UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
(Mestrado)

RAFAEL CASTRO DOS SANTOS NASCIMENTO

Sobre o Teorema de Mordell

Maringá-PR
2022

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001 e do Ministério da Ciência, Tecnologia e Inovação - Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq - Brasil (133597/2020-2).

UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Sobre o Teorema de Mordell

Rafael Castro dos Santos Nascimento

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos para obtenção do título de Mestre em Matemática.
Área de concentração: Álgebra.

Orientador: Prof. Dr. Marcelo Escudeiro Hernandes.

Maringá-PR, 8 de abril de 2022

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Setorial BSE-DMA-UEM, Maringá, PR, Brasil)

Nascimento, Rafael Castro dos Santos
N244s Sobre o Teorema de Mordell / Rafael Castro dos Santos Nascimento. -- Maringá, 2022.
110 f. : il.

Orientador: Prof. Dr. Marcelo Escudeiro Hernandes
Dissertação (Mestrado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática - Área de Concentração: Álgebra, 2022.

1. Teorema de Bézout. 2. Pontos racionais. 3. Curvas elípticas. 4. Teorema de Nagell-Lutz. 5. Teorema de Mordell. 6. Bézout Theorem. 7. Rational points. 8. Elliptic curves. 9. Nagell-Lutz Theorem. 10. Mordell Theorem. I. Hernandes, Marcelo Escudeiro, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Programa de Pós-Graduação em Matemática - Área de Concentração: Álgebra. III. Título.

CDD 22.ed. 512.7

Edilson Damasio CRB9-1.123

RAFAEL CASTRO DOS SANTOS NASCIMENTO

SOBRE O TEOREMA DE MORDELL

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Prof. Dr. Marcelo Escudeiro Hernandes - UEM (Presidente)
Prof. Dr. Thiago Henrique de Freitas - UTFPR
Profa. Dra. Irene Naomi Nakaoka - UEM

Aprovado em: 31 de março de 2022.
Local de defesa: Videoconferência – Google Meet (https://meet.google.com/oac-sunh-jdk)

Agradecimentos

Agradeço primeiramente aos meus pais, José e Damaris, por terem me apoiado desde sempre.

Ao meu orientador Prof. Dr. Marcelo Escudeiro Hernandes por sempre me manter motivado, pelos ótimos conselhos e pela paciência.

Aos professores do PMA - UEM com os quais tive a oportunidade cursar as disciplinas e contribuíram muito para meu aprendizado.

Aos membros da banca pelas inúmeras sugestões.

Por fim, ao CNPq pelo apoio financeiro.

Resumo

Neste trabalho, estudaremos o conjunto dos pontos racionais em curvas cúbicas regulares definidas sobre o corpo dos números racionais. Primeiramente apresentaremos alguns resultados sobre interseções entre curvas algébricas e mostraremos que se o conjunto dos pontos racionais de uma cúbica regular for não vazio ele admite uma estrutura de grupo abeliano. Nosso principal objetivo neste trabalho é demonstrar o Teorema de Mordell o qual garante que o grupo dos pontos racionais de uma cúbica regular é finitamente gerado.

Palavras-chave: Teorema de Bézout; pontos racionais; curvas elípticas; Teorema de Nagell-Lutz; Teorema de Mordell.

Abstract

In this work we study the set of rational points in non singular cubics defined over the rational numbers field. Firstly we present some results concerning intersection of algebraic curves and we show that if the set of rational points of a non singular cubic is non empty then it admits an abelian group structure. Our main aim in this work is to proof the Mordell Theorem that ensures that the group of rational points of a non singular cubic is finitely generated.

Keywords: Bézout Theorem; rational points; elliptic curves; Nagell-Lutz Theorem; Mordell Theorem.

Sumário

Introdução

A teoria das equações Diofantinas é um campo da teoria de números que busca por soluções de equações polinomiais no anel dos números inteiros ou no corpo dos números racionais.

Um exemplo de equação Diofantina surge quando consideramos o problema de escrever um inteiro c como diferença de um quadrado e um cubo, algebricamente tal problema se traduz em encontrar soluções para a equação Diofantina (equação de Bachet)

$$y^2 - x^3 = c.$$

Uma surpreendente propriedade dessa equação é que se tivermos uma solução $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ com $y \neq 0$, então

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3} \right) \tag{1}$$

também será uma solução racional. A fórmula que acabamos de apresentar é conhecida como *fórmula de duplicação* e foi descoberta por Bachet em 1621.

