo 1.6. Considere as duas variedades

$$V_1 : Y^2 = X^3 + X \quad \text{e} \quad V_2 : Y^2 = X^3 + X^2.$$

Usando o fato anterior, vemos que qualquer ponto singular das variedades dadas satisfazem respectivamente,

$$V_1^{\text{sing}} : 3X^2 + 1 = 2Y = 0 \quad \text{e} \quad V_2^{\text{sing}} : 3X^2 + 2X = 2Y = 0.$$

Assim V_1 é não-singular, enquanto V_2 tem o ponto singular $(0, 0)$.

Figura 1.1. Curva suave e curva singular.

Existe outro critério de suavidade em termos de funções sobre a variedade V. Para cada ponto $P \in V$, definimos um ideal M_P de $\bar{K}[V]$ por

$$M_P = \{f \in \bar{K}[V] : f(P) = 0\}.$$

Note que M_P é ideal maximal, pois a aplicação

$$\bar{K}[V]/M_P \longrightarrow \bar{K}, \quad f \longmapsto f(P),$$

é um isomorfismo.
O quociente M_P/M_P^2 é um $\bar{K}$-espaço vetorial de dimensão finita.

Proposição 1.1. Seja V uma variedade. Um ponto $P \in V$ é não-singular se, e somente se,

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

Prova. Pode ser vista em [2, I.5.1].

Exemplo 1.7. Considere o ponto $P = (0, 0)$ nas variedades V_1 e V_2 do exemplo anterior. Nos dois casos, M_P é um ideal de $\bar{K}[V]$ gerado por X e Y, e M_P^2 é um

ideal gerado por X^2, XY e Y^2. No caso de V_1 temos que

$$X = Y^2 - X^3 \equiv 0 \pmod{M_P^2},$$

assim M_P/M_P^2 é gerado apenas por Y. Por outro lado, para V_2 não existem relação não trivial entre X e Y módulo M_P^2, ou seja, X e Y são geradores de M_P/M_P^2. Como cada V_i tem dimensão um, a proposição anterior implica que V_1 é suave, enquanto que V_2 não é.

Definição 1.6. O anel local de V em P, denotado por $\bar{K}[V]_P$, é a localização de $\bar{K}[V]$ em M_P. Em outras palavras,

$$\bar{K}[V]_P = \{F \in \bar{K}(V) : F = f/g \text{ para algum } f, g \in \bar{K}[V] \text{ com } g(P) \neq 0\}.$$

Note que se $F = f/g \in \bar{K}[V]_P$, então $F(P) = f(P)/g(P)$ é bem definido. As funções em $\bar{K}[V]_P$ são ditas regulares (ou definidas) em P.

1.2 Variedades Projetivas

Definição 1.7. O espaço projetivo sobre um corpo K é um conjunto $\mathbb{P}^n = \mathbb{P}^n(\bar{K}) = \{P = (x_0, \ldots, x_n) \in \mathbb{A}^{n+1} : x_i \neq 0, \exists i = 0, \ldots, n\}$ módulo a relação de equivalência

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Leftrightarrow (x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n), \lambda \in \bar{K}.$$

Denotaremos a classe associada por $[x, y, z]$ e chamaremos os $x_i's$ de coordenadas homogêneas. O *corpo mínimo de definição para P^n sobre K* é o conjunto

$$K(P) = K(x_0/x_i, \ldots, x_n/x_i), \quad \forall i, \ x_i \neq 0.$$

O grupo de Galois age de forma idêntica como no caso afim.

Definição 1.8. Diremos que $f \in \bar{K}[X]$ é homogêneo de grau d se

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n), \quad \forall \lambda \in \bar{K}^*.$$

Um ideal $I \subset \bar{K}[X]$ é *homogêneo* se é gerado por polinômios homogêneos.

Seja f um polinômio homogêneo e seja $P \in \mathbb{P}^n$. Estamos interessados nos casos em que $f(P) = 0$. Assim, para cada ideal homogêneo I associamos o subconjunto de $\mathbb{P}^n$ da forma

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0, \ \forall f \in I \text{ homogêneo}\}.$$

Definição 1.9. Um conjunto algébrico projetivo é qualquer conjunto da forma V_I, para I um ideal homogêneo. Se V é conjunto algébrico projetivo, o ideal (homogêneo) de V, denotado por $I(V)$, é um ideal de $\bar{K}[X]$ gerado por

$$\{f \in \bar{K}[X] : f \text{ é homogêneo e } f(P) = 0,\ \forall P \in V\}.$$

Se V é definido sobre K, então o conjunto de K-pontos racionais de V é o conjunto

$$V(K) = V \cap \mathbb{P}^n(K).$$

Exemplo 1.8. Seja V um conjunto algébrico em $\mathbb{P}^2$ dado pela equação

$$X^2 + Y^2 = Z^2.$$

Então para qualquer corpo K com $\text{char}(K) \neq 2$, o conjunto $V(K)$ é isomorfo a $\mathbb{P}^1(K)$, através do mapa

$$\mathbb{P}^1(K) \longrightarrow V(K), \qquad [s,t] \longmapsto [s^2 - t^2, 2st, s^2 + t^2].$$

Observação 1.3. Um ponto de $\mathbb{P}^n(\mathbb{Q})$ tem a forma $[x_0, \ldots, x_n]$ com $x_i \in \mathbb{Q}$. Como estamos no espaço projetivo, podemos multiplicar por $\lambda \in \mathbb{Q}$ tal que os denominadores dessa n-upla sejam eliminados. Em outras palavras, todo ponto $P \in \mathbb{P}^n(\mathbb{Q})$ podem ser escritos com coordenadas homogêneas $[x_0, \ldots, x_n]$ satisfazendo

$$x_0, \ldots, x_n \in \mathbb{Z} \ \text{ e } \ \text{mdc}(x_0, \ldots, x_n) = 1.$$

Assim se um ideal de um conjunto algébrico $V/\mathbb{Q}$ é gerado por polinômios homogêneos $f_1, \ldots, f_m \in \mathbb{Q}[X]$, então descrever $V(\mathbb{Q})$ é o mesmo que encontrar soluções para as equações polinomiais

$$f_1(X_0, \ldots, X_n) = \cdots = f_m(X_0, \ldots, X_n) = 0.$$

Exemplo 1.9. O conjunto algébrico

$$V : X^2 + Y^2 = 3Z^2$$

é definido sobre $\mathbb{Q}$. Entretanto, $V(\mathbb{Q}) = \emptyset$. De fato, suponha que $[x, y, z] \in V(\mathbb{Q})$ com $x, y, z \in \mathbb{Z}$ e $\text{mdc}(x, y, z) = 1$. Então

$$x^2 + y^2 \equiv 0 \pmod 3.$$

Consequentemente x^2 e y^2 são divisíveis por 3^2. Segue da equação de V que 3 também divide z, o que contradiz o fato que $\text{mdc}(x, y, z) = 1$.

Definição 1.10. Um conjunto algébrico projetivo é chamado de variedade se $I(V) \lhd \bar{K}[X]$ é primo. Neste caso o anel de coordenadas projetivas da variedade V é

$$\bar{K}[V] = \frac{\bar{K}[X]}{I(V)}.$$

O espaço projetivo contém $n+1$ cópias de $\mathbb{A}^1$, visto que considerando o hiperplano $H : \ x_i = 0$ e $U_i = H_i^C$, a função $\phi_i^{-1} : \ U_i \to \mathbb{A}^n$, tal que

$$[x_0, \ldots, \ x_n] \mapsto \left(\frac{x_0}{x_i}, \ldots, \ \frac{x_{i-1}}{x_i}, \ \frac{x_{i+1}}{x_i}, \ldots, \ \frac{x_n}{x_i} \right),$$

é uma bijeção. Desta forma, tendo fixado i, com $x_i \neq 0$ as quantidades x_j/x_i estão bem definidas, então identificamos $\mathbb{A}^n$ com o conjunto U_i em $\mathbb{P}^n$ via o mapa ϕ_i.

Agora seja V um conjunto algébrico projetivo com ideal homogêneo $I(V) \subset \bar{K}[X]$. Então $V \cap \mathbb{A}^n$ é um conjunto algébrico com ideal dado por

$$I(V \cap \mathbb{A}^n) = \{ f(Y_1, \ldots, \ Y_{i-1}, 1, Y_{i+1}, \ldots, \ Y_n) \ : \ f(X_0, \ldots, \ X_n) \in I(V) \}.$$

O processo de trocar $f(Y_0, \ldots, \ Y_n)$ por $f(Y_1, \ldots, \ Y_{i-1}, 1, Y_{i+1}, \ldots, \ Y_n)$ é chamado desomogeneização com respeito a Y_i. A homogeneização de um polinômio $f(X) \in \bar{K}[X]$, é dada por

$$f^*(X_0, \ldots, \ X_n) = X_i^d f \left(\frac{X_0}{X_i}, \ \frac{X_1}{X_i}, \ldots, \ \frac{X_{i-1}}{X_i}, \ \frac{X_{i+1}}{X_i}, \ldots, \ \frac{X_n}{X_i} \right),$$

onde $d = \deg(f)$.

Definição 1.11. Seja $V \subset \mathbb{A}^n$ um conjunto algébrico afim com ideal $I(V)$, e considere V como subconjunto de $\mathbb{P}^n$ via

$$\phi_i : V \subset \mathbb{A}^n \longrightarrow \mathbb{P}^n.$$

O fecho projetivo de V, denotado por $\bar{V}$, é o conjunto algébrico projetivo cujo ideal homogêneo $I(\bar{V})$ é gerado por

$$\{ f^*(X) : f \in I(V) \}.$$

Proposição 1.2. a) Seja V variedade afim. Então $\bar{V}$ é variedade projetiva e $V =$

$\bar{V} \cap \mathbb{A}^n$.
b) Seja V variedade projetiva. Então $V \cap \mathbb{A}^n$ é variedade afim com

$$V \cap \mathbb{A}^n = \emptyset \text{ ou } V = \bar{V} \cap \mathbb{A}^n.$$

c) Se uma variedade afim é definida sobre K, então $\bar{V}$ é também definida sobre K.
Prova. Veja em [2, I.2.3]. □

Observação 1.4. De acordo com a proposição anterior, cada variedade pode ser identificada com uma única variedade projetiva. Em termos de notação, uma vez que é relativamente fácil tratar com coordenadas afins, estaremos dizendo "seja V variedade projetiva" porém escrevendo em equações de coordenadas não homogêneas, entendido que V é o fecho projetivo da variedade afim W indicada. Os pontos $V \backslash W$ são os chamados pontos no infinito de V.

Exemplo 1.10. Seja V uma variedade projetiva dada pela equação

$$V : Y^2 = X^3 + 17.$$

Isso significa que V é uma variedade em $\mathbb{P}^2$ dada pela equação homogênea

$$\bar{Y}^2\bar{Z} = \bar{X}^3 + 17\bar{Z}^3,$$

onde estamos identificando

$$X = \bar{X}/\bar{Z}, \quad Y = \bar{Y}/\bar{Z}.$$

Esta variedade tem o ponto $[0, 1, 0]$ no infinito, obtido escrevendo $\bar{Z} = 0$. Assim, por exemplo,

$$V(\mathbb{Q}) = \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) : y^2 = x^3 + 17\} \cup \{[0, 1, 0]\}.$$

Muitas propriedades importantes da variedade projetiva V podem ser definidas em termos de sua subvariedade afim $V \cap \mathbb{A}^n$.

Definição 1.12. Seja V/K variedade projetiva e $\mathbb{A}^n \subset \mathbb{P}^n$ tal que $V \cap \mathbb{A}^n \neq \emptyset$. A dimensão de V é a dimensão de $V \cap \mathbb{A}^n$.

O corpo de função de V, denotado por $K(V)$, é o corpo de função de $V \cap \mathbb{A}^n$ e o mesmo vale para $\bar{K}(V)$. Para diferentes escolhas de $\mathbb{A}^n$, os $K(V)$s são isomorfos.

Definição 1.13. Seja V variedade projetiva, $P \in V$, e escolha $\mathbb{A}^n \subset \mathbb{P}^n$ e $P \in \mathbb{A}^n$. Então V é não singular (ou suave) em P se $V \cap \mathbb{A}^n$ é singular em P. O anel local de V em P, denotado por $\bar{K}[V]_P$, é o anel local de $V \cap \mathbb{A}^n$ em P. Uma função $F \in \bar{K}(V)$ é singular (ou definida) em P se está em $\bar{K}[V]_P$, caso em que se pode avaliar no ponto P.

Observação 1.5. O corpo de funções de $\mathbb{P}^n$ pode também ser descrito como subcorpo de $\bar{K}(X_0, \ldots, X_n)$ consistindo das funções racionais $F(X) = f(X)/g(X)$ para cada f e g polinômios homogêneos de mesmo grau. Tal expressão dá uma função bem definida $\mathbb{P}^n$ em todo ponto P onde $g(P) \neq 0$. Similarmente, o corpo de função de uma variedade projetiva V é o corpo de funções racionais $F(X) = f(X)/g(X)$ tal que:
(i) f e g são homogêneos de mesmo grau;
(ii) $g \notin I(V)$;
(iii) f_1/g_1 e f_2/g_2 são identificadas se $f_1 g_2 - f_2 g_1 \in I(V)$.

1.3 Mapas entre Variedades

Definição 1.14. Seja V_1 e $V_2 \subset \mathbb{P}^n$ variedades projetivas. Um mapa racional de V_1 em V_2 é um mapa da forma

$$\phi : V_1 \to V_2$$
$$\phi = [f_0, \ldots, f_n],$$

onde $f_0, \ldots, f_n \in \bar{K}(V_1)$ estão bem definidos em todo ponto $P \in V_1$,

$$\phi(P) = [f_0(P), \ldots, f_n(P)] \in V_2.$$

Se V_1 e V_2 são definidos sobre K, então $G_{\bar{K}/K}$ age em ϕ da forma:

$$\phi^\sigma(P) = [f_0^\sigma(P), \ldots, f_n^\sigma(P)].$$

Se existir $\lambda \in \bar{K}^*$ tal que $\lambda f_0, \ldots, \lambda f_n \in K(V_1)$, então diremos que ϕ é *definido* sobre K. Na verdade ϕ é definido sobre K se, e somente se, $\phi = \phi^\sigma$ para todo $\sigma \in G_{\bar{K}/K}$.

Um mapa racional não precisa ser bem definido em todo ponto de V_1. Entretanto é possível avaliar $\phi(P)$ em pontos $P \in V_1$ onde algum f_i não for regular, simplesmente substituindo cada f_i por gf_i, por um $g \in \bar{K}(V_1)$. Desse modo introduzimos a seguinte definição:

Definição 1.15. Um mapa racional $\phi = [f_0, \ldots, f_n] : V_1 \longrightarrow V_2$ é regular (definido) em $P \in V_1$ se existir $g \in \bar{K}(V_1)$ tal que:
(i) cada gf_i é regular em P, ou seja, $gf_i \in \bar{K}[V]_P$.
(ii) exite algum i para o qual $(gf_i)(P) \neq 0$.

Se tal g existe, então definimos

$$\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)].$$

Pode ser necessário tomar diferentes gs para diferentes pontos. Um mapa que é regular em todo ponto é chamado um morfismo.

Exemplo 1.11. Considere que $\text{char}(K) \neq 2$ e seja V a variedade

$$\phi : V \longrightarrow \mathbb{P}^1, \qquad \phi = [X + Z, Y].$$

Vemos que ϕ é regular em todo ponto de V, exceto no ponto $[1, 0, -1]$, onde $X+Z = Y = 0$. No entanto, fazendo

$$(X + Z)(X - Z) \equiv -Y^2 \pmod{I(V)},$$

temos que

$$\phi = [X + Z, Y] = [X^2 - Z^2, Y(X - Z)] = [-U^2, Y(X - Z)] = [-Y, X - Z].$$

Assim

$$\phi([1, 0, -1]) = [0, 2] = [0, 1],$$

então ϕ é regular em todo ponto de V, ou seja, ϕ é um morfismo.

Observação 1.6. Seja $V_1 \subset \mathbb{P}^m$ e $V_2 \subset \mathbb{P}^n$ variedades projetivas. Lembramos que funções em $\bar{K}(V_1)$ podem ser descritas como quocientes de polinômios homogêneos em $\bar{K}[X_0, \ldots, X_m]$ tendo o mesmo grau. Assim, multiplicando o mapa racional $\phi = [f_0, \ldots, f_n]$ por um polinômio homogêneo para eliminar os denominadores dos f_is obtemos a seguinte definição alternativa:

Definição 1.16. Um mapa racional $\phi : V_1 \longrightarrow V_2$ é um mapa da forma $\phi = [\phi_0(X), \ldots, \phi_n(X)]$, onde:
(i) $\phi_i(X) \in \bar{K}[X] = \bar{K}[X_0, \ldots, X_n]$ são polinômios homogêneos, não todos em $I(V_1)$, tendo o mesmo grau.
(ii) para todo $f \in I(V_2)$, $f(\phi_0(X), \ldots, \phi_n(X)) \in I(V_1)$.

Claramente, $\phi(P)$ é bem definido dado que algum $\phi_i(P) \neq 0$. Entretanto, mesmo se todo $\phi(P) = 0$, é possível modificar ϕ de modo que $\phi(P)$ faça sentido. Mais precisamente:

Um mapa racional $\phi = [\phi_0, \ldots, \phi_n] : V_1 \longrightarrow V_2$ como acima é regular (ou definido) em $P \in V_1$ se existe polinômios homogêneos $\psi_0, \ldots, \psi_n$ tal que
(i) $\exists \psi_0, \ldots, \psi_n$ tendo o mesmo grau.
(ii) $\phi_i\psi_j \equiv \phi_j\psi_i (\text{mod } I(V_1)) \ \ \forall\ 0 \leq i,\ j \leq n$;
(iii) $\psi(P) \neq 0$ para algum i.

Se isso ocorre, então podemos definir

$$\phi(P) = [\psi_0(P), \ldots, \psi_n(P)].$$

Observação 1.7. Seja $\phi = [\phi_0, \ldots, \phi_n] : \mathbb{P}^m \to \mathbb{P}^n$ mapa racional, onde os $\phi_i \in \bar{K}[X]$ são polinômios homogêneos de mesmo grau. Como $\bar{K}[X]$ é um domínio de fatoração única, podemos assumir que os ϕ_is não tem fator em comum. Então ϕ é regular no ponto $P \in \mathbb{P}^m$ se, e somente se, algum $\phi_i(P) \neq 0$. Consequentemente ϕ é um morfismo se, e somente se, os ϕ_is não tem fator em comum em $\mathbb{P}^m$.

Definição 1.17. Sejam V_1 e V_2 variedades. Diremos que V_1 e V_2 são isomorfas, e escrevemos $V_1 \simeq V_2$, se existir morfismos $\phi : V_1 \to V_2$ e $\psi : V_2 \to V_1$ tais que $\psi \circ \phi$ e $\phi \circ \psi$ são mapas identidade em V_1 e V_2 respectivamente. Diremos que V_1/K e V_2/K são isomorfos sobre K se ϕ e ψ podem ser definidos sobre K.
Note que ϕ e ψ devem ser morfismos e não apenas mapas racionais.

Observação 1.8. Se $\phi : V_1 \to V_2$ é um isomorfismo sobre K, então ϕ identifica $V_1(K)$ com $V_2(K)$ de modo natural. Consequentemente, para problemas diofantinos, é suficiente estudar as classes de K-isomorfismo de variedades.

Exemplo 1.12. Usando a observação (1.7), vemos que o mapa racional

$$\phi : \mathbb{P}^2 \to \mathbb{P}^2, \quad \phi = [X^2, XY, Z^2],$$

é regular exceto no ponto $[0, 1, 0]$.

Exemplo 1.13. Considere as variedades

$$V_1 : X^2 + Y^2 = Z^2 \quad \text{e} \quad V_2 : X^2 + Y^2 = 3Z^2.$$

Essas variedades não são isomorfas sobre $\mathbb{Q}$, pois $V_2(\mathbb{Q}) = \emptyset$, conforme vimos anteriormente, e $V_1(\mathbb{Q})$ contém muitos pontos, ou de modo mais preciso, $V_1(\mathbb{Q}) =$

$\mathbb{P}^1(\mathbb{Q})$ através do mapa

$$\psi : \mathbb{P}^1 \longrightarrow V, \quad \psi = [S^2 - T^2, 2ST, S^2 + T^2],$$

que é um morfismo e inverso do morfismo $\phi = [X + Z, Y]$, como já vimos. Entretanto as variedades V_1 e V_2 são isomorfas sobre $\mathbb{Q}(\sqrt{3})$, com isomorfismo dado por

$$\varphi : V_2 \longrightarrow V_1, \quad \varphi = [X, Y, \sqrt{3}Z].$$

Capítulo 2

Curvas Algébricas

Apresentaremos neste capítulo os fatos básicos sobre as curvas algébricas, que precisaremos no decorrer do estudo de curvas elípticas.

2.1 Curvas

Por uma curva entenderemos uma variedade projetiva de dimensão um. Em geral trabalharemos com curvas não-singulares.

A seguir, definiremos alguns conceitos que serão necessários para a teoria ao longo da seção.

Definição 2.1. Seja K um corpo. Uma valorização discreta sobre K é qualquer mapa $v : K^* \to \mathbb{Z}$, onde $K^* = K - \{0\}$ é grupo multiplicativo de K, tal que
(1) $v(xy) = v(x) + v(y)$,
(2) $v(x + y) \geq \min(v(x), v(y))$.

Definição 2.2. Diremos que um anel A é anel de valorização discreta se existir uma valorização v sobre K tal que $v(x) \geq 0$, para todo $x \in A$.
Observe que nesse caso A é um domínio, pois necessariamente $A \subset K$.

A demonstração do próximo resultado pode ser visto em [11].

Proposição 2.1. Seja A um domínio Noetheriano local, M seu ideal maximal e $K = A/M$. Então as seguintes afirmações são equivalente:
(i) A é anel de valorização discreta.
(ii) M é principal.
(iii) $\dim_K M/M^2 = 1$.

Proposição 2.2. Seja C uma curva e $P \in C$ um ponto suave. Então $\bar{K}[C]_P$ é um anel de valorização discreta.

Prova. Como vimos no capítulo anterior, o espaço vetorial M_P/M_P^2 tem dimensão 1 sobre o corpo $\bar{K} = \bar{K}[C]_P/M_P$. Pela proposição anterior, é equivalente $\bar{K}[C]_P$ ser anel de valorização discreta e M_P/M_P^2 ter dimensão 1, o que queríamos provar. □

Definição 2.3. Seja C uma curva e P um ponto não-singular. A valorização (normalizada) no anel local $\bar{K}[C]_P$ é dado por

$$\begin{aligned} \mathrm{ord}_P : \ & \bar{K}[C]_P \longrightarrow \{0,\ 1,\ 2, \ldots\} \\ & \mathrm{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in \mathcal{M}_P^d\}. \end{aligned}$$

Este mapa está bem definido. De fato, considere $f,\ g \in \bar{K}[C]_P$ funções tais que $f = g$. Então,

$$\mathrm{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in \mathcal{M}_P^d\} = \sup\{d \in \mathbb{Z} : g \in \mathcal{M}_P^d\} = \mathrm{ord}_P(g),$$

ou seja, ord_P está bem definida.

Escrevendo $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, podemos extender ord_P da forma:

$$\mathrm{ord}_P : \ \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}.$$

De fato, supondo que os valores $f_1/g_1 = f_2/g_2$, segue que

$$\begin{aligned} \mathrm{ord}_P(1) = 0 &\implies \mathrm{ord}_P\big(\frac{f_1.g_1}{g_1.f_1}\big) = 0 \\ &\implies \mathrm{ord}_P\big(\frac{f_1.g_2}{g_1.f_2}\big) = 0 \\ &\implies \mathrm{ord}_P\big(\frac{f_1}{f_2}\big) - \mathrm{ord}_P\big(\frac{g_1}{g_2}\big) = 0 \\ &\implies (\mathrm{ord}_P(f_1) - \mathrm{ord}_P(f_2)) - (\mathrm{ord}_P(g_1) - \mathrm{ord}_P(g_2)) = 0 \\ &\implies \mathrm{ord}_P(f_1) - \mathrm{ord}_P(g_1) = \mathrm{ord}_P(f_2) - \mathrm{ord}_P(g_2) \\ &\implies \mathrm{ord}_P\big(\frac{f_1}{g_1}\big) = \mathrm{ord}_P\big(\frac{f_2}{g_2}\big). \end{aligned}$$

Um uniformizador para C em P é qualquer função $t \in \bar{K}(C)$ com $\mathrm{ord}_P(t) = 1$, ou seja, é um gerador para $\mathcal{M}_P$.

Definição 2.4. Sejam C, P como descrito anteriormente e $f \in \bar{K}(C)$. A *ordem* de f em P é $\mathrm{ord}_P(f)$. Se $\mathrm{ord}_P(f) > 0$, então f tem zero em P. Se $\mathrm{ord}_P(f) < 0$, então

f tem polo em P. Se $\mathrm{ord}_P(f) \geqslant 0$, então f é regular em P, e podemos calcular $f(P)$. Senão diremos que f tem polo em P, escrevendo $f(P) = \infty$.

Proposição 2.3. Seja C uma curva suave e $f \in \bar{K}(C)$ com $f \neq 0$. Então existe um número finito de pontos de C em que f tem pólo ou zero. Além disso, se f não tem polos, então $f \in \bar{K}$.

Prova. Veja [2] e [10].

Exemplo 2.1. Considere as duas curvas seguintes:

$$C_1 : Y^2 = X^3 + X \quad \text{e} \quad C_2 : Y^2 = X^3 + X^2.$$

Lembremos da convenção que fizemos anteriormente, apesar de escrevermos as curvas C_1 e C_2 como equações afins, elas possuem ponto no infinito, formado pelos pontos da curva menos os pontos afins. Seja $P = (0, 0)$. Então C_1 é suave em P enquanto que C_2 não é. O ideal maximal M_P do anel local $\bar{K}[C_2]_P$ não é um anel de valorização discreta.

A proposição a seguir é útil quando tratamos com curvas sobre corpos de características $p > 0$.

Proposição 2.4. Sejam C/K uma curva e $t \in K(C)$ um uniformizador de algum ponto não singular $P \in C(K)$. Então $K(C)$ é extensão separável finita de $K(t)$.

Prova. O corpo $K(C)$ é uma extensão algébrica finita, visto que é finitamente gerado sobre K, tendo grau de transcendência um sobre K, pois C é curva, e $t \notin K$. Seja $x \in K(C)$. Mostremos que x é separável sobre $K(t)$.

Qualquer que seja x, ele é algébrico sobre $K(t)$, pois a extensão tem grau de transcendência finito sobre K. Seja $\Phi = \min x$, então:

$$\sum a_{ij} t^i x^j = 0, \quad \text{onde} \quad \Phi(T, X) = \sum a_{ij} T^i X^j \in K[X, T].$$

Se Φ contém um termo não nulo $a_{ij} T^i X^j$ com $j \not\equiv 0 (\mathrm{mod}\, p)$, então $\partial\Phi(t, X)/\partial X \neq 0$, logo x é separável sobre $K(t)$.

Suponha, como alternativa, que $\Phi(T, X) = \Psi(T, X^p)$. Vamos mostrar por contradição. Devemos notar que se $F(T, X) \in K[T, X]$ é um polinômio, então $F(T^p, X^p) = F^p(T, X)$. De fato, assumimos anteriormente que K é perfeito, o que implica que todo elemento de K é uma potência p-ésima, ou seja, $k = k^p$. Assim, se $F(T, X) = \sum \alpha_{ij} T^i X^j$, então escrevendo $\alpha_{ij} = \beta_{ij}^p$ obtemos $F(T^p, X^p) = (\sum \beta_{ij} T^i X^j)^p$.

Reagrupamos os termos em $\Phi(T,X) = \Psi(T,X^p)$ de acordo com as potências de T módulo p. Assim,

$$\Phi(T,X) = \Psi(T,X^p) = \sum_{k=0}^{p-1} \Big(\sum_{i,j} b_{ijk} T^{ip} X^{jp} \Big) T^k = \sum_{k=0}^{p-1} \phi_k(T,X)^p T^k.$$

Por suposição temos que $\Phi(t,x) = 0$. Por outro lado, como t é uniformizador em P, temos:

$$\operatorname{ord}_P(\phi_k(t,x)^p t^k) = p \operatorname{ord}_P(\phi_k(t,x)) + k \operatorname{ord}_P(t) \equiv k \pmod{p}.$$

Assim cada um dos termos da soma $\sum \phi_k(t,x)^p t^k$ tem ordem distinta em P, então todo termo deve anular,

$$\phi_0(t,x) = \phi_1(t,x) = \cdots = \phi_{p-1}(t,x) = 0.$$

Mas ao menos um dos $\phi_k(T,X)$'s deve envolver X, e para esse k, a relação $\phi_k(t,x) = 0$ contradiz nossa escolha de $\Phi(t,X)$ como polinômio mínimo para x sobre $K(t)$. (Note que $\deg_X \phi_k(T,X) \leq \frac{1}{p} \deg_X \Phi(T,X)$.) Assim temos uma contradição, o que implica na prova de que x é separável sobre $K(t)$. □

2.2 Mapas entre Curvas

Começamos com um resultado fundamental para mapas racionais entre curvas suaves:

Proposição 2.5. Seja C uma curva, $V \subset \mathbb{P}^N$ uma variedade, $P \in C$ um ponto não-singular e $\phi : C \to V$ um mapa racional. Então ϕ é regular em P. Em particular, se C é suave, então ϕ é um morfismo.

Prova. Dado $\phi = [f_0, \ldots, f_N]$ com $f_i \in \bar{K}(C)$, escolha um uniformizador $t \in \bar{K}(C)$ para C em P. Seja

$$n = \min_{0 \leqslant i \leqslant N} \{\operatorname{ord}_P(f_i)\}.$$

Então

$$\operatorname{ord}_P(t^{-n} f_i) \geqslant 0 \text{ para todo } i \text{ e } \operatorname{ord}_P(t^{-n} f_j) = 0 \text{ para algum } j,$$

como foi visto na última observação do capítulo anterior. Assim, cada t^{-n} é regular em P e $(t^{-n} f_j)(P) \neq 0$. Assim ϕ é regular em P.

O resultado anterior não vale para dimensão maior do que 1. Por exemplo:

$$\phi : \mathbb{P}^2 \to \mathbb{P}^2, \quad \phi = [X^2,\ XY,\ \mathbb{Z}^2],$$

que ϕ é regular em todo ponto exceto em $P = [0, 1, 0]$.

Agora supondo o caso de uma curva $C :\ Y^2Z = X^3 + X^2Z$ e considerando o mapa racional $\phi = [Y, X] : V \to \mathbb{P}^1$, vemos que ϕ não é regular em $[0, 0, 1]$, uma vez que temos também $\phi(P) = [0, 0]$. □

Exemplo 2.2. Seja C/K uma curva suave e $f \in K(C)$. Então f define um mapa racional que também será denotado por f:

$$f : C \to \mathbb{P}^1, \qquad P \mapsto f(P).$$

$$f(P) = \begin{cases} [f(P), 1], \text{ se } f \text{ é regular em } P, \\ [1, 0], \text{ se } f \text{ tem polo em } P. \end{cases}$$

De modo contrário, seja

$$\phi :\ C \to \mathbb{P}^1, \quad \phi = [f, g]$$

um mapa racional sobre K. Então ou $g = 0$, caso em que temos ϕ constante $[1, 0]$, ou um mapa correspondendo à função f/g, conforme visto logo acima.
Denotando o mapa anterior por ∞, temos a seguinte correspondência biunívoca:

$$K(C) \cup \{\infty\} \longleftrightarrow \{\text{mapas } C \to \mathbb{P}^1 \text{ definidos sobre } K\}.$$

Frequentemente iremos identificar esses dois conjuntos.

Ao longo deste texto apresentaremos resultados para identificar os conjuntos acima. O próximo teorema é um importante fato sobre morfismos entre curvas.

Teorema 2.1. Seja $\phi : C_1 \to C_2$ um morfismo entre curvas. Então ϕ é sobrejetor ou é constante.

Prova. A demonstração deste teorema pode ser vista em [2, II.6.8].

Sejam C_1/K e C_2/K curvas e $\phi : C_1 \to C_2$ um mapa racional não constante definido sobre K. Então a seguinte composição com ϕ induz a uma injeção entre corpos de funções fixando K,

$$\phi^* : K(C_2) \to K(C_1), \quad \phi^* f = f \circ \phi.$$

Teorema 2.2. Sejam C_1/K e C_2/K curvas.
(a) Seja $\phi : C_1 \to C_2$ um mapa racional definido sobre K. Então $K(C_1)$ é uma extensão finita de $\phi^*(K(C_2))$.
(b) Seja $\iota : K(C_2) \to K(C_1)$ um mapa racional injetivo entre corpos de funções fixando K. Então existe um único mapa não constante $\phi : C_1 \to C_2$ definido sobre K tal que $\phi^* = \iota$.
(c) Seja $\mathbb{K} \subset K(C_1)$ um subcorpo de índice finito contendo K. Então existe uma curva suave C'/K, única a menos de K-isomorfismo, e um mapa não constante $\phi : C_1 \to C'$ definido sobre K tal que $\phi^*(K(C')) = \mathbb{K}$.

Prova. (a) Como o corpo $K(C_1)$ é extensão finitamente gerada com grau de transcendência 1 do corpo K e como $\phi^*(K(C_2)) \in K(C_1)$, segue que a extensão é algébrica finitamente gerada.

(b) Suponha, renomeando se necessário, que C_2 não esteja contido no hiperplano $X_0 = 0$. Seja $C_1 \subset \mathbb{P}^N$. Definindo $\phi : C_1 \to C_2$ da forma

$$\phi = [1, \iota(X_1/X_0), \ldots, \iota(X_N/X_0)]$$

temos que

$$\phi^* f = f \circ \phi = f \circ [1, \iota(X_1/X_0), \ldots, \iota(X_N/X_0)].$$

Como ι fixa o corpo de base K, temos que

$$f \circ [1, \iota(X_1/X_0), \ldots, \iota(X_N/X_0)] = f \circ [\iota(X_0/X_0), \iota(X_1/X_0), \ldots, \iota(X_N/X_0)],$$

ou seja, $f \circ \iota$. O mapa ϕ não é constante pois os X_i/X_0's não são todos constantes e ι é injetora. Finalmente, se $\psi = [f_0, \ldots, f_N]$ for outro mapa com $\psi^* = \iota$, então para cada i,

$$f_i/f_0 = \psi^* g_i = \iota(g_i),$$

o que mostra que $\psi = \phi$.

(c) O caso em que K é algebricamente fechado pode ser visto em [2, I.6.12]. O caso geral é demonstrado de modo similar, ou deduzido a partir dos caso em que os $G_{\bar{K}/K}$-invariantes são algebricamente fechados. □

Definição 2.5. Seja $\phi : C_1 \to C_2$ mapa entre curvas definidas sobre K. Se ϕ é constante, definimos o *grau* de ϕ como sendo 0. Caso contrário diremos que ϕ é

mapa finito de grau:

$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$

Diremos que ϕ é separável, inseparável, ou puramente inseparável se a extensão $K(C_1)/\phi^* K(C_2)$ tem a correspondente propriedade, e denotaremos os graus separáveis e inseparáveis por $\deg_s \phi$ e $\deg_i \phi$, respectivamente.