A fórmula descoberta por Bachet não é intuitiva, o que nos faz perguntar como foi obtida. A resposta é dada pelo uso de ferramentas da Geometria Algébrica! Suponhamos que $P = (x, y)$ seja uma solução racional da equação de Bachet, com $y \neq 0$. Portanto, P é um ponto na curva dada pelas soluções reais da equação, como ilustrado na Figura 1. A reta tangente à curva no ponto P irá intersectar a curva em um outro ponto, o qual denotaremos por Q. Então calculando algebricamente as coordenadas de Q, obteremos a fórmula de duplicação de Bachet. Mesmo que ainda não seja claro porque as coordenadas do ponto Q nos dão uma solução para o problema e careça de uma justificativa (que será consequência do resultado principal deste trabalho), o fato instiga o estudo de questões gerais envolvendo soluções racionais de equações como apresentamos. No Capítulo 1 veremos mais detalhes do porquê sempre temos uma reta tangente passando por um

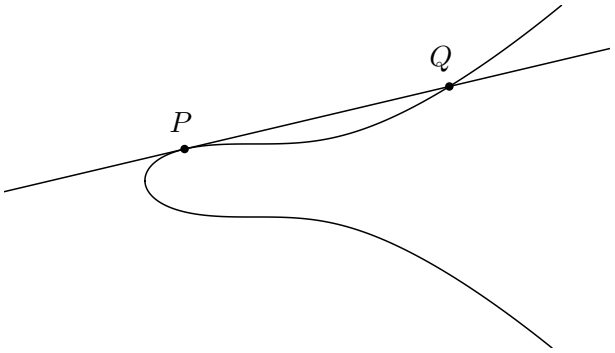


Figura 1: Duplicação de um ponto.

ponto da curva, porque essa reta intersecta a curva em um outro ponto e não em dois ou mais pontos.

O tipo mais simples de equação Diofantina é o polinômio em uma variável

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Assumindo que $a_0, \ldots, a_n$ sejam inteiros. Então pelo lema de Gauss, as soluções racionais não nulas dessa equação têm a forma p/q, com q dividindo a_n e p dividindo a_0. Isso limita o número de possíveis soluções a um pequeno número de possibilidades o que permite verificar facilmente quais dessas possibilidades são de fato soluções da equação. Portanto as equações Diofantinas em uma variável são relativamente fáceis de se resolver.

Quando trabalhamos com equações Diofantinas com duas variáveis, a situação muda drasticamente, o conjunto de soluções reais para uma equação $f(x, y) = 0$ define (em geral) uma curva no plano xy. Tais curvas são chamadas de *curvas algébricas* para indicar que elas são o conjunto de soluções de uma equação polinomial. Com o objetivo de obter informações acerca de pontos racionais em curvas algébricas, consideremos inicialmente as curvas definidas por uma equação polinomial de grau um, ou seja, *equações lineares*.

Consideremos uma equação linear com coeficientes inteiros

$$f(x, y) = ax + by + c = 0. \tag{2}$$

Como f tem grau um então $(a, b) \in \mathbb{Q}^2$ é um vetor não nulo, ou seja, $a^2 + b^2 \neq 0$. Sendo assim

$$(x_0, y_0) := \left(-\frac{ca}{a^2 + b^2}, -\frac{cb}{a^2 + b^2} \right)$$

é uma solução racional para a Equação (2). Reciprocamente, sejam (x_1, y_1) uma solução racional para a Equação (2) e $\overrightarrow{v} = (b, -a)$. Então $\overrightarrow{v} \in \mathbb{Q}^2$ é um vetor ortogonal a (a, b)

e, portanto, gera o espaço ortogonal a $(a, b) \in \mathbb{Q}^2$. Como

$$a\,(x_1 - x_0) + b\,(y_1 - y_0) = 0,$$

temos que $(x_1 - x_0, y_1 - y_0)$ é ortogonal a (a, b), consequentemente, existe um único $t \in \mathbb{Q}$, tal que

$$(x_1, y_1) = (x_0, y_0) + t\,\overrightarrow{v},$$

ou seja, existe uma função injetora entre o conjunto das soluções de (2) e o conjunto dos números racionais. Além disso, essa função tem inversa $t \to (x_0, y_0) + t\,\overrightarrow{v}$. Portanto, obtemos uma bijeção entre as soluções de uma equação Diofantina linear com duas variáveis e o conjunto dos números racionais.

No caso das equações definidas por um polinômio de grau dois, também chamadas de equações quadráticas (ou seja, determinam seções cônicas), veremos na Seção 2.1 que se essas equações tiverem uma solução, então elas terão infinitas soluções e todas elas podem ser descritas. Mais ainda, como na fórmula de duplicação de Bachet, a interseção entre a curva e uma reta terá um papel crucial para obter estas soluções. Além disso, existem métodos para determinar uma solução racional, caso exista alguma.

Em contraste com as equações lineares e quadráticas, as soluções racionais de equações cúbicas não são totalmente entendidas, e mesmo nos casos em que uma resposta completa seja conhecida, a prova envolve uma combinação de técnicas de álgebra, geometria e teoria de números. Portanto, as equações cúbicas com duas variáveis são o primeiro exemplo de equações Diofantinas que merecem um estudo mais aprofundado.

Um exemplo de equação cúbica é a equação de Bachet $y^2 - x^3 = c$ que mencionamos anteriormente. Vimos que a fórmula (de duplicação) de Bachet consiste em considerar

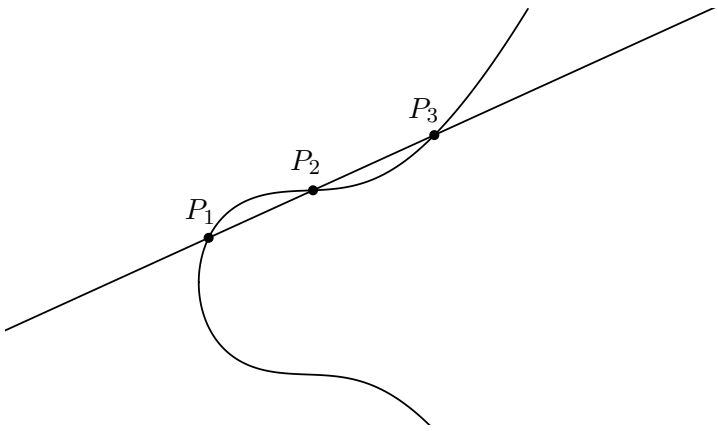


Figura 2: Adição de dois pontos.

um ponto P na cúbica, traçar a reta tangente por P e tomar o outro ponto da interseção da reta com a cúbica. Similarmente, se começarmos com dois pontos P_1 e P_2 na cúbica, podemos traçar a reta passando por P_1 e P_2 e tomar o terceiro ponto de interseção P_3. Isso irá funcionar para a maioria das escolhas de pontos P_1 e P_2, pois a maioria das retas intersectam uma cúbica em três pontos. Nós poderíamos descrever esse procedimento, ilustrado na Figura 2, como um modo de "somar" dois pontos na curva e obter um terceiro ponto. Surpreendentemente, com pequenas modificações, essa operação geométrica torna o conjunto das soluções racionais de uma curva cúbica em um grupo abeliano! Em 1901, Poincaré propôs que esse grupo é gerado por um subconjunto finito de pontos, esse resultado foi provado em 1922 por Mordell e será nosso principal objetivo neste trabalho.

Este trabalho está estruturado da seguinte maneira:

No Capítulo 1, faremos um estudo das interseções entre curvas algébricas, para tal, introduziremos o plano projetivo o qual é um ambiente mais propício para esse estudo.

No Capítulo 2, começaremos analisando os pontos racionais nas curvas quadráticas e nas cúbicas singulares.

No Capítulo 3, seguiremos para nosso principal objeto de estudo, as cúbicas regulares, para as quais mostraremos que se o conjunto de seus pontos racionais é não vazio, então ele admite uma estrutura de grupo abeliano. Além disso, podemos reescrever essas cúbicas em uma forma mais simples, a qual nos permitirá apresentar fórmulas explícitas para a operação de grupo dos pontos racionais.

No Capítulo 4, teremos como objetivo demonstrar o Teorema de Nagell-Lutz que dá uma caracterização dos pontos de torção e nos permite concluir que existe uma quantidade finita de tais pontos.

No Capítulo 5, demonstraremos um caso especial do Teorema de Mordell, o qual garante que o grupo dos pontos racionais de cúbica regular é finitamente gerado. Inicialmente, apresentaremos condições suficientes para determinar se um grupo abeliano é finitamente gerado, sem a necessidade de apresentar seus geradores e na sequência mostraremos que o grupo dos pontos racionais de uma cúbica regular, satisfaz tais condições.

Capítulo 1

Neste capítulo abordaremos sucintamente conceitos relacionados ao plano projetivo e curvas algébricas. Para maiores detalhes indicamos [Vai17] ou [Ful08].

1.1 Coordenadas Homogêneas e o Plano Projetivo

Sendo $\mathbb{K}$ um corpo de números, isto é, que contém $\mathbb{Q}$, consideraremos o espaço afim $\mathbb{A}^n_{\mathbb{K}}$ como sendo $\mathbb{K}^n$. Quando não houver confusão de que corpo estamos considerando, denotaremos $\mathbb{A}^n_{\mathbb{K}}$ simplesmente por $\mathbb{A}^n$, em particular nos referiremos ao espaço $\mathbb{A}^2$ como plano afim. É neste ambiente que consideraremos os objetos que abordaremos, tais como: retas, cônicas, cúbicas, etc;

A interseção entre cúbicas e retas terá um papel crucial para nosso estudo de pontos racionais em cúbicas, pois é por meio destas interseções que definiremos uma estrutura de grupo no conjunto dos pontos racionais da cúbica. Em geral, uma reta passando por dois pontos de uma cúbica irá intersectar a cúbica em um terceiro ponto, mas há casos em que isso não ocorre, como ilustrado na Figura 1.1.