Definição 2.6. Seja $\phi : C_1 \to C_2$ mapas não constantes de curvas definidas sobre K. Do teorema anterior, sabemos que $K(C_1)$ é extensão finita de $\phi^* K(C_2)$. Usamos o mapa norma relativa a ϕ^* para definir o mapa em outra direção,

$$\phi_* : K(C_1) \to K(C_2), \quad \phi_* = (\phi^*)^{-1} \circ N_{K(C_1)/\phi^* K(C_2)}.$$

Corolário 2.1. Sejam C_1 e C_2 curvas suaves e $\phi : C_1 \to C_2$ um mapa de grau um. Então ϕ é um isomorfismo.

Prova. Por definição, $\deg \phi = 1$ significa que $\phi^* \bar{K}(C_2) = \bar{K}(C_1)$, assim ϕ^* é um isomorfismo de corpos de função. Consequentemente do teorema (2.2.b) temos que, correspondendo ao inverso do mapa $(\phi^*)^{-1} : \bar{K}(C_1) \to \bar{K}(C_2)$, existe um mapa racional $\psi : C_2 \to C_1$ tal que $\psi^* = (\phi^*)^{-1}$. Assim, como C_2 é suave, da proposição (2.5), ψ é morfismo. Então, como $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ é mapa identidade em $\bar{K}(C_2)$, e como $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ é o mapa identidade em $\bar{K}(C_1)$, temos pelo teorema (2.2.b) que $\phi \circ \psi$ e $\psi \circ \phi$ são, respectivamente, mapa identidade em C_2 e em C_1. Em consequencia disso, ϕ e ψ são isomorfismos □

Observação 2.1. O resultado anterior demonstra a relação próxima entre as curvas suaves e seus corpos de função. Podemos observar com precisão começando pelo seguinte mapa de equivalência entre categorias:

$$C/K \longrightarrow K(C)$$
$$\phi : C_1 \to C_2 \longrightarrow \phi^* : K(C_2) \to K(C_1)$$

Exemplo 2.3. *Curvas Hiperelípticas.* Suponha que $char(K) \neq 2$. Escolhemos um polinômio $f(x) \in K[x]$ de grau d e consideramos a curva afim C_0/K dada pela equação

$$C_0 \ : \ y^2 = f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d.$$

Suponha

$$2y_0 = f'(x_0) = 0,$$

o que significa que $y_0 = 0$ e x_0 é raiz dupla de $f(x)$. Consequentemente se assumirmos

que o discriminante de f é não nulo, então a curva afim $y^2 = f(x)$ será não singular.

Se olharmos C_0 como curva em $\mathbb{P}^2$ homogeneizando sua equação afim, então é facil ver que os pontos no infinito são singulares sempre que $d \geq 4$. Por outro lado, o ítem (c) da proposição anterior nos mostra que existe alguma curva projetiva C/K cujo corpo de funções é tal que $K(C_0) = K(x, y)$. Aqui há um problema: o fato de que esta curva é suave mas não é subconjunto de $\mathbb{P}^2$. Por exemplo, considerando o caso em que $d = 4$, C_0 tem equação afim:

$$C_0 \ : \ y^2 = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4.$$

Definimos o mapa

$$[1, x, y, x^2] : C_0 \to \mathbb{P}^3.$$

Escrevendo $[X_0, X_1, X_2, X_3] = [1, x, y, x^2]$, o ideal da imagem deste mapa contém os seguintes dois polinômios homogêneos:

$$\begin{aligned} F &= X_3X_0 - X_1^2, \\ G &= X_2^2X_0^2 - a_0X_1^4 - a_1X_1^3X_0 - a_2X_1^2X_0^2 - a_3X_1X_0^3 - a_4X_0^4. \end{aligned}$$

Entretanto, o conjunto dos zeros desses dois polinômios não é a curva que queremos C, pois ele inclui a reta $X_0 = X_1 = 0$. Assim substituimos $X_1^2 = X_0X_3$ em G e cancelamos X_0^2 para obter o seguinte polinômio quadrático:

$$H = X_2^2 - a_0X_3^2 - a_1X_1X_3 - a_2X_0X_3 - a_3X_0X_1 - a_4X_0^2.$$

Afirmamos que o ideal gerado por F e H nos dá a curva C. Para isso, notamos que se $X_0 \neq 0$, então desomogeneizando com respeito a X_0 temos a seguinte equação:

$$z = x^2 \quad \text{e} \quad y^2 = a_0z^2 + a_1xz + a_2z + a_3x + a_4.$$

Substituindo a primeira equação na segunda obtemos a curva original C_0. Assim

$$C_0 \cong C \cap \{X_0 \neq 0\}.$$

Prosseguindo, se $X_0 = 0$, então segue que $X_1 = 0$, e então $X_2 = \pm\sqrt{a_0}X_3$. Assim C tem dois pontos $[0, 0, \pm\sqrt{a_0}, 1]$ no hiperplano $X_0 = 0$. (Note que $a_0 \neq 0$, pois assumimos que $f(x)$ tem grau 4.) Para verificar que C é não singular nesses dois pontos, desomogeneizamos com respeito a X_3, definindo $u = X_0/X_3$, $v = X_1/X_3$ e

$w = X_2/X_3$. Isso nos fornece as equações:

$$u = v^2 \quad \text{e} \quad w^2 = a_0 + a_1 v + a_2 u + a_3 uv + a_4 u^2,$$

de onde obtemos a equação afim

$$w^2 = a_0 + a_1 v + a_2 v^2 + a_3 v^3 + a_4 v^4.$$

Também, pelo fato de que $f(x)$ não tem raízes duplas, vemos que os pontos $(v, w) = (0, \pm\sqrt{a_0})$ são não singulares.

A discussão anterior será resumida na seguinte proposição, sem demonstração por hora.

Proposição 2.6. Seja $f(X) \in K[x]$ um polinômio de grau 4 com disc $(f) \neq 0$. Existe uma curva projetiva suave $C \subset \mathbb{P}^3$ com as seguintes propriedades:
(i) $C \cap \mathbb{A}^3$, $\mathbb{A}^3 = \{X_0 \neq 0\}$, é isomorfo a curva afim $y^2 = f(x)$.
(ii) Seja $f(x) = a_0 x^4 + \cdots + a_4$. Então a interseção de C com o hiperplano $X_0 = 0$ consiste dos pontos $[0, 0, \pm\sqrt{a_0}, 1]$.

A seguir estudaremos o comportamento de um mapa entre curvas na vizinhança de um ponto qualquer.

Definição 2.7. Seja $\phi : C_1 \to C_2$ um mapa não constante de curvas suaves, e seja $P \in C_1$. O *índice de ramificação de ϕ em P*, denotado por $e_\phi(P)$, é o número

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)}),$$

onde $t_{\phi(P)} \in K(C_2)$ é um uniformizador de $\phi(P)$. Note que $e_\phi(P) \geq 1$. Diremos que ϕ é não ramificado em P se $e_{\phi(P)} = 1$, e que ϕ é não ramifimicado se for não ramificado em todo ponto de C_1.

Proposição 2.7. Seja $\phi : C_1 \to C_2$ um mapa não constante entre curvas suaves.
(a) Para todo $Q \in C_2$,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

(b) Para um número finito de $Q \in C_2$,

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

(c) Seja $\psi : C_2 \to C_3$ outro mapa não constante entre curvas suaves. Então para todo $P \in C_1$,

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

Prova. (a) Veja [2, II.6.9].
(b) Veja [2, II.6.8].
(c) Seja $t_{\phi P}$ e $t_{\psi\phi P}$ uniformizadores. Por definição, as funções

$$t_{\phi P}^{e_\psi(\phi P)} \quad \text{e} \quad \psi^* t_{\psi\phi P},$$

tendo a mesma ordem em $\phi(P)$. Aplicando ϕ^* e tomando a ordem no ponto P ficamos com

$$\mathrm{ord}_P\left(\phi^* t_{\phi P}^{e_\psi(\phi P)}\right) = \mathrm{ord}_P((\psi\phi)^* t_{\psi\phi P}),$$

o que queríamos. □

Corolário 2.2. O mapa $\phi : C_1 \to C_2$ é não ramificado se, e somente se,

$$\#\phi^{-1}(Q) = \deg\,(\phi) \quad \forall Q \in C_2.$$

Prova. Do ítem (a) da proposição anterior, vemos que $\#\phi^{-1}(Q) = \deg\,(\phi)$ se, e somente se,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \#\phi^{-1}(Q).$$

Como $e_\phi(P) \geq 1$, a igualdade ocorre se, e somente se, $e_\phi(P) = 1$. □

Exemplo 2.4. Considere o mapa

$$\phi : \mathbb{P}^1 \to \mathbb{P}^1, \quad \phi([X, Y]) = [X^3(X - Y), Y^5].$$

Então ϕ é ramificado nos pontos $[0, 1]$ e $[1, 1]$. Consequentemente,

$$e_\phi([0, 1]) = 3 \quad \text{e} \quad e_\phi([1, 1]) = 2,$$

então

$$\sum_{P \in \phi^{-1}([0,1])} e_\phi(P) = e_\phi([0, 1]) + e_\phi([1, 1]) = 5 = \deg\,\phi,$$

o que concorda com o ítem (a) da proposição anterior.

O mapa de Frobenius

Considere $\mathrm{char}\,(K) = p > 0$ e seja $q = p^r$. Para qualquer polinômio $f \in K[X]$, seja $f^{(q)}$ o polinômio obtido de f elevando cada coeficiente de f à potência q. Então para cada curva C/K, podemos definir uma nova curva $C^{(q)}/K$ como uma curva

onde o ideal homogêneo é dado por:

$$I(C^{(q)}) = \text{ ideal gerado por } \{f^{(q)} : f \in I(C)\}.$$

Consequentemente, existe um mapa natural de C em $C^{(q)}$, chamado de q-ésimo morfismo de Frobenius, dado por

$$\phi : C \to C^{(q)}, \quad \phi([x_0, \ldots, x_n]) \in C.$$

Para mostrarmos que o mapa está bem definido, é suficiente mostrar que para todo ponto $P = [x_0, \ldots, x_n] \in C$, a imagem $\phi(P)$ é zero de cada gerador $f^{(q)}$ de $I(C^{(q)})$. Calculando

$$\begin{aligned} f^{(q)}(\phi(P)) &= f^{(q)}(x_0^q, \ldots, x_n^q) \\ &= (f(x_0, \ldots, x_n))^q \quad \text{pois } \operatorname{char}(K) = p, \\ &= 0 \qquad\qquad\qquad\quad \text{pois } f(P) = 0. \end{aligned}$$

Exemplo 2.5. Seja C uma curva em $\mathbb{P}^2$ dada pela equação

$$C \ : \ Y^2Z = X^2 + aXZ^2 + bZ^3.$$

Então $C^{(q)}$ é a curva dada pela equação

$$C^{(q)} \ : \ Y^2Z = X^2a^qXZ^2 + b^qZ^3.$$

A seguinte proposição descreve a propriedade básica dos mapas de Frobenius

Proposição 2.8. Seja K corpo de característica $p > 0$, $q = p^r$, C/K uma curva, e seja $\phi : C \to C^{(q)}$ o q-ésimo morfismo de Frobenius. Então
(a) $\phi^* K(C^{(q)}) = K(C)^q = \{f^q : f \in K(C)\}$.
(b) ϕ é puramente inseparável.
(c) $\deg \phi = q$.
(Estamos considerando K um corpo perfeito. Se K não for perfeito, então (b) e (c) permanecem verdadeiros, mas (a) deverá ser modificado.)

Prova. (a) Sabemos que $K(C)$ consiste de quocientes f/g de polinômios homogêneos de mesmo grau, vemos que $\phi^* K(C^{(q)})$ é um subcorpo de $K(C)$ dado pelos quocientes

$$\phi^* \left(\frac{f}{g}\right) = \frac{f(X_0^q, \ldots, X_n^q)}{g(X_0^q, \ldots, X_n^q)}.$$

Da mesma forma, $K(C)^q$ é subcorpo de $K(C)$ dado pelos polinômios

$$\frac{f(X_0,\ldots,X_n)}{g(X_0,\ldots,X_n)}.$$

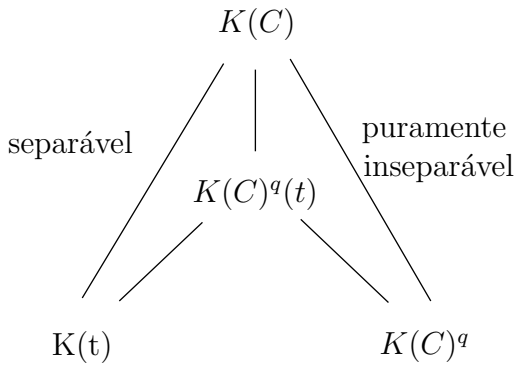
Entretanto, como K é perfeito, sabemos que todo elemento de K é uma q-ésima potência, assim

$$(K[X_0,\ldots,X_n])^q = K[X_0^q,\ldots,X_n^q].$$

Assim o conjunto dos quocientes $f(X_i^q)/g(X_i^q)$ e o conjunto dos quocientes $f(X_i)^q/g(X_i)^q$ são o mesmo subcorpo de $K(C)$.

(b) Segue diretamente do ítem anterior.

(c) Tomando, se necessário, uma extensão de K, podemos assumir que existe um ponto suave $P \in K(C)$. Seja $t \in K(C)$ um uniformizador em P. Então pela proposição (2.4) $K(C)$ é separável sobre $K(t)$. Considerando a torre de corpos formada,



segue que $K(C) = K(C)^q(t)$, e portanto pelo ítem (a)

$$\deg \phi = [K(C)^q(t) : K(C)^q].$$

Observamos agora que $t^q \in K(C)^q$, assim afim de provar que $\deg \phi = q$, precisamos mostrar que $t^{q/p} \notin K(C)^q$. Mas se $t^{q/p} = f^q$ para algum $f \in K(C)$, então

$$\frac{q}{p} = \mathrm{ord}_P(t^{q/p}) = q.\mathrm{ord}_P(f),$$

o que é um absurdo, uma vez que a ordem é um número inteiro.

□

Corolário 2.3. Todo mapa entre curvas suaves $\psi : C_1 \to C_2$ sobre um corpo de

característica $p > 0$ se fatora da forma

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2$$

onde $q = \deg_i(\psi)$, o mapa ϕ é o q-ésimo mapa de Frobenius, e λ é um mapa separável.

Prova. Seja $\mathbb{K}$ o fecho separável de $\psi^*K(C_2)$ em $K(C_1)$. Então $K(C_1)/\mathbb{K}$ é puramente inseparável de grau q, assim $K(C_1)^q \subset \mathbb{K}$. Dos ítens (a) e (c) da proposição anterior temos que,

$$K(C_1)^q = \phi^*(K(C_1^{(q)})) \quad \text{e} \quad [K(C_1) : \phi^*(K(C_1^{(q)}))] = q.$$

Comparando graus, concluímos que $\mathbb{K} = \phi^*(C_1^{(q)})$. Temos agora uma torre de corpos de funções

$$K(C_1)/\phi^*K(C_1^{(q)})/\psi^*K(C_2),$$

e do ítem (b) da proposição anterior, isso corresponde ao mapa que queríamos

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2 \qquad (\psi : C_1 \to C_2)$$

□

2.3 Divisores

O grupo divisor de uma curva C, denotado por $\mathrm{Div}(C)$, é o grupo abeliano livre gerado pelos pontos da curva C. Dessa forma um divisor $D \in \mathrm{Div}(C)$ é a soma formal

$$D = \sum_{P \in C} n_P(P),$$

onde $n_P \in \mathbb{Z}$ e $n_P = 0$ para uma quantidade finita de pontos $P \in C$. O grau de D é definido por

$$\deg D = \sum_{P \in C} n_P.$$

Um divisor de grau zero gera um subgrupo de $\mathrm{Div}(C)$, denotado por

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : \deg D = 0\}.$$

Se C é definido sobre K, tomamos a ação $G_{\bar{K}/K}$ no grupo $\mathrm{Div}(C)$ e $\mathrm{Div}^0(C)$ da forma,

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma).$$

Então o divisor D é definido sobre K se $D^\sigma = D$ para todo $\sigma \in G_{\bar{K}/K}$. Notamos que se $D = n_1(P_1) + \cdots + n_r(P_r)$ com $n_1, \ldots, n_r \neq 0$, então dizer que D é definido sobre K não significa que $P_1, \ldots, P_r \in C(K)$. É suficiente para o grupo $G_{\bar{K}/K}$ permutar os P_i's de forma apropriada. Denotamos o grupo dos divisores definidos sobre K por $\mathrm{Div}_K(C)$, e similarmente $\mathrm{Div}^0_K(C)$.

Agora considere a curva C suave, e seja $f \in \bar{K}(C)^*$. Então podemos associar a f o divisor $\mathrm{div}(f)$ dado por

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Pela definição, este é um divisor. Se $\sigma \in G_{\bar{K}/K}$, então é fácil ver que

$$\mathrm{div}(f^\sigma) = (\mathrm{div}(f))^\sigma.$$

Em particular, se $f \in K(C)$, então $\mathrm{div}(f) \in \mathrm{Div}_K(C)$. Como cada ord_P é uma valorização, o mapa

$$\mathrm{div} : \bar{K}(C)^* \longrightarrow \mathrm{Div}(C)$$

é um homomorfismo entre grupos abelianos.

Definição 2.8. Um divisor $D \in \mathrm{Div}(C)$ é principal se tem a forma $D = \mathrm{div}(f)$ para algum $f \in \bar{K}(C)^*$. Dois divisores são linearmente equivalentes, escrevemos $D_1 \sim D_2$, se $D_1 - D_2$ é principal. A *classe de grupos divisores* (ou *grupo de Picard*) de C, denotado $\mathrm{Pic}(C)$, é o quociente de $\mathrm{Div}(C)$ por seu subgrupo de divisores principais. Tomamos $\mathrm{Pic}_K(C)$ como subgrupo de $\mathrm{Pic}(C)$ fixado por $G_{\bar{K}/K}$. Note que em geral, $\mathrm{Pic}_K(C)$ não é o quociente de $\mathrm{Div}_K(C)$ por seu subgrupo de divisores principais. Mas existe um caso em que isso é verdade.

Proposição 2.9. Seja C uma curva suave e seja $f \in \bar{K}(C)^*$.
(a) $\mathrm{div}(f) = 0$ se, e somente se, $f \in \bar{K}^*$.
(b) $\deg(\mathrm{div}(f)) = 0$.

Prova. (a) Se $\mathrm{div}(f) = 0$, então f não tem polos, assim o mapa associado $f : C \to \mathbb{P}^1$, com $P \mapsto [f(P), 1]$ não é sobrejetivo. Então da proposição (2.5) segue que o mapa é constante, então $f \in \bar{K}^*$. Se $f \in \bar{K}^*$ então a ordem em todo

ponto é nula, ou seja, $\mathrm{div}(f) = 0$.
(b) A demonstração pode ser vista em [2, II.6.10], ou a observação (2.3) no final desta seção. □

Exemplo 2.6. Em $\mathbb{P}^1$, todo divisor de grau zero é principal. Para isso, suponha que $D = \sum n_P(P)$ tem grau 0. Escrevendo $P = [\alpha_P, \beta_P] \in \mathbb{P}^1$, vemos que D é o divisor da função

$$\prod_{P \in \mathbb{P}^1} (\beta_P X - \alpha_P Y)^{n_P}.$$

Note que $\sum n_P = 0$ garante que a função está em $K(\mathbb{P}^1)$. Segue que o mapa de grau $\deg : \mathrm{Pic}(\mathbb{P}^1) \to \mathbb{Z}$ é um isomorfismo. A recíproca é verdadeira, ou seja, se C é uma curva suave e $\mathrm{Pic}(C) \cong \mathbb{Z}$, então C é isomorfo a $\mathbb{P}^1$.

Exemplo 2.7. Sejam K tal que $\mathrm{char}(K) \neq 2$. Seja $e_1, e_2, e_3 \in \bar{K}$ distintos, e considere a curva

$$C \ : \ y^2 = (x - e_1)(x - e_2)(x - e_3).$$

Podemos chegar que C é suave e que tem um ponto singular no infinito, que denotaremos P_∞. Para $i = 1, 2, 3$, seja $P_i = (e_1, 0) \in C$. Então

$$\begin{aligned} \mathrm{div}(x - e_i) &= 2(P_i) - 2(P_\infty) \\ \mathrm{div}(y) &= (P_1) + (P_2) + (P_3) - 3(P_\infty). \end{aligned}$$

Segue da proposição (2.9.b) que os divisores principais formam um subgrupo de $Div^0(C)$. Dessa forma definimos:

Definição 2.9. A classe dos grupos divisores de grau 0 de C é o quociente de $\mathrm{Div}^0(C)$ pelo subgrupo dos divisores principais. Denotamos esse grupo por $\mathrm{Pic}^0(C)$. Similarmente, escremos $\mathrm{Pic}^0_K(C)$ como subgrupo de $\mathrm{Pic}^0(C)$ fixado por $G_{\bar{K}/K}$.

Observação 2.2. A definição acima e a proposição (2.9) podem ser resumidas no fato de existir a sequência exata

$$1 \longrightarrow \bar{K}^* \longrightarrow \bar{K}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \longrightarrow \mathrm{Pic}^0(C) \longrightarrow 0.$$

Seja $\phi : C_1 \to C_2$ um mapa não constante de curvas suaves. Como vimos, ϕ induz os seguintes mapas nos corpos de funções de C_1 e C_2,

$$\phi^* : \bar{K}(C_2) \longrightarrow \bar{K}(C_1) \quad \text{e} \quad \phi_* : \bar{K}(C_1) \longrightarrow \bar{K}(C_2).$$

Similarmente definimos os mapas de grupos divisores da seguinte forma:

$$\begin{aligned} \phi^* : \mathrm{Div}(C_2) &\to \mathrm{Div}(C_1), & \phi_* : \mathrm{Div}(C_1) &\to \mathrm{Div}(C_2), \\ (Q) &\mapsto \sum_{P \in \phi^{-}1(Q)} e_\phi(P)(P), & (P) &\mapsto (\phi P), \end{aligned}$$

e estender $\mathbb{Z}$ linearmente a divisores arbitrários.

Exemplo 2.8. Seja C uma curva suave, $f \in \bar{K}(C)$ uma função não constante, e seja $f : C \to \mathbb{P}^1$ o mapa como ocorre no exemplo 2.2. Então pela definição,

$$\mathrm{div}(f) = f^*((0) - (\infty)).$$

Proposição 2.10. Seja $\phi : C_1 \to C_2$ um mapa não constante entre curvas suaves.

(a) $\deg(\phi^* D) = (\deg \phi)(\deg D)$ para todo $D \in \mathrm{Div}(C_2)$.
(b) $\phi^*(\mathrm{div} f) = \mathrm{div}(\phi^* f)$ para todo $f \in \bar{K}(C_2)^*$.
(c) $\deg(\phi_* D) = \deg D$ para todo $D \in \mathrm{Div}(C_1)$.
(d) $\phi_*(\mathrm{div} f) = \mathrm{div}(\phi_* f)$ para todo $f \in \bar{K}(C_1)^*$.
(e) $\phi_* \circ \phi^*$ age como multiplicação por $\deg \phi$ em $\mathrm{Div}(C_2)$.
(f) Se $\psi : C_2 \to C_3$ é outro mapa como acima, então

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

Prova. (a) Pela definição de $\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$ escrevemos:

$$\begin{aligned} \deg(\phi^* D) &= \deg\left(\phi^* \sum_{Q \in C_2} n_Q (Q)\right) \\ &= \deg\left(\sum_{Q \in C_2} n_Q \phi^* Q\right) && \text{pela definição de } \phi^* \\ &= \deg\left(\sum_{Q \in C_2} \left(\sum_{P \in \phi^{-1}(Q)} e_\phi(P)(Q)\right)\right) \\ &= \deg\left(\sum_{Q \in C_2} n_Q (\deg \phi)(Q)\right) && \text{pela proposição (2.7a)} \\ &= \sum_{Q \in C_2} n_Q (\deg \phi) \\ &= (\deg D)(\deg \phi) \end{aligned}$$

(b) Observe que $\mathrm{ord}_{\phi P}(f) = \mathrm{ord}_{\phi P}(f)\mathrm{ord}_{\phi P}(t_{\phi P})$, ou seja, f e $t_{\phi P}^{\mathrm{ord}_{\phi P}(f)}$ têm a mesma ordem em ϕP. Multiplicando essas duas funções por ϕ^* e tomando a ordem em P

temos:

$$\begin{aligned}\mathrm{ord}_P(\phi^* f) &= \mathrm{ord}_P(\phi^* t_{\phi P}^{\mathrm{ord}_{\phi P}(f)}) \\ &= \mathrm{ord}_P(\phi^* t_{\phi P}).\mathrm{ord}_{\phi P}(f) \\ &= e_\phi(P)\mathrm{ord}_{\phi P}(f).\end{aligned}$$

Agora escrevemos:

$$\begin{aligned}\phi^*(\mathrm{div} f) &= \phi^*\left(\sum_{Q\in C_2} \mathrm{ord}_Q(f)(Q)\right) \\ &= \sum_{Q\in C_2} \mathrm{ord}_Q(f)\phi^*(Q) \\ &= \sum_{Q\in C_2} \mathrm{ord}_Q(f)\left(\sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P)\right) \qquad = \sum_{P\in C_1} \mathrm{ord}_{\phi P}(f)e_\phi(P)(P) \\ &= \sum_{P\in C_1} \mathrm{ord}_P(\phi^* f)(P) \qquad\qquad \text{pela observação inicial,} \\ &= \mathrm{div}(\phi^* f).\end{aligned}$$

(c) Segue da definição.
(d) Veja [9, Capítulo 1, Proposição 22].
(e) Segue da proposição (2.7a).
(f) Segue do ítem (c) da proposição (2.7). □

Observação 2.3. Da proposição anterior, vemos que ϕ^* e ϕ_* levam divisores de grau 0 a divisores de grau 0, e divisores principais para divisores principais. Assim eles induzem os mapas

$$\phi^* : \mathrm{Pic}^0(C_2) \longrightarrow \mathrm{Pic}^0(C_1) \qquad \text{e} \qquad \phi_* : \mathrm{Pic}^0(C_1) \longrightarrow \mathrm{Pic}^0(C_2).$$

Em particular, se $f \in \bar{K}(C)$ fornece o mapa $f : C \to \mathbb{P}^1$, então

$$\deg \mathrm{div}(f) = \deg f^*((0) - (\infty)) = \deg f - \deg f = 0.$$

Isso fornece uma prova para a proposição (2.9b).

2.4 Diferenciais

Nesta seção discutiremos o espaço vetorial das formas diferenciais na curva. Este espaço vetorial serve para dois propósitos. Primeiro, ele nos fornece uma forma perfeita para a regra do cálculo de linearização. Segundo, ele nos dá um critério útil para determinar quando um mapa algébrico é separável.

Definição 2.10. Seja C uma curva. O espaço das formas diferenciais (meromórficas) em C, denotado por Ω_C, é o $\bar{K}$-espaço vetorial gerado pelos símbolos da forma dx para $x \in \bar{K}(C)$, tal que valem as relações:

Seja $\phi : C_1 \to C_2$ um mapa não constante entre curvas. O mapa de corpos de funções associado $\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ induz um mapa entre os diferenciais,

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}, \quad \phi^*\Big(\sum f_i dx_i\Big) = \sum (\phi^* f_i) d(\phi^* x_i).$$

Este mapa fornece um critério útil para determinar quando ϕ é separável.

Proposição 2.11. Seja C uma curva.
(a) Ω_C é $\bar{K}(C)$-espaço vetorial de dimensão 1.
(b) Seja $x \in \bar{K}(C)$. Então dx é uma $\bar{K}(C)$-base para Ω_C se, e somente se, $\bar{K}(C)/\bar{K}(x)$ é uma extensão separável finita.
(c) Seja $\phi : C_1 \to C_2$ um mapa não constante entre curvas. Então ϕ é separável se, e somente se, o mapa

$$\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}$$

é injetivo, ou equivalentemente, não nulo.

Prova. (a) Tome como referência [10, III §4, Teorema 3].
(b) Veja em [10, §4, Teorema 4].
(c) Usando os ítens (a) e (b), escolha $y \in \bar{K}(C_2)$ tal que $\Omega_{C_2} = \bar{K}(C_2)dy$ e tal que $\bar{K}(C_2)/\bar{K}(y)$ é extensão separável. Note que então $\phi^*\bar{K}(C_2)$ é separável sobre $\phi^*\bar{K}(y) = \bar{K}(\phi^* y)$. Agora

$$\begin{aligned}
\phi^* \text{ é injetivo} &\iff d(\phi^* y) \neq 0 \\
&\iff d(\phi^* y) \text{ é base para } \Omega_{C_1} \text{ (de (a))} \\
&\iff \bar{K}(C_1)/\bar{K}(\phi^* y) \text{ é separável (de (b))} \\
&\iff \bar{K}(C_1)/\phi^*\bar{K}(C_2) \text{ é separável,}
\end{aligned}$$

onde a última equivalência segue pois conhecemos que $\phi^*\bar{K}(C_2)/\bar{K}(\phi^* y)$ é separável. □

Proposição 2.12. Sejam C uma curva $P \in C$, e $t \in \bar{K}(C)$ um uniformizador em P.
(a) Para todo $\omega \in \Omega_C$ existe uma única função $g \in \bar{K}(C)$, que depende de ω e t, satisfazendo

$$\omega = gdt.$$

Denotamos g por ω/dt.
(b) Seja $f \in \bar{K}(C)$ regular em P. Então df/dt também é regular em P.
(c) Seja $\omega \in \Omega_C$ com $\omega \neq 0$. A quantidade

$$\mathrm{ord}_P(\omega/dt)$$

depende apenas de ω e P, independente da escolha do uniformizador t. Chamamos este valor de ordem de ω em P e o denotamos por $\mathrm{ord}_P(\omega)$.
(d) Seja $x,\ f \in \bar{K}(C)$ com $x(P) = 0$, e seja $p = \mathrm{char}K$. Então

$$\begin{aligned} &\mathrm{ord}_P(fdx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1 && \text{se } p = 0 \text{ ou } p \not| \mathrm{ord}_P(x), \\ &\mathrm{ord}_P(fdx) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(x), && \text{se } p > 0 \text{ e } p | \mathrm{ord}_P(x). \end{aligned}$$

(e) Seja $\omega \in \Omega_C$ com $\omega \neq 0$. Então

$$\mathrm{ord}_P(\omega) = 0 \quad \text{para quase todo } P \in C.$$

Prova. (a) Sabemos da proposição (2.4) que $\bar{K}(C)/\bar{K}(t)$ é extensão separável finita. Pela proposição (2.11b) anterior, dt é base para Ω_C. Dado $\omega \in \Omega_C$, pelo ítem (2.11a) anterior, existe um único $g \in \bar{K}(C)$ dependendo de ω e t tal que

$$\omega = gdt.$$

(b) Veja [2, IV.2.1].
(c) Seja t' outro uniformizador para P. Então do ítem (b) vemos que dt/dt' e dt'/dt são ambos regulares em P, assim $\mathrm{ord}_P(dt'/dt) = 0$. O resultado então vem do fato de que

$$\omega = gdt' = g(dt'/dt)dt.$$

(d) Escreva $x = ut^n$ com $n = \mathrm{ord}_P(x) \geq 1$, então $\mathrm{ord}_P(u) = 0$. Logo

$$dx = [nut^{n-1} + (du/dt)t^n]dt.$$

De (b) sabemos que du/dt é regular em P. Consequentemente se $n \neq 0$, então o

primeiro termo será dominante no sentido de dar a igualdade:

$$\mathrm{ord}_P(fdx) = \mathrm{ord}_P(fnut^{n-1}dt) = \mathrm{ord}_P(f) + n - 1.$$

Por outro lado, se $p > 0$ e $p|n$, então o primeiro termo se anula, e encontramos que

$$\mathrm{ord}_P(fdx) = \mathrm{ord}_P(f(du/dt)t^n dt) \geq \mathrm{ord}_P(f) + n.$$

(e) Escolha algum $x \in \bar{K}(C)$ tal que $\bar{K}(C)/\bar{K}(x)$ é separável e escreva $\omega = fdx$. De [2, IV.2.2a] o mapa $x : C \to \mathbb{P}^1$ ramifica em apenas um número finito de pontos de C. Consequentemente descartando um número finito de pontos, podemos restringir nossa atenção aos pontos $P \in C$ tais que

$$f(P) \neq 0, \quad f(P) \neq \infty, \quad x(P) \neq \infty,$$

e o mapa $x : C \to \mathbb{P}^1$ é não ramificado em P. As duas condições em x implicam que $x - x(P)$ é um uniformizador de P, então

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(fd(x - x(P))) = 0.$$

Consequentemente $\mathrm{ord}_P(\omega) = 0$ para quase todo P. □

Definição 2.11. Seja $\omega \in \Omega_C$. O divisor associado a ω é

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}(C).$$

O diferencial $\omega \in \Omega_C$ é regular (ou holomorfico) se

$$\mathrm{ord}_P(\omega) \geq 0 \quad \text{para todo } P \in C.$$

Ele é não nulo se

$$\mathrm{ord}_P(\omega) \leq 0 \quad \text{para todo } P \in C.$$

Observação 2.4. Se $\omega_1, \omega_2 \in \Omega_C$ são diferenciais não nulos, então a proposição anterior implica que existe uma função $f \in \bar{K}(C)^*$ tal que $\omega_1 = f\omega_2$. Assim

$$\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2),$$

o que mostra que a seguinte definição faz sentido.

Definição 2.12. A classe canônica de divisores de C é a imagem no $\mathrm{Pic}(C)$ de

$\mathrm{div}(\omega)$ para qualquer diferencial não nulo $\omega \in \Omega_C$. Qualquer divisor na classe de divisor é chamado divisor canônico.

Exemplo 2.9. Mostraremos a seguir que não existem diferenciais holomorficos em $\mathbb{P}^1$. Se t é função coordenada em $\mathbb{P}^1$, então

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

Para ver isso, note que para todo $\alpha \in \bar{K}$, a função $t - \alpha$ é um uniformizador em α, assim

$$\mathrm{ord}_\alpha(dt) = \mathrm{ord}_\alpha(d(t-\alpha)) = 0.$$

Entretanto, em $\infty \in \mathbb{P}^1$ precisamos usar a função tal que $1/t$ é seu uniformizador, então

$$\mathrm{ord}_\infty(dt) = \mathrm{ord}_\infty\Big(- t^2 d\Big(\frac{1}{t}\Big)\Big) = -2.$$

Assim dt não é holomórfico. Agora para qualquer diferencial não nulo $\omega \in \Omega_{\mathbb{P}^1}$, podemos usar a proposição anterior para calcular

$$\deg \mathrm{div}(\omega) = \deg \mathrm{div}(dt) = -2$$

assim ω não pode ser holomorfico.

Exemplo 2.10. Seja C a curva dada por

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3),$$

onde continuamos com a notação da proposição anterior. Então

$$\mathrm{div}(dx) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

(Note que $dx = d(x - e_i) = -x^2 d(1/x)$). Assim vemos que

$$\mathrm{div}(dx/y) = 0.$$

Consequentemente o diferencial dx/y é holomórfico e não nulo.

2.5 O teorema de Riemann-Roch

Seja C uma curva. Colocamos uma ordem parcial no $\mathrm{Div}(C)$ da seguinte maneira.

Definição 2.13. Um divisor $D = \sum n_P(P)$ é positivo (ou efetivo), denotado por

$$D \geq 0,$$

se $n_P \geq 0$ para todo $P \in C$. Similarmente, para quaisquer dois divisores $D_1,\ D_2 \in \mathrm{Div}(C)$, escrevemos

$$D_1 \geq D_2$$

para indicar que $D_1 - D_2$ é positivo.

Exemplo 2.11. Seja $f \in \bar{K}(C)^*$ uma função regular exceto no ponto $P \in C$, e suponha que tem polo de ordem no máximo n em P. Este requerimento de f pode ser resumido pela desigualdade

$$\mathrm{div}(f) \geq -n(P).$$

Similarmente,

$$\mathrm{div}(f) \geq (Q) - n(P)$$

diz que f tem um zero em Q. Assim desigualdades entre divisores são uma ferramente útil para descrever pólos ou zeros de funções.

Definição 2.14. Seja $D \in \mathrm{Div}(C)$. Associamos a D o conjunto de funções

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

O conjunto $\mathcal{L}(D)$ é $\bar{K}$-espaço vetorial de dimensão finita como veremos a seguir, onde a dimensão será denotada como:

$$\ell(D) = \dim_{\bar{K}} \mathcal{L}(D).$$

Proposição 2.13. Seja $D \in \mathrm{Div}(C)$.
(a) Se $\deg D < 0$, então

$$\mathcal{L} = \{0\} \quad \text{e} \quad \ell(D) = 0.$$

(b) $\mathcal{L}$ é um $\bar{K}$-espaço vetorial de dimensão finita.
(c) Se $D' \in \mathrm{Div}(C)$ é linearmente equivalente a D, então

$$\mathcal{L}(D) \cong \mathcal{L}(D'), \quad \text{e assim} \quad \ell(D) = \ell(D').$$

Prova. (a) Seja $f \in \mathcal{L}(D)$ com $f \neq 0$. Então da proposição (2.9b) temos que

$$0 = \deg \mathrm{div}(f) \geq \deg(-D) = -\deg D,$$

assim $\deg D \geq 0$.
(b) Veja [2, II.5.19].

(c) Se $D = D' + \mathrm{div}(g)$, então o mapa

$$\mathcal{L}(D) \longrightarrow \mathcal{L}(D'), \quad f \longmapsto fg$$

é um isomorfismo □

Exemplo 2.12. Seja $K_C \in \mathrm{Div}(C)$ um divisor canônico de C, escreva

$$K_C = \mathrm{div}(\omega).$$

Então cada função $f \in \mathcal{L}(K_C)$ tem a propriedade que

$$\mathrm{div}(f) \geq -\mathrm{div}(\omega), \quad \text{então} \quad \mathrm{div}(f\omega) \geq 0.$$

Em outras palavras, $f\omega$ é holomórfico. Reciprocamente, se o diferencial $f\omega$ é holomórfico, então $f \in \mathcal{L}(K_C)$. Como todo diferencial em C tem a forma $f\omega$ para algum f, temos estabelecido um isomorfismo de $\bar{K}$-espaços vetoriais,

$$\mathcal{L}(K_C) \cong \{\omega \in \Omega_C : \omega \text{ é holomórfico } \}.$$

Como observação, a dimensão $\ell(K_C)$ desses espaços é um importante invariante da curva C.

Estamos prontos para estabelecer o resultado fundamental da geometria algébrica de curvas. Sua importância está no fato de termos a habilidade de dizer se existem funções em C tendo zeros e pólos pré-estabelecidos .

Teorema 2.3. (Riemann-Roch) Seja C uma curva suave e seja K_C um divisor canônico em C. Então existe um inteiro $g \geq 0$, chamado de gênero de C, tal que todo divisor $D \in \mathrm{Div}(C)$,

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

Prova. Não faremos a prova aqui, mas poderemos vê-la em [3, Capítulo 1]. □

Corolário 2.4. (a) $\ell(K_C) = g$.
(b) $\deg K_C = 2g - 2$.
(c) Se $\deg D > 2g - 2$, então

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

Prova. (a) Usando Riemman-Roch (2.3), com $D = 0$. Notamos que $\mathcal{L}(0) = \bar{K}$ da

proposição (2.3), e assim $\ell(0) = 1$.
(b) Use o ítem (a) e Riemman-Roch (2.3) com $D = K_C$.
(c) De (b) temos $\deg(K_C - D) < 0$. Agora basta usar o teorema (2.3) e a proposição (2.13.a), obtendo o resultado. □

Exemplo 2.13. Seja $C = \mathbb{P}^1$. O exemplo (2.9) nega a existência de diferenciais holomórficos em C, então usando a identificação vista no exemplo (2.12), vemos que $\ell(K_C) = 0$. Pelo corolário (2.4), $\mathbb{P}^1$ tem gênero 0, e o teorema de Riemann-Roch fica

$$\ell(D) - \ell(-2(\infty) - D) = \deg D + 1.$$

Em particular, se $\deg D \geq -1$, então

$$\ell(D) = \deg D + 1.$$

Exemplo 2.14. Seja C a curva

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3),$$

onde continuamos com a notação dos exemplos (2.7) e (2.10). Vemos no exemplo (2.10) que

$$\operatorname{div}(dx/y) = 0,$$

assim a classe canônica em C é trivial, isto é, podemos tomar $K_C = 0$. Consequentemente usando o corolário (2.4a) encontramos

$$g = \ell(K_C) = \ell(0) = 1,$$

assim C tem gênero um. Então o teorema de Riemann-Roch diz que

$$\ell(D) = \deg D \quad \text{dado que } \deg D \geq 1.$$

Consideramos os seguintes casos especiais.

(i) Seja $P \in C$. Então $\ell((P)) = 1$. Mas $\mathcal{L}((P))$ contém uma função constante, que não tem pólos assim isso mostra que não existem funções em C tendo um único pólo simples.
(ii) Relembremos que P_∞ é o ponto no infinito em C. Então $\ell(2(P_\infty)) = 2$, e $\{1, x\}$ fornecem uma base para $\mathcal{L}(2(P_\infty))$.
(iii) Similarmente, o conjunto $\{1, x, y\}$ é uma base para $\mathcal{L}(3(P_\infty))$, e $\{1, x, y, x^2\}$ uma base para $\mathcal{L}(4(P_\infty))$.

(iv) Agora observamos que as sete funções $1, x, y, x^2, xy, x^3, y^2$ estão todas em $\mathcal{L}(6(P_\infty))$, mas $\ell(6(P_\infty)) = 6$, assim estas funções são necessariamente $\bar{K}$-linearmente dependentes. A equação $y^2 = (x - e_1)(x - e_2)(x - e_3)$ usada para definir C da a equação dependência linear entre eles.

O próximo resultado nos diz que se C e D são definidos sobre K, então são em $\mathcal{L}(D)$.

Proposição 2.14. Seja C/K uma curva suave e seja $D \in \mathrm{Div}_K(C)$. Então $\mathcal{L}(D)$ tem base formada de funções em $K(C)$.

Prova. Como D é definido sobre K, temos

$$f^\sigma \in \mathcal{L}(D^\sigma) = \mathcal{L}(D) \quad \text{para todo } f \in \mathcal{L}(D) \text{ e todo } \sigma \in G_{\bar{K}/K}.$$

Assim $G_{\bar{K}/K}$ age em $\mathcal{L}(D)$, e a conclusão segue do seguinte lema:

Lema 2.1. Seja V um $\bar{K}-$espaço vetorial, e assuma que $G_{\bar{K}/K}$ age continuamente em V de maneira compatível com sua ação em $\bar{K}$. Seja

$$V_K = V^{G_{\bar{K}/K}} = \{\mathbf{v} \in V : \mathbf{v}^\sigma = \mathbf{v} \text{ para todo } \sigma \in G_{\bar{K}/K}\}.$$

Então

$$V \cong \bar{K} \otimes_K V_K,$$

isto é, o espaço vetorial V tem base nos vetores $G_{\bar{K}/K}$-invariantes.

Prova. Sabemos que V_K é um K-espaço vetorial, assim é suficiente demostrar que todo $\mathbf{v} \in V$ é uma $\bar{K}$-combinação linear de vetores em V_K. Seja $\mathbf{v} \in V$ e L/K extensões finitas de Galois tal que $\mathbf{v}$ é fixado por $G_{\bar{K}/L}$. (Assumir que $G_{\bar{K}/K}$ age continuamente em V significa que o subgrupo $\{\sigma \in G_{\bar{K}/K} : \mathbf{v}^\sigma = \mathbf{v}\}$ tem índice finito em K, assim podemos tomar L como fecho de Galois deste corpo fixado.)
Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base para L/K, e seja $\{\sigma_1, \ldots, \sigma_n\} = G_{L/K}$. Para cada $1 \leq i \leq n$, consideramos o vetor

$$\mathbf{w}_i = \sum_{j=1}^{n} (\alpha_i \mathbf{v})^{\sigma_j} = \mathrm{Traço}_{L/K}(\alpha_i \mathbf{v}).$$

O elemento $\mathbf{w}_i \in G_{\bar{K}/K}$ é um invariante, assim $\mathbf{w}_i \in V_K$. Um resultado básico da teoria dos corpos, [4, III, Proposição 9], diz que a matriz $(\alpha_i^{\sigma_j})_{1 \leq i,j \leq n}$ é não singular, assim cada $\mathbf{v}^{\sigma_j}$, e em particular $\mathbf{v}$, é uma combinação L-linear dos $\mathbf{w}_i$'s. $\square$

Concluímos esta seção com a relação clássica conectando gêneros de curvas com mapas não constantes.

Teorema 2.4. (Hurwitz) Seja $\phi : C_1 \to C_2$ um mapa separável não constante de curvas suaves de gêneros g_1 e g_2, respectivamente. Então

$$2g_1 - 2 \geq (\deg \phi)(2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1).$$

A igualdade é válida se, e somente se, uma das seguintes condições é verdadeira:
(i) $\mathrm{char}(K) = 0$.
(ii) $\mathrm{char}(K) = p > 0$ e p não divide $e_\phi(P)$ para todo $P \in C_1$.

Prova. Seja $\omega \in \Omega_C$ um diferencial não nulo, seja $P \in C_1$, e seja $Q = \phi(P)$. Como ϕ é separável, a proposição (2.11) nos diz que $\phi^*\omega \neq 0$. Precisamos relacionar os valores de $\mathrm{ord}_P(\phi^*\omega)$ e $\mathrm{ord}_Q(\omega)$. Escrevemos $\omega = f dt$ com $t \in \bar{K}(C_2)$ um uniformizador de Q. Fazendo $e = e_\phi(P)$, temos que $\phi^* t = u s^e$, onde s é um uniformizador de P e $u(P) \neq 0, \infty$. Consequentemente

$$\phi^*\omega = (\phi^* f) d(\phi^* t) = (\phi^* f) d(u s^e) = (\phi^* f)[e u s^{e-1} + (du/ds) s^e] ds.$$

Da proposição (2.12) temos $\mathrm{ord}_P(du/ds) \geq 0$, assim temos que

$$\mathrm{ord}_P(\phi^*\omega) \geq \mathrm{ord}_P(\phi^* f) + e - 1,$$

com a igualdade válida se, e somente se, $e \neq 0$ em K. Ainda,

$$\mathrm{ord}_P(\phi^* f) = e_\phi(P)\mathrm{ord}_Q(f) = e_\phi(P)\mathrm{ord}_Q(\omega).$$

Consequentemente fazendo sobre todo $P \in C_1$ fica

$$\begin{aligned} \deg \mathrm{div}(\phi^*\omega) &\geq \sum_{P \in C_1} [e_{\phi(P)}\mathrm{ord}_{\phi(P)}(\omega) + e_\phi(P) - 1] \\ &= \sum_{Q \in C_2} \sum_{P \in \phi^{-1}(Q)} e_\phi(P)\mathrm{ord}_Q(\omega) + \sum_{P \in C_1} (e_\phi(P) - 1) \\ &= (\deg \phi)(\deg \mathrm{div}(\omega)) + \sum_{P \in C_1} (e_\phi(P) - 1), \end{aligned}$$

onde a última igualdade segue da proposição (2.7a). A fórmula de Hurwitz é uma consequência do corolário (2.4b). □

Capítulo 3

A Geometria das Curvas Elípticas

Curvas elípticas, nosso principal objeto de estudo, são curvas de gênero um, tendo um específico ponto base. Na maior parte desse estudo, estaremos interessados em estudar as propriedades aritméticas dessas curvas. Em outras palavras, estamos interessados em analizar seus pontos definindo-os sobre um corpo de interesse aritmético, tais como os corpos finitos, corpos (p-ádicos) locais, e corpos (de números) globais. Entretanto, antes de assim fazermos estamos bem advertidos que o estudo das propriedades dessas curvas na situação simples de um corpo algebricamente fechado, isto é, no estudo de sua geometria. Isso reflete o princípio geral da Geometria Diofantina, o qual se atenta em estudar qualquer problema significante, em que é essencial ter um desenvolvimento através da geometria antes de ter algum progresso na teoria numérica. O propósito deste capítulo é fazer um estudo intensivo da geometria das curvas elípticas sobre corpos algebricamente fechados.

Começamos nossas primeiras duas seções descrevendo as curvas elípticas por meio de equações de Weiertrass. Usando essas equações explícitas, mostramos que o conjunto dos pontos de uma curva elíptica forma um grupo abeliano, entre outras coisas, e que a lei de grupo é dada por funções racionais. Na seção 3, usamos o teorema de Riemann-Roch para estudar curvas elípticas e mostrar que toda curva elíptica tem equação de Weiertrass, assim o resultado das primeiras duas seções podem ser aplicados.

3.1 Equação de Weierstrass

O objetivo desta seção é mostrar que em geral para estudar as curvas elípticas podemos escrevê-la como o local geométrico em $\mathbb{P}^2$ descrito por equações cúbicas, onde existe o chamado ponto base, como sendo a reta no infinito. A forma geral da

equação cúbica é:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

O ponto base é $\mathcal{O} = [0, 1, 0]$, e $a_1, \ldots, a_6 \in \bar{K}$.

Para facilitar a notação, escreveremos a equação de Weiertrass usando coordenadas não homogêneas $x = X/Z$ e $y = Y/Z$,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

sempre lembrando do ponto no infinito $\mathcal{O} = [0, 1, 0]$. Como anteriormente, se $a_1, \ldots, a_6 \in K$, então E é dito ser definido sobre K.

Se $\mathrm{char}(\bar{K}) \neq 2$, então podemos simplificar a equação completando quadrados. Assim a substituição

$$y \longmapsto \frac{1}{2}(y - a_1x - a_3)$$

fornece uma equação da forma

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

onde

$$b_2 = a_1^2 + 4a_4, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

Definimos os seguintes valores

$$\begin{aligned}
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= c_4^3/\Delta,
\end{aligned}$$

e o diferencial

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

Podemos verificar que

$$4b_8 = b_2b_6 - b_4^2 \quad \text{e} \quad 1728\Delta = c_4^3 - c_6^2.$$

Se ainda $\text{char}(\bar{K}) \neq 2, 3$, então a substituição

$$(x, y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

elimina o termo x^2, tornando a equação de Weierstrass mais simples

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Definição 3.1. O valor Δ é chamado o discriminante da equação de Weierstrass, o valor j é chamado o j-invariante da curva elíptica, e ω é o invariante diferencial associado a equação de Weierstrass.

Exemplo 3.1. O local geométrico real da equação de Weierstrass é observado nas seguintes figuras:

Cúspide: uma direção tangente. Nó: duas direções tangentes.

Figura 3.1. Cúspide e Nó.

Tendo esses exemplos em mente, consideramos a seguinte situação. Seja $P = (x_0, y_0)$ um ponto singular da curva

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Então do exemplo (1.5),

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Segue que existem $\alpha, \beta \in \bar{K}$ tais que a expansão em série de Taylor de $f(x, y)$ em P tem a forma

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3.$$

Definição 3.2. Com a notação anterior, o ponto singular P é um nó se $\alpha \neq \beta$.

Neste caso, as retas

$$y - y_0 = \alpha(x - x_0) \quad \text{e} \quad y - y_0 = \beta(x - x_0)$$

são as retas tangentes em P. Se $\alpha = \beta$, então diremos que P é uma cúspide, caso em que a reta tangente em P é dada por

$$y - y_0 = \alpha(x - x_0).$$

Precisamos responder a questão: O que faz com que uma equação de Weierstrass represente uma única curva elíptica? Considerando a reta no infinito como $Z = 0$ em $\mathbb{P}^2$, é necessário que ela intersecte a curva E apenas no ponto $[0, 1, 0]$. Veremos que a única mudança de variáveis que mantém fixo $[0, 1, 0]$ e que preserva a forma geral da equação de Weierstrass é

$$x = u^2x' + r \quad \text{e} \quad y = u^3y' + u^2sx' + t,$$

onde $u, r, s, t \in \bar{K}$ e $u \neq 0$. A lista a seguir resume o resultado dos coeficientes e elementos que se obtém fazendo esta substituição.

ua_1'	$=$	$a_1 + 2s$
u^2a_2'	$=$	$a_2 - sa_1 + 3r - s^2$
u^3a_3'	$=$	$a_3 + ra_1 + 2t$
u^4a_4'	$=$	$a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
u^6a_6'	$=$	$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$
u^2b_2'	$=$	$b_2 + 12r$
u^4b_4'	$=$	$b_4 + rb_2 + 6r^2$
u^6b_6'	$=$	$b_6 + 2rb_4 + r^2b_2 + 4r^3$
u^8b_8'	$=$	$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$
u^4c_4'	$=$	c_4
u^6c_6'	$=$	c_6
$u^{12}\Delta'$	$=$	Δ
j'	$=$	j
$u^{-1}\omega'$	$=$	ω

Tabela 3.1. Fórmula de mudança de variáveis para equação de Weierstrass.

Pode-se notar que o elemento j não tem variação, o que motiva o seu nome. É um invariante da classe de isomorfismos da curva que o define, e não depende da escolha da equação em particular. Para corpos algebricamente fechados, a recíproca é verdadeira, como veremos mais tarde.

Observação 3.1. Como vimos, se a característica de K é diferente de 2 e 3, então qualquer curva sobre K tem uma equação de Weierstrass mais simples que a forma geral. Assim qualquer prova onde envolva muitas manipulações algébricas se torna simples nesses casos, onde K é restrito. Por outro lado, mesmo se o caso for em que $\text{char}(K) = 0$, ou seja, $K \supseteq \mathbb{Q}$, uma importante ferramenta é o processo de redução dos coeficientes de uma equação módulo p para vários primos p, incluindo os casos $p = 2$ e $p = 3$. Assim mesmo para $K \supseteq \mathbb{Q}$, é importante entender curvas elípticas em todas características. Consequentemente, faremos o seguinte a partir daqui: Todo teorema será iniciado com a forma geral da equação de Weierstrass, mas a fim de fazer com que a demonstração se torna reduzida, assumiremos a característica de K como sendo diferente de 2 ou 3 fazendo a prova nestes casos. Faremos a demonstração geral posteriormente.

Considerando a característica de K diferente de 2 ou 3, a curva elíptica terá equação de Weierstrass da forma

$$E : y^2 = x^3 + Ax + B,$$

onde temos os valores

$$\Delta = -16(4A^3 + 27B^2) \quad \text{e} \quad j = -1728\frac{(4A)^3}{\Delta}.$$

A única mudança de variáveis que preserva esta forma é

$$x = u^2x' \quad \text{e} \quad y = u^3y' \quad \text{para algum } u \in \bar{K}^*,$$

e assim,

$$u^4A' = A, \quad u^6B' = B, \quad u^{12}\Delta' = \Delta.$$

A seguinte proposição descreve algumas propriedades geométricas por meio de valores definidos no início da seção.

Proposição 3.1. (a) A curva dada pela equação de Weierstrass satisfaz:
(i) É não singular se, e somente se, $\Delta \neq 0$.
(ii) Tem nó se, e somente se, $\Delta = 0$ e $c_4 \neq 0$.
(iii) Tem cúspide se, e somente se, $\Delta = c_4 = 0$.

Nos casos (ii) e (iii), existe um único ponto singular.
(b) Duas curvas elípticas são isomorfas sobre $\bar{K}$ se, e somente se, possuem o mesmo j-invariante.
(c) Seja $j_0 \in \bar{K}$. Existe uma curva elíptica definida sobre $K(j_0)$ cujo j-invariante é

igual a j_0.

Prova. Seja E curva dada pela equação de Weierstrass

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Mostraremos que o ponto no infinito não é singular. Assim, olhando para a curva com coordenadas homogêneas,

$$\begin{aligned} F(X, Y, Z) &= Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \\ &= 0 \end{aligned}$$

com o ponto $\mathcal{O} = [0, 1, 0]$. Como

$$\frac{\partial F}{\partial Z}(\mathcal{O}) = 1 \neq 0,$$

vemos que $\mathcal{O}$ é não singular em E.

A seguir suponha que E é não singular, digamos em $P_0 = (x_0, y_0)$. Mudando as coordenadas como

$$x = x' + x_0 \quad y = y' + y_0$$

deixamos Δ e c_4 invariantes, assim sem perder generalidade podemos assumir que E é singular em $(0, 0)$. Então

$$a_6 = f(0, 0) = 0, \quad a_4 = \frac{\partial f}{\partial x}(0, 0) = 0, \quad a_3 = \frac{\partial f}{\partial y}(0, 0) = 0,$$

e portanto a equação para E tem a forma

$$E : f(x, y) = y^2 + a_1xy - a_2x^2 - x^3 = 0,$$

onde

$$c_4 = (a_1^2 + 4a_2)^2 \quad \text{e} \quad \Delta = 0.$$

Por definição, E tem nó, respectivamente cúspide, em $(0, 0)$ se a forma quadrática $y^2 + a_1xy - a_2x^2$ tem fatores distintos, respectivamente iguais, o que ocorre se, e somente se, o discriminante da forma quadrática satisfaz

$$a_1^2 + 4a_2 \neq 0 \quad \text{(respectivamente } a_1^2 + 4a_2 = 0).$$

Isso mostra que ter cúspide ou nó implicam conforme o enunciado.

Para completar a prova dos ítens (i) até (iii), resta mostrar que se E é não

singular, então $\Delta \neq 0$. Para simplificar os cálculos, consideramos $\text{char}(K) \neq 2$ e consideramos a equação de Weierstrass da forma

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

A curva E é singular se, e somente se, existe um ponto $(x_0, y_0) \in E$ tal que

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0.$$

Em outras palavras, pontos singulares são exatamente os pontos da forma $(x_0, 0)$ tais que x_0 é a raíz dupla do polinômio cúbico $4x^3 + b_2x^2 + 2b_4x + b_6$. Esse polinômio tem raíz dupla se, e somente se, seu discriminante, que é igual a 16Δ, se anula. Isso completa a prova dos ítens em questão. Além disso, como o polinômio cúbico não tem duas raízes duplas, E tem no máximo um ponto singular.
(b) Se duas curvas elípticas são isomorfas, então sabemos que têm o mesmo j-invariante. Para a recíproca, consideremos que $\text{char}(K) \geq 5$ (veja como referência a observação 3.1). Seja E e E' curvas elípticas com o mesmo j-invariante, com as equações

$$E : y^2 = x^3 + Ax + B,$$
$$E' : y'^2 = x'^3 + A'x' + B'.$$

Suponha que $j(E) = j(E')$, o que significa que

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2},$$

onde

$$A^3B'^2 = A'^3B^2.$$

Olhamos agora para o isomorfismo da forma $(x, y) = (u^2x', u^3y')$ e consideramos três casos:
Caso 1: $A = 0$ ($j = 0$). Então $B \neq 0$, pois $\Delta \neq 0$, assim $A' = 0$, e obtemos um isomorfismo usando $u = (B/B')^{1/6}$.
Caso 2: $B = 0$ ($j = 1728$). Então $A \neq 0$, e $B' = 0$, temos que $u = (A/A')^{1/4}$.
Caso 3: $AB \neq 0$ ($j \neq 0, 1728$). Então $A'B' \neq 0$, pois se algum deles for 0, então os dois devem ser 0, o que contradiz $\Delta' \neq 0$. Tomando $u = (A/A')^{1/4} = (B/B')^{1/6}$ dá o isomorfismo desejado.
(c) Considere $j_0 \neq 0, 1728$ e considere a curva

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

Temos que

$$\Delta = \frac{j_0^3}{(j_0 - 1728)^3} \quad \text{e} \quad j = j_0.$$

Isso dá a curva desejada, em qualquer característica, visto que $j_0 \neq 0, 1728$.
Para completar a prova, usamos as duas curvas

$$\begin{aligned} E : y^2 + y = x^3, \qquad & \Delta = -27, \quad j = 0, \\ E : y^2 = x^3 + x, \qquad & \Delta = -64, \quad j = 1728. \end{aligned}$$

Note que para característica 2 ou 3 temos que $1728 = 0$, assim mesmo nesse caso uma das duas curvas será não singular e preencherá o valor que falta para j. □

Observe que os ítens (b) e (c) da proposição anterior garantem que a aplicação $\mathcal{C} \to K$, onde $\mathcal{C}$ é o conjunto das classes de isomorfismos da curva elíptica definida por $[C] \mapsto j(C)$, sendo uma bijeção.

Proposição 3.2. Seja E uma curva elíptica. Então o invariante diferencial ω associado a equação de Weierstrass para E é holomórfica e não nula, ou seja, $\mathrm{div}(\omega) = 0$.

Prova. Seja $P = (x_0, y_0) \in E$ e

$$E : F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

assim,

$$\omega = \frac{d(x - x_0)}{F_y(x, y)} = -\frac{d(y - y_0)}{F_x(x, y)}.$$

Assim P não é polo de ω, pois senão teríamos $F_y(P) = F_x(P) = 0$, o que faria com que P fosse ponto singular de E. O mapa

$$E \longrightarrow \mathbb{P}^1, \qquad [x, y, 1] \longmapsto [x, 1],$$

é de grau 2, assim $\mathrm{ord}_P(x - x_0) \leq 2$, e teremos a igualdade $\mathrm{ord}_P(x - x_0) = 2$ se, e somente se, o polinômio quadrático $F(x_0, y)$ tem raíz dupla. Em outras palavras, ou $\mathrm{ord}_P(x - x_0) = 1$, ou $\mathrm{ord}_P(x - x_0) = 2$ e $F_y(x_0, y_0)$. Assim em ambos os casos, podemos usar a proposição (2.12) para calcular

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(x - x_0) - \mathrm{ord}_P(F_y) - 1 = 0.$$

Isso mostra que ω não tem polos ou zeros da forma (x_0, y_0), então sobra checar o que acontece com $\mathcal{O}$.

Seja t um uniformizador para $\mathcal{O}$. Como $\mathrm{ord}_{\mathcal{O}}(x) = -2$ e $\mathrm{ord}_{\mathcal{O}}(y) = -3$, vemos que $x = t^{-2}f$ e $y = t^{-3}g$ para funções f e g satisfazendo $f(\mathcal{O}) \neq 0, \infty$ e $g(\mathcal{O}) \neq 0, \infty$. Agora

$$\omega = \frac{dx}{F_y(x,y)} = \frac{-2t^{-3}f + t^{-2}f'}{2t^{-3}g + a_1t^{-2}f + a_3}dt = \frac{-2f + tf'}{2g + a_1tf + a_3t^3}dt,$$

onde $f' = df/dt$, conforme a proposição (2.12). Em particular, o ítem (2.12b) nos mostra que f' é regular em $\mathcal{O}$. Consequentemente, considerando $\mathrm{char}(K) \neq 2$, a função

$$\frac{-2f + tf'}{2g + a_1tf + a_3t^3}$$

é regular e não nula em $\mathcal{O}$, e assim,

$$\mathrm{ord}_{\mathcal{O}}(\omega) = 0.$$

Por outro lado, se $\mathrm{char}(K) = 2$, então escrevendo $\omega = dy/F_x(x,y)$ obtemos:

$$\begin{aligned}\omega = \frac{dy}{F_x(x,y)} &= \frac{d(t^{-3}g)}{-3x^2 - 2a_2x + a_1y - a_4} \\ &= \frac{-3t^{-4}g + t^{-3}g'}{-3t^{-4}f^2 - 2a_2t^{-2}f + a_1t^{-3}g - a_4}dt \\ &= \frac{-3g + tg'}{-3f^2 - 2a_2t^2f + a_1tg - a_4t^4}dt.\end{aligned}$$

Vemos que essa função é regular e não nula em $\mathcal{O}$. Portanto segue o resultado. □

Vejamos agora o que ocorre com uma curva quando a equação de Weierstrass é singular.

Proposição 3.3. Se a curva E dada por uma equação de Weierstrass é singular, então existe um mapa racional $\phi : E \to \mathbb{P}^1$ de grau um, ou seja, a curva E é birracional em $\mathbb{P}^1$.
(Note que, como E é singular, não podemos usar o corolário (2.1) para concluir que $E \cong \mathbb{P}^1$.)

Prova. Fazendo uma mudança linear de coordenadas, podemos assumir que o ponto singular é $(x,y) = (0,0)$. Calculando as derivadas parciais, vemos que a equação de Weierstrass tem a forma

$$E : y^2 + a_1xy = x^3 + a_2x^2.$$

Então o mapa racional

$$E \longrightarrow \mathbb{P}^1, \qquad (x,y) \to [x,y],$$

tem grau um, pois tem um inverso dado por tem inverso dado por

$$\mathbb{P}^1 \longrightarrow E, \quad [1,t] \longmapsto (t^2 + a_1 t - a_2, t^3 + a_1 t^2 - a_2 t).$$

(Para encontrar essa fórmula, seja $t = y/x$ e note que dividindo a equação de Weierstrass de E por x^2 ficamos com $t^2 + a_1 t = x + a_2$. Isso mostra que x e $y = xt$ estão em $\bar{K}(t)$.) □

3.2 A forma de Legendre

Para alguns casos podemos usar outra forma para a equação de Weierstrass, onde ela se mostra mais conveniente.

Definição 3.3. Uma equação de Weierstrass está na *forma de Legendre* se pudermos escrevê-la como

$$y^2 = x(x-1)(x-\lambda).$$

Proposição 3.4. Considere $\mathrm{char}(K) \neq 2$.
(a) Toda curva elíptica é isomorfa (sobre $\bar{K}$) a uma curva elíptica na forma de Legendre

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

para algum $\lambda \in \bar{K}$ com $\lambda \neq 0, 1$.
(b) O j-invariante de E_λ é

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}.$$

(c) O mapa

$$\bar{K} - \{0,1\} \longrightarrow \bar{K}, \quad \lambda \longmapsto j(E_\lambda),$$

é sobrejetor e seis para um, exceto nos casos $j = 0$ e $j = 1728$, onde é dois para um e três para um, respectivamente (a menos que $\mathrm{char}(K) = 3$, onde temos bijeção para os casos $j = 0$ e $j = 1728$.)

Prova. (a) Como $\mathrm{char}(K) \neq 2$, sabemos que E tem equação de Weierstrass da forma

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6.$$

Substituindo (x, y) por $(x, 2y)$ e fatorando a parte cúbica ficamos com a equação

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

para algum $e_1, e_2, e_3 \in \bar{K}$. Além disso,

$$\Delta = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \neq 0,$$

vemos que os e_is são distintos. Agora, substituindo

$$x = (e_2 - e_1)x' + e_1, \quad y = (e_2 - e_1)^{3/2}y'$$

temos a forma da equação de Legendre com

$$\lambda = \frac{e_3 - e_1}{e_2 - e_1} \in \bar{K}, \quad \lambda \neq 0, 1.$$

(b) Pela definição,

$$\begin{aligned} j &= \frac{c_4^3}{\Delta} \\ &= \frac{2^{12}(\lambda^2 - \lambda + 1)^3}{\Delta} \\ &= \frac{2^{12}(\lambda^2 - \lambda + 1)^3}{2^4(0-1)^2(0-\lambda)^2(1-\lambda)^2} \\ &= 2^8.\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2.(\lambda - 1)^2} \end{aligned}$$

como queríamos.
(c) Usamos o fato de que um j-invariante classifica uma curva elíptica, a menos de isomorfismo, conforme a proposição (3.1b). Assim, suponha $j(E_\lambda) = j(E_\mu)$. Então $E_\lambda \cong E_\mu$, logo suas equações de Weierstrass na forma de Legendre são relacionadas pela mudança de coordenadas

$$x = u^2x' + r \quad y = u^3y'.$$

Igualando temos

$$x(x-1)(x-\mu) = \left(x + \frac{r}{u^2}\right)\left(x + \frac{r-1}{u^2}\right)\left(x + \frac{r-\lambda}{u^2}\right),$$

existem seis maneiras de relacionarmos os termos uns aos outros, resultando nas seguintes seis possibilidades

$$\mu \in \left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\right\}.$$

Então $\lambda \to j(E_\lambda)$ é exatamente uma correspondência seis a seis, a menos que dois

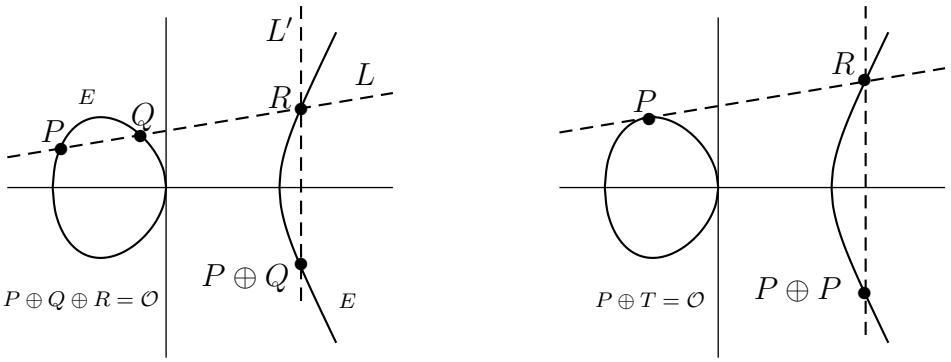
dos valores para μ coincidirem. Igualando os valores em pares vemos que isso ocorre apenas quando $\lambda = -1$ e $\lambda^2 - \lambda + 1 = 0$, para cada conjunto temos respectivamente três e dois elementos. Esses valores para j correspondem respectivamente a $j = 1728$ e $j = 0$. □

3.3 A Lei de Grupo

Seja E uma curva elíptica dada pela equação de Weierstrass. Assim $E \subset \mathbb{P}^2$ consiste dos pontos $P = (x, y)$ satisfazendo a equação de Weierstrass, junto com o ponto no infinito $\mathcal{O} = [0, 1, 0]$. Seja $L \subset \mathbb{P}^2$ uma reta. Então, como a equação tem grau três, a reta L intersecta E em três pontos, digamos P, Q, R. Se L é tangente a E, então P, Q, R não são necessariamente distintos. Tomando $L \cap E$ com multiplicidades temos três pontos, conforme o teorema de Bézout [2, I.7.8].