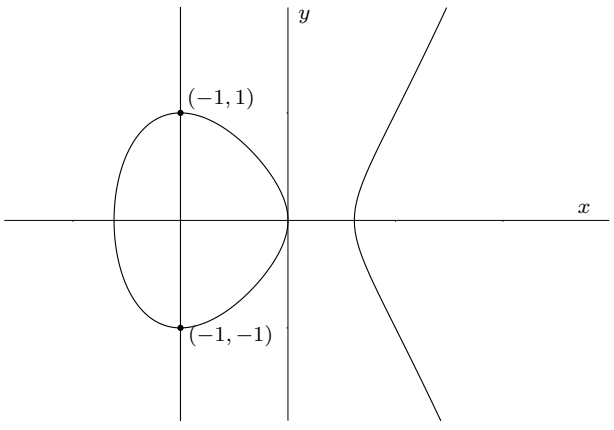


Figura 1.1: Cúbica $y^2 = x^3 + x^2 - x$ e reta $x = -1$ com somente dois pontos de interseção.

Mesmo considerando interseções entre retas pode ocorrer situação semelhante, duas retas paralelas não têm interseção, enquanto interseções entre duas retas não paralelas (que corresponde à situação genérica) se intersectam em exatamente um ponto.

Como usaremos estas interseções para definir uma estrutura de grupo, precisamos considerar um ambiente mais propício que o espaço afim para que a quantidade de pontos nas interseções seja sempre a mesma. Veremos que, para tanto, a situação é contornada ao adicionar pontos ao plano afim obtendo um outro espaço.

Vejamos como abordar a situação iniciando com o estudo de interseções entre duas retas.

Uma propriedade do plano afim é que dois pontos determinam uma única reta passando por eles, esta propriedade será de grande importância ao nosso estudo. Portanto, será de nosso interesse que o espaço que construiremos também satisfaça essa propriedade.

Além da propriedade acima, temos que no plano afim, duas retas não paralelas se intersectam em um único ponto. Para estender essa propriedade para retas paralelas, construiremos um novo espaço incluindo pontos ao plano afim, de modo que estes pontos incluídos sejam as interseções entre retas paralelas e a propriedade de que dois pontos determinam uma reta seja satisfeita.

Incluir apenas um ponto não é suficiente para contemplar todas as retas paralelas. Para verificar isso, consideremos L_1 e L_2 retas paralelas e P o ponto adicional que estamos impondo como sendo a interseção. Analogamente, consideremos L_1' e L_2' retas paralelas e P' o ponto adicional que admitimos ser a interseção de L_1' e L_2', como ilustrado na Figura 1.2. Suponhamos que L_1 e L_1' não sejam paralelas. Então L_1 e L_1' se intersectam

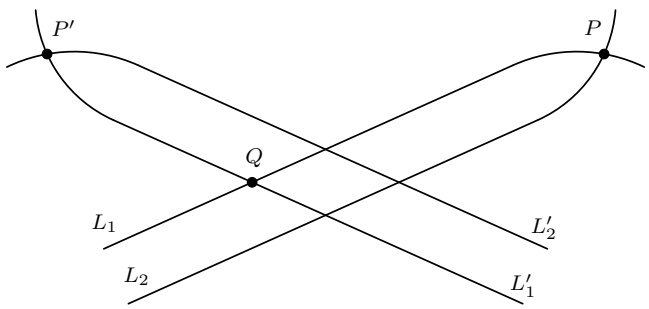


Figura 1.2: Retas paralelas com interseção no infinito.

em algum ponto $Q \in \mathbb{A}^2$. Mas, se quisermos que duas retas quaisquer, neste novo espaço, tenham exatamente um ponto em comum, os pontos P e P' deverão ser distintos. Caso contrário, os pontos P e Q determinam duas retas distintas L_1 e L_1'. Logo, precisamos adicionar um novo ponto para cada uma das direções no plano afim[1].

Deste modo, definimos um novo espaço, que chamaremos *plano projetivo*, como sendo

$$\mathbb{P}^2 = \mathbb{A}^2 \dot{\cup} \{\text{direções em } \mathbb{A}^2\}.$$

Os pontos em $\mathbb{P}^2$ que não estão em $\mathbb{A}^2$, são frequentemente chamados *pontos no infinito*. Pela forma que definimos os pontos no infinito, é natural definirmos as retas em $\mathbb{A}^2$ com o ponto no infinito especificado pela sua direção como sendo uma reta em $\mathbb{P}^2$. Além destas retas, definimos também o conjunto dos pontos no infinito, o qual denotaremos por L_∞, como sendo uma reta em $\mathbb{P}^2$. Diferentemente das demais retas, não é tão intuitiva a definição de L_∞ ser uma reta em $\mathbb{P}^2$, mas se interpretarmos $\mathbb{P}^2$ de uma maneira um pouco diferente, veremos que esta definição faz sentido.

Seja π_1 o plano afim $\{(x, y, 1) \in \mathbb{A}^3\}$. Consideraremos pontos de $\mathbb{A}^2$ como sendo pontos de π_1, usando a bijeção dada por $(x, y) \leftrightarrow (x, y, 1)$. Sejam $O = (0, 0, 0) \in \mathbb{A}^3$ a origem e π_2 o plano afim $\{(x, y, 0) \in \mathbb{A}^3\}$. Como π_1 e π_2 são planos afins paralelos, eles contêm as mesmas direções, Além disso, para cada direção em π_2 existe exatamente uma reta contida em π_2 que passa pela origem e tem a direção considerada. Então pontos no infinito podem ser identificados com retas em π_2 que contêm a origem.

Para cada ponto P no plano π_1 temos que a reta $\overline{PO} \subset \mathbb{A}^3$, ou seja, a reta de $\mathbb{A}^3$ que passa por P e O, não está contida em π_2. Reciprocamente, cada reta de $\mathbb{A}^3$ que contém a origem e não está contida em π_2 irá intersectar π_1 em exatamente um ponto. Logo, existe uma bijeção entre os pontos em π_1 e as retas de $\mathbb{A}^3$ que contém a origem e não estão contidas em π_2. Portanto, podemos identificar

$$\mathbb{P}^2 \longleftrightarrow \{ \text{ retas em } \mathbb{A}^3 \text{ que contêm } O \}.$$

As retas projetivas induzidas pela identificação acima, correspondem aos planos de $\mathbb{A}^3$ que contêm a origem, em particular $L_\infty = \pi_2$. Esta identificação nos permite também constatar facilmente que em $\mathbb{P}^2$ duas retas projetivas se intersectam em exatamente um ponto do plano projetivo e que dado dois pontos distintos no plano projetivo, existe exatamente uma reta projetiva passando por estes pontos.

[1] O conceito de direção é o mesmo visto na definição de vetor em um curso de Geometria Analítica.

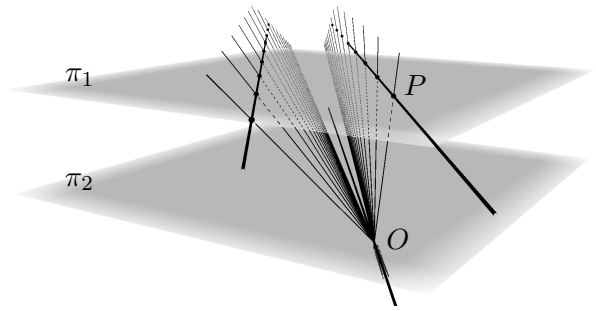


Figura 1.3: Retas paralelas em π_1 com interseção no infinito.

Apesar desta representação de $\mathbb{P}^2$ ser muito útil para visualizar aspectos geométricos do $\mathbb{P}^2$, ela não é a melhor escolha para realizar cálculos algébricos. Como pontos no plano projetivo podem ser identificados como retas do espaço afim $\mathbb{A}^3$ que passam pela origem, podemos tirar proveito das coordenadas de $\mathbb{A}^3$ para uma descrição algébrica de $\mathbb{P}^2$.

Retas em $\mathbb{A}^3$ que passam pela origem são $\mathbb{K}$-subespaços vetoriais de dimensão um, ou seja, são os $\mathbb{K}$-subespaços vetoriais gerados por um vetor não nulo. Cada um destes subespaços poderá ter mais de um gerador, mas identificando os geradores de um mesmo subespaço de dimensão um em uma única classe, teremos uma bijeção entre as retas passando pela origem e a classe de seus geradores, denotaremos a classe de um gerador (a, b, c) por $[a : b : c]$, logo obtemos uma nova descrição para o plano projetivo

$$\mathbb{P}^2 \longleftrightarrow \left\{ [a : b : c] \, ; (a, b, c) \in \mathbb{A}^3 \setminus \{(0, 0, 0)\} \right\}.$$

Observamos que $[a : b : c] = [ta : tb : tc]$ para todo $t \in \mathbb{K}^*$. Dizemos que $a, b, c \in \mathbb{K}$ são *coordenadas homogêneas* de $[a : b : c] \in \mathbb{P}^2$, consequentemente, um ponto $[a : b : c] \in \mathbb{P}^2$ não tem coordenadas homogêneas univocamente determinadas.