Definiremos a lei de adição $\oplus$ em E conforme a seguinte definição:

Definição 3.4. Sejam $P, Q \in E$ e L a reta que passa por P e Q (se esses pontos são iguais, a reta L será tangente a E em P), e R o terceiro ponto de interseção entre L e E. Seja L' a reta entre R e $\mathcal{O}$. Então L' intersecta E em R, $\mathcal{O}$, e em um terceiro ponto. Denotamos este terceiro ponto por $P \oplus Q$.



Adição de pontos distintos

Adição de um ponto a ele mesmo

Figura 3.2. Lei de composição.

Proposição 3.5. A adição tem as seguintes propriedades:
(a) Se a reta L intersecta E nos pontos P, Q, R, então

$$(P \oplus Q) \oplus R = \mathcal{O}.$$

(b) $P \oplus \mathcal{O} = P$ para todo $P \in E$.
(c) $P \oplus Q = Q \oplus P$ para todo $P, Q \in E$.
(d) Seja $P \in E$. Então existe um ponto de E, denotado por $\ominus P$, satisfazendo

$$P \oplus (\ominus P) = \mathcal{O}.$$

(e) Seja $P, Q, R \in E$. Então

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

Em outras palavras, a adição acima torna E um grupo abeliano com o elemento identidade $\mathcal{O}$. Além disso:
(f) Suponha que E é definido sobre K. Então

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

é subgrupo de E.

Prova. (a) Seja L a reta que passa por P e Q em E, com R o terceiro ponto de interseção de $L \cap E$. A, a reta L' definida por $\mathcal{O}$ e R tem como terceiro ponto $P \oplus Q$. Agora, reta que passa por $P \oplus Q$ e R é L', tendo $\mathcal{O}$ como terceiro ponto de interseção a E. Como $\mathcal{O}$ tem multiplicidade 3 na reta tangente a E, segue o resultado.
(b) Tomando a reta que passa por P e $\mathcal{O}$ obtemos o terceiro ponto de interseção R com a curva elíptica. Então tomamos a reta que passa por R e $\mathcal{O}$, que é a reta inicial, intersectando E no terceiro ponto, o próprio ponto P. Portanto segue o resultado.
(c) Segue pois a construção de $P \oplus Q$ é simétrica em P e Q.
(d) A reta que passa por P e Q intersecta E em R. Utilizando os ítens (a) e (b) anteriores, encontramos que

$$\mathcal{O} = (P \oplus \mathcal{O}) \oplus R = P \oplus R.$$

(e) Demonstrado na próxima seção, proposição (3.8).
(f) Se P e Q tem coordenadas em K, então a equação das retas que passam por eles tem coeficientes em K. Se, ainda, E é definido sobre K, então o terceiro ponto de interseção tem coordenadas dadas por uma combinação de coordenadas racionais dos coeficientes da reta e de E, assim estão em K.

Daqui em diante não usaremos mais os símbolos $\oplus$ e $\ominus$, simplificando pelos símbolos $+$ e $-$ para as operações na curva elíptica E. Para $m \in \mathbb{Z}$ e $P \in E$,

tomamos

$$[m]P = P + \cdots + P, \quad [m]P = -P - \cdots - P, \quad [0]P = \mathcal{O}.$$

Vamos agora deduzir fórmulas explícitas para a operação no grupo E. A equação de Weierstrass é escrita como

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Seguindo a demonstração do item (d) anterior, a fim de calcular $-P_0$, onde $P_0 = (x_0, y_0) \in E$, tomamos a reta L através de P_0 e $\mathcal{O}$ encontrando o terceiro ponto de interseção com E. Assim a reta L é dada por

$$L : x - x_0 = 0.$$

Substituindo na equação de E, vemos que o polinômio quadrático $F(x_0, y)$ tem raiz y_0 e y_0', onde $-P = (x_0, y_0')$. Escrevendo

$$f(x_0, y) = c(y - y_0)(y - y_0')$$

e igualando o coeficiente de y^2 temos $c = 1$, e similarmente igualando os coeficientes de y temos $y_0' = -y_0 - a_1x_0 - a_3$. Disso temos

$$-P_0 = -(x_0, y_0) = (x_0, -y_0 - a_1x_0 - a_3).$$

A seguir vamos deduzir a fórmula para a adição em E. Sejam

$$P_1 = (x_1, y_1) \quad \text{e} \quad P_2 = (x_2, y_2)$$

pontos em E. Se $x_1 = x_2$ e $y_1 + y_2 + a_1x_2 + a_3 = 0$, então $P_1 + P_2 = \mathcal{O}$. Caso contrário a reta L que intersecta P_1 e P_2 tem equação da forma

$$L : y = \lambda x + \nu.$$

Substituindo a equação da reta L na equação de E, vemos que $F(x, \lambda x + \nu)$ tem raízes x_1, x_2, x_3 onde $P_3 = (x_3, y_3)$ é o terceiro ponto de $L \cap E$. Da proposição anterior,

$$P_1 + P_2 + P_3 = \mathcal{O}.$$

Escrevendo

$$F(x, \lambda x + \nu) = x(x - x_1)(x - x_2)(x - x_3)$$

e igualamos os coeficientes. O coeficiente de x^3 fornece $c = -1$, e então o coeficiente de x^2 fornece

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2.$$

Isso fornece fórmula para x_3, e substituindo na equação de L temos o valor de $y_3 = \lambda x_3 + \nu$. Finalmente, para encontrar $P_1 + P_2 = -P_3$, aplicamos a fórmula da negação para P_3. Então acabamos de provar:

Fórmulas Explícitas em $(E, +)$. Seja E uma curva elíptica dada pela equação de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

(a) Seja $P_0 = (x_0, y_0)$. Então

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

A seguir seja,

$$P_1 + P_2 = P_3 \quad \text{com} \quad P_i = (x_i, y_i) \in E \ \text{ para } i = 1, 2, 3.$$

(b) Se $x_1 = x_2$ e $y_1 + y_2 + a_1x_2 + a_3 = 0$, então

$$P_1 + P_2 = \mathcal{O}.$$

Senão, defina λ e ν da seguinte forma:
Para $x_1 \neq x_2$:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{e} \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1},$$

Para $x_1 = x_2$:

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 + a_1y_1}{2y_1 + a_1x_1 + a_3} \quad \text{e} \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

Então $y = \lambda x + \nu$ é a reta entre P_1 e P_2, ou tangente a E se $P_1 = P_2$.
(c) Com a notação usada acima, $P_3 = P_1 + P_2$ tem coordenadas

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

(d) Como caso especial de (c), temos para $P_1 \neq \pm P_2$.

$$x(P_1 + P_2) = \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 + a_1\Big(\frac{y_2 - y_1}{x_2 - x_1}\Big) - a_2 - x_1 - x_2,$$

e a fórmula de duplicação para $P = (x, y) \in E$,

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

onde b_2, b_4, b_6, b_8 são os polinômios em a_i's dados no início do capítulo.

Definição 3.5. Com a notação anterior, a função $f \in \bar{K}(E) = \bar{K}(x, y)$ é dita ser par se $f(P) = f(-P)$ para todo $P \in E$.

Corolário 3.1. Seja $f \in \bar{K}(E)$. Então

$$f \text{ é par se, e somente se, } f \in \bar{K}(x).$$

Prova. Sabemos que se $P = (x_0, y_0)$, então $-P = (x_0, -y_0 - a_1x_0 - a_3)$. Então segue que todo elemento de $\bar{K}(x)$ é par. Suponha agora que $f \in \bar{K}(x, y)$ é par. Usando a equação de Weierstrass para E, podemos escrever f na forma

$$f(x, y) = g(x) + h(x)y \quad \text{ para algum } g, h \in \bar{K}(x).$$

Então assumimos que a paridade de f implica que

$$\begin{aligned} f(x, y) &= f(x, -y - a_1x - a_3), \\ g(x) + h(x)y &= f(x) + h(x)(-y - a_1x - a_3), \\ (2y + a_1x + a_3)h(x) &= 0. \end{aligned}$$

Isso vale para todo $(x, y) \in E$. Assim, ou h é identicamente nulo ou então $(2y + a_1x + a_3) = 0$. Este último implica que o discriminante Δ seja nulo, contradizendo o fato que a equação de Weierstrass é não singular, conforme o início do capítulo. Consequentemente $h = 0$, e então $f(x, y) = g(x) \in \bar{K}(x)$. □

Exemplo 3.2. Seja $E/\mathbb{Q}$ curva elíptica

$$E : y^2 = x^3 + 17.$$

Observe que a curva contém os pontos

$$P_1 = (-2, 3), \quad P_2 = (-1, 4), \quad P_3 = (2, 5), \quad P_4 = (4, 9), \quad P_5 = (8, 23).$$

Usando a fórmula de adição, podemos verificar o seguinte:

$$P_5 = [-2]P_1, \quad P_4 = P_1 - P_3, \quad [3]P_1 - P_3 = (52, 375).$$

Existem muitos outros pontos com coordenadas racionais e não inteiras, por exemplo,

$$[2]P_2 = \Big(\frac{127}{64}, -\frac{2651}{512}\Big), \quad P_2 + P_3 = \Big(-\frac{8}{9}, -\frac{109}{27}\Big).$$

Não demonstraremos aqui, mas é verdadeiro que para todo ponto racional $P \in E(\mathbb{Q})$ pode ser escrito da forma

$$P = [m]P_1 + [n]P_3 \quad \text{para algum } m, n \in \mathbb{Z},$$

e com essa identificação, o grupo $E(\mathbb{Q})$ é isomorfo a $\mathbb{Z} \times \mathbb{Z}$. Além disso, existem apenas 16 pontos inteiros $P = (x, y) \in E$, isto é, pontos com $x, y \in \mathbb{Z}$. Estes fatos ilustram dois teoremas fundamentais na aritmética de curvas elípticas, que diz que o grupo dos pontos racionais de uma curva elíptica é finitamente gerado (Teorema de Mordell-Weil). Mais tarde voltaremos a esse teorema.

Estrutura de Grupo no Caso Singular

Suponha que a equação de Weierstrass tem discriminante $\Delta = 0$. Nesse caso a curva tem um ponto singular. Vamos analizar onde a soma falha. Desconsiderando o ponto singular a estrutura de grupo em E estudada se torna mais simples.

Antes será interessante observar o seguinte exemplo. Considere a curva elíptica

$$E : y^2 = x^3 + 17.$$

Esta é uma curva elíptica definida sobre $\mathbb{Q}$ com discriminante $\Delta = 2^4 3^3 17$. Reduziremos os coeficientes de E módulo p, então consideramos E como uma curva definida sobre o corpo finito $\mathbb{F}_p$. Para quase todo primo, aqueles onde $\Delta \not\equiv 0 (\text{mod } p)$, a curva reduzida é não singular, e consequentemente é uma curva elíptica definida sobre $\mathbb{F}_p$. Entretanto, para primos p que dividem Δ, a curva reduzida tem ponto singular, assim já não é uma curva elíptica. Quando tratamos com curvas elípticas não singulares, encontramos curvas singulares aparecendo naturalmente.

Definição 3.6. Seja E uma curva dada pela equação de Weierstrass. A parte não singular de E, denotada por E_{ns}, é o conjunto dos pontos não singulares de E. Similarmente, se E é definida sobre K, então $E_{ns}(K)$ é o conjunto dos pontos não singulares de $E(K)$.

Lembramos do início do capítulo que se E é singular, então existem duas

possibilidades para a singularidade, chamada nó ou cúspide.

Proposição 3.6. Seja E uma curva dada por equação de Weierstrass com $\Delta = 0$, ou seja, E tem ponto singular S. Então a definição (3.4) torna E_{ns} um grupo abeliano.
(a) Suponha que E tem nó, ou seja $c_4 \neq 0$, e seja

$$y = \alpha_1 x + \beta_1 \quad \text{e} \quad y = \alpha_2 x + \beta_2$$

retas tangentes distintas de E em S. Então o mapa

$$E_{ns} \longrightarrow \bar{K}^*, \quad (x, y) \longmapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$$

é um isomorfismo de grupos abelianos.
(b) Suponha que E tenha uma cúspide, ou seja $c_4 = 0$, e seja

$$y = \alpha x + \beta$$

a reta tangente a E em S. Então o mapa

$$E_{ns} \longrightarrow \bar{K}^+, \quad (x, y) \longmapsto \frac{x - x(S)}{y - \alpha x - \beta}$$

é um isomorfismo de grupos abelianos.

Prova. Observe que E_{ns} é fechado sobre a lei de composição, uma vez que a reta L intersecta E_{ns} em dois pontos, então L não contém o ponto S. De fato S é um ponto singular de E, então S tem multiplicidade no mínimo dois na interseção $E \cap L$. Assim se L também contiver S, então $E \cap L$ consistirá de quatro pontos (contando com suas multiplicidades), contradizendo o teorema de Bézout [2, I.7.8]. Verificamos que o mapa nos ítens (a) e (b) são bijeções entre conjuntos com a propriedade de que se a reta L não contém S e intersecta E_{ns} em três pontos, então a imagem de cada ponto em $\bar{K}^*$ (respectivamente $\bar{K}^+$) é multiplicada por 1 (respectivamente somada a 0). Usando essa propriedade, provamos que a lei de composição torna E_{ns} um grupo abeliano e que os mapas referidos são isomorfismos entre grupos.

Como a lei de composição e os mapas em (a) e (b) são definidos em termos de retas em $\mathbb{P}^2$, é suficiente provar o teorema depois de uma mudança de coordenadas. Começamos por considerar o ponto singular como $(0, 0)$, ficando a equação de Weierstrass como

$$y^2 + a_1 xy = x^3 + a_2 x^2.$$

Seja $s \in \bar{K}$ raiz de $s^2 + a_1 s - a_2 = 0$. Substituindo y por $y + sx$ eliminamos o

termo x^2, dando a seguinte equação para E, que escreveremos usando coordenadas homogêneas:

$$E : Y^2Z + AXYZ - X^3 = 0.$$

Note que E tem um nó se $A \neq 0$ e uma cúspide se $A = 0$.
(a) As retas tangentes a E em $S = [0, 0, 1]$ são $Y = 0$ e $Y + AX = 0$, assim temos o seguinte mapa

$$E_{ns} \longrightarrow \bar{K}^*, \quad [X, Y, Z] \longmapsto 1 + \frac{AX}{Y}.$$

É conveniente fazer uma mudança de variáveis da seguinte forma:

$$X = A^2X' - A^2Y', \quad Y = A^3Y', \quad Z = Z'.$$

Substituindo na equação da curva temos

$$E : XYZ - (X - Y)^3 = 0.$$

Desomogeneizando ($Y = 1$, $x = X/Y$ e $z = Z/Y$), temos que

$$E : xz - (x - 1)^3 = 0$$

e o mapa

$$E_{ns} \longrightarrow \bar{K}^*, \quad (x, z) \longmapsto x.$$

(Note que nesse novo sistema de coordenadas, o ponto singular é agora o ponto no infinito.) O mapa inverso é

$$\bar{K}^* \longrightarrow E_{ns}, \quad t \longmapsto \left(t, \frac{(t-1)^3}{t}\right),$$

assim temos a bijeção entre conjuntos $\bar{K}^* \longleftrightarrow E_{ns}$. Falta demonstrar que se uma reta, que não intersecta $[0, 0, 1]$, intersecta E em três pontos $(x_1, z_1)(x_2, z_2)$ e (x_3, y_3), então $x_1x_2x_3 = 1$. Toda reta tem a forma $z = ax + b$, assim as três coordenadas x x_1, x_2 ex_3 são raízes do polinômio cúbico

$$x(ax + b) - (x - 1)^3 = -x^3 + (a + 3)x^2 + (b - 3)x + 1.$$

No termos constante vemos que $x_1x_2x_3 = 1$, como queríamos.
(b) Neste caso $A = 0$ e a reta tangente a E em $S = [0, 0, 1]$ é $Y = 0$, assim temos o mapa

$$E_{ns} \longrightarrow \bar{K}^+, \quad [X, Y, Z] \longmapsto X/Y.$$

Dezomogeneizando com $Y = 1$, obtemos

$$E : z - x^3 = 0,$$

$$E_{ns} \longrightarrow \bar{K}^+, \quad (x, z) \longmapsto x.$$

O mapa inverso é $t \mapsto (t, t^3)$. Finalmente, a reta $z = ax + b$ intersecta E em três pontos $(x_1, z_1)(x_2, z_2)$ e (x_3, z_3), então olhando para o termo quadrático x^2 em

$$(ax + b) - x^3$$

temos que $x_1 + x_2 + x_3 = 0$. □

3.4 Curvas Elípticas

Como vimos, uma curva suave de gênero um tem estrutura de grupo abeliano. Evidenciando seu elemento neutro, podemos definir essa curva da seguinte forma.

Definição 3.7. Uma curva elíptica é o par $(E, \mathcal{O})$, onde E é a curva não singular de gênero um e $\mathcal{O} \in E$. A curva elíptica E é definida sobre K se E é definido sobre K como curva e $\mathcal{O} \in E(K)$.

A seguir estudaremos alguns resultados que farão com que esta definição se conecte com o estudo feito nos primeiros capítulos.

Proposição 3.7. Seja E uma curva elíptica definida sobre K.
(a) Existem funções $x, y \in K(E)$ tais que o mapa

$$\phi : E \longrightarrow \mathbb{P}^2, \quad \phi = [x, y, 1],$$

nos dá um isomorfismo de E/K na curva dada pela equação de Weierstrass

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

com coeficientes $a_1, \ldots, a_6 \in K$ satisfazendo $\phi(\mathcal{O}) = [0, 1, 0]$. As funções x e y são chamadas coordenadas de Weierstrass para a curva elíptica E.
(b) Quaisquer duas equações de Weierstrass para E como no ítem anterior são relacionadas por uma mudança de variáveis da forma

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t,$$

com $u \in K^*$ e $r, s, t \in K$.
(c) Reciprocamente, toda curva cúbica suave C dada por uma equação de Weierstrass é uma curva elíptica definida sobre K cujo ponto base é $\mathcal{O} = [0, 1, 0]$.

Prova. (a) Olhamos para o espaço vetorial $\mathcal{L}(n(\mathcal{O}))$ para $n = 1, 2, \ldots$. Pelo teorema de Riemann-Roch, (2.3) com $g = 1$,

$$\ell(n(\mathcal{O})) = \dim \mathcal{L}(n(\mathcal{O})) = n \quad \text{para todo } n \geq 1.$$

Assim podemos escolher funções $x, y \in K(E)$ tais que $\{1, x\}$ é uma base para $\mathcal{L}(2(\mathcal{O}))$ e que $\{1, x, y\}$ é base para $\mathcal{L}(3(\mathcal{O}))$. Note que x tem um polo de ordem 2 em $\mathcal{O}$, e similarmente y tem polo de ordem 3 em $\mathcal{O}$.

Observe que $\mathcal{L}(6(\mathcal{O}))$ tem dimensão 6, mas contém as sete seguintes funções:

$$1, x, y, x^2, xy, y^2, x^3.$$

Segue que existe uma relação linear dada por

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0,$$

onde pela proposição (2.14) podemos tomar $A_1, \ldots, A_7 \in K$. Note que $A_6A_7 \neq 0$, pois caso contrário todo termo teria necessariamente polo em $\mathcal{O}$ de diferentes ordens, e assim todo A_j's seriam nulos. Substituindo x e y por $-A_6A_7x$ e $A_6A_7^2y$, respectivamente, e dividindo por $A_6^3A_7^4$ temos uma equação cúbica na forma de Weierstrass. Isso fornece um mapa

$$\phi : E \longrightarrow \mathbb{P}^2, \quad \phi = [x, y, 1],$$

onde a imagem de C está no local geométrico descrito pela equação de Weierstrass. Note que $\phi : E \longrightarrow C$ é um morfismo pela proposição (2.5) e sobrejetor pelo teorema (2.1). Consequentemente temos que $\phi(\mathcal{O}) = [0, 1, 0]$, pois y tem polo de ordem maior do que x no ponto $\mathcal{O}$.

A seguir mostraremos que o mapa $\phi : E \to C \subset \mathbb{P}^2$ tem grau um. Isso equivale demonstrar que $K(E) = K(x, y)$. Considere o mapa $[x, 1] : E \to \mathbb{P}^1$. Como x tem dois polos em $\mathcal{O}$ e nenhum outro polo, a proposição (2.7a) nos diz que o mapa acima tem grau 2. Assim $[K(E) : K(E)] = 2$. Similarmente, o mapa $[y, 1] : E \to \mathbb{P}^1$ tem grau 3, assim $[K(E) : K(y)] = 3$. Logo $[K(E) : K(x, y)]$ divide 2 e 3, ou seja, é igual a 1.

Mostremos agora que C é suave. Suponha por absurdo que C é singular. Então da proposição (3.3), existe um mapa racional $\psi : C \to \mathbb{P}^1$ de grau um. Segue que

a composição $\psi \circ \phi : E \to \mathbb{P}^1$ é um mapa de grau um entre curvas suaves, assim pelo corolário (2.1), é um isomorfismo. Isso contradiz o fato de que E tem gênero um e $\mathbb{P}^1$ tem gênero zero, do exemplo (2.13). Sendo assim C é suave, e aplicando o corolário (2.1) concluímos que o mapa $\phi : E \to C$ é um isomorfismo.
(b) Sejam $\{x, y\}$ e $\{x', y'\}$ dois conjuntos de funções coordenadas de Weierstrass em E. Então x e x' têm polos de ordem 2 em $\mathcal{O}$, e y e y' têm polo de ordem 3 em $\mathcal{O}$. Consequentemente $\{1, x\}$ e $\{1, x'\}$ são ambos bases para $\mathcal{L}(2(\mathcal{O}))$, e similarmente $\{1, x, y\}$ e $\{1, x', y'\}$ são ambos bases para $\mathcal{L}(3(\mathcal{O}))$. Assim existem as constantes

$$u_1, u_2 \in K^* \quad \text{e} \quad r, s_2, t \in K$$

tais que

$$x = u_1 x' + r \quad \text{e} \quad y = u_2 y' + s_2 x' + t.$$

Como (x, y) e (x', y') satisfazem a equação de Weierstrass e os termos Y^2 e X^3 têm coeficientes 1, temos $u_1^3 = u_2^2$. Escrevendo $u = u_2/u_1$ e $s = s_2/u^2$ colocamos a fórmula de mudança de coordenadas na forma desejada.
(c) Seja E dada por uma equação de Weierstrass. Vimos que o diferencial

$$\omega = \frac{dx}{2y + a_1 x + a_3} \in \Omega_E$$

não tem zeros nem polos, assim $\operatorname{div}(\omega) = 0$. O teorema de Riemann-Roch nos diz que

$$2 \text{ gênero}(E) - 2 = \deg \operatorname{div}(\omega) = 0,$$

assim E tem gênero um, e tomando $[0, 1, 0]$ como ponto de base fazemos com que E se torne curva elíptica. □

Corolário 3.2. Seja E/K uma curva elíptica com funções coordenadas de Weierstrass x e y. Então

$$K(E) = K(x, y) \quad \text{e} \quad [K(E) : K(x)] = 2.$$

Prova. Estes fatos foram demonstrados ao longo da proposição anterior. □

Observação 3.2. Note que a proposição (3.7b) não implica que se duas equações de Weierstrass têm coeficientes em K, então toda mudança de variáveis que mapeia um ao outro tem coeficientes em K. Por exemplo a equação

$$y^2 = x^3 - x,$$

tem coeficientes em $\mathbb{Q}$, e é mapeado nele mesmo pela substituição

$$x = -x', \quad y = \sqrt{-1}y'.$$

Usaremos a seguir o teorema de Riemann-Roch para descrever a lei de grupo nos pontos de uma curva elíptica E. Observe que não será da mesma forma como fizemos quando E é dado por uma equação de Weierstrass. Começaremos com um lema que distingue $\mathbb{P}^1$ de curvas de gênero um.

Lema 3.1. Seja C uma curva de gênero um, e seja $P, Q \in C$. Então

$$(P) \sim (Q) \quad \text{se, e somente se,} \quad P = Q.$$

Prova. Suponha que $(P) \sim (Q)$ e escolha $f \in \bar{K}(C)$ tal que

$$\operatorname{div}(f) = (P) - (Q).$$

Então $f \in \mathcal{L}((Q))$. O teorema de Riemman-Roch nos diz que

$$\dim \mathcal{L}((Q)) = 1.$$

Mas $\mathcal{L}((Q))$ contém a função constante, e então, $f \in \bar{K}$ e $P = Q$. □

Proposição 3.8. Seja $(E, \mathcal{O})$ uma curva elíptica.
(a) Para todo divisor de grau zero $D \in \operatorname{Div}^0(E)$ existe um único ponto $P \in E$ tal que $D \sim (P) - (\mathcal{O})$. Portanto

$$\begin{aligned} \sigma : \operatorname{Div}^0(E) &\longrightarrow E \\ D &\longmapsto P, \qquad \text{está bem definido.} \end{aligned}$$

(b) O mapa σ acima é sobrejetor.
(c) Seja $D_1, D_2 \in \operatorname{Div}^0(E)$. Então

$$\sigma(D_1) = \sigma(D_2) \quad \text{se, e somente se,} \quad D_1 \sim D_2.$$

Assim σ induz uma bijeção:

$$\sigma : \operatorname{Pic}^0(E) \longrightarrow E.$$

(d) O mapa inverso de σ é o mapa

$$\kappa : E \longrightarrow \mathrm{Pic}^0(E), \qquad P \longmapsto (\text{classe de divisores de } (P) - (\mathcal{O})).$$

(e) Se E é dado por uma equação de Weierstrass, então a "lei geométrica de grupo" em E descrita pela definição (3.4) e a "lei algébrica de grupo" induzida de $\mathrm{Pic}^0(E)$ usando σ são as mesmas.

Prova. (a) Como E tem gênero um, o teorema de Riemann-Roch diz que

$$\dim \mathcal{L}(D + (\mathcal{O})) = 1.$$

Seja $f \in \mathcal{L}(D + (\mathcal{O}))$, assim $\{f\}$ é base desse espaço vetorial. Como

$$\mathrm{div}(f) \geq -D - (\mathcal{O}) \quad \text{e} \quad \deg(\mathrm{div}(f)) = 0,$$

segue que

$$\mathrm{div}(f) = -D - (\mathcal{O}) + (P)$$

para algum $P \in E$. Consequentemente

$$D \sim (P) - (\mathcal{O}),$$

o que demonstra o resultado.

Agora suponha um ponto $P' \in E$ com a mesma propriedade. Então

$$(P) \sim D + (\mathcal{O}) \sim (P'),$$

e assim o lema (3.1) mostra que $P = P'$. Portanto P é único.
(b) Para qualquer $P \in E$,

$$\sigma((P) - (\mathcal{O})) = P.$$

(c) Seja $D_1, D_2 \in \mathrm{Div}^0(E)$, e considere $P_i = \sigma(D_i)$ para $i = 1, 2$. Então da definição de σ temos que

$$(P_1) - (P_2) \sim D_1 - D_2.$$

Assim, se $P_1 = P_2$, então $D_1 \sim D_2$. Reciprocamente, se $D_1 \sim D_2$, então $(P_1) \sim (P_2)$, então $P_1 = P_2$ pelo lema (3.1).
(d) Para cada $P \in E$, temos bem definido a classe $\bar{D} \in \mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim$. Esse mapa é o inverso da bijeção σ, conforme enunciado.
(e) Seja E dado por equação de Weierstrass e $P, Q \in E$. É suficiente mostrarmos

que

$$\kappa(P+Q) = \kappa(P) + \kappa(Q).$$

Seja

$$f(X,Y,Z) = \alpha X + \beta Y + \gamma Z = 0$$

dado pela reta $L \in \mathbb{P}^2$ entre os pontos P e Q, com R o terceiro ponto de interseção de L e E, e

$$f'(X,Y,Z) = \alpha' X + \beta' Y + \gamma' Z = 0$$

a reta L' através de R e $\mathcal{O}$. Então da definição de adição em E e pelo fato de que $Z = 0$ intersecta E em $\mathcal{O}$ com multiplicidade 3, temos

$$\begin{aligned} \operatorname{div}(f/Z) &= (P) + (Q) + (R) - 3(\mathcal{O}) \\ \operatorname{div}(f'/Z) &= (R) + (P+Q) - 2(\mathcal{O}). \end{aligned}$$

Portanto

$$(P+Q) - (P) - (Q) + (\mathcal{O}) = \operatorname{div}(f'/f) \sim 0,$$

e assim

$$\kappa(P+Q) - \kappa(P) - \kappa(Q) = 0.$$

Isso mostra que κ é um homomorfismo de grupos. □

Corolário 3.3. Seja E uma curva elíptica e $D = \sum_P (P) \in \operatorname{Div}(E)$. Então D é um divisor principal se, e somente se,

$$\sum_{P \in E} n_P = 0 \quad \text{e} \quad \sum_{P \in E} [n_P]P = \mathcal{O}.$$

Notamos que a primeira soma é de números inteiros, e a segunda é a adição na curva E.

Prova. Da proposição (2.9b), todo divisor principal tem grau 0. Considere $D \in \operatorname{Div}^0(E)$. Da proposição (3.8a,e) temos que

$$D \sim 0 \iff \sigma(D) = \mathcal{O} \iff \sum_{P \in E} [n_P]\sigma((P) - (\mathcal{O})) = \mathcal{O},$$

como $\sigma((P) - (\mathcal{O})) = P$, temos o resultado desejado. □

Demonstraremos agora um fato fundamental que diz que a lei de adição em uma curva elíptica é um morfismo. A adição em E é o mapa $E \times E \to E$ sendo a

variedade $E \times E$ de dimensão 2.

Teorema 3.1. Seja E/K uma curva elíptica. Então as equações que nos fornecem a lei de grupo em E define os morfismos

$$\begin{array}{rcl} + : E \times E & \longrightarrow & E \\ (P_1, P_2) & \longmapsto & P_1 + P_2 \end{array} \qquad \text{e} \qquad \begin{array}{rcl} - : E & \longrightarrow & E, \\ P & \longmapsto & -P. \end{array}$$

Prova. Primeiramente observamos pela fórmula da negação que:

$$(x, y) \longmapsto (x, -y - a_1 x - a_3)$$

é um mapa racional de $E \to E$. Como E é suave, segue da proposição (2.5) que esse mapa é um morfismo.

Fixando o ponto $Q \neq \mathcal{O}$ de E e considerando a translação por Q

$$\tau : E \longrightarrow E, \quad \tau(P) = P + Q.$$

Como a fórmula de adição fornece um mapa racional, τ é racional. Novamente usando a proposição (2.5) temos um morfismo. Como τ tem inverso, que é $P \mapsto P - Q$, temos que τ é isomorfismo.

Consideremos agora o mapa de adição $+ : E \times E \to E$. Do ítem (c) das Fórmulas Explícitas em $(E, +)$, temos que a adição é um morfismo faltando apenas estudarmos os casos

$$(P, P), \quad (P, -P), \quad (P, \mathcal{O}), \quad (\mathcal{O}, P),$$

pois para os pares que não sejam dessa forma, temos bem definido em $E \times E$ as funções racionais

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{e} \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

Para demonstrarmos os quatro casos de pares acima, tomamos τ_1 e τ_2 translações sobre os pontos Q_1 e Q_2, respectivamente. Considere a composição de mapas

$$\phi : E \times E \xrightarrow{\tau_1 \times \tau_2} E \times E \xrightarrow{+} E \xrightarrow{\tau_1^{-1}} E \xrightarrow{\tau_2^{-1}} E.$$

Como a lei de grupo em E é associativa e comutativa temos que

$$\begin{aligned}(P_1, P_2) &\xrightarrow{\pi_1 \times \pi_2} (P_1 + Q_1, P_2 + Q_2) \\ &\xrightarrow{+} P_1 + Q_1 + P_2 + Q_2 \\ &\xrightarrow{\pi_1^{-1}} P_1 + P_2 + Q_2 \\ &\xrightarrow{\pi_2^{-1}} P_1 + P_2.\end{aligned}$$

Assim o mapa racional ϕ é a soma entre os pontos.

Além disso, como τ_is são isomorfismos, segue do exposto acima que ϕ é morfismo exceto possivelmente nos pares de pontos da forma

$$(P - Q_1, P - Q_2), \quad (P - Q_1, -P - Q_2), \quad (P - Q_1, -Q_2), \quad (-Q_1, P - Q_2),$$

sendo Q_1 e Q_2 pontos quaisquer da curva E. Então, variando Q_1 e Q_2, podemos encontrar um número finito de mapas racionais entre conjuntos

$$\phi_1, \phi_2, \ldots, \phi_n : E \times E \longrightarrow E$$

com as seguintes propriedades:
(i) ϕ_1 é o mapa de adição dado no ítem (c) das fórmulas em E.
(ii) Para cada $(P_1, P_2) \in E \times E$, algum dos ϕ_i's é definido em (P_1, P_2).
(iii) Se ϕ_i e ϕ_j são definidos em (P_1, P_2), então $\phi_i(P_1, P_2) = \phi_j(P_1, P_2)$.

Segue que a adição é bem definida em $E \times E$, então é um morfismo. □

Observação 3.3. Durante a demonstração da proposição anterior, notamos que as fórmulas de adição dadas no início do capítulo tornam $+ : E \times E \to E$ um morfismo exceto possivelmente nos pontos da forma $(P, \pm P)$, $(P, \mathcal{O})$ ou $(\mathcal{O}, P)$. Ao invés de usar translações para tornar menos difícil, podemos trabalhar diretamente com a definição de morfismo usando equações explícitas. Para isso devemos considerar alguns casos.

Seja $(x_1, y_1; x_2, y_2)$ coordenadas de Weierstrass em $E \times E$. Mostraremos explicitamente que a adição é um morfismo em pontos da forma (P, P) com $P \neq \mathcal{O}$ e $[2]P \neq \mathcal{O}$. Notamos que a adição é definida em geral pelas fórmulas explícitas em E, ítem (c):

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} = y_1 - \lambda x_1,$$
$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \qquad y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Aqui vemos λ, ν, x_3, y_3 como funções em $E \times E$, e a adição é dada pelo mapa $[x_3, y_3, 1] : E \times E \to E$. Assim para mostrar que a adição é um morfismo em (P, P), é suficiente mostrar que λ é um morfismo em (P, P). Assumimos que os pares (x_1, y_1) e (x_2, y_2) satisfazem a mesma equação de Weierstrass. Subtraindo uma equação de outra e fatorando temos o seguinte:

$$(y_1 - y_2)(y_1 + y_2 + a_1x_1 + a_3) \\ = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 + a_2x_1 + a_2x_2 + a_4 - a_1y_2).$$

Assim λ, como função em $E \times E$, pode ser escrita como

$$\lambda(P_1, P_2) = \frac{x_1^2 + x_1x_2 + x_2^2 + a_2x_1 + a_2x_2 + a_4 - a_1y_2}{y_1 + y_2 + a_1x_1 + a_3}.$$

Além disso, tomando escrevendo $P = (x, y)$ temos que

$$\lambda(P, P) = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}.$$

Consequentemente λ é um morfismo em (P, P), dado que $2y(P) + a_1x(P) + a_3 \neq 0$, excluindo-se o caso em que $[2]P \neq \mathcal{O}$.