Seja $r \subset \mathbb{A}^2$ a reta afim definida pela equação $\alpha x + \beta y + \gamma = 0$. Como temos um sistema de coordenadas em $\mathbb{P}^2$, estamos aptos para obter uma equação para a reta projetiva correspondente a r. Seja $(x_0, y_0) \in \mathbb{A}^2$ um ponto de r, então o ponto $[x_0 : y_0 : 1]$ é um ponto na reta projetiva correspondente e satisfaz

$$\langle (x_0, y_0, 1) \, , (\alpha, \beta, \gamma) \rangle = 0.$$

Além disso, o ponto no infinito associado a r, corresponde à reta afim de mesma direção passando pela origem, ou seja, é a reta

$$\alpha x + \beta y = 0, \quad z = 0.$$

Em termos de coordenadas homogêneas, esse ponto no infinito é $[\beta : -\alpha : 0]$.

Logo, os pontos $[X : Y : Z]$ na reta projetiva correspondente a r, satisfazem a condição $\langle (X, Y, Z), (\alpha, \beta, \gamma) \rangle = 0$, ou seja,

$$\alpha X + \beta Y + \gamma Z = 0. \tag{1.1}$$

Por outro lado, se um ponto $[X : Y : Z]$ do plano projetivo satisfaz a Equação (1.1) e $Z \neq 0$, então $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$ é um ponto de r. Se um ponto $[X : Y : Z]$ do plano projetivo satisfaz a Equação (1.1) e $Z = 0$, então $[X : Y : Z] = [\beta : -\alpha : 0]$ é o ponto no infinito de r. Portanto, os pontos que satisfazem a Equação (1.1), são pontos da reta projetiva correspondente a r. Daí, podemos concluir que a reta projetiva correspondente a reta r é definida pela Equação (1.1), que se identifica naturalmente com um plano em $\mathbb{A}^3$, passando pela origem.

Exemplo 1.1. Consideremos as retas afins r_1 e r_2, definidas pelas equações $x = 1$ e $x = 2$, respectivamente. Essas retas são paralelas, portanto não se intersectam no plano afim. Pelo que discutimos acima, as retas projetivas correspondentes a r_1 e r_2 são definidas por $X - Z = 0$ e $X - 2Z = 0$, respectivamente, e se intersectam no ponto no infinito $[0 : 1 : 0]$.

1.2 Curvas no Plano Projetivo

Construímos o plano projetivo para contornar o fato de que retas paralelas, no plano afim, não se intersectam. Uma pergunta natural que surge é o que ocorre com a interseção de curvas de maior grau?

Mencionamos na Introdução que uma curva algébrica afim (ou simplesmente curva afim) é definida da seguinte forma:

Definição 1.2. Uma *curva afim* é o conjunto de pontos $(x, y) \in \mathbb{A}^2$ que anula o polinômio não constante $f \in \mathbb{K}[x, y]$, ou seja, $C = \{(x, y) \in \mathbb{A}^2; f(x, y) = 0\}$. Neste caso, indicamos $C : f(x, y) = 0$.

Nesta seção, definiremos o que é uma curva no plano projetivo a partir de uma curva afim, como fizemos no caso de retas, além disso, estudaremos algumas de suas propriedades.

Seja $C_0 : f(x,y) = 0$ uma curva algébrica afim. Queremos definir uma curva projetiva C que seja uma extensão natural de C_0, ou seja, a bijeção $(x,y) \leftrightarrow [x:y:1]$ induz uma bijeção entre pontos de C_0 e pontos de $C - L_\infty$. Esta condição é equivalente a dizer que $[X:Y:Z] \in C$ com $Z \neq 0$ se, e somente se, $f(X/Z, Y/Z) = 0$. Obviamente a equação $f(X/Z, Y/Z) = 0$ não faz sentido quando $Z = 0$, mas se multiplicarmos a equação por uma potência suficientemente grande de Z obteremos uma equação polinomial nas variáveis X, Y e Z. Ao tomarmos d como sendo o grau máximo dentre os monômios de f, temos que Z^d é a menor potência de Z tal que $Z^d f(X/Z, Y/Z)$ é um polinômio nas variáveis X, Y e Z. Além disso, esse polinômio não é divisível por Z. Definindo $F(X,Y,Z) = Z^d f(X/Z, Y/Z)$, temos que F satisfaz a condição

$$F(tX, tY, tZ) = t^d F(X,Y,Z), \tag{1.2}$$

daí segue que a equação $F = 0$ é bem definida no plano projetivo.

Chamamos os polinômios que satisfazem esta condição (1.2) de *polinômios homogêneos de grau d*. Denotaremos o grau do polinômio homogêneo F por $\delta(F)$, também denotaremos o grau do polinômio $F \in \mathbb{K}[X,Z][Y]$ por $\delta_Y(F)$. A condição (1.2) é equivalente a afirmar que F é uma combinação linear dos monômios $X^i Y^j Z^k$ com $i + j + k = d$.

Uma propriedade importante dos polinômios homogêneos é que eles satisfazem

$$XF_X + YF_Y + ZF_Z = \delta(F) F, \tag{1.3}$$

tal relação é chamada *Identidade de Euler*. Para demonstrar sua validade, basta verificar primeiramente para os monômios da forma $X^i Y^j Z^k$, e o caso geral segue pela linearidade da derivada.