3.5 Isogenias

Estudamos até o momento a geometria de curvas elípticas individualmente. Faremos agora um estudo dos mapas entre essas curvas. Como cada curva elíptica tem seu elemento neutro, é natural que este mapa preserve essa propriedade.

Definição 3.8. Sejam E_1 e E_2 curvas elípticas. Uma isogenia de E_1 em E_2 é um morfismo

$$\phi : E_1 \longrightarrow E_2 \quad \text{satisfazendo} \quad \phi(\mathcal{O}) = \mathcal{O}.$$

Duas curvas elípticas E_1 e E_2 são isogêneas se existe uma isogenia de E_1 em E_2 com $\phi(E_1) \neq \{\mathcal{O}\}$. Veremos mais tarde que isso é uma relação de equivalência.

Segue do teorema (2.1) que uma isogenia satisfaz

$$\phi(E_1) = \mathcal{O} \quad \text{ou} \quad \phi(E_1) = E_2.$$

Como vimos a respeito de mapas entre curvas no início desse estudo, exceto para o caso da isogenia definida por $[0](P) = \mathcal{O}$ para todo $P \in E_1$, toda isogenia é um mapa

finito entre curvas. Consequentemente obtemos a injetividade usual entre corpos de funções:

$$\phi^* : \bar{K}(E_2) \longrightarrow \bar{K}(E_1).$$

Também, o grau de ϕ, $\deg \phi$, é o grau da extensão finita $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$. Seguiremos usando as mesmas notações estabelecidas no início do capítulo 2.
Curvas elípticas são grupos abelianos, então os mapas entre essas curva formam um grupo. Denotaremos o conjunto das isogenias de E_1 em E_2 por

$$\mathrm{Hom}(E_1, E_2) = \{\text{isogenias, } E_1 \to E_2\}.$$

A soma de duas isogenias é definida por

$$(\phi + \psi)(P) = \phi(P) + \psi(P),$$

e o teorema (3.1) implica que $\phi + \psi$ é um morfismo, assim é uma isogenia. Consequentemente $\mathrm{Hom}(E_1, E_2)$ é um grupo.

Se $E_1 = E_2$, então podemos compor isogenias. Então se E é uma curva elíptica, tomamos

$$\mathrm{End}(E) = \mathrm{Hom}(E, E),$$

o anel onde a adição é dada como vimos acima e a multiplicação é dada pela composição entre isogenias,

$$(\phi\psi)(P) = \phi(\psi(P)).$$

O anel $\mathrm{End}(E)$ é chamado anel de endomorfismo de E. Os elementos invertíveis de $\mathrm{End}(E)$ formam o grupo de automorfismos de E, que denotaremos por $\mathrm{Aut}(E)$.

Claramente, se E_1, E_2, e E são definidos sobre um corpo K, então podemos restringir nossa atenção a aquelas isogenias definidas sobre K. O correspondente grupo de isogenias é denotado subescrevendo o corpo K:

$$\mathrm{Hom}_K(E_1, E_2), \quad \mathrm{End}_K(E), \quad \mathrm{Aut}_K(E).$$

Observe no seguinte exemplo como $\mathrm{Aut}_K(E)$ pode ser estritamente maior que $\mathrm{Aut}_K(E)$.

Exemplo 3.3. Para cada $m \in \mathbb{Z}$ definimos a multiplicação pela m-isogenia

$$[m] : E \longrightarrow E$$

de modo natural. Assim se $m > 0$, então

$$[m](P) = P + P + \cdots + P, \quad m \text{ vezes.}$$

Para $m < 0$, definimos $[m](P) = [-m](-P)$, onde também vale que $[0](P) = \mathcal{O}$. Usando o teorema (3.1), induzimos facilmente que $[m]$ é um morfismo, consequentemente uma isogenia, pois $\mathcal{O} \mapsto \mathcal{O}$.

Note que se E é definido sobre K, então $[m]$ é definido sobre K. Analisaremos o grupo de isogenias mostrando que se $m \neq 0$, a m-isogenia é não constante.

Proposição 3.9. (a) Sejam E/K uma curva elíptica e $m \in \mathbb{Z}$ com $m \neq 0$. Então o m-mapa

$$[m] : E \longrightarrow E$$

é não contante.
(b) Seja E_1 e E_2 curvas elípticas. Então o grupo de isogenias

$$\mathrm{Hom}(E_1, E_2)$$

é um $\mathbb{Z}$-módulo livre de torção.
(c) Seja E uma curva elíptica. Então o anel de endomorfismo $\mathrm{End}(E)$ é um anel de característica 0, sem divisores de zero.

Prova. (a) Mostremos primeiramente que $[2] \neq [0]$. A fórmula de duplicação, vista anteriormente nas fórmulas explícitas em E, diz que se o ponto $P = (x, y) \in E$ tem ordem 2, então deve satisfazer

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0.$$

Se $\mathrm{char}(K) \neq 2$, isso mostra que existem finitos pontos dessa forma. Além disso, mesmo se $\mathrm{char}(K) = 2$, o único modo de ter $[2] = [0]$ é para polinômios cúbicos identicamente nulos, o que significa que $b_2 = b_6 = 0$, assim $\Delta = 0$. Consequentemente, para todo caso, $[2] \neq [0]$. Usando o fato que $[mn] = [m] \circ [n]$, reduzimos os casos para quando m é ímpar.

Assuma que $\mathrm{char}(K) \neq 2$. Então, usando algoritmo de divisão, vemos que o polinômio

$$4x^3 + b_2x^2 + 2b_4x + b_6$$

não divide o polinômio

$$x^4 - b_4x^2 - 2b_6x - b_8.$$

Mais precisamente, se o primeiro polinômio divide o segundo, então $\Delta = 0$. Portanto podemos encontrar $x_0 \in \bar{K}$ tal que o primeiro polinômio se anula em alta ordem em x_0 mais que o segundo. Escolhendo $y_0 \in \bar{K}$ tal que $P_0 = (x_0, y_0) \in E$, a fórmula de duplicação implica que $[2]P_0 = \mathcal{O}$. Em outras palavras, mostramos que E tem um ponto P_0 de ordem 2. Então para inteiros ímpares m temos

$$[m]P_0 = P_0 \neq \mathcal{O},$$

assim segue que $[m] \neq [0]$.

Para os casos em que $\mathrm{char}(K) = 2$ e m ímpar, faremos adiante com o corolário (3.7).

(b) Segue do item (a). Suponha que $\phi \in \mathrm{Hom}(E_1, E_2)$ e $m \in \mathbb{Z}$ satisfaz

$$[m] \circ \phi = [0].$$

Tomando os graus temos

$$(\deg[m])(\deg \phi) = 0,$$

assim ou $m = 0$, ou (a) implica que $\deg[m] \geq 1$, caso em que devemos ter $\phi = [0]$.

(c) Seguindo do ítem (b), o anel de endomorfismo $\mathrm{End}(E)$ tem característica 0. Suponha que $\phi, \psi \in \mathrm{End}(E)$ satisfaz $\phi \circ \psi = [0]$. Então

$$(\deg \phi)(\deg \psi) = \deg(\phi \circ \psi) = 0.$$

Segue que ou $\phi = [0]$ ou $\psi = [0]$. Consequentemente $\mathrm{End}(E)$ é um domínio. □

Definição 3.9. Seja E uma curva elíptica e seja $m \in \mathbb{Z}$ com $m \geq 1$. O subgrupo de m-torção de E, denotado por $E[m]$, é o conjunto dos pontos de E de ordem m,

$$E[m] = \{P \in E : [m]P = \mathcal{O}\}.$$

Definição 3.10. O subgrupo de torção de E, denotado por E_{tor}, é o conjunto dos pontos de ordem finita,

$$E_{tor} = \bigcup_{m=1}^{\infty} E[m].$$

Se E é definido sobre K, então $E_{tor}(K)$ denota os pontos de ordem finita em $E(K)$.

O fato mais importante sobre o $[m]$-mapa é seu grau m^2, de onde podemos deduzir a estrutura do grupo $E[m]$. Demonstraremos esse fato mais tarde como um corolário.

Observação 3.4. Suponha que $\mathrm{char}(K) = 0$. Então o mapa

$$[\ ] : \mathbb{Z} \longrightarrow \mathrm{End}(E)$$

é bijetor. Se $\mathbb{Z} \subsetneq E$, então diremos que E tem multiplicação complexa.

Exemplo 3.4. Suponha que $\mathrm{char}(K) \neq 2$ e $i \in \bar{K}$ tal que $i^2 = -1$. Então, como feito na observação (3.2), a curva elíptica E/K dada pela equação

$$E : y^2 = x^3 - x$$

tem anel de endomorfismo $\mathrm{End}(E) \supsetneq \mathbb{Z}$, uma vez que contém o mapa $[i]$, dado por

$$[i] : (x, y) \longmapsto (-x, iy).$$

Assim E tem multiplicação complexa. Notamos que $[i]$ é definido sobre K se, e somente se, $i \in K$. Consequentemente mesmo se E for definido sobre K, pode acontecer que $\mathrm{End}_K(E)$ seja estritamente menor que $\mathrm{End}(E)$.

Continuando, observamos que

$$[i] \circ [i](x, y) = [i](-x, iy) = (x, -y) = -(x, y),$$

assim $[i] \circ [i] = [-1]$. Assim existe o anel de homomorfismos

$$\mathbb{Z}[i] \longrightarrow \mathrm{End}(E), \qquad m + ni \longmapsto [m] + [n] \circ [i].$$

Se $\mathrm{char}(K) = 0$, esse mapa é um isomorfismo, $\mathbb{Z}[i] \cong \mathrm{End}(E)$, caso em que

$$\mathrm{Aut}(E) \cong \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$$

é um grupo cíclico de ordem 4.

Exemplo 3.5. Suponha $\mathrm{char}(K) \neq 2$ e $a, b \in K$ satisfazendo $b \neq 0$ e $r := a^2 - 4b \neq 0$. Considere as duas curvas elípticas

$$E_1 : y^2 = x^3 + ax^2 + bx$$
$$E_2 : Y^2 = X^3 - 2aX^2 + rX.$$

Existem isogenias de grau 2 entre essas curvas:

$$\phi : E_1 \longrightarrow E_2, \qquad \hat{\phi} : E_2 \longrightarrow E_1,$$
$$(x,y) \longmapsto \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right), \qquad (X,Y) \longmapsto \left(\frac{Y^2}{4X^2}, \frac{Y(r-X^2)}{8X^2}\right).$$

Observamos que $\hat{\phi} \circ \phi = [2]$ em E_1 e $\phi \circ \hat{\phi} = [2]$ em E_2. Os mapas ϕ e $\hat{\phi}$ são exemplos de isogenias duais, vistas mais a frente.

Exemplo 3.6. Sejam $\mathrm{char}(K) = p > 0$, $q = p^r$, e E/K curva elíptica dada por uma equação de Weierstrass. Lembramos do capítulo 2 que a curva $E^{(q)}$ é definida elevando os coeficientes da equação de E a q-ésima potência, e o morfismo de Frobenius ϕ_q é definido por

$$\phi_q : E \longrightarrow E^{(q)}, \qquad (x,y) \longmapsto (x^q, y^q).$$

Como $E^{(q)}$ é o conjunto dos zeros da equação de Weierstrass, ele é uma curva elíptica, dado que sua equação é não singular. Escrevendo em termos dos coeficientes de Weierstrass e usando o fato de que mapa de q-ésima potência $K \to K$ é homomorfismo, fica claro que

$$\Delta(E^{(q)}) = \Delta(E)^q \quad \text{e} \quad j(E^{(q)}) = j(E)^q.$$

Em particular, a equação de E^q é não singular.

Suponha que $K = \mathbb{F}_q$ é corpo finito com q elementos. Então o q-ésimo mapa em K é o mapa identidade, assim $E^{(q)} = E$ e ϕ_q é um endomorfismo de E, chamado endomorfismo de Frobenius. O conjunto de pontos fixados por ϕ_q é o grupo finito $E(\mathbb{F}_q)$. Esse fato é a base da prova do teorema de Hasse, que demonstra uma estimativa para $\#E(\mathbb{F}_q)$.

Exemplo 3.7. Seja E/K uma curva elíptica e seja $Q \in E$. Então definimos o mapa translação por Q por

$$\tau_Q : E \longrightarrow E, \qquad P \longmapsto P + Q.$$

O mapa τ_Q é claramente um isomorfismo, pois τ_{-Q} é seu inverso. Claramente, não é isogenia a menos que $Q = \mathcal{O}$.

Dado o morfismo

$$F : E_1 \longrightarrow E_2$$

entre curvas elípticas, a composição

$$\phi = \tau_{-F(\mathcal{O})} \circ F$$

é uma isogenia, pois $\phi(\mathcal{O}) = \mathcal{O}$. Assim qualquer morfismo F entre curvas elípticas pode ser escrito como

$$F = \tau_{F(\mathcal{O})} \circ \phi,$$

isto é, como uma composição de uma isogenia e uma translação.

Uma isogenia é um mapa entre curvas elípticas que envia $\mathcal{O}$ a $\mathcal{O}$. Como uma curva elíptica é um grupo, é mais natural focarmos nossa atenção a aquelas isogenias que são homomorfismos entre grupos. Entretanto, como demonstraremos que toda isogenia é automaticamente um homomorfismo.

Teorema 3.2. Seja $\phi : E_1 \longrightarrow E_2$ uma isogenia. Então

$$\phi(P + Q) = \phi(P) + \phi(Q) \quad \text{para todo } P, Q \in E_1.$$

Prova. Se $\phi(P) = \mathcal{O}$ para todo $P \in E$, então não temos o que demonstrar. Caso contrário, ϕ é um mapa finito, assim pela observação (2.3), ele induz o homomorfismo

$$\phi_* : \mathrm{Pic}^0(E_1) \longrightarrow \mathrm{Pic}^0(E_2)$$

definido por

$$\phi_*(\text{classe de } \sum n_i(P_i)) = \text{classe de } \sum n_i(\phi P_i).$$

Por outro lado, como $\phi(\mathcal{O}) = \mathcal{O}$, obtemos o seguinte diagrama comutativo:

$$\begin{array}{ccc} E_1 & \xrightarrow[\kappa_1]{\cong} & \mathrm{Pic}^0(E_1) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_*} \\ E_2 & \xrightarrow[\kappa_2]{\cong} & \mathrm{Pic}^0(E_2) \end{array}$$

Como κ_1, κ_2, e ϕ_* são todos homomorfismos de grupos e κ_2 é injetor, segue que ϕ é um homomorfismo. □

Corolário 3.4. Seja $\phi : E_1 \to E_2$ uma isogenia não nula. Então

$$\ker \phi = \phi^{-1}(\mathcal{O})$$

é um grupo finito.

Prova. Do teorema anterior, é um subgrupo de E, e é finito (de ordem no máximo $\deg \phi$) da proposição (2.7a). □

Os próximos três resultados abrangem a teoria básica de Galois dos corpos de funções elípticas.

Teorema 3.3. Seja $\phi : E_1 \to E_2$ uma isogenia não nula.
(a) Para todo $Q \in E_2$,

$$\#\phi^{-1}(Q) = \deg_s \phi.$$

Consequentemente, para todo $P \in E_1$,

$$e_\phi(P) = \deg_i \phi.$$

(b) O mapa

$$\ker \phi \longrightarrow \mathrm{Aut}(\bar{K}(E_1)/\phi^*\bar{K}(E_2)), \quad T \longmapsto \tau_T^*,$$

é um isomorfismo, onde τ_T é o mapa translação por T e τ_T^* é o automorfismo que τ_T induz em $\bar{K}(E_Q)$.
(c) Suponha que ϕ é separável. Então ϕ é não ramificado,

$$\#\ker \phi = \deg \phi,$$

e $\bar{K}(E_1)$ é uma extensão de Galois de $\phi^*\bar{K}(E_2)$.

Prova. (a) Da proposição (2.7b) sabemos que

$$\#\phi^{-1}(Q) = \deg_s \phi \quad \text{para um número finito de } Q \in E_2.$$

Para qualquer $Q, Q' \in E_2$, se escolhermos algum $R \in E_1$ com $\phi(R) = Q' - Q$, então pelo fato que ϕ é um homomorfismo temos que existe uma correspondência biunívoca

$$\phi^{-1}(Q) \longrightarrow \phi^{-1}(Q'), \quad P \longmapsto P + R.$$

Consequentemente

$$\#\phi^{-1}(Q) = \deg_s \phi \quad \text{para todo } Q \in E_2.$$

Agora sejam $P, P' \in E_1$ com $\phi(P) = \phi(P') = Q$, e $R := P' - P$. Então $\phi(R) = \mathcal{O}$, assim $\phi \circ \tau_R = \phi$. Além disso, usando o ítem c da proposição (2.7) e o fato que τ_R é

um isomorfismo,

$$e_\phi(P) = e_{\phi\circ\tau_R}(P) = e_\phi(\tau_R(P))e_{\tau_R}(P) = e_\phi(P').$$

Consequentemente todo ponto em $\phi^{-1}(Q)$ tem o mesmo índice de ramificação. Calculando temos

$$\begin{aligned}(\deg_s\phi)(\deg_i\phi) = \deg\phi &= \sum_{P\in\phi^{-1}(Q)} e_\phi(P) \qquad \text{de (2.7a)},\\ &= (\#\phi^{-1}(Q))e_\phi(P) \quad \text{para todo } P\in\phi^{-1}(Q),\\ &= (\deg_s\phi)e_\phi(P) \qquad \text{do visto acima.}\end{aligned}$$

Cancelando $\deg_s\phi$ temos que o resultado segue.
(b) Primeiramente, se $T\in\ker\phi$ e $f\in\bar{K}(E_2)$, então

$$\tau_T^*(\phi^* f) = (\phi\circ\tau_T)^* f = \phi^* f,$$

pois $\phi\circ\tau_T = \phi$. Portanto como automorfismo de $\bar{K}(E_1)$, o mapa τ_T^* fixa $\phi^*\bar{K}(E_2)$, assim o mapa está bem definido. A seguir, como

$$\tau_S\circ\tau_T = \tau_{S+T} = \tau_T\circ\tau_S,$$

o mapa em (b) é um homomorfismo. Por fim, de (a) temos

$$\#\ker\phi = \deg_s\phi,$$

e pela teoria de Galois sabemos que

$$\#\mathrm{Aut}(\bar{K}(E_1)/\phi^*\bar{K}(E_2)) \le \deg_s\phi.$$

Então, para provar que o mapa $T\to\tau_T^*$ é um isomorfismo, é suficiente mostrar que é injetor. Se τ_T^* fixa $\bar{K}(E_1)$, então em particular toda função em E_1 tem o mesmo valor em T e em $\mathcal{O}$. Isso implica que $T=\mathcal{O}$, por exemplo, a função coordenada x tem polo em $\mathcal{O}$ e nenhum outro polo.
(c) Se ϕ é separável, então de (a) vemos que

$$\#\phi^{-1}(Q) = \deg\phi \quad \text{para todo } Q\in E_2.$$

Assim, pelo corolário (2.2), ϕ é não ramificado, e fazendo $Q=\mathcal{O}$ temos

$$\#\ker\phi = \deg\phi.$$

Então de (b) vemos que

$$\#\mathrm{Aut}(\bar{K}(E_1)/\phi^*\bar{K}(E_2)) = [\bar{K}(E_1) : \phi^*\bar{K}(E_2)],$$

assim $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$ é uma extensão de Galois. □

Corolário 3.5. Sejam

$$\phi : E_1 \longrightarrow E_2 \quad \text{e} \quad \psi : E_1 \longrightarrow E_3$$

isogenias não constantes, e considere ϕ separável. Se

$$\ker \phi \subset \ker \psi,$$

então existe uma única isogenia

$$\lambda : E_2 \longrightarrow E_3$$

satisfazendo $\psi = \lambda \circ \phi$.

Prova. Como ϕ é separável, o teorema (3.3) nos diz que $\bar{K}(E_1)$ é uma extensão de Galois de $\phi^*\bar{K}(E_2)$. Então a inclusão $\ker \phi \subset \ker \psi$ e a identificação do ítem (3.3b) implica que todo elemento de $\mathrm{Gal}(\bar{K}(E_1)/\phi^*\bar{K}(E_2))$ fixa $\psi^*\bar{K}(E_3)$. Consequentemente, pela teoria de Galois, existe a inclusão

$$\psi^*\bar{K}(E_3) \subset \phi^*\bar{K}(E_2) \subset \bar{K}(E_1).$$

Pelo teorema (2.2b) temos o mapa

$$\lambda : E_2 \longrightarrow E_3$$

satisfazendo

$$\phi^*(\lambda^*\bar{K}(E_3)) = \psi^*\bar{K}(E_3),$$

e isso implica que

$$\lambda \circ \phi = \psi.$$

Como $\lambda(\mathcal{O}) = \lambda(\phi(\mathcal{O})) = \psi(\mathcal{O}) = \mathcal{O}$, segue que λ é uma isogenia. □

Proposição 3.10. Sejam E uma curva elíptica e Φ um subgrupo finito de E.

Existem uma única curva elíptica E' e uma isogenia separável

$$\phi : E \longrightarrow E' \quad \text{satisfazendo} \quad \ker \phi = \Phi.$$

Prova. Cada ponto $T \in \Phi$ nos dá um automorfismo τ_T^* de $\bar{K}(E)$. Seja $\bar{K}(E)^\Phi$ um subcorpo de $\bar{K}(E)$ fixado por todos os elementos de Φ. A teoria de Galois nos diz que $\bar{K}(E)$ é uma extensão de Galois de $\bar{K}(E)^\Phi$ com grupo de Galois isomorfo a Φ.

O corpo $\bar{K}(E)^\Phi$ tem grau de transcendência 1 sobre $\bar{K}$, assim do teorema (2.2c) existem uma única curva $C/\bar{K}$ e um morfismo finito

$$\phi : E \longrightarrow C \quad \text{satisfazendo} \quad \phi^* \bar{K}(C) = \bar{K}(E)^\Phi.$$

A seguir mostraremos que ϕ é não ramificado. Sejam $P \in E$ e $T \in \Phi$. Para toda função $f \in \bar{K}(C)$,

$$f(\phi(P+T)) = (\tau_T^* \circ \phi^*) f(P) = (\phi^* f)(P) = f(\phi(P)),$$

visto que τ_T^* fixa todo elemento de $\bar{K}(C)$. Segue de $\phi(P+T) = \phi(P)$. Sejam $Q \in C$ e $P \in E$ com $\phi(P) = Q$. Então

$$\phi^{-1}(Q) \supset \{P + T : T \in \Phi\}.$$

Entretanto, sabemos também do corolário (2.2) que

$$\#\phi^{-1}(Q) \leq \deg \phi = \#\Phi,$$

com a igualdade sendo válida se, e somente se, ϕ é não ramificado. Como os pontos $P+T$ são distintos quando T varia entre os pontos de Φ, concluímos que ϕ é não ramificado em Q. Assim ϕ é não ramificado.

Por fim, aplicamos a fórmula de Hurwitz, corolário (2.2), a ϕ. Como ϕ é não ramificado podemos escrever

$$2 \text{ gênero}(E) - 2 = (\deg \phi)(\text{gênero}(C) - 2).$$

Disso concluímos que C também tem gênero 1, então C é uma curva elíptica e ϕ é uma isogenia se tomarmos $\phi(\mathcal{O})$ como elemento neutro de C. □

3.6 O invariante diferencial

Seja E/K uma curva elíptica dada por

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Vimos no início do capítulo que o diferencial

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

não tem zeros nem polos. Veremos a seguir que ω é um invariante com respeito a translações.

Proposição 3.11. Sejam E e ω como acima, $Q \in E$, e $\tau_Q : E \to E$ uma translação por Q, conforme o exemplo (3.7). Então

$$\tau_Q^*\omega = \omega.$$

Prova. Escreva $x(P + Q)$ e $y(P + Q)$ em termos de $x(P), x(Q), y(P)$, e $y(Q)$ usando a fórmula de adição para curvas elípticas. Então calculamos de forma usual o diferencial $dx(P + Q)$ como função racional vezes $dx(P)$, tratando $x(Q)$ e $y(Q)$ como constantes. Desse modo para um valor Q fixado temos,

$$\frac{dx(P+Q)}{2y(P+Q)a_1x(P+Q) + a_3} = \frac{dx(P)}{2y(P) + a_1x(P) + a_3}.$$

Como Ω_E é um espaço vetorial um-dimensional, pela proposição (2.11), existe uma função $a_Q \in \bar{K}(E)^*$, dependendo a princípio de Q, tal que

$$\tau_Q^*\omega = a_Q\omega.$$

Note que $a_Q \neq 0$, pois τ_Q é um isomorfismo. Calculando temos,

$$\begin{aligned} \mathrm{div}(a_Q) &= \mathrm{div}(\tau_Q^*\omega) - \mathrm{div}(\omega) \\ &= \tau_Q^*\mathrm{div}(\omega) - \mathrm{div}(\omega) \\ &= 0 \qquad \text{pois } \mathrm{div}(\omega) = 0 \text{ da proposição (3.2).} \end{aligned}$$

Consequentemente a_Q é uma função em E sem zeros e sem polos, assim a proposição (2.3) nos diz que é uma constante, ou seja, $a_Q \in \bar{K}^*$. A seguir consideremos o mapa

$$f : E \longrightarrow \mathbb{P}^1, \qquad Q \longmapsto [a_Q, 1].$$

Do diferencial acima, vemos que a_Q pode ser escrito como função racional de $x(Q)$ e $y(Q)$. Então f é um mapa racional de E em $\mathbb{P}^1$, não sobrejetor, pois não vem como valores $[0,1]$ e $[1,0]$. Concluímos da proposição (2.3) e do teorema (2.1) que f é constante. Assim a_Q não depende de Q, e encontramos seu valor notando que

$$a_Q = a_{\mathcal{O}} = 1 \qquad \text{para todo } Q \in E.$$

Isso completa a prova de $\tau_Q^*\omega = \omega$. □

O cálculo diferencial é uma ferramenta de linearização. Assim vemos a enorme utilidade do invariante diferencial em uma curva elíptica, nos permitindo linearizar a lei de adição, que de outra forma seria bastante complicada, na curva.

Teorema 3.4. Sejam E e E' curvas elípticas, ω um invariante diferencial em E, e

$$\phi, \psi : E' \longrightarrow E$$

isogenias. Então

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega.$$

Os dois sinais de soma acima representam diferentes operações. A primeira adição ocorre em $\mathrm{Hom}(E', E)$, o qual é a lei de grupo em E. A segunda é a adição usual no espaço vetorial dos diferenciais Ω_E.

Prova. Se $\phi = [0]$ ou $\psi = [0]$, o resultado é imediato. Se $\phi + \psi = [0]$, então usando o fato de que

$$\psi^* = (-\phi)^* = \phi^* \circ [-1]^*,$$

é suficiente checar que

$$[-1]^*\omega = -\omega.$$

A fórmula da negação

$$[-1](x, y) = (x, -y - a_1x - a_3)$$

nos permite calcular

$$\begin{aligned}[-1]^* \left(\frac{dx}{2y + a_1x + a_3} \right) &= \frac{dx}{2(-y - a_1x - a_3) + a_1x + a_3} \\ &= -\frac{dx}{2y + a_1x + a_3},\end{aligned}$$

o que é o resultado desejado. Consideramos agora que ϕ, ψ, e $\phi + \psi$ são todos não nulos. Seja (x_1, y_1) e (x_2, y_2) coordenadas de Weierstrass "independentes" em E.

Por independentes entendemos que satisfazem a equação de Weierstrass dada em E, e mais nenhuma outra relação algébrica. Mais formalmente,

$$([x_1, y_1, 1], [x_2, y_2, 1])$$

fornece coordenadas para $E \times E$ estando dentro de $\mathbb{P}^2 \times \mathbb{P}^2$. Seja

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2),$$

assim x_3 e y_3 são combinações racionais de x_1, x_2, y_1, y_2 dados pela fórmula de adição em E. Além disso para qualquer (x, y), seja $\omega(x, y)$ o correspondente invariante diferencial,

$$\omega(x, y) = \frac{dx}{2y + a_1 x + a_3}.$$

Então, usando a fórmula de adição da página 65 e as regras da diferenciação, podemos expressar $\omega(x_3, y_3)$ em termos de $\omega(x_1, y_2)$ e $\omega(x_2, y_2)$. Disso temos

$$\omega(x_3, y_3) = f(x_1, y_1, x_2, y_2)\omega(x_1, y_1) + g(x_1, y_1, x_2, y_2)\omega(x_2, y_2),$$

onde f e g são funções racionais nas variáveis indicadas. Lembramos que pelo fato de que x_i e y_i satisfazem a equação de Weierstrass dada, os diferenciais dx_i e dy_i são relacionados por

$$(2y_i + a_1 x_i + a_3)dy_i = (3x_i^2 + 2a_2 x_i + a_4 - a_1 y_i)dx_i.$$

Dessa forma, $\omega(x_3, y_3)$ pode ser expresso como combinação $\bar{K}(x_1, y_1, x_2, y_2)$-linear de dx_1 e dx_2.

Afirmamos que f e g são identicamente 1. De fato, suponha que fixemos valores para x_2 e y_2, escolhendo algum $Q \in E$ e definindo

$$x_2 = x(Q) \qquad \text{e} \qquad y_2 = y(Q).$$

Então

$$dx_2 = dx(Q) = 0, \qquad \text{assim} \qquad \omega(x_2, y_2) = 0,$$

enquanto que por (3.11) temos que

$$\omega(x_3, y_3) = \tau_Q^* \omega(x_1, y_1) = \omega(x_1, y_1).$$

Substituindo na expressão para $\omega(x_3, y_3)$ encontramos que

$$f(x_1, y_1, x(Q), y(Q)) = 1$$

como função racional em $\bar{K}(x_1, y_1)$. Assim f não depende de x_1 e y_1, então $f \in \bar{K}(x_2, y_2)$. Mas também encontramos que $f(x_2, y_2)$ satisfaz $f(x(Q), y(Q)) = 1$ para todo ponto $Q \in E$, assim f deve ser identicamente 1. O mesmo argumento usamos para x_2 e y_2 no lugar de x_1 e y_1, mostrando que g é também identicamente 1.

Recapitulando, mostramos que se

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2) \qquad (+ \text{ como adição em } E)$$

então

$$\omega(x_3, y_3) = \omega(x_1, y_1) + \omega(x_2, y_2) \qquad (+ \text{ como adição em } \Omega_E).$$

Agora seja (x', y') coordenadas de Weierstrass em E' e escreva

$$(x_1, y_1) = \phi(x', y'), \qquad (x_2, y_2) = \psi(x', y'), \qquad (x_3, y_3) = (\phi + \psi)(x', y').$$

Substituindo em $\omega(x_3, y_3) = \omega(x_1, y_1) + \omega(x_2, y_2)$ ficamos com

$$(\omega \circ (\phi + \psi))\,(x', y') = (\omega \circ \phi)(x', y') + (\omega \circ \psi)(x', y'),$$

o que significa que

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega.$$

□

Corolário 3.6. Sejam ω um invariante diferencial para curva elíptica E, e $m \in \mathbb{Z}$. Então

$$[m]^*\omega = m\omega.$$

Prova. A afirmação é válida para $m = 0$, pois $[0]$ é o mapa constante, e é verdadeira para $m = 1$, pois $[1]$ é o mapa identidade. Suponha por indução que o corolário é válido para m. Mostremos para $[m + 1]$.

$$\begin{aligned} [m+1]^*\omega &= [m]^*\omega + [1]^*\omega && \text{pelo teorema anterior} \\ &= m\omega + \omega && \text{pela hipótese de indução} \\ &= (m+1)\omega \end{aligned}$$

Então pelo princípio de indução finita, $[m]^*\omega = m\omega$. □

Como primeira indicação de utilidade do invariante diferencial, faremos uma nova demonstração, menos computacional, para a proposição (3.9a).

Corolário 3.7. Sejam E/K uma curva elíptica e $m \in \mathbb{Z}$. Suponha que $m \neq 0$ em K. Então a multiplicação pelo m-mapa em E é um endomorfismo separável finito.

Prova. Seja ω um invariante diferencial em E. Então do corolário (3.6) e pelo fato de $m \neq 0$ temos que

$$[m]^*\omega = m\omega \neq 0,$$

assim $[m] \neq [0]$. Então $[m]$ é finito, e a proposição (2.11c) nos diz que $[m]$ é separável. □

Como segunda aplicação do teorema (3.4) e do corolário (3.6), examinaremos quando uma combinação linear envolvendo morfismo de Frobenius é separável.

Corolário 3.8. Sejam E uma curva elíptica definida sobre um corpo finito $\mathbb{F}_q$ de característica p, $\phi : E \to E$ o q-ésimo morfismo de Frobenius, exemplo (3.6), e $m, n \in \mathbb{Z}$. Então o mapa

$$m + n\phi : E \longrightarrow E$$

é separável se, e somente se, $p \not| m$. Em particular, o mapa $1 - \phi$ é separável.

Prova. Seja ω um invariante diferencial em E. Da proposição (2.11c) sabemos que o mapa $\psi : E \to E$ é inseparável se, e somente se, $\psi^*\omega = 0$. Aplicamos esse critério ao mapa $\psi = m + n\phi$. Usando o teorema (3.4) e seu corolário (3.6), calculamos

$$(m + n\phi)^*\omega = m\omega + n\phi^*\omega.$$

Note que $\phi^*\omega = 0$, pois ϕ é inseparável, ou, pelo cálculo direto,

$$\phi^*\left(\frac{dx}{2y + a_1x + a_3}\right) = \frac{d(x^q)}{2y^q + a_1x^q + a_3} = \frac{qx^{q-1}dx}{2y^q + a_1x^q + a_3} = 0.$$

Então

$$(m + n\phi)^*\omega = [m]^*\omega + [n]^* \circ \phi^*\omega = m\omega.$$

Como $m\omega = 0$ se, e somente se, $p|m$, obtemos o resultado desejado. □

Corolário 3.9. Sejam E/K uma curva elíptica e ω um invariante diferencial não nulo de E. Definimos o mapa de $\mathrm{End}(E)$ a $\bar{K}$ da forma:

$$\mathrm{End}(E) \longrightarrow \bar{K}, \qquad \phi \longmapsto a_\phi \quad \text{tal que } \phi^*\omega = a_\phi\omega.$$

(a) O mapa $\phi \mapsto a_\phi$ é homomorfismo entre aneis.
(b) O núcleo de $\phi \mapsto a_\phi$ é o conjunto dos endomorfismos inseparáveis de E.
(c) Se $\mathrm{char}(K) = 0$, então $\mathrm{End}(E)$ é um anel comutativo.