Definição 1.3. Uma *curva projetiva* é o conjunto de pontos $[X:Y:Z] \in \mathbb{P}^2$ que anula um polinômio homogêneo $F \in \mathbb{K}[X,Y,Z]$, ou seja, $C = \{[X:Y:Z] \in \mathbb{P}^2; F(X,Y,Z) = 0\}$. Neste caso, indicamos $C : F(X,Y,Z) = 0$. O *grau* da curva C é o grau do polinômio F.

O processo de obter o polinômio homogêneo F a partir do polinômio f é chamado de *homogeneização* de f e o polinômio F obtido da homogeneização de f é denotado por f^*. A curva $C : F(X,Y,Z) = 0$ obtida de $C_0 : f(x,y) = 0$ pela homogeneização de f é chamada de fecho projetivo de C_0 e denotada por C_0^*.

Se $P = [a:b:c]$ é um ponto da curva projetiva $C : F(X,Y,Z) = 0$ com $c \neq 0$, então

$$\left(\frac{a}{c}, \frac{b}{c}\right) \in \mathbb{A}^2 \subset \mathbb{P}^2 = \mathbb{A}^2 \cup \{ \text{ direções em } \mathbb{A}^2 \ \}.$$

Como $P \in C$, temos que $F(a,b,c) = 0$, combinando com o fato que F é homogêneo de grau d concluímos que

$$0 = \frac{1}{c^d} F(a,b,c) = F\left(\frac{a}{c}, \frac{b}{c}, 1\right),$$

ou seja, considerando o polinômio $f(x,y)$ como

$$f(x,y) = F(x,y,1),$$

então temos uma bijeção

$$\{[a:b:c] \in C; c \neq 0\} \longrightarrow \{(x,y) \in \mathbb{A}^2; f(x,y) = 0\},$$
$$[a:b:c] \longmapsto (a/c, b/c).$$

Chamamos a curva $C_0 : f(x,y) = 0$ de *parte afim* da curva projetiva C.

Vimos que ao considerarmos uma curva projetiva $C : F(X,Y,Z) = 0$, então podemos escrever C como a união de sua parte afim e seus pontos no infinito.

O processo de obter $f(x,y) = F(x,y,1)$ a partir do polinômio homogêneo $F(X,Y,Z)$, é chamado *desomogeneização (com respeito à variável Z)*. Quando não houver confusão quanto a variável de desomogeneização, denotaremos a desomogeneização de F por F_*.

O seguinte lema lista algumas propriedades quanto a homogeneização/desomogeneização de polinômios não constantes, como enunciado em [Vai17, Exercício 63] ou [Ful08, Seção 2.6]:

Lema 1.4. *Sejam $f, g \in \mathbb{K}[x,y]$ não constantes e $F, G \in \mathbb{K}[X,Y,Z]$ homogêneos e não constantes, então:*

(i) $f = (f^*)_*$;

(ii) Em geral, $(F_*)^*$ *divide* F. *Se* Z *não divide* F, *então* $F = (F_*)^*$;

(iii) $(fg)^* = f^* g^*$;

(iv) $(FG)_* = F_* G_*$.

Demonstração. Demonstraremos apenas o item (iii), os demais seguem de maneira análoga.

Consideremos $f = f_0 + f_1 + \cdots + f_m$ e $g = g_0 + g_1 + \cdots + g_n$, com $f_i, g_i \in \mathbb{K}[x,y]$ homogêneos de grau i e $f_m g_n \neq 0$.

Pela homogeneidade dos polinômios f_i's e g_i's e pelo fato dos polinômios f e g terem graus m e n, respectivamente, temos que

$$f^* = f\left(\frac{X}{Z}, \frac{Y}{Z}\right) Z^m = f_0(X,Y) Z^m + f_1(X,Y) Z^{m-1} + \cdots + f_m(X,Y) \quad \text{e}$$
$$g^* = g\left(\frac{X}{Z}, \frac{Y}{Z}\right) Z^n = g_0(X,Y) Z^n + g_1(X,Y) Z^{n-1} + \cdots + g_n(X,Y).$$

Portanto, $f^*g^* = \sum_{k=0}^{m+n} H_k$, com H_k dado por

$$\begin{aligned} H_k &= \sum_{i=0}^{k} \left(\left(f_i(X,Y) Z^{m-i} \right) \left(g_{k-i}(X,Y) Z^{n-k+i} \right) \right) \\ &= \sum_{i=0}^{k} \left(f_i(X,Y) g_{k-i}(X,Y) Z^{m+n-k} \right). \end{aligned} \tag{1.4}$$