Prova. Como na demonstração da proposição (3.11), o fato de que Ω_E é um $\bar{K}(E)$-espaço vetorial de dimensão 1, a proposição (2.11) implica que $\phi^*\omega = a_\phi\omega$ para alguma função $a_\phi \in \bar{K}(E)$. Afirmamos que $a_\phi \in \bar{K}$. Isso é claro se $a_\phi = 0$, enquanto que se $a_\phi \neq 0$, usamos o fato de que $\mathrm{div}(\omega) = 0$ para calcular

$$\mathrm{div}(a_\phi) = \mathrm{div}(\phi^*\omega) - \mathrm{div}(\omega) = \phi^*\mathrm{div}(\omega) - \mathrm{div}(\omega) = 0.$$

Consequentemente a_ϕ não tem zeros nem polos, assim a proposição (2.3) diz que $a_\phi \in \bar{K}$.
(a) Usamos o teorema (3.4) para calcular

$$a_{\phi+\psi}\omega = (\phi \circ \psi)^*\omega = \psi^*(\phi^*\omega) = \psi^*(a_{phi}\omega) = a_\phi\psi^*(\omega) = a_\phi a_\psi\omega,$$

o que mostra que $a_{\phi\circ\psi} = a_\phi a_\psi$.
(b) Temos que

$$a_\phi = 0 \qquad \Longleftrightarrow \phi^*\omega = 0 \qquad \Longleftrightarrow \phi \text{ é inseparável, proposição (2.11c).}$$

(c) Se $\mathrm{char}(K) = 0$, então todo endomorfismo é separável, assim (b) nos diz que $\mathrm{End}(E)$ é imerso em $\bar{K}^*$. Então $\mathrm{End}(E)$ é comutativo. □

3.7 A Isogenia Dual

Seja $\phi : E_1 \to E_2$ uma isogenia não constante. Vimos na observação (2.3) que ϕ induz o mapa

$$\phi^* : \mathrm{Pic}^0(E_2) \longrightarrow \mathrm{Pic}^0(E_1).$$

Por outro lado, pela proposição (3.8), para $i = 1$ e 2 temos o isomorfismo de grupos

$$\kappa_i : E_1 \longrightarrow \mathrm{Pic}^0(E_i), \qquad P \longmapsto \text{classe de } (P) - (\mathcal{O}).$$

Isso nos dá um homomorfismo na direção oposta de ϕ, a saber, a composição

$$E_2 \xrightarrow{\kappa_2} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1.$$

Mais tarde nesta seção, verificaremos que esse mapa pode ser calculado como faremos a seguir. Sejam $Q \in E_2$, e escolha um $P \in E_1$ satisfazendo $\phi(P) = Q$. Então

$$\kappa_1^{-1} \circ \phi^* \circ \kappa_2(Q) = [\deg \phi](P).$$

Aqui não está claro que o homomorfismo $\kappa_1^{-1} \circ \phi^* \circ \kappa_2$ é uma isogenia, isto é, se é dado por um mapa racional. O processo para encontrar o ponto P satisfazendo $\phi(P) = Q$ envolve tomar raízes de várias equações polinomiais. Se ϕ é separável, precisaremos verificar que aplicando $[\deg \phi]$ a P obtemos a raiz conjugada aparecendo simetricamente. Se ϕ é inseparável, esta aproximação é mais complicada. Mostraremos agora que em todo caso existe uma isogenia que pode ser calculada da maneira descrita acima.

Teorema 3.5. Seja $E_1 \to E_2$ uma isogenia não constante de grau m.
(a) Existe uma única isogenia

$$\hat{\phi} : E_2 \longrightarrow E_1 \qquad \text{satisfazendo} \quad \hat{\phi} \circ \phi = [m].$$

(b) Como homomorfismo de grupos, $\hat{\phi}$ é igual a composição

$$\begin{array}{ccccccc} E_2 & \longrightarrow & \mathrm{Div}^0(E_2) & \xrightarrow{\phi^*} & \mathrm{Div}^0(E_1) & \xrightarrow{\text{soma}} & E_1, \\ Q & \longmapsto & (Q) - (\mathcal{O}) & & \sum n_P(P) & \longmapsto & \sum [n_P]P. \end{array}$$

Prova. (a) Primeiro mostraremos a unicidade. Suponha que $\hat{\phi}$ e $\hat{\phi}'$ são duas isogenias conforme o enunciado. Então

$$(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = [0].$$

Como ϕ é não constante, segue do teorema (2.1) que $\hat{\phi} - \hat{\phi}'$ deve ser constante, assim $\hat{\phi} = \hat{\phi}'$.

A seguir suponha que $\psi : E_2 \to E_3$ é outra isogenia não constante, digamos de grau n, e suponha sabermos que $\hat{\phi}$ e $\hat{\psi}$ existe. Então

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm].$$

Assim $\hat{\phi} \circ \hat{\psi}$ e $\widehat{\psi \circ \phi}$ são iguais. Então usando o corolário (2.3) para escrever uma isogenia arbitrária ϕ como uma composição, é suficiente provar a existencia de $\hat{\phi}$ quando ϕ é ou separável ou igual ao morfismo de Frobenius.

Caso 1. ϕ ***é separável.*** Como ϕ tem grau m, temos do teorema (3.3c) que

$$\#\ker\phi = m,$$

assim todo elemento de $\ker\phi$ tem ordem dividindo m, isto é,

$$\ker\phi \subset \ker[m].$$

Segue imediatamente do corolário (3.5) que existe uma isogenia

$$\hat{\phi} : E_2 \longrightarrow E_1 \qquad \text{satisfazendo} \qquad \hat{\phi}\circ\phi = [m].$$

Caso 2. ϕ ***é um morfismo de Frobenius.*** Se ϕ é o morfismo de Frobenius de potência q com $q = p^e$, então ϕ é claramente a composição do p-ésimo morfismo de Frobenius com ele mesmo e vezes. Então é suficiente provar que $\hat{\phi}$ existe se ϕ é o morfismo de Frobenius de potência p, assim em particular, $\deg\phi = p$ pela proposição (2.8).

Olhamos para a multiplicação pelo p-mapa em E. Seja ω um invariante diferencial. Então do corolário (3.6) e o fato de que $\mathrm{char}(K) = p$, vemos que

$$[p]^*\omega = p\omega = 0.$$

Concluímos da proposição (3.9c) que $[p]$ não é separável, e assim quando decompormos $[p]$ como morfismo de Frobenius seguido pelo mapa separável, do corolário (2.3), o morfismo de Frobenius aparece. Em outras palavras,

$$[p] = \psi\circ\phi^e$$

para algum inteiro $e \geq 1$ e alguma isogenia separável ψ. Então podemos tomar

$$\hat{\phi} = \psi\circ\phi^{e-1}.$$

(b) Seja $Q \in E_2$. Então a imagem de Q sob a composição indicada é

$$\begin{aligned}
&\text{soma}(\phi^*((Q)-(\mathcal{O}))) \\
&\quad = \sum_{P\in\phi^{-1}(Q)} [e_\phi(P)]P - \sum_{T\in\phi^{-1}(\mathcal{O})} [e_\phi(T)]T && \text{pela definição de } \phi^*, \\
&\quad = [\deg_i \phi]\left(\sum_{P\in\phi^{-1}(Q)} P - \sum_{T\in\phi^{-1}(\mathcal{O})} T\right) && \text{do teorema (3.3a)}, \\
&\quad = [\deg_i \phi]\circ[\#\phi^{-1}(Q)]P && \text{para qualquer } P\in\phi^{-1}(Q), \\
&\quad = [\deg\phi]P && \text{de (3.3a)}.
\end{aligned}$$

Mas pela construção,

$$\hat{\phi}(Q) = \hat{\phi}\circ\phi(P) = [\deg\phi]P,$$

assim os dois mapas são os mesmo. □

Definição 3.11. Seja $\phi : E_1 \to E_2$ uma isogenia. A isogenia dual a ϕ é a isogenia

$$\hat{\phi} : E_2 \longrightarrow E_1$$

dada pelo teorema (3.5a). (Estamos assumindo que $\phi \neq [0]$. Se $\phi = [0]$, então definimos $\hat{\phi} = [0]$.)

O próximo teorema nos dá uma propriedade básica da isogenia dual. Desse fato básico poderemos deduzir um número importante de corolários, incluindo a descrição do núcleo da multiplicação pelo m-mapa.

Teorema 3.6. Sejam

$$\phi : E_1 \longrightarrow E_2$$

uma isogenia:
(a) $m = \deg\phi$. Então

$$\hat{\phi}\circ\phi = [m] \quad \text{em } E_1 \qquad \text{e} \qquad \phi\circ\hat{\phi} = [m] \quad \text{em } E_2.$$

(b) $\lambda : E_2 \to E_3$ outra isogenia. Então

$$\widehat{\lambda\circ\phi} = \hat{\phi}\circ\hat{\lambda}.$$

(c) $\psi : E_1 \to E_2$ outra isogenia. Então

$$\widehat{\phi+\psi} = \hat{\phi}+\hat{\psi}.$$

(d) Para todo $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m] \qquad \text{e} \qquad \deg[m] = m^2.$$

(e)$\deg \hat{\phi} = \deg \phi$.
(f)$\hat{\hat{\phi}} = \phi$.

Prova. Se ϕ é constante, então o teorema segue, da mesma forma quando λ e ψ são constantes em (b) e (c). Assumiremos que todas as isogenias são não constantes.
(a) A primeira equação segue pela definição de $\hat{\phi}$. Para a segunda parte, consideramos

$$(\phi \circ \hat{\phi}) \circ \phi = \phi \circ [m] = [m] \circ \phi.$$

Então $\phi \circ \hat{\phi} = [m]$, pois ϕ é não constante.
(b) Escrevendo $n = \deg \lambda$, temos

$$(\hat{\phi} \circ \hat{\lambda}) \circ (\lambda \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm].$$

A unicidade vista em (3.5a) implica que

$$\hat{\phi} \circ \hat{\lambda} = \widehat{\lambda \circ \phi}.$$

(c) Sejam $x_1, y_1 \in K(E_1)$ e $x_2, y_2 \in K(E_2)$ coordenadas de Weierstrass. Consideremos E_2 como curva elíptica definida sobre o corpo $K(E_1) = K(x_1, y_1)$, caso em que a característica é 0. Tudo o que fizemos em curvas elípticas considera o fato em que o corpo de base seja perfeito. Seguindo, outra forma de dizer que $\phi : E_1 \to E_2$ é uma isogenia é notar que $\phi(x_1, y_1) \in E_2(K(x_1, y_1))$, e similarmente para $\psi(x_1, y_1)$ e $(\phi + \psi)(x_1, y_1)$. Agora considere o divisor

$$D = \operatorname{div}((\phi + \psi)(x_1, y_1)) - \operatorname{div}(\phi(x_1, y_1)) + \operatorname{div}(\psi(x_1, y_1)) + (\mathcal{O}) \in \operatorname{Div}_{K(x_1,y_1)}(E_2).$$

Pela definição de $\phi + \psi$ temos que $D = \mathcal{O}$, então o corolário (3.3) nos diz que D é linearmente equivalente a 0. Assim existe a função

$$f \in K(x_1, y_1)(E_2) = K(x_1, y_1, x_2, y_2)$$

a qual, quando considerada como função de x_2 e y_2, tem divisor D.

Agora, vendo de outra forma, considere f como função de x_1 e y_1. Em outras palavras, veremos f como função em E_1 considerado como curva elíptica definida sobre $K(x_2, y_2)$. Suponha que $P_1 \in E_1(\overline{K(x_2, y_2)})$ é um ponto satisfazendo $\phi(P_1) =$

(x_2, y_2). Examinando D, mais precisamente o termo $-\mathrm{div}(\phi(x_1, y_1))$, vemos que f tem polo em P_1, isto é, a função $f(x_1, y_1; x_2, y_2)$ tem polo se x_1, y_1, x_2, y_2 satisfazendo $(x_2, y_2) = \phi(x_1, y_1)$. Então

$$\mathrm{ord}_{P_1}(f) = e_\phi(P_1).$$

Similarmente, f tem polo em P_1 se $(x_2, y_2) = \psi(P_1)$, e tem zero em P_1 se $(x_2, y_2)(\phi + \psi)(P_1)$. Segue que como função de x_1 e y_1, o divisor de f tem a forma

$$(\phi + \psi)^*((x_2, y_2)) - \phi^*((x_2, y_2)) - \psi^*((x_2, y_2)) + \sum n_i(P_1) \in \mathrm{Div}_{\overline{K(x_2,y_2)}}(E_1),$$

onde os P_i's estão em $E_1(\bar{K})$, isto é, $\sum n_i(P_i) \in \mathrm{Div}_{\bar{K}}(E_1)$. como esse é o divisor da função, ele soma a $\mathcal{O}$, assim usando o teorema (3.5b), concluímos que o ponto

$$\widehat{(\phi + \psi)}(x_2, y_2) - \hat{\phi}(x_2, y_2) - \hat{\psi}(x_2, y_2)$$

não depende de (x_2, y_2), isto é, ele está em $E_1(\bar{K})$. Escrevendo $(x_2, y_2) = \mathcal{O}$ mostra que é igual a $\mathcal{O}$, o que demonstra que

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}.$$

(d) É válido para $m = 0$ pela definição, e também para o caso em que $m = 1$. Usando (c) com $\phi = [m]$ e $\psi = [1]$ temos

$$\widehat{[m + 1]} = \widehat{[m]} + \widehat{[1]},$$

e por indução temos que $\widehat{[m]} = [m]$ vale para todo m.

Agora seja $d = \deg[m]$ considerando a multiplicação pelo m-mapa. Assim

$$\begin{aligned} [d] &= \widehat{[m]} \circ [m] && \text{definição de isogenia dual} \\ &= [m^2] && \text{pois } \widehat{[m]} = [m]. \end{aligned}$$

Usando a proposição (3.9b), que diz que o anel de endomorfismo de uma curva elíptica é um $\mathbb{Z}$-módulo livre de torção, segue que $d = m^2$.
(e) Seja $m = \deg \phi$. Usando (d) e (a), temos que

$$m^2 = \deg[m] = \deg(\phi \circ \hat{\phi}) = (\deg \phi)(\deg \hat{\phi}) = m(\deg \hat{\phi}).$$

Então $m = \deg \hat{\phi}$.
(f) Novamente, seja $m = \deg \phi$. Então, usando (a), (b) e (c), temos que

$$\hat{\phi} \circ \phi = [m] = \widehat{[m]} = \widehat{\hat{\phi} + \phi} = \hat{\phi} \circ \hat{\hat{\phi}}.$$

Portanto

$$\phi = \hat{\hat{\phi}}.$$

□

Definição 3.12. Seja A um grupo abeliano. A função

$$d : A \longrightarrow \mathbb{R}$$

é uma forma quadrática se satisfaz as seguintes condições:
(i) $d(\alpha) = d(-\alpha)$ para todo $\alpha \in A$.
(ii) O produto

$$A \times A \longrightarrow \mathbb{R}, \qquad (\alpha, \beta) \longmapsto d(\alpha + \beta) - d(\alpha) - d(\beta),$$

é bilinear.
A forma quadrática d é positiva definida se satisfaz:
(iii) $d(\alpha) \geq 0$ para todo $\alpha \in A$.
(iv) $d(\alpha) = 0$ se, e somente se, $\alpha = 0$.

Corolário 3.10. Sejam E_1 e E_2 curvas elípticas. O mapa de grau

$$\deg : \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$$

é uma forma quadrática positiva e definida.

Prova. Este mapa satisfaz os ítens (i), (iii) e (iv), ficando apenas (ii) para demonstrarmos, ou seja, que o par

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

é bilinear. Para provarmos isso, usamos o mapa injetor

$$[\ ] : \mathbb{Z} \longrightarrow \mathrm{End}(E_1)$$

e calculamos

$$\begin{aligned}
[\langle \phi, \psi \rangle] &= [\deg(\phi + \psi)] - [\deg(\phi)] - [\deg(\psi)] \\
&= \widehat{(\phi + \psi)} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\
&= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi \qquad \text{do teorema (3.6c).}
\end{aligned}$$

Usando (3.6c) novamente, vemos que a última expressão é linear em ϕ e em ψ, o que conclui a prova. □

Corolário 3.11. Sejam E uma curva elíptica e $m \in \mathbb{Z}$ com $m \neq 0$. Então:
(a) $\deg[m] = m^2$.
(b) Se $m \neq 0$ em K, isto é, se ou $\mathrm{char}(K) = 0$ ou $p = \mathrm{char}(K) > 0$ e $p \not| m$, então

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(c) Se $\mathrm{char}(K) = p > 0$, então uma das seguintes afirmações é verdadeira:

$$(i) \quad E[p^e] = \{\mathcal{O}\} \quad \text{para todo } e = 1, 2, 3, \ldots$$
$$(ii) \quad E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}} \quad \text{para todo } e = 1, 2, 3, \ldots$$

(Lembramos que $E[m]$ é outra notação para $\ker[m]$, o conjunto dos pontos de ordem m em E.)

Prova. (a) Foi provado no teorema (3.6d).
(b) Pelo que assumimos em m e o fato de que $\deg[m] = m^2$, temos que $[m]$ é mapa finito e separável. Consequentemente do teorema (3.3c),

$$\#E[m] = \deg[m] = m^2.$$

Além disso, para todo inteiro d que divide m, temos similarmente que

$$\#E[d] = d^2.$$

Escrevendo o grupo finito $E[m]$ como produto de grupos cíclicos, vemos que a única possibilidade é

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(c) Seja ϕ o p-ésimo morfismo de Frobenius. Então

$$\begin{aligned} \#E[p^e] &= \deg_s[p^e] && \text{do teorema (3.3a),} \\ &= (\deg_s(\hat{\phi} \circ \phi))^e && \text{do teorema (3.6a),} \\ &= (\deg_s \hat{\phi})^e && \text{da proposição (2.8b).} \end{aligned}$$

Do teorema (3.6e) e da proposição (2.8c) temos

$$\deg \hat{\phi} = \deg \phi = p,$$

assim existem dois casos: $\hat{\phi}$ separável ou não. Se $\hat{\phi}$ é inseparável, então $\deg_s \hat{\phi} = 1$, assim

$$\#E[p^e] = 1 \qquad \text{para todo } e.$$

Caso contrário $\hat{\phi}$ é separável, assim $\deg_s \hat{\phi} = p$ e

$$\#E[p^e] = p^e \qquad \text{para todo } e.$$

Novamente escrevendo $E[p^e]$ como produto de grupos cíclicos, vemos que

$$E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}}.$$

□

3.8 O Módulo de Tate

Sejam E/K uma curva elíptica e $m \geq 2$ um inteiro, relativamente primo com a $\mathrm{char}(K)$ se $\mathrm{char}(K) > 0$. Como vimos,

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}},$$

um isomorfismo entre grupos. Entretanto, o grupo $E[m]$ vem com uma estrutura de grupo bem maior. Por exemplo, cada elemento σ do grupo de Galois $G_{\bar{K}/K}$ age em $E[m]$, pois se $[m]P = \mathcal{O}$, então

$$[m](P^\sigma) = ([m]P)^\sigma = \mathcal{O}^\sigma = \mathcal{O}.$$

Assim obtemos a representação

$$G_{\bar{K}/K} \longrightarrow \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

onde o último isomorfismo envolve a escolha de uma base para $E[m]$. Individualmente, para cada m, essas representações não são completamente satisfatórias, pois é geralmente mais fácil tratar com representações cuja matriz tem coeficientes num anel de característica 0. Vamos colocar em forma as representações mod m, variando m, a fim de criar uma representação na característica 0. Para fazer

isso, imitamos a construção do limite inverso dos inteiros l-ádicos $\mathbb{Z}_\ell$ de um grupo finito $\mathbb{Z}/\ell^n\mathbb{Z}$.

Definição 3.13. Sejam E uma curva elíptica e $\ell \in \mathbb{Z}$ um primo. O módulo ℓ-ádico de Tate de E é o grupo

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

o limite inverso tomado com respeito ao mapa

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

Como cada $E[\ell^n]$ é um $\mathbb{Z}/\ell^n\mathbb{Z}$-módulo, vemos que o módulo de Tate tem estrutura natural como $\mathbb{Z}_\ell$-módulo. Além disso, como a multiplicação pelo l-mapa é sobrejetiva, a topologia do limite inverso em $T_\ell(E)$ é equivalente a topologia ℓ-ádica que possui por ser $\mathbb{Z}_\ell$-módulo.

Proposição 3.12. Como $\mathbb{Z}_\ell$-módulo, o módulo de Tate tem a seguinte estrutura:
(a) $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ se $\ell \neq \mathrm{char}(K)$.
(b) $T_p(E) \cong \{0\}$ *ou* $\mathbb{Z}$ se $p = \mathrm{char}(K) > 0$.

Prova. Segue do teorema (3.6b,c). □

A ação de $G_{\bar{K}/K}$ em cada $E[\ell^n]$ comuta com a multiplicação pelo ℓ-mapa, usado para formar o limite inverso, assim $G_{\bar{K}/K}$ também age em $T_\ell(E)$. Além disso, como o "quase"-finito grupo $G_{\bar{K}/K}$ age continuamente em cada grupo finito $E[\ell^n]$, a ação resultante em $T_\ell(E)$ também é contínua.

Definição 3.14. A representação ℓ-ádica (de $G_{\bar{K}/K}$ associada a E) é o homomorfismo

$$\rho_\ell : G_{\bar{K}/K} \longrightarrow \mathrm{Aut}(T_\ell(E))$$

induzido pela ação de $G_{\bar{K}/K}$ nos pontos de ℓ^n-torção de E.

De agora em diante ℓ se refere a um número primo diferente da caraterística de K.

Observação 3.5. Se escolhermos uma $\mathbb{Z}_\ell$-base para $T_\ell(E)$, obtemos a representação

$$G_{\bar{K}/K} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell),$$

e então usamos a inclusão natural $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell$, dando a representação

$$G_{\bar{K}/K} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Desse modo obtemos uma representação de dimensão dois para $G_{\bar{K}/K}$ sobre um corpo de característica 0. Mais intrinsecamente, podemos evitar a escolha de base pelo uso do mapa natural

$$\rho_\ell : G_{\bar{K}/K} \longrightarrow \mathrm{Aut}(T_l(E)) \hookrightarrow \mathrm{Aut}(T_l(E)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Observação 3.6. A construção acima é análoga à seguinte: Seja

$$\mu_{\ell^{n+1}} \xrightarrow{\zeta \mapsto \zeta^\ell} \mu_{\ell^n},$$

e então tomando o limite inverso ficamos com o módulo de Tate de K.

$$T_\ell(\mu) = \varprojlim_n \mu_{\ell^n}.$$

(Mais formalmente, $T_\ell(\mu)$ é módulo de Tate do grupo multiplicativo $\bar{K}^*$.) Como grupo abstrato temos

$$\mu_{\ell^n} \cong \mathbb{Z}/\ell^n\mathbb{Z} \qquad \text{e} \qquad T_\ell(\mu) \cong \mathbb{Z}_\ell.$$

Além disso, a ação natural de $G_{\bar{K}/K}$ em cada μ_{ℓ^n} induz uma ação em $T_\ell(\mu)$, assim obtemos uma representação 1-dimensional

$$G_{\bar{K}/K} \longrightarrow \mathrm{Aut}(T_\ell(\mu)) \cong \mathbb{Z}_\ell^*.$$

Para $K = \mathbb{Q}$ a representação ciclotômica é sobrejetiva, pois os polinômios ciclotômicos de potência ℓ são irredutíveis sobre $\mathbb{Q}$.

O módulo de Tate é uma ferramenta útil para estudar isogenias. Seja

$$\phi : E_1 \longrightarrow E_2$$

uma isogenia entre curvas elípticas. Então ϕ induz os mapas

$$\phi : E_1[\ell^n] \longrightarrow E_2[\ell^n],$$

e então induz um mapa $\mathbb{Z}_\ell$-linear

$$\phi_\ell : T_\ell(E_1) \longrightarrow T_\ell(E_2).$$

Obtemos então o homomorfismo natural

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)).$$

Além disso, se $E_1 = E_2 = E$, então o mapa

$$\mathrm{End}(E) \longrightarrow \mathrm{End}(T_\ell(E))$$

é um homomorfismo par entre anéis. O seguinte teorema nos dá uma forte informação sobre a estrutura de $\mathrm{Hom}(E_1, E_2)$.

Teorema 3.7. Sejam E_1 e E_2 curvas elípticas e seja $\ell \neq \mathrm{char}(K)$ um primo. Então o mapa natural

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)), \qquad \phi \mapsto \phi_\ell,$$

é injetivo.

Prova. Primeiramente vamos provar a seguinte afirmação:

> Seja $M \subset \mathrm{Hom}(E_1, E_2)$ um subgrupo finitamente gerado, e seja
> $M^{\mathrm{div}} = \{\phi \in \mathrm{Hom}(E_1, E_2) : [m] \circ \phi \in M \text{ para algum inteiro } m \geq 1\}$.
> Então M^{div} é finitamente gerado.

Para provar isso, estendemos o mapa grau a um espaço vetorial de dimensão finita $M \otimes \mathbb{R}$, com a topologia natural de $\mathbb{R}$. Então o mapa de grau é contínuo, assim o conjunto

$$U = \{\phi \in M \otimes \mathbb{R} : \deg \phi < 1\}$$

é uma vizinhança aberta de 0. Além disso, como pela proposição (3.9b) $\mathrm{Hom}(E_1, E_2)$ é um $\mathbb{Z}$-módulo livre de torção, existe uma inclusão natural

$$M^{\mathrm{div}} \subset M \otimes \mathbb{R}.$$

Consequentemente, temos que

$$M^{\mathrm{div}} \cap U = \{0\},$$

uma vez que toda isogenia não nula tem grau no mínimo um. Portanto M^{div} é um subgrupo discreto do espaço vetorial $M \otimes \mathbb{R}$, assim é finitamente gerado. Isso completa a prova da afirmação acima.

Voltamos para a prova do teorema (3.7). Seja $\phi \in \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$, e suponha que $\phi_\ell = 0$. Seja

$$M \subset \mathrm{Hom}(E_1, E_2)$$

um subgrupo finitamente gerado com a propriedade de que $\phi \in M \otimes \mathbb{Z}_\ell$. Então, com a mesma notação usada acima, o grupo M^{div} é finitamente gerado, assim também é livre, pois a proposição (3.9b) nos diz que é livre de torção. Seja

$$\psi_1, \ldots, \psi_t \in \mathrm{Hom}(E_1, E_2)$$

uma base para M^{div}, e escreva

$$\phi = \alpha_1\psi_1 + \cdots + \alpha_t\psi_t \quad \text{com} \quad \alpha_1, \ldots, \alpha_t \in \mathbb{Z}_\ell.$$

Agora escolhemos algum $n \geq 1$ e $a_1, \ldots, a_t \in \mathbb{Z}$ com

$$a_i \equiv \alpha_i \pmod{\ell^n}.$$

Então assumindo que $\phi_\ell = 0$ temos que a isogenia

$$\psi = [a_1] \circ \psi_1 + \cdots + [a_t] \circ \psi_t \in \mathrm{Hom}(E_1, E_2)$$

se anula em $E_1[\ell^n]$. Segue do corolário (3.5) que ψ se fatora através de $[\ell^n]$, assim existe uma isogenia

$$\lambda \in \mathrm{Hom}(E_1, E_2) \qquad \text{satisfazendo} \qquad \psi = [\ell^n] \circ \lambda.$$

Além disso, $\lambda \in M^{\mathrm{div}}$, então existem inteiros $b_i \in \mathbb{Z}$ tais que

$$\lambda = [b_1] \circ \psi_1 + \cdots + [b_t] \circ \psi_t.$$

Então, como os ψ_i's formam uma $\mathbb{Z}$-base para M^{div}, o fato de que $\psi = [\ell^n] \circ \lambda$ implica que

$$a_i = \ell^n b_i,$$

e portanto

$$\alpha_i \equiv 0 \pmod{\ell^n}.$$

Isso vale para todo n, assim concluímos que $\alpha_i = 0$, e então que $\phi = 0$. □

Observação 3.7. O fato de usarmos M^{div} ao invés de M, é porque é essencial que ϕ, ψ e λ sejam escritos em termos de uma $\mathbb{Z}$-base que não dependa da escolha de ℓ^n.

Corolário 3.12. Sejam E_1 e E_2 curvas elípticas. Então

$$\mathrm{Hom}(E_1, E_2)$$

é um $\mathbb{Z}$-módulo livre de posto no máximo 4.

Prova. Sabemos da proposição (3.9b) que $\mathrm{Hom}(E_1, E_2)$ é livre de torção. Isso implica que

$$\mathrm{rank}_{\mathbb{Z}_\ell}\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \leq \mathrm{rank}_{\mathbb{Z}_\ell}\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)).$$

Por fim, escolhendo uma $\mathbb{Z}_\ell$-base para $T_\ell(E_1)$ e $T_\ell(E_2)$, vemos da proposição (3.12a) que

$$\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)) = M_2(\mathbb{Z}_\ell)$$

é um grupo aditivo de matriz 2×2 com coeficientes em $\mathbb{Z}_\ell$. O posto de $M_2(\mathbb{Z}_\ell)$ com relação a $\mathbb{Z}_\ell$ é 4, o que mostra que o posto de $\mathrm{Hom}(E_1, E_2)$ é no máximo 4. □

Observação 3.8. Por definição, uma isogenia é definida sobre K se comutar com a ação $G_{\bar{K}/K}$. Similarmente, podemos definir

$$\mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$$

o grupo dos mapas $\mathbb{Z}_\ell$-lineares de $T_\ell(E_1)$ a $T_\ell(E_2)$ que comutam com a ação $G_{\bar{K}/K}$ dados pela representação ℓ-ádica. Então temos o homomorfismo

$$\mathrm{Hom}_K(E_1, E_2) \times \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2)),$$

e o teorema (3.7) mostra que esse homomorfismo é injetor. O fato importante é que muitas vezes ele é um isomorfismo.

Teorema 3.8. Seja $\ell \neq \mathrm{char}(K)$ um número primo. O mapa

$$\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$$

é um isomorfismo em duas situações:
(a) K é um corpo finito (Tate [5])
(b) K é corpo de números. (Faltings [6,7])

Observação 3.9. Poderíamos questionar a respeito do tamanho da imagem de $\rho_\ell(G_{\bar{K}/K})$ em $\mathrm{Aut}(T_\ell(E))$. O teorema seguinte fornece uma resposta para corpos de números.

Teorema 3.9. (Serre) Sejam K corpo de números e E/K uma curva elíptica sem múltiplicação complexa.
(a) $\rho_\ell(G_{\bar{K}/K})$ é um índice finito em $\mathrm{Aut}(T_\ell(E))$ para todo primo $\ell \neq \mathrm{char}(K)$.
(b) $\rho_\ell(G_{\bar{K}/K}) = \mathrm{Aut}(T_\ell(E))$ para quase todo número primo ℓ.
Prova. Veja [13] e [14].

3.9 O Grupo de Automorfismo

Se uma curva elíptica é dada por uma equação de Weierstrass, é em geral uma tarefa não trivial determinar a estrutura exata do seu anel de endomorfismo. A situação é bem mais simples quando se trata do grupo de automorfismo.

Teorema 3.10. Seja E/K uma curva elíptica. Então seu grupo de automorfismo $\mathrm{Aut}(E)$ é um grupo finito de ordem dividindo 24. Mais precisamente, a ordem de $\mathrm{Aut}(E)$ é dada pela seguinte tabela:

$\#\mathrm{Aut}(E)$	$j(E)$	$\mathrm{char}(K)$
2	$j(E) \neq 0, 1728$	—
4	$j(E) = 1728$	$\mathrm{char}(K) \neq 2, 3$
6	$j(E) = 0$	$\mathrm{char}(K) \neq 2, 3$
12	$j(E) = 0 = 1728$	$\mathrm{char}(K) = 3$
24	$j(E) = 0 = 1728$	$\mathrm{char}(K) = 2$

Prova. Considere $\mathrm{char}(K) \neq 2, 3$. Então E é dado pela seguinte equação:

$$E : y^2 = x^3 + Ax + B,$$

e todo automorfismo de E tem a forma

$$x = u^2 x', \qquad y = u^3 y'.$$

Se $AB \neq 0$, isto é se $j(E) \neq 0, 1728$, então as únicas possibilidades são $u = \pm 1$. Similarmente, Se $B = 0$, então $j(E) = 1728$ com $u^4 = 1$, e se $A = 0$, então $j(E) = 0$ com $u^6 = 1$. Assim $\mathrm{Aut}(E)$ é cíclico de ordem 2, 4 ou 6, dependendo se $AB \neq 0$, $B = 0$, ou $A = 0$. □

Corolário 3.13. Sejam E/K uma curva sobre um corpo de característica diferente de 2 e 3, e

$$n = \begin{cases} 2 & \text{se } j(E) \neq 0, 1728, \\ 4 & \text{se } j(E) = 1728, \\ 6 & \text{se } j(E) = 0. \end{cases}$$

Então existe um isomorfismo natural de $G_{\bar{K}/K}$-módulos

$$\mathrm{Aut}(E) \cong \mu_n.$$

Prova. Verificamos no teorema anterior que o mapa

$$[\ ] : \mu_n \longrightarrow E, \qquad [\zeta](x, y) = (\zeta^2 x, \zeta^3 y),$$

é um isomorfismo de grupos abstratos. Este mapa comuta com a ação $G_{\bar{K}/K}$, e consequentemente é um isomorfismo de $G_{\bar{K}/K}$-módulos. □

Capítulo 4

Curvas Elípticas Sobre Corpos de Números

O objetivo deste capítulo é provar o teorema de Mordell-Weil que diz que o grupo $E(K)$ é finitamente gerado. A partir desta informação e pelo teorema de classificação de grupos abelianos finitamente gerados o grupo $E(K)$ tem a forma:

$$E(K) \simeq \prod \mathbb{Z}_{n_i} \times \mathbb{Z}^r,$$

onde a parte finita é denominada o grupo de torção da curva elíptica, $E(K)_{tor}$, e o inteiro não negativo r como o *posto* de $E(K)$.

Para demonstrarmos o teorema de Mordell-Weill, precisamos da sua versão fraca, que não será demonstrada aqui. Como referência veja [1].

Teorema 4.1. (Versão Fraca do Teorema de Mordell-Weil) Seja E/K curva elíptica e $m \geq 2$ um número inteiro. Então

$$E(K)/mE(K)$$

é um grupo finito.

4.1 O procedimento de descida

Provaremos nesta seção que o conjunto dos pontos racionais de uma curva elíptica é finitamente gerado. Já sabemos que o grupo $E(K)/mE(K)$ é finito. Mas esta informação não é suficiente para nosso propósito pois, por exemplo, se considerarmos $K = \mathbb{R}$ podemos escrever $\mathbb{R}/m\mathbb{R} = 0$, para todo inteiro $m \geq 1$, sendo $\mathbb{R}$ um grupo que não é finitamente gerado.

Teorema 4.2. (Teorema da Descida) Seja A um grupo abeliano. Suponha que exista uma função

$$h : A \to \mathbb{R},$$

com as seguintes propriedades:
(i) Seja $Q \in A$. Existe uma constante C_1, dependendo de A e Q, tal que

$$h(P + Q) \leq 2h(P) + C_1, \forall P \in A.$$

(ii) Existem um inteiro $m \geq 2$ e uma constante C_2 dependendo de A, tal que,

$$h(mP) \geq m^2 h(P) - C_2, \forall P \in A.$$

(iii) Para toda constante C_3, o conjunto $\{P \in A | h(P) \leq C_3\}$ é finito. Suponha ainda que para todo inteiro m como no item (ii), o grupo quociente A/mA é finito. Então A é finitamente gerado.

Prova. Sejam $P \in A$, e $Q_1, ..., Q_r \in A$ os representantes das classes em A/mA. Escreva

$$P = mP_1 + Q_{i_1} \quad \text{para algum } 1 \leq i_1 \leq r.$$

Continuando desta forma,

$$\begin{aligned} P_1 &= mP_2 + Q_{i_2} \\ &\vdots \\ P_{n-1} &= mP_n + Q_{i_n}. \end{aligned}$$

Agora para qualquer j:

$$\begin{aligned} h(P_j) &\leq \frac{1}{m^2}[h(mP_j) + C_2] \text{ de (ii)} \\ &= \frac{1}{m^2}[h(P_{j-1} - Q_{i_j}) + C_2] \\ &\leq \frac{1}{m^2}[2h(P_{j-1}) + C_1' + C_2] \text{ de (i)}, \end{aligned}$$

onde tomamos C_1' como sendo o máximo das constantes que aparece em cada vez que usamos (i), para $Q = -Q_i$, $1 \leq i \leq r$. Note que C_1' e C_2 não dependem de P.

Usando a desigualdade acima repetidas vezes, começando por P_n, chegamos em

P da seguinte forma:

$$\begin{aligned} h(P_n) &\leq \big(\frac{2}{m^2}\big)^n h(P) + \big[\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \cdots + \frac{2^{n-1}}{m^{2n}}\big](C_1' + C_2) \\ &< \big(\frac{2}{m^2}\big)^n h(P) + \frac{C_1' + C_2}{m^2 - 2} \\ &\leq 2^{-n} h(P) + (C_1' + C_2)/2 \quad \text{pois } m \geq 2. \end{aligned}$$

Segue que, para n suficientemente grande,

$$h(P_n) \leq 1 + (C_1' + C_2)/2.$$

Como vimos que vale

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j},$$

segue que todo $P \in A$ é combinação linear dos pontos no conjunto

$$\{Q_1, ..., Q_r\} \cup \{Q \in A \ : \ h(Q) \leq 1 + (C_1' + C_2)/2\}.$$

De (iii), este conjunto é finito, o que prova que A é finitamente gerado. □

Observação 4.1. Para tornar o teorema da descida prático precisamos encontrar os geradores do grupo A. Para isso calculamos as constantes $C_1 = C_1(Q_i)$ para cada representante de A/mA. Em seguida calculamos também as constantes C_2, e por fim, dada qualquer constante C_3, determinamos os elementos do conjunto finito $\{P \in A \ : \ h(P) \leq C_3\}$.

4.2 O teorema de Mordell-Weil sobre $\mathbb{Q}$

Nesta seção provaremos o seguinte caso especial do teorema de Mordell-Weil:

Teorema 4.3. Seja $E/\mathbb{Q}$ uma curva elíptica. Então o grupo $E(\mathbb{Q})$ é finitamente gerado.

Sabemos da primeira seção que $E(\mathbb{Q})/2E(\mathbb{Q})$ é finito. Queremos aplicar o teorema da descida neste caso, então precisamos definir o que vem a ser função altura em $E(\mathbb{Q})$ e mostrar que tem as requeridas propriedades.

Definição 4.1. Seja $t = \frac{p}{q} \in \mathbb{Q}$ uma fração reduzida. A altura neste caso é definida como $H(t) = max\{|p|, |q|\}$.

Definição 4.2. A altura (logarítmica) em $E(\mathbb{Q})$, relativa a uma dada equação de Weierstrass, é a função:

$$h_x : E(\mathbb{Q}) \to \mathbb{R}$$

$$h_x(P) = \begin{cases} \log H(x(P)), & P \neq \mathcal{O} \\ 0, & P = \mathcal{O} \end{cases}$$

$h_x(P)$ é sempre não negativo.

Lema 4.1. Seja $E/\mathbb{Q}$ curva elíptica dada pela equação de Weierstrass

$$E \ : \ y^2 = x^3 + Ax + B, \quad A, \ B \in \mathbb{Z}.$$

a) Seja $P_0 \in E(\mathbb{Q})$. Existe uma constante C_1 dependendo de P_0, A e B tal que

$$h_x(P + P_0) \leqslant 2h_x(P) + C_1, \ \ \forall P \in E(\mathbb{Q});$$

b) Existe uma constante C_2 dependendo de A e B tal que

$$h_x([2]P) \geqslant 4h_x(P) - C_2 \quad \forall P \in E(\mathbb{Q});$$

c) Para toda constante C_3 o conjunto

$$\{P \in E(\mathbb{Q}) \ : \ h_x(P) \leqslant C_3\}$$

é finito.

Prova. Podemos assumir que $C_1 > \max\{h_x(P_0), \ h_x([2]P_0)\}$, o que garante que o ítem a) é verdadeiro se $P_0 = \mathcal{O}$ ou se $P \in \{\mathcal{O}, \ \pm P_0\}$. Em qualquer outro caso escrevemos

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \qquad \text{e} \qquad P_0 = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right),$$

onde temos as frações totalmente simplificadas. Pela fórmula de adição,

$$x(P + P_0) = \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0.$$

Expandindo esta expressão e usando o fato de que esses pontos estão na curva E vemos que

$$x(P+P_0) = \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}.$$

Usando a função altura de número racional e "cancelando" alguns termos nesta fração de modo que a altura fique menor, temos a estimativa:

$$H(x(P+P_0)) \leq C_1' m$$

onde C_1' é uma expressão simple em termos de A, B, a_0, b_0 e d_0. Como $H(x(P)) = \max\{|a|,\ |d|^2\}$, temos quase o que queremos, a menos do termo $|bd|$ que aparece no m. Para resolver este problema usamos o fato de que o ponto P está na curva elíptica, então ele satisfaz a equação de Weierstrass, de modo que:

$$b^2 = a^3 + Aad^4 + Bd^6.$$

Assim

$$|b| \leq C_1'' \max\{|a|^{3/2},\ |d|^3\},$$

que combinada com a estimativa para $H(x(P+P_0))$ fica:

$$H(x(P+P_0)) \leq C_1 \max\{|a|^2,\ |d|^4\} = C_1 H(x(P))^2.$$

Aplicando o logarítmo temos o resultado que queríamos.
(b) Escolhendo C_2 tal que

$$C_2 \geq \max\{h_x(T)\ :\ T \in E(\mathbb{Q})[2]\},$$

podemos assumir que $[2]P \neq \mathcal{O}$. Então escrevendo $P = (x, y)$, a fórmula da duplicação nos diz que:

$$x([2]P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

É conveniente definirmos os polinômios homogêneos:

$$F(X,Z) = X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4,$$
$$G(X,Z) = 4X^3Z + 4AXZ^3 + 4BZ^4.$$

Se escrevermos $x = x(P) = a/b$ como fração reduzida, então $x([2]P)$ pode ser escrito

como razão entre inteiros:

$$x([2]P) = F(a,b)/G(a,b).$$

Em contraste com o ítem anterior desta demonstração, estamos procurando um limite inferior para $H(x([2]P))$, então se mostra importante que façamos simplificações de termos tanto no numerador quanto no denominador. A partir daqui, a ideia é usar o fato que $F(X,1)$ e $G(X,1)$ são relativamente primos como polinômios, então eles geram todo o ideal de $\mathbb{Q}[X]$, o que nos leva à lista de equações, que não serão demonstradas aqui:

Afirmação: Sejam $\Delta = 4A^3 + 27B^2$,

$$F(X,Z) = X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4,$$
$$G(X,Z) = 4X^3Z + 4AXZ^3 + 4BZ^4,$$
$$f_1(X,Z) = 12X^2Z + 16AZ^3,$$
$$g_1(X,Z) = 3X^3 - 5AXZ^2 - 27BZ^3,$$
$$f_2(X,Z) = 4(4A^3+27B^2)X^3 - 4A^2BX^2Z + 4A(3A^3+22B^2)XZ^2 + 12B(A^3+8B^2)Z^3,$$
$$g_2(X,Z) = A^2BX^3 + A(5A^3+32B^2)X^2Z + 2B(13A^3+96B^2XZ^2 - 3A^2(A^3+8B^2)Z^3).$$

Então as seguintes igualdades são válidas em $\mathbb{Q}[X,Z]$:

$$f_1(X,Z)F(X,Z) - g_1(X,Z)G(X,Z) = 4\Delta Z^7$$
$$f_2(X,Z)F(X,Z) + g_2(X,Z)G(X,Z) = 4\Delta X^7.$$

Prova. Como $F(X,Z)$ e $G(X,Z)$ são polinômios homogêneos relativamente primos (pois $\Delta \neq 0$), igualdades desse tipo devem existir. Para encontrar os polinômios f_1, g_1, f_2, g_2 podemos usar o algoritmo Euclidiano ou a teoria de resultantes. □

Retornando para a prova do lema, considere

$$\delta = \text{mdc}(F(a,b),\ G(a,b)),$$

como sendo o "cancelamento" para a fração $x([2]P)$. Das equações

$$f_1(a,b)F(a,b) - g_1(a,b)G(a,b) = 4\Delta b^7,$$
$$f_2(a,b)F(a,b) - g_2(a,b)G(a,b) = 4\Delta a^7,$$

vemos que δ divide 4Δ. Isso nos fornece

$$|\delta| \leq |4\Delta|,$$

e consequentemente

$$H(x([2]P)) \geq \frac{\max\{|F(a,b)|, |G(a,b)|\}}{|4\Delta|}.$$

Por outro lado, obtemos das equações anteriores as seguintes estimativas

$$|4\Delta b^7| \leq 2\max\{|f_1(a,b)|, |g_1(a,b)|\}\max\{|F(a,b)|, |G(a,b)|\},$$
$$|4\Delta a^7| \leq 2\max\{|f_2(a,b)|, |g_2(a,b)|\}\max\{|F(a,b)|, |G(a,b)|\}.$$

Observando as expressões para f_1, f_2, g_1, g_2 em (VIII.4.3), temos

$$\max\{|f_1(a,b)|, |g_1(a,b)|, |f_2(a,b)|, |g_2(a,b)|\} \leq C\max\{|a|^3, |b|^3\},$$

onde C é uma constante que depende de A e B. Combinando estas três desigualdades temos

$$\max\{|4\Delta a^7|, |4\Delta b^7|\} \leq 2C\max\{|a|^3, |b|^3\}\max\{|F(a,b)|, |G(a,b)|\}.$$

Cancelando $\max\{|a|^3, |b|^3\}$ da desigualdade obtemos

$$\frac{\max\{|F(a,b)|, |G(a,b)|\}}{|4\Delta|} \geq (2C)^{-1}\max\{|a|^4, |b|^4\},$$

e então usando o fato que $\max\{|a|, |b|\} = H(x(P))$ obtemos

$$H(2([2]P)) \geq (2C)^{-1}H(x(P))^4.$$

(c) Para qualquer constante C, o conjunto

$$\{t \in \mathbb{Q} : H(t) \leq C\}$$

é finito. De fato, ele tem no máximo $(2C+1)^2$ elementos, visto que o numerador e o denominador de t são inteiros entre $-C$ e C. Além disso, dado qualquer valor para x, existem no máximo dois valores para y onde (x, y) é ponto de E. Portanto

$$\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$$

é também um conjunto finito. □

Provar o teorema (4.3) é agora uma questão de aplicar o que já provamos.

Prova. de (4.3). Sabemos do teorema (4.1) que $E(\mathbb{Q}/2E(\mathbb{Q}))$ é finito. Segue do lema (4.1) que a função altura

$$h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

satisfaz as condições necessárias para aplicarmos o procedimento de descida, com $m = 2$. Concluímos do teorema (4.2) que $E(\mathbb{Q})$ é finitamente gerado. □

4.3 Alturas em Espaços Projetivos

Com o objetivo de demonstrar o caso geral do teorema de Mordell-Weil, precisamos definir a função altura nos pontos K-racionais de uma curva elíptica. Curvas elípticas são dadas como subconjuntos de espaços projetivos, assim neste estudo teremos a função altura definida em todo espaço projetivo, e então na próxima seção examinaremos suas propriedades quando restrita aos pontos de uma curva elíptica.

Exemplo 4.1. Seja $P \in \mathbb{P}^N(\mathbb{Q})$ um ponto com coordenadas racionais. Como $\mathbb{Z}$ é um domínio de ideais principais, podemos encontrar coordenadas homogêneas

$$P = [x_0, \ldots, x_N]$$

satisfazendo

$$x_0, \ldots, x_N \in \mathbb{Z} \quad \text{e} \quad \text{mdc}(x_0, \ldots, x_N) = 1.$$

Então uma medida natural para a altura de P é

$$H(P) = \max\{|x_0|, \ldots, |x_N|\}.$$

Com esta definição, fica claro que para qualquer constante C, o conjunto

$$\{P \in \mathbb{P}^N(\mathbb{Q}) \leq C\}$$

é um conjunto finito, e possui $(2C + 1)^N$ elementos. Esta é o tipo de propriedade que precisamos para o procedimentos de descida descrito no teorema (4.2).

Se generalizarmos o exemplo (4.1) para corpos numéricos arbitrários, teremos a

dificuldade de que o anel de inteiros não precisa ser domínio de ideais principais.

Definição 4.3. O conjunto padrão dos valores absolutos em $\mathbb{Q}$, que denotaremos por $M_{\mathbb{Q}}$, consiste do seguinte:
(i) $M_{\mathbb{Q}}$ contém um valor absoluto arquimediano, definido por

$$|x|_\infty = \text{ valor absoluto usual } = \max\{x, -x\}.$$

(ii) Para cada primo $p \in \mathbb{Z}$, o conjunto $M_{\mathbb{Q}}$ contém um valor absoluto não arquimediano p-ádico definido por

$$\left|p^n \frac{a}{b}\right|_p = p^{-n} \quad \text{para } a, b \in \mathbb{Z} \text{ satisfazendo } p \not| ab.$$

O conjunto dos valores absolutos padrão em um corpo de números K, denotado por M_K, é o conjunto de todos os valores absolutos em K cuja restrição a $\mathbb{Q}$ é um dos valores absolutos em $M_{\mathbb{Q}}$.

Definição 4.4. Seja $v \in M_K$. O grau local em v, denotado por n_v, é

$$n_v = [K_v : \mathbb{Q}_v],$$

onde K_v e $\mathbb{Q}_v$ denotam os completamentos de K e $\mathbb{Q}$ com respeito ao valor absoluto v.

Com essa definição, estabelecemos dois fatos básicos da teoria algébrica dos números, que usaremos daqui em diante mas que não será demonstrado aqui.

Fórmula de Extensão. Sejam $L/K/\mathbb{Q}$ uma torre de corpos numéricos, e $v \in M_K$. Então

$$\sum_{\substack{w \in M_L \\ w|v}} n_w = [L : K] n_v.$$

(com $w|v$ estamos dizendo que w restrito a K é igual a v.)

Fórmula do Produto. Seja $x \in K^*$. Então

$$\prod_{v \in M_K} |x|_v^{n_v} = 1.$$

Para as demonstrações dessas fórmulas veja [15, II §1 e V §1].

Definição 4.5. Seja $P \in \mathbb{P}^N(K)$ um ponto com coordenadas homogêneas

$$P = [x_0, \ldots, x_N], \qquad x_0, \ldots, x_N \in K.$$

A altura de P (relativa a K) é

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v}.$$

Proposição 4.1. Seja $P \in \mathbb{P}^N(K)$.
(a) A altura $H_K(P)$ não depende da escolha das coordenadas homogêneas para P.
(b) A altura satisfaz

$$H_K(P) \geq 1.$$

(c) Seja L/K uma extensão finita. Então

$$H_L(P) = H_K(P)^{1/[K:\mathbb{Q}]}.$$

Prova. (a) Qualquer outra escolha de coordenadas homogêneas para P tem a forma $[\lambda x_0, \ldots, \lambda x_N]$, para algum $\lambda \in K^*$. Usando a fórmula do produto, temos

$$\begin{aligned}\prod_{v \in M_K} \max\{|\lambda x_0|_v, \ldots, |\lambda x_N|_v\}^{n_v} &= \prod_{v \in M_K} |\lambda|^{n_v} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v} \\ &= \prod_{v \in M_K} \max\{|x_0|v, \ldots, |x_N|_v\}^{n_v}.\end{aligned}$$

(b) Dado qualquer ponto P no espaço projetivo, podemos encontrar coordenadas homogêneas para P de modo que uma de suas coordenadas seja 1. Então todo fator no produto que define $K_K(P)$ é no mínimo 1.
(c) Calculando temos

$$\begin{aligned}H_L(P) &= \prod_{w \in M_L} \max\{|x_i|_w\}^{n_w} \\ &= \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max\{|x_i|_v\}^{n_w} \quad \text{pois } x_i \in K, \\ &= \prod_{v \in M_K} \max\{|x_i|_v\}^{[L:K]n_v} \quad \text{da fórmula de extensão}, \\ &= H_K(P)^{[L:K]}.\end{aligned}$$

Observação 4.2. Se $K = \mathbb{Q}$, então $H_{\mathbb{Q}}$ faz sentido como ideia intuitiva de função altura. Para ver isso, seja $P \in \mathbb{P}^N(\mathbb{Q})$ e escolha coordenadas homogêneas $[x_0, \ldots, x_N]$ para P com $x_i \in \mathbb{Z}$ e $\text{mdc}(x_0, \ldots, x_N) = 1$. Então, para qualquer valor absoluto não

arquimediano $v \in M_{\mathbb{Q}}$, temos que $|x_i|_v \leq 1$ para todo i e $|x_i|_v = 1$, para pelo menos um i. Então da definição de $H_{\mathbb{Q}}(P)$, o único fator que contribui para a definição do produto é o valor absoluto não arquimediano, então

$$H_{\mathbb{Q}}(P) = \max\{|x_0|_\infty, \ldots, |x_N|_\infty\}.$$

Em particular, segue que para qualquer constante C, o conjunto

$$\{P \in \mathbb{P}^N(\mathbb{Q}) : H_{\mathbb{Q}}(P) \leq C\}$$

é finito.

Definição 4.6. Seja $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$. A altura absoluta de P, denotada por $H(P)$, é definida como segue. Escolha um corpo de número K tal que $P \in \mathbb{P}^N(K)$. Então

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]},$$

onde tomamos a raíz positiva. Vimos da proposição (4.1c) que $H(P)$ é bem definida, independente da escolha de K, e (4.1b) implica que $H(P) \geq 1$.

A seguir faremos um estudo de como a função altura muda sob mapas entre espaços projetivos. Relembrando definição:

Definição 4.7. Um morfismo de grau d entre espaços projetivos é um mapa

$$F : \mathbb{P}^N \longrightarrow \mathbb{P}^M, \quad F(P) = [f_0(P), \ldots, f_M(P)],$$

onde $f_0, \ldots, f_M \in \bar{\mathbb{Q}}[X_0, \ldots, X_N]$ são polinômios homogêneos de grau d não tendo zero em comum em $\bar{\mathbb{Q}}^N$ além de $x_0 = \cdots = x_N = 0$. Se F pode ser escrito usando polinômios f_i com coeficientes em K, então F é dito ser definido sobre K.

Teorema 4.4. Seja $F : \mathbb{P}^N \longrightarrow \mathbb{P}^M$ um morfismo de grau d. Então existem constantes positivas C_1 e C_2 dependendo de F, tal que

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d \quad \text{para todo } P \in \mathbb{P}^N(\bar{\mathbb{Q}}).$$

Prova. Escrevendo $F = [f_0, \ldots, f_M]$ com f_i polinômios homogêneos sem zero em comum, e $P = [x_0, \ldots, x_N] \in \mathbb{P}^N(\bar{\mathbb{Q}})$ um ponto com coordenadas algébricas. Seja K um corpo de números que contém $x_0, \ldots, x_N$ e também contém todos os coeficientes de todos os f_i. Para cada valor absoluto $v \in M_K$, sejam

$$|P|_v = \max_{0 \leq i \leq N} |x_i|_v \quad \text{e} \quad |F(P)|_v = \max_{0 \leq j \leq M} |f_j(P)|_v,$$

e também definimos

$$|F|_v = \max\{|a|_v : a \text{ é coeficiente de algum } f_i\}.$$

Então, da definição de altura, temos

$$H_K(P) = \prod_{v \in M_K} |P|_v^{n_v} \quad \text{e} \quad H_K(F(P)) = \prod_{v \in M_K} |F(P)|_v^{n_v},$$

o que nos faz definir

$$H_K(F) = \prod_{v \in M_K} |F|_v^{n_v}.$$

Em outras palavras, $H_K(F) = H([a_0, a_1, \ldots])$, onde os a_js são os coeficientes de f_i. Sejam $C_1, C_2, \ldots$ constantes que dependem apenas de M, N e d, e

$$\epsilon(v) = \begin{cases} 1 & \text{se } v \in M_K^\infty, \\ 0 & \text{se } v \in M_K^0. \end{cases}$$

Para ilustrar a utilidade da função ϵ, observamos que a desigualdade triangular pode ser escrita como

$$|t_1 + \cdots + t_n|_v \leq n^{\epsilon(v)} \max\{|t_1|_v, \ldots, |t_n|_v\}$$

para todo $v \in M_K$, arquimediano ou não.

Com essa notação, retomamos a demonstração do teorema (4.4). Comecemos pelo limite superior. Seja $v \in M_K$. A desigualdade triangular nos diz

$$|f_i(P)|_v \leq C_1^{\epsilon(v)} |F|_v |P|_v^d,$$

pois f_i é homogêneo de grau d. Aqui C_1 poderia ser igual ao número de termos em f_i, que é no máximo $\binom{N+d}{N}$, ou seja, o número de monômios de grau d em $N+1$ variáveis. Como a estimativa vale para todo i, encontramos

$$|F(P)|_v \leq C_1^{\epsilon(v)} |F|_v |P|_v^d.$$

Elevando a v_n-ésima potência, multiplicando por todo $v \in M_K$, tomando a $[K : \mathbb{Q}]$-ésima raiz e usando a fórmula de extensão, temos o limite superior desejado

$$H(F(P)) \leq C_1 H(F) H(P)^d,$$

onde usamos as fórmulas

$$\sum_{v\in M_K} \epsilon(v) n_v = \sum_{v\in M_K^\infty} n_v = [K:\mathbb{Q}].$$

Observamos que nesta parte da demonstração não usamos o fato de que os f_is não têm zeros em comum. Entretanto, usaremos essa propriedade para demonstrar a outra parte da desigualdade.

Considere o conjunto

$$\{Q \in \mathbb{A}^{N+1}(\bar{\mathbb{Q}}) : f_0(Q) = \cdots = f_M(Q) = 0\}$$

consistindo apenas do ponto $(0,\ldots,0)$. Segue do Nullstellensatz [2, I.1.3A] e [8, Teorema 1.6] que o ideal gerado por $f_0,\ldots,f_M \in \bar{\mathbb{Q}}[X_0,\ldots,X_N]$ contém alguma potência de cada um dos $X_0,\ldots,X_N$, pois cada X_i também se anula no ponto $(0,\ldots,0)$. Assim existem polinômios $g_{ij} \in \bar{\mathbb{Q}}[X_0,\ldots,X_N]$ e um inteiro $e \geq 1$ tal que

$$X_i^e = \sum_{j=0}^{M} g_{ij} f_j \quad \text{para cada } 0 \leq i \leq N.$$

Trocando K por uma extensão finita se necessário, podemos assumir que cada um dos $g_{ij} \in K[X_0,\ldots,X_N]$, e descartando todo termo do lado direito exceto aqueles que são homogêneos de grau e, podemos considerar que cada g_{ij} é homogêneo de grau $e-d$. Além disso podemos estabelecer a seguinte notação:

$$\begin{aligned} |G|_v &= \max\{|b|_v : b \text{ é coeficiente de algum } g_{ij}\}, \\ H_K(G) &= \prod_{v\in M_K} |G|_v^{n_v}. \end{aligned}$$

Observamos que e e $H_K(G)$ podem ser limitados em termos de M, N, d e $H_K(F)$.

Mostremos agora que e e $H_K(G)$ não dependem do ponto P. Como $P = [x_0;\ldots;x_N]$, vemos que a fórmula para X_i^e implica que

$$\begin{aligned} |x_i|_v^e = \left|\sum_{j=0}^{M} g_{ij}(P) f_j(P)\right|_v &\leq C_2^{\epsilon(v)} \max_{0\leq j\leq M} |g_{ij}(P) f_j(P)|_v \\ &\leq C_2^{\epsilon(v)} \max_{0\leq j\leq M} |f_{ij}(P)||F(P)|_v. \end{aligned}$$

Tomando o máximo sobre i temos

$$|P|_v^e \leq C_2^{\epsilon(v)} \max_{\substack{0\leq j\leq M \\ 0\leq i\leq N}} |g_{ij}(P)|_v |F(P)|_v.$$

Cada um dos g_{ij} é homogêneo de grau $e-d$, assim aplicando a desigualdade triangular obtemos

$$|g_{ij}(P)|_v \leq C_3^{\epsilon(v)}|G|_v|P|_v^{e-d},$$

onde C_3 pode depender de e, mas como observado anteriormente, podemos limitar e em termos de M, N e d. Substituindo a última desigualdade na anterior e multiplicando por $|P|^{d-e}$ temos

$$|P|_v^e \leq C_v^{\epsilon(v)}|G|_v|F(P)|_v.$$

Elevando a n_v-ésima potência, multiplicando por $v \in M_K$ e tomando a $[K:\mathbb{Q}]$-ésima raiz obtemos o resultado desejado. □

Observação 4.3. Como indicado na prova do teorema (4.4), a dependência de C_1 em F na desigualdade

$$C_1 H(P)^d \leq H(F(P))$$

não é totalmente direta. É possível expressar C_1 em termos dos coeficientes de certos polinômios cuja existência é garantida pelo Nullstelensatz, mas esse método nos leva a uma estimativa bem pobre.

Registraremos a seguir o caso especial do teorema (4.4) para um automorfismo de $\mathbb{P}^N$.

Corolário 4.1. Seja $A \in \mathrm{GL}_{N+1}(\bar{\mathbb{Q}})$. A multiplicação pela matriz A induz um automorfismo $A : \mathbb{P}^N \to \mathbb{P}^N$. Existem constantes positivas C_1 e C_2, em função dos coeficientes da matriz A, tal que

$$C_1 H(P) \leq H(AP) \leq C_2 H(P) \quad \text{para todo } P \in \mathbb{P}^N(\bar{\mathbb{Q}}).$$

Prova. É o teorema (4.4) anterior para o caso de morfismos de grau um. □

A seguir investigaremos a relação entre os coeficientes de um polinômio e a altura de suas raízes.

Notação. Para $x \in \bar{\mathbb{Q}}$, seja

$$H(x) = H([x,1]),$$

e similarmente para $x \in K$, seja

$$H_K(x) = H_K([x,1]).$$

Teorema 4.5. Seja

$$f(T) = a_0T^d + a_1T^{d-1} + \cdots + a_d = a_0(T - \alpha_1)\cdots(T - \alpha_d) \in \bar{\mathbb{Q}}[T]$$

um polinômio de grau d. Então

$$2^{-d}\prod_{j=1}^{d} H(\alpha_j) \leq H([a_0, \ldots, a_d]) \leq 2^{d-1}\prod_{j=1}^{d} H(\alpha_j).$$

Prova. Primeiramente note que a desigualdade a ser demonstrada permanece a mesma quando $f(T)$ é multiplicada por uma constante não nula. Então basta provarmos o resultado para um polinômio mônico, assim assumimos que $a_0 = 1$. Seja $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$, e para $v \in M_K$, considere

$$\epsilon(v) = \begin{cases} 2 & \text{se } v \in M_K^{\infty}, \\ 1 & \text{se } v \in M_K^{0}. \end{cases}$$

Note que essa notação difere da notação usada na prova do teorema anterior. Nesse contexto, a desigualdade triangular fica

$$|x + y|_v \leq \epsilon(v)\max\{|x|_v, |y|_v\} \quad \text{para } v \in M_K \text{ e } x, y \in K.$$

Se $v \in M_K^0$ e $|x|_v \neq |y|_v$, então a desigualdade triangular se torna uma igualdade. Queremos mostrar que

$$\epsilon(v)^{-d}\prod_{j=1}^{d}\max\{|\alpha_j|_v, 1\} \leq \max_{0\leq i\leq d}\{|\alpha_i|_v\} \leq \epsilon(v)^{d-1}\prod_{j=1}^{d}\max\{|\alpha_j|_v, 1\}.$$

Uma vez feito isso, elevando a n_v-ésima potência, multiplicando por todo $v \in M_K$, e extraindo a $[K : \mathbb{Q}]$-ésima raiz temos o resultado desejado.

A prova é feita por indução sobre $d = \deg(f)$. Para $d = 1$ temos que $f(T) = T - \alpha_1$, assim a desigualdade é clara. Considere agora que o resultado é válido para todos os polinômios de grau $d - 1$, com raízes em K. Escolha um índice k tal que

$$|\alpha_k|_v \geq |\alpha_j|_v \quad \text{para todo } 0 \leq j \leq d,$$

e defina o polinômio

$$\begin{aligned} g(T) &= (T - \alpha_1)\cdots(T - \alpha_{k-1})(T - \alpha_{k+1})\cdots(T - \alpha_d) \\ &= b_0T^{d-1} + b_1T^{d-2} + \cdots + b_{d-1}. \end{aligned}$$

Assim $f(T) = (T - \alpha_k)g(T)$, e então comparando os coeficientes

$$a_i = b_i - \alpha_k b_{i-1}.$$

Se fizermos $b_{-1} = b_d = 0$, então o resultado vale para todo $0 \leq i \leq d$. Comecemos com a desigualdade superior:

$$\begin{aligned}
\max_{0\leq i\leq d}\{|a_i|_v\} &= \max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} \\
&\leq \epsilon(v) \max_{0\leq i\leq d}\{|b_i|_v, |\alpha_k b_{i-1}|_v\} \qquad \text{desigualdade triangular,} \\
&\leq \epsilon(v) \max_{0\leq i\leq d}\{|b_i|_v\} \max\{|\alpha_k|_v, 1\} \\
&\leq \epsilon(v)^{d-1} \prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\} \qquad \text{hipótese de indução aplicado a } g.
\end{aligned}$$

A seguir, provaremos a desigualdade inferior considerando dois casos. Primeiro, se $|\alpha_k|_v \leq \epsilon(v)$, então escolhendo o índice k temos

$$\prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\} \leq \max\{|\alpha_k|_v, 1\}^d \leq \epsilon(v)^d,$$

assim temos o resultado. Suponha agora que $|\alpha_k|_v > \epsilon(v)$, e lembre que $a_0 = 1$. Então

$$\max_{0\leq i\leq d}\{|a_i|_v\} = \max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} \geq \epsilon(v)^{-1} \max_{0\leq i\leq d-1}\{|b_i|_v\}\{|\alpha_k|_v, 1\}.$$

A última desigualdade será igualdade para $v \in M_K^0$, enquanto que para $v \in M_K^\infty$ estamos usando o fato

$$\begin{aligned}
\max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} &\geq (|\alpha_k|_v - 1) \max_{0\leq i\leq d-1}\{|b_i|_v\} \\
&> \epsilon(v)^{-1}|\alpha_k|_v \max_{0\leq i\leq d-1}\{|b_i|_v\}, \quad \text{pois } |\alpha_k|_v > \epsilon(v) = 2.
\end{aligned}$$

Aplicando a hipótese de indução a g temos a desigualdade inferior, o que completa a prova. □

Nossa primeira aplicação do teorema (4.5) é mostrar que existem um número finito de pontos de altura limitada num espaço projetivo. Para isso, primeiramente mostramos que a ação do grupo de Galois não afeta a altura de um ponto.

Teorema 4.6. Sejam $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$ e $\sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}$. Então

$$H(P^\sigma) = H(P).$$

Prova. Seja $K/\mathbb{Q}$ um corpo tal que $P \in \mathbb{P}^N(K)$. O corpo K pode não ser extensão de Galois sobre $\mathbb{Q}$, mas nesse caso σ nos dá um isomorfismo $\sigma : K \xrightarrow{\sim} K^\sigma$, e σ identificando os conjuntos de valores absolutos de K e K^σ,

$$\sigma : M_K \xrightarrow{\sim} M_K^\sigma \qquad v \longmapsto v^\sigma.$$

Se $x \in K$ e $v \in M_K$, então o valor absoluto associado v^σ satisfaz $|x^\sigma| = |x|_v$. É claro que σ também induz um isomorfismo $K_v \xrightarrow{\sim} K_{v^\sigma}^\sigma$, assim o grau local satisfaz $n_v = n_{v^\sigma}$. Assim podemos calcular:

$$\begin{aligned} H_{K^\sigma}(P^\sigma) &= \prod_{w \in M_{K^\sigma}} \max\{|x_i^\sigma|_w\}^{n_w} \\ &= \prod_{v \in M_K} \max\{|x_i^\sigma|_{v^\sigma}\}^{n_{v^\sigma}} \\ &= \prod_{v \in M_K} \max\{|x_i|_v\}^{n_v} \\ &= H_K(P). \end{aligned}$$

Como $[K : \mathbb{Q}] = [K^\sigma : \mathbb{Q}]$, obtemos que $H(P^\sigma) = H(P)$, como queríamos. □

Teorema 4.7. Sejam C e d constantes. Sendo $\mathbb{Q}(P)$ o corpo mínimo de definição de P, então o conjunto

$$\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : H(P) \leq C \text{ e } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

é finito. Em particular, para qualquer corpo de números K,

$$\{P \in \mathbb{P}^N(K) : H_K(P) \leq C\}$$

é um conjunto finito.

Prova. Seja $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$, com $P[x_0, \ldots, x_N]$ coordenadas homogêneas de P com

$x_j = 1$, para algum $0 \leq j \leq N$. Então $\mathbb{Q} = \mathbb{Q}(x_0, \ldots, x_N)$, e podemos estimar

$$\begin{aligned} H(\mathbb{Q}(P)) &= \prod_{v \in M_{\mathbb{Q}(P)}} \max\{|x_i|_v\}^{n_v} \\ &\geq \max_{0 \leq i \leq N} \left(\prod_{v \in M_{\mathbb{Q}(P)}} \max\{|x_i|_v, 1\}^{n_v} \right) \\ &= \max_{0 \leq i \leq N} H_{\mathbb{Q}(P)}(x_i). \end{aligned}$$

Assim, se $H(P) \leq C$ e $[\mathbb{Q}(P) : \mathbb{Q}] \leq d$, então

$$\max_{0 \leq i \leq N} H_{\mathbb{Q}(P)}(x_i) \leq C \qquad \text{e} \qquad \max_{0 \leq i \leq N} [\mathbb{Q}(x_i) : \mathbb{Q}] \leq d.$$

Assim para demonstrarmos o resultado basta demonstrarmos que

$$\{x \in \bar{\mathbb{Q}} : H(x) \leq C \text{ e } [\mathbb{Q}(x) : \mathbb{Q}] \leq d\}$$

é um conjunto finito, reduzindo assim ao caso em que $N = 1$. Suponha que $x \in \bar{\mathbb{Q}}$ e $e = [\mathbb{Q}(x) : \mathbb{Q}]$, ou seja, $e \leq d$. Além disso, sejam $x_1, \ldots, x_e \in \bar{\mathbb{Q}}$ os conjugados de x, onde definimos $x_1 = x$. O polinômio mínimo de x sobre $\mathbb{Q}$ é

$$f_x(T) = (T - x_1) \cdots (T - x_e) = T^e + a_1 T^{e-1} + \cdots + a_e \in \mathbb{Q}[T].$$

Podemos calcular

$$\begin{aligned} H([1, a_1, \ldots, a_e]) &\leq 2^{e-1} \prod_{j=1}^{e} H(x_j) && \text{de (4.5)}, \\ &= 2^{e-1} H(x)^e && \text{de (4.6)}, \\ &\leq (2C)^d && \text{pois } H(x) \leq C \text{ e } e \leq d. \end{aligned}$$

Como $a_i \in \mathbb{Q}$, para todo i, segue que para quaisquer C e d, existem finitas possibilidades para o polinômio $f_x(T)$. Como cada polinômio $f_x(T)$ tem no máximo d raízes em K, contribuindo com no máximo d elementos para nosso conjunto, temos que ele é finito, como queríamos. □

4.4 Alturas em Curvas Elípticas

Faremos nesta seção o uso da teoria geral de alturas como desenvolvida anteriormente, a fim de construirmos funções altura entre curvas elípticas. O teorema principal nos mostrará claramente a relação entre a função altura e a lei de

grupo numa curva elíptica. Do seu corolário deduziremos os resultados que restaram e que nos ajudarão a demonstrar o teorema de Mordell-Weil para o caso de corpos numéricos arbitrários.

Sejam f e g funções reais definidas num conjunto $\mathcal{S}$. Escrevemos

$$f = g + \mathcal{O}(1)$$

se existir constantes C_1 e C_2 tal que

$$C_1 \leq f(P) - g(P) \leq C_2, \qquad \text{para todo } P \in \mathcal{S}.$$

Se apenas a primeira desigualdade é satisfeita, então escrevemos $f \geq g + \mathcal{O}(1)$, e similarmente se apenas a segunda desigualdade for verdadeira, então escrevemos $f \leq g + \mathcal{O}(1)$.

Seja E/K uma curva elíptica. Relembremos do exemplo (2.2) que qualquer função não constante $f \in \bar{K}(E)$ determina um morfismo sobrejetor, que também denotaremos por f,

$$f : E \longrightarrow \mathbb{P}^1, \qquad P \longmapsto \begin{cases} [1,0] & \text{se } P \text{ é polo de } f, \\ [f(P),1] & \text{caso contrário.} \end{cases}$$

Pode ser razoável usar f para definir a função altura em $E(\bar{K})$ escrevendo $H_f(P) = H(f(P))$. Entretanto, a função algura H tende a ser multiplicativa, como por exemplo no teorema (4.4), enquanto que para o que queremos é mais conveniente ter uma função altura que tenha propriedade aditiva. Isso nos coloca diante da seguinte definição:

Definição 4.8. A altura absoluta logarítmica num espaço projetivo é a função

$$h : \mathbb{P}^N(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}, \qquad h(P) = \log H(P).$$

Note que pela proposição (4.1b), $h(P) \geq 0$ para todo P.

Definição 4.9. Seja E/K uma curva elíptica, e seja $f \in \bar{K}(E)$ uma função. A altura em E relativa a f é a função

$$h_f : E(\bar{K}) \longrightarrow \mathbb{R}, \qquad h_f(P) = h(f(P)).$$

Faremos a seguir um dos resultados visto na seção anterior, onde tínhamos como universo todo o espaço projetivo.

Proposição 4.2. Sejam E/K uma curva elíptica, $f \in K(E)$ uma função não constante. Então para qualquer constante C, o conjunto

$$\{P \in E(K) : h_f(P) \leq C\}$$

é um conjunto finito de pontos.

Prova. A função $f \in K(E)$ é definida sobre K, assim temos que $f(P) \in \mathbb{P}^1(K)$, para $P \in E(K)$. Consequentemente f nos dá um mapa finito um a um do conjunto C considerado ao conjunto

$$\{Q \in \mathbb{P}^1(K) : H(Q) \leq e^C\}.$$

Finalmente, sabemos do teorema (4.7) que este conjunto é finito. □

O próximo teorema mostrará a relação fundamental entre funções altura e adição em uma curva elíptica.

Teorema 4.8. Sejam E/K uma curva elíptica e $f \in K(E)$ uma função par. Então para todo $P, Q \in E(\bar{K})$ temos

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + \mathcal{O}(1).$$

As constantes intrínsecas a $\mathcal{O}(1)$ dependem da curva E e da função f, mas independe dos pontos P e Q.

Prova. Escolha uma equação para E/K da forma

$$E : y^2 = x^3 + Ax + B.$$

Começamos provando o teorema para uma função particular $f = x$. o caso geral será visto a seguir como um corolário.

Como $h_x(\mathcal{O}) = 0$ e $h_x(-P) = h_x(P)$, o resultado desejado é claro se $P = \mathcal{O}$ ou se $Q = \mathcal{O}$. Assuma que $P \neq \mathcal{O}$ e $Q \neq \mathcal{O}$, e escreva

$$\begin{aligned} x(P) &= [x_1, 1], & x(Q) &= [x_2, 1], \\ x(P+Q) &= [x_3, 1], & x(P-Q) &= [x_4, 1]. \end{aligned}$$

Onde x_3 ou x_4 podem ser ∞ se $P = \pm Q$. Utilizando a fórmula de adição da página

65 podemos escrever

$$\begin{aligned} x_3 + x_4 &= \frac{2(x_1+x_2)(A+x_1x_2)+4B}{(x_1+x_2)^2-4x_1x_2}, \\ x_3x_4 &= \frac{(x_1x_2-A)^2-4B(x_1+x_2)}{(x_1+x_2)^2-4x_1x_2}. \end{aligned}$$

Definimos o mapa $g : \mathbb{P}^2 \to \mathbb{P}^2$ por

$$g([t,u,v]) = [u^2 - 4tv, 2u(At+v) + 4Bt^2, (v-At)^2 - 4Btu].$$

Então as fórmulas para x_3 e x_4 mostram que o seguinte diagrama comuta

$$\begin{array}{ccccc} E \times E & & \xrightarrow{G} & & E \times E \\ \downarrow & & & & \downarrow \\ \mathbb{P}^1 \times \mathbb{P}^1 & & & & \mathbb{P}^1 \times \mathbb{P}^1 \\ \downarrow & & & & \downarrow \\ \mathbb{P}^2 & & \xrightarrow{g} & & \mathbb{P}^2 \end{array}$$

com σ descendo pelos dois lados.

onde

$$G(P,Q) = (P+Q, P-Q),$$

e onde o mapa vertical σ é a composição dos dois mapas

$$E \times E \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1, \qquad (P,Q) \longmapsto (x(P), x(Q)),$$

e

$$\mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^2, \qquad ([\alpha_1,\beta_1],[\alpha_2,\beta_2]) \longmapsto [\beta_1\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1, \alpha_1\alpha_2].$$

A ideia principal é ver t, u e v representando $1, x_1 + x_2$, e x_1x_2, assim $g([t,u,v])$ fica $[1, x_3 + x_4, x_3x_4]$.

A seguir mostraremos que g é um morfismo, e assim poderemos aplicar o teorema (4.4). Pela definição, devemos mostrar que os três polinômios homogêneos que definem g não têm zeros em comum, a não ser $t = u = v = 0$. Suponha que $g([t,u,v]) = 0$. Se $t = 0$, então de

$$u^2 - 4tv = 0 \qquad \text{e} \qquad (v-At)^2 - 4Btu = 0$$

vemos que $u = v = 0$. Assim podemos assumir que $t \neq 0$, então podemos definir o valor $x = u/2t$.

A partir desse novo x, a equação $u^2 - 4tv = 0$ pode ser escrita como $x^2 = v/t$.

Dividindo temos

$$2u(At+v)+4Bt^2=0 \qquad \text{e} \qquad (v-At)^2-4Btu=0$$

e assim por t^2 e reescrevendo em termos de x obtemos as equações

$$\begin{aligned}\psi(x) &= 4x(A+x^2)+4B &&= 4x^3+4Ax+4B=0,\\ \phi(x) &= (x^2-A)^2-8Bx &&= x^4-2Ax^2-8Bx+A^2=0.\end{aligned}$$

Estes polinômios são familiares, pois sua razão é a função racional que aparece na fórmula de duplicação vista na página (65). Para demonstrar que $\psi(X)$ e $\phi(X)$ não tem raízes em comum, é suficiente verificar a seguinte identidade,

$$(12X^2+16A)\phi(X)-(3X^3-5AX-27B)\psi(X)=4(4A^3+27B^2)\neq 0.$$

Segue então que g é um morfismo, completando a demonstração.

Voltamos ao diagrama comutativo e calculamos

$$\begin{aligned}h(\sigma(P+Q,P-Q)) &= h(\sigma\circ G(P,Q))\\ &= h(g\circ\sigma(P,Q))\\ &= 2h(\sigma(P,Q))+\mathcal{O}(1), \qquad \text{do teorema (4.4)},\end{aligned}$$

pois g é um morfismo de grau 2. Para completar a demonstração do teorema (4.8) quando $f=x$, mostraremos que

$$h(\sigma(R_1,R_2))=h_x(R_1)+h_x(R_2)+\mathcal{O}(1) \qquad \text{para todo } R_1,R_2\in E(\bar{K}).$$

Então, aplicando essa relação para cada lado da equação

$$h(\sigma(P+Q,P-Q))=2h(\sigma(P,Q))+\mathcal{O}(1)$$

nos fornece o resultado desejado.

Se $R_1=\mathcal{O}$ ou $R_2=\mathcal{O}$, então $h(\sigma(R_1,R_2))$ é igual a $h_x(R_1)+h_x(R_2)$. Caso contrário escrevemos

$$x(R_1)=[\alpha_1,1] \qquad \text{e} \qquad x(R_2)=[\alpha_2,1],$$

e então

$$h(\sigma(R_1,R_2))=h([1,\alpha_1+\alpha_2,\alpha_1\alpha_2]) \quad \text{e} \quad h_x(R_1)+h_x(R_2)=h(\alpha_1)+h(\alpha_2).$$

Aplicamos o teorema (4.5) ao polinômio $(T+\alpha_1)(T+\alpha_2)$ para obter a estimativa

que queríamos

$$h(\alpha_1) + h(\alpha_2) - \log 4 \leq h([1, \alpha_1 + \alpha_2, \alpha_1\alpha_2]) \leq h(\alpha_1) + h(\alpha_2) + \log 2.$$

Por fim, para demonstrar o resultado para uma função par $f \in K(E)$, provaremos no próximo lema que

$$h_f = \frac{1}{2}(\deg f)h_x + \mathcal{O}(1).$$

Dessa forma, multiplicamos h_x escrito dessa forma por $\frac{1}{2}\deg f$, obtendo assim o que queríamos. □

Lema 4.2. Dados $f, g \in K(E)$ funções pares, então

$$(\deg g)h_f = (\deg f)h_g + \mathcal{O}(1).$$

Prova. Sejam $x, y \in K(E)$ coordenadas de Weierstrass para E/K. Sabemos do corolário (3.1) que o subcorpo de $K(E)$ consistindo das funções pares é $K(x)$, e assim podemos encontrar uma função racional $r(X) \in K(X)$ tal que o seguinte diagrama é comutativo.

$$\begin{array}{ccc} E & & \\ {\scriptstyle x}\downarrow & \searrow^{f} & \\ \mathbb{P}^1 & \xrightarrow{r} & \mathbb{P}^1. \end{array}$$

Consequentemente, usando o teorema (4.4) e a proposição (2.5), onde r é um morfismo, deduzimos que

$$h_f = h_x \circ r = (\deg r)h_x + \mathcal{O}(1).$$

O diagrama nos diz que

$$\deg f = (\deg x)(\deg r) = 2\deg r,$$

assim temos que

$$2h_f = (\deg f)h_x + \mathcal{O}(1).$$

Fazendo da mesma forma para g temos

$$2h_g = (\deg g)h_x + \mathcal{O}(1),$$

e combinando essas equações temos que

$$(\deg g)h_f = (\deg f)h_g + \mathcal{O}(1),$$

como queríamos. □

Corolário 4.2. Sejam E/K uma curva elíptica, e $f \in K(E)$ uma função par.
(a) Seja $Q \in E(\bar{K})$. Então

$$h_f(P+Q) \leq 2h_f(P) + \mathcal{O}(1) \qquad \text{para todo } P \in E(\bar{K}),$$

onde $\mathcal{O}(1)$ depende de E, f e Q.
(b) Seja $m \in \mathbb{Z}$. Então

$$h_f([m]P) = m^2 h_f(P) + \mathcal{O}(1) \qquad \text{para todo } P \in E(\bar{K}),$$

onde $\mathcal{O}(1)$ depende de E, f, e m.

Prova. (a) Como $h_f(P-Q) \geq 0$, aplicando o teorema (4.8) obtemos o resultado.
(b) Como f é par, é suficiente considerarmos apenas quando $m \geq 0$. O resultado é imediato para os casos $m = 0$ e $m = 1$. Faremos a prova por indução sobre m. Suponha que o resultado vale para $m-1$ e para m. Mostremos para $m+1$. Substituindo P e Q no teorema (4.8) por $[m]P$ e P, respectivamente, encontramos que

$$\begin{aligned} h_f([m+1]P) &= -h_f([m-1]P) + 2h_f([m]P) + 2h_f(P) + \mathcal{O}(1) \\ &= (-(m-1)^2 + 2m^2 + 2)h_f(P) + \mathcal{O}(1), \text{ por hipótese de indução} \\ &= (m+1)^2 h_f(P) + \mathcal{O}(1). \end{aligned}$$

O que completa a prova. □

Observação 4.4. O teorema (4.8), o lema (4.2) e o corolário (4.2) também são verdadeiros para funções ímpares, pos f^2 é par, e de fato vale que $h_{f^2} = 2h_f$. Mais geralmente, nosso resultado é verdadeiro para quaisquer $f \in K(E)$ "dentro" de um ϵ. Precisamente, diremos do corolário (4.2b) que, para todo $\epsilon > 0$ é válido que

$$(1-\epsilon)m^2 h_f + \mathcal{O}(1) \leq h_f \circ [m] \leq (1+\epsilon)m^2 h_f + \mathcal{O}(1),$$

onde $\mathcal{O}(1)$ depende de E, f, m, e ϵ.

Podemos agora completar a prova do teorema de Mordell-Weil.

Teorema 4.9. (**Mordell-Weil**) Sejam K um corpo de número, E/K uma curva elíptica. Então o grupo $E(K)$ é finitamente gerado.

Prova. Escolha qualquer função par não constante $f \in K(E)$, por exemplo, f poderia ser a coordenada x na equação de Weierstrass. Mostremos que a função altura

$$h_f : E(K) \longrightarrow \mathbb{R}$$

tem as seguintes propriedades:
(i) Seja $Q \in E(K)$. Existe uma constante C_1, depende de E, f e Q, tal que

$$h_f(P+Q) \leq 2h_f(P) + C_1 \qquad \text{para todo } P \in E(K).$$

(ii) Existe uma contante C_2 dependendo de E e f, tal que

$$h_f([2]P) \geq 4h_f(P) - C_2 \qquad \text{para todo } P \in E(K).$$

(iii) Para todo constante C_3, o conjunto

$$\{P \in E(K) : h_f(P) \leq C_3\}$$

é um conjunto finito.

O ítem (i) é uma reafirmação do corolário (4.2a), enquanto que (ii) é imediato quando $m = 2$, o caso em (4.2b), e (iii) é feito no teorema (4.1). Isso completa a prova do teorema de Mordell-Weil. □

Capítulo 5

Pontos Integrais em Curvas Elípticas

Muitas curvas elípticas tem infinitos pontos racionais, apesar do teorema de Mordell-Weil nos dizer que o grupo dos pontos racionais é finitamente gerado. Outra questão natural no sentido Diofantino é determinar quantos pontos em uma dada equação de Weierstrass (afim) tem coordenadas inteiras. Neste capítulo veremos um pouco sobre como podemos tratar esse caso.

5.1 Aproximação Diofantina

O problema fundamental quando se trata de aproximação Diofantina é a questão de quão próximo um número irracional pode ser aproximado por um número racional.

Exemplo 5.1. Para qualquer número racional p/q, sabemos que o valor $|p/q - \sqrt{2}|$ é estritamente positivo, e como $\mathbb{Q}$ é denso em $\mathbb{R}$, uma escolha aproximada de p/q pode ser tão pequena como desejarmos. O problema é fazê-lo tão pequeno sem tornar p e q tão grande. Os próximos resultados ilustram a ideia.

Proposição 5.1. (Dirichlet) Seja $\alpha \in \mathbb{R}$ com $\alpha \notin \mathbb{Q}$. Então existem infinitos números racionais $p/q \in \mathbb{Q}$ tal que

$$\left| \frac{p}{q} - \alpha \right| \leq \frac{1}{q^2}.$$

Prova. Seja Q um número inteiro grande e olhemos para o conjunto dos números reais

$$\{q\alpha - [q\alpha] : q = 0, 1, \ldots, Q\},$$

onde $[\,\cdot\,]$ denota o maior inteiro. Como α é irracional, esse conjunto contém $Q+1$ números distintos no intervalo de 0 a 1. Dividindo o intervalo $[0, 1]$ em Q tamanhos

iguais e aplicando o princípio da casa do pombo, encontramos que existem inteiros $0 \leq q_1 < q_2 \leq Q$ satisfazendo

$$|(q_1\alpha - [q_1\alpha]) - (q_2\alpha - [q_2\alpha])| \leq \frac{1}{Q}.$$

Então

$$\left|\frac{[q_2\alpha] - [q_1\alpha]}{q_2 - q_1} - \alpha\right| \leq \frac{1}{(q_2 - q_1)Q} \leq \frac{1}{(q_2 - q_1)^2}.$$

Isso fornece uma aproximação racional a α tendo a propriedade desejada.

Finalmente, obtemos uma lista de aproximações, seja p/q um valor para o qual $|p/q - \alpha|$ é pequeno. Então tomando $Q > |p/q - \alpha|^{-1}$ garante que tenhamos uma nova aproximação que não esteja na nossa lista. Consequentemente existe infinitos números racionais satisfazendo as condições da proposição. □

Observação 5.1. O resultado de Hurwitz diz que $1/q^2$ do lado direito da proposição de Dirichlet pode ser substituído por $1/(\sqrt{5}q^2)$, e este resultado é o melhor possível.

Proposição 5.2. (Liouville [12]) Seja $\alpha \in \bar{\mathbb{Q}}$ tendo grau $d \geq 2$ sobre $\mathbb{Q}$, ou seja, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$. Existe uma constante $C > 0$, dependendo de α, tal que para todo número racional p/q temos

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{C}{q^d}.$$

Prova. Seja

$$f(T) = a_0T^d + a_1T^{d-1} + \cdots + a_d \in \mathbb{Z}[T]$$

o polinômio mínimo de α, e seja

$$C_1 = \sup\{f'(t) : \alpha - 1 \leq t \leq \alpha + 1\}.$$

Então pelo teorema do valor médio temos que

$$\left|f\left(\frac{p}{q}\right)\right| = \left|f\left(\frac{p}{q}\right) - f(\alpha)\right| \leq C_1\left|\frac{p}{q} - \alpha\right|.$$

Por outro lado, sabemos que $q^d f(p/q) \in \mathbb{Z}$, e além disso $f(p/q) \neq 0$, pois f não tem raizes racionais. Então

$$\left|q^d f\left(\frac{p}{q}\right)\right| \geq 1.$$

Escrevendo $C = \min\{C_1^{-1}, 1\}$ e combinando as últimas duas desigualdades ficamos com

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{C}{q^d} \qquad \text{para todo } p/q \in \mathbb{Q}.$$

Observação 5.2. Liouville usou este teorema para provar a existência de números transcendentes. Nota-se que no teorema de Liouville é bem fácil encontrar explicitamente um valor para a constante C em termos de α. Isto marca um contraste com o restante dos resultados que estudaremos no restante desta seção.

O teorema de Dirichlet diz que todo número real pode ser aproximado por números racionais com $1/q^2$, enquanto que o resultado devido a Liouville nos diz que números algébricos de grau d podem ser aproximados não mais que C/q^d. Para irracionalidades quadráticas existe pouco a dizer, mas se $d \geq 3$, então é natural perguntarmos para o melhor expoente que ocorre em q. Não existe razão particular para restringir valores aproximados em $\mathbb{Q}$, assim nos permitimos variar sobre um corpo numérico fixado K. Finalmente, ao medir a aproximação podemos usar qualquer valor absoluto em K.

Definição 5.1. Seja $\tau(d)$ uma função do tipo $\tau : \mathbb{N} \to \mathbb{R}$. Um corpo de número K é dito ter expoente de aproximação τ se ele tem a seguinte propriedade:

Dados $\alpha \in \bar{K}$, $d = [K(\alpha) : K]$, e $v \in M_K$ um valor absoluto em K que possa extender a $K(\alpha)$ de algum modo. Então para qualquer constante C existe um número finito de $x \in K$ satisfazendo a desigualdade

$$|x - \alpha| < C H_K(x)^{-\tau(d)}.$$

A estimativa elementar de Liouville diz que $\mathbb{Q}$ tem expoente de aproximação $\tau(d) = d + \epsilon$ para qualquer $\epsilon > 0$. Este resultado foi sucessivamente melhorado por alguns matemáticos:

Liouville	1851	$\tau(d) = d + \epsilon$
Thue	1909	$\tau(d) = \frac{1}{2}d + 1 + \epsilon$
Siegel	1921	$\tau(d) = 2\sqrt{d} + \epsilon$
Gelfond, Dyson	1947	$\tau(d) = \sqrt{2d} + \epsilon$
Roth	1955	$\tau(d) = 2 + \epsilon$

Em vista de Liouville, o resultado de Roth é o melhor possível, além disso é conjecturado que ϵ possa ser substituído por alguma função $\epsilon(d) \to 0$ quando $d \to \infty$.

Enunciamos, sem demonstração, o teorema de Roth.

Teorema 5.1. (Roth) Para todo $\epsilon > 0$, todo corpo de numérico K de grau d tem expoente de aproximação

$$\tau(d) = 2 + \epsilon.$$

Exemplo 5.2. Vejamos como os teoremas de aproximação diofantina tratam as equações diofantinas. Considere o problema de resolver a equação

$$x^3 - 2y^3 = a$$

em inteiros $x, y \in \mathbb{Z}$, onde $a \in \mathbb{Z}$ é fixado. Suponha que (x, y) é solução, com $y \neq 0$. Seja ζ uma raíz cúbica primitiva da unidade, e fatore a equação como

$$\left(\frac{x}{y} - \sqrt[3]{2}\right)\left(\frac{x}{y} - \zeta\sqrt[3]{2}\right)\left(\frac{x}{y} - \zeta^2\sqrt[3]{2}\right) = \frac{a}{y^3}.$$

Os segundo e terceiro fatores são limitados, assim obtemos uma estimativa da forma

$$\left|\frac{x}{y} - \sqrt[3]{2}\right| \leq \frac{C}{y^3},$$

onde a constante C é independente de x e y. Pelo teorema de Roth acima ou pelo teorema de Thue com $\tau(d) = \frac{1}{2}d + 1 + \epsilon$, vemos que existem apenas finitas possibilidades para x e y. Então a equação

$$x^3 - 2y^3 = a$$

tem finitas soluções inteiras.

Observação 5.3. O que foi dito no teorema de Roth é que existe um número finitos elementos de K tendo uma certa propriedade. A prova não nos dá um procedimento efetivo para encontrarmos todos os elementos desse conjunto finito. Notamos que como consequência, todo resultado de finitude que demonstramos na seção 2 não são efetivos, pois dependem do teorema de Roth. Similarmente, do exemplo (5.2), não é produzido vizinhança explícita para x e y em termos de a. Entretanto, existem outros métodos, baseados em estimativas para formas lineares em logaritmos, os quais são efetivos nesse sentido.

5.2 Funções Distância

Desigualdades diofantinas tais como

$$|x - \alpha|_v < CH_K(x)^{-\tau(d)}$$

consistem de duas partes. Primeiro, exite a função altura $H_K(x)$, que mede o tamanho aritmético de x. Segundo, existe o valor $|x-\alpha|_v$, que é medida topológica ou

métrica da distância entre x e α, ou seja, ele mede a distância na topologia v-ádica. Nessa seção definiremos a noção de distância v-ádica em curvas, deduziremos algumas propriedades básicas, reinterpretando alguns resultados de aproximação diofantina, em termos dessa função distância.

Definição 5.2. Seja C/K uma curva, $v \in M_K$, e fixe um ponto $Q \in C(K_v)$. Escolha uma função $t_Q \in K_v(C)$ que tenha um zero de ordem $e \geq 1$ em Q e nenhum outro zero. Então para $P \in C(K_v)$, definimos que a distância v-ádica de P em Q por

$$d_v(P,Q) = \min\left\{|t_Q(P)|_v^{1/e}, 1\right\}.$$

(Se t_Q tem polo em P, definimos formalmente $|t_Q(P)| = \infty$, assim $d_v(P,Q) = 1$.)

Observação 5.4. Para ver que t_Q existe, usamos o teorema de Riemann-Roch. Lá é dito que se C tem gênero g e se $e \geq g+1$, então $\ell(e(Q)) \geq 2$, assim existe uma função não constante $f \in \mathcal{L}(e(Q))$. A função f tem polo em Q e nenhum outro, então podemos tomar $t_Q = 1/f$.

Observação 5.5. Na prática, fixamos um ponto Q e usamos a função distância $d_v(P,Q)$ para medir a distância de P a Q quando P varia. É claro que a função distância d_v tem propriedade qualitativa direita, isto é, $d_v(P,Q)$ é pequeno quando P está v-adicalmente próximo a t_Q. Por outro lado, o valor de $d_v(P,Q)$ depende da escolha da função t_Q, assim uma notação diferente poderia ser $d_v(P,t_Q)$. Entretanto, como usamos d_v para medir a razão com que a variação do ponto ao se aproximar do ponto fixado, o próximo resultado mostra que a escolha de t_Q é irrelevante para o enunciado em nosso teorema.

Proposição 5.3. Seja $Q \in C(K_v)$ e $F \in K_v(C)$ uma função que se anula em Q. Então o limite

$$\lim_{\substack{P \in C(K_v) \\ P \to Q}} \frac{\log |F(P)|_v}{\log d_v(P,Q)} = \operatorname{ord}_Q(F)$$

existe e é independente da escolha da função t_Q usada para definir $d_v(P,Q)$.
Aqui $P \to Q$ significa que $P \in C(K_v)$ se aproxima de Q na topologia v-ádica, isto é, $d_v(P,Q) \to 0$.

Prova. Seja t_Q uma função que se anula apenas em Q que usaremos para definir $d_v(\cdot, Q)$. Seja $e = \operatorname{ord}_Q(t_Q)$ e $f = \operatorname{ord}_Q(F)$. Então a função $\phi = F^e/t_Q^f$ não tem nem zero nem polo em Q, assim $|\phi(P)_v|$ é limitado além do 0 e ∞ quando P tende a Q.

Então

$$\begin{aligned}\lim_{\substack{P\in C(K_v)\\ P\underset{v}{\longrightarrow}Q}} \frac{\log|F(P)|_v}{\log d_v(P,t_Q)} &= \lim_{\substack{P\in C(K_v)\\ P\underset{v}{\longrightarrow}Q}} \frac{\log|F(P)|_v}{\log|t_Q(P)|_v^{1/e}} \\ &= f + \lim_{\substack{P\in C(K_v)\\ P\underset{v}{\longrightarrow}Q}} \frac{1}{e}\cdot\frac{\log|\phi(P)|_v}{\log|t_Q(P)|_v} \\ &= f.\end{aligned}$$

□

Observação 5.6. O uso da função t_Q na definição de distância é artificial e não generaliza variedades de dimensões maiores. Uma alternativa para a definição é usar uma lista finita de funções $t_1,\ldots,t_r \in K(E)$ com a propriedade de que cada t_i anula em Q tal que $t_1,\ldots,t_r$ não tenham outro zero em comum. Então, se e_i denota a ordem de t_i em Q, a função distância d_v pode ser definida por

$$d_v(P,Q) = \min\left\{\max\{|t_1(P)|_v^{1/e_1},\ldots,|t_r(P)|_v^{1/e_r}\},1\right\}.$$

A seguir examinaremos o efeito de mapas finitos na distância entre pontos. Temos que observar que isso depende do índice de ramificação do mapa, não do seu grau. Compare com o teorema (4.4), do capítulo anterior.

Proposição 5.4. Sejam C_1/K, C_2/K curvas, $\phi : C_1 \to C_2$ um mapa finito definido sobre K, $Q \in C_1(K_v)$ e $e_\phi(Q)$ o índice de ramificação de ϕ em Q. Então

$$\lim_{\substack{P\in C_1(K_v)\\ P\underset{v}{\longrightarrow}Q}} \frac{\log d_v(\phi(P),\phi(Q))}{\log d_v(P,Q)} = e_\phi(Q).$$

Prova. Sejam $t_Q \in K_v(C_1)$ uma função que se anula com ordem $e_1 \geq 1$ em Q e que não tenha outras raízes, e também $t_{\phi(Q)} \in K_v(C_2)$ uma função que se anula com ordem $e_2 \geq 1$ em $\phi(Q)$ sem outras raizes. Segue da definição de índice de ramificação que

$$\mathrm{ord}_Q t_{\phi(Q)}\circ\phi = e_\phi(P)\mathrm{ord}_{\phi(Q)}t_{\phi(Q)} = e_\phi(P)e_2,$$

assim as funções $(t_{\phi(Q)}\circ\phi)^{e_1}$ e $t_Q^{e_\phi(P)e_2}$ se anulam com mesma ordem em Q. Consequentemente a função

$$f = \frac{(t_{\phi(Q)}\circ\phi)^{e_1}}{t_Q^{e_\phi(Q)e_2}} \in K_v(C_1)$$

não tem zeros nem polos em Q. Segue que $|f(P)|_v$ é limitado além de 0 e ∞ quando $P \underset{v}{\longrightarrow} Q$. Além disso

$$\begin{aligned}\frac{\log d_v(\phi(P),\phi(Q))}{\log d_v(P,Q)} &= \frac{\log |t_{\phi(Q)}(\phi(P))|_v^{1/e_2}}{\log |t_Q(P)|_v^{1/e_1}} \\ &= \frac{e_\phi(Q)\log |t_Q(P)|_v^{1/e_1} + \log |f(P)|_v}{\log |t_Q(P)|_v^{1/e_1}} \\ &\longrightarrow e_\phi(Q) \qquad \text{quando } P \underset{v}{\longrightarrow} Q\end{aligned}$$

□

Agora reinterpretaremos o teorema de Roth em termos de funções distância.

Corolário 5.1. Sejam $v \in M_K$ um valor absoluto, C/K uma curva, $f \in K(C)$ uma função não constante e $Q \in C(\bar{K})$. Então

$$\liminf_{\substack{P\in C(K)\\ P \underset{v}{\longrightarrow} Q}} \frac{\log d_v(P,Q)}{\log H_K(f(P))} \geq -2.$$

(Se Q não é um ponto de acumulação v-ádico de $C(K)$, então definimos lim inf como sendo 0.)

Prova. Substituindo f por $1/f$ se necessário, podemos assumir que $f(Q) \neq \infty$. (Note que $H_K((1/f)(P)) = H_K(f(P))$.) A função $f - f(Q)$ é nula em Q, digamos com ordem e, assim da proposição (5.3) temos

$$\liminf_{\substack{P\in C(K)\\ P \underset{v}{\longrightarrow} Q}} \frac{\log |f(P)-f(Q)|_v}{d_v(P,Q)} = e.$$

Consequentemente,

$$\begin{aligned}\liminf_{\substack{P\in C(K)\\ P \underset{v}{\longrightarrow} Q}} \frac{\log d_v(P,Q)}{\log H_K(f(P))} &= \liminf_{\substack{P\in C(K)\\ P \underset{v}{\longrightarrow} Q}} \frac{\log |f(P)-f(Q)|_v}{e\log H_K(f(P))} \\ &= \frac{1}{e}\liminf_{\substack{P\in C(K)\\ P \underset{v}{\longrightarrow} Q}} \left(\frac{\log(H_K(f(P))^\tau |f(P)-f(Q)|_v)}{\log H_K(f(P))} - \tau\right).\end{aligned}$$

Basta definirmos $\tau = 2 + \epsilon$. Pelo teorema de Roth

$$H_K(f(P))^\tau |f(P)-f(Q)|_v \geq 1$$

para quase todo $P \in C(K)$. Ainda

$$\liminf_{\substack{P \in C(K) \\ P \xrightarrow[v]{} Q}} \frac{\log d_v(P,Q)}{\log H_K(f(P))} \geq -\frac{\tau}{e} \geq -\frac{2+\epsilon}{e}.$$

Como $\epsilon > 0$ é arbitrário e $e \geq 1$, obtemos o resultado como queríamos. □

A seguir enunciamos o teorema de Siegel, que é na verdade uma melhoria no resultado da aproximação diofantina.

Teorema 5.2. (Siegel) Sejam E/K uma curva elíptica com $\#E(K) = \infty$, $f \in K(E)$ uma função não constante, $v \in M_K$, e $Q \in E(\bar{K})$. Então

$$\lim_{\substack{P \in E(K) \\ h_f(P) \to \infty}} \frac{\log d_v(P,Q)}{h_f(P)} = 0.$$

Prova. A demonstração pode ser vista em [1, capítulo IX].

REFERÊNCIAS

[1] Silverman, J. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986

[2] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[3] S.Lang. *Introduction to algebraic and abelian functions*, volume 89 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1982.

[4] S. Lang. *Number theory III*, volume 60 of *Encyclopedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1991.

[5] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134-144, 1966.

[6] G.Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent.Math.*, 73(3):349-366, 1983.

[7] G.Faltings. Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry (Storrs, Conn.,* 1984*)*, pages 9-27. Springer, New York, 1986. Translated from the German original [Invent. Math.73 (1983), no. 3, 349-366; ibid.75 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz.

[8] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts* in Mathematics. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[9] S. Lang. *Algebraic number theory*, volume 110 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1994.

[10] I. R. Shafarevich. B*asic algebraic geometry*. Springer-Verlag, Berlin, study edition, 1977. Translated from the Russian by K. A. Hirsch, Revised printing of Grundlehren der mathematischen Wissenschaften, Vol. 213, 1974.

[11] Atiyah, M.F. and Macdonald, L.G. (1969) *Introduction to Commutative Algebra.* Addison-Wesley Publishing Company.

[12] J. Liouville. Sur des classes très-étendues de quantités dont la irrationalles algébriques. *C. R. Acad. Paris*, 18:883-885 and 910-911, 1844.

[13] J.-P. Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math., 15(4):259-331, 1972.

[14] J.-P. Serre. *Abelian l-adic representations and elliptic curves, volume 7 of*

Research Notes in Mathematics. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[15] S. Lang. *Algebraic number theory*, volume 110 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1994.

[16] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.