Por outro lado, o polinômio fg tem grau $m+n$ e é dado por $fg = \sum_{k=0}^{m+n} h_k$, com h_k sendo o polinômio homogêneo de grau k determinado por $h_k = \sum_{i=0}^{k} f_i g_{k-i}$. Logo,

$$(fg)^* = \left(\sum_{k=0}^{m+n} h_k \right)^* = \left(\sum_{k=0}^{m+n} h_k \left(\frac{X}{Z}, \frac{Y}{Z} \right) \right) Z^{m+n} = \sum_{k=0}^{m+n} \left(h_k \left(\frac{X}{Z}, \frac{Y}{Z} \right) Z^{m+n} \right). \tag{1.5}$$

Uma vez que h_k é homogêneo de grau k, temos que $h_k\left(\frac{X}{Z}, \frac{Y}{Z}\right) Z^{m+n} = h_k(X,Y) Z^{m+n-k}$. Portanto, pela Equação (1.4) e Equação (1.5), temos que

$$\begin{aligned} (fg)^* &= \sum_{k=0}^{m+n} \left(h_k(X,Y) Z^{m+n-k} \right) \\ &= \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} \left(f_i(X,Y) g_{k-i}(X,Y) \right) Z^{m+n-k} \right) \\ &= \sum_{k=0}^{m+n} H_k \\ &= f^*g^*. \end{aligned}$$

□

Exemplo 1.5. A desomogeneização do polinômio homogêneo $F = XZ$ é o polinômio $F_* = x$, mas $(F_*)^* = X \neq F$. Esse exemplo mostra a importância de F não ser divisível por Z, para obter a igualdade na propriedade (ii) do lema anterior.

Uma consequência das propriedades (i) e (ii) do Lema 1.4, é que existe uma bijeção entre curvas afins e curvas projetivas que não contêm todos os pontos no infinito.

No processo de desomogeneização em relação à variável Z descrito acima, estamos realizando uma identificação do plano afim $\mathbb{A}^2$ com o plano $Z = 1$ contido em $\mathbb{A}^3$. Podemos fazer o mesmo tipo de identificação com qualquer plano $\pi \subset \mathbb{A}^3$ que não passa pela origem, sendo $(a(r,s), b(r,s), c(r,s))$ uma parametrização para π, podemos definir a equação afim

$$f_\pi(r,s) = F(a(r,s), b(r,s), c(r,s)),$$

como sendo a desomogeneização com respeito ao plano π.

Diremos que uma curva C é *definida sobre os racionais* se ela pode ser definida por uma equação polinomial com coeficientes no corpo dos números racionais.

Note que dado $F \in \mathbb{Q}[X,Y,Z]$, as soluções das equações $F = 0$ e $cF = 0$ são as mesmas para qualquer racional c não nulo. Ao escolhermos c não nulo adequado, temos que cF é um polinômio com coeficientes inteiros. Isto permite concluir que uma curva algébrica definida sobre os racionais é, na verdade o conjunto de soluções de uma equação polinomial com coeficientes inteiros.

Definição 1.6. Seja $C : F(X,Y,Z) = 0$ uma curva projetiva definida sobre os racionais. O conjunto dos *pontos racionais* de C, o qual denotaremos por $C(\mathbb{Q})$, é o conjunto dos pontos de C que têm coordenadas em $\mathbb{Q}$, ou seja,

$$C(\mathbb{Q}) = \{[a:b:c] \in \mathbb{P}^2; F(a,b,c) = 0 \text{ e } a,b,c \in \mathbb{Q}\}.$$

Alguns dos mais famosos teoremas em teoria dos números envolvem questões relacionas a determinar o conjunto dos pontos racionais $C(\mathbb{Q})$ de certas curvas. Por exemplo, o Último Teorema de Fermat, provado por Wiles em 1994, garante que as curvas projetivas

$$C_N : X^N + Y^N = Z^N,$$

com $N > 2$, não têm pontos racionais com todas as coordenadas não nulas.

Similarmente ao caso projetivo, se $C_0 : f(x,y) = 0$ é uma curva afim definida sobre os racionais, então o conjunto dos pontos racionais de C_0, que denotaremos por $C_0(\mathbb{Q})$, consiste em todos $(r,s) \in C_0$ com $r,s \in \mathbb{Q}$. Por definição, C_0 é a parte afim de seu fecho projetivo C, então $C(\mathbb{Q})$ consiste em $C_0(\mathbb{Q})$ juntamente com os pontos no infinito que forem racionais.

De modo análogo, definimos o conjunto dos *pontos inteiros* de C e C_0, o qual denotamos por $C(\mathbb{Z})$ e $C_0(\mathbb{Z})$, respectivamente, como sendo o conjunto dos pontos de C e C_0

que têm coordenadas inteiras, ou seja,

$$C(\mathbb{Z}) = \{[a:b:c] \in \mathbb{P}^2; F(a,b,c) = 0 \text{ e } a,b,c \in \mathbb{Z}\} \text{ e}$$
$$C_0(\mathbb{Z}) = \{(r,s) \in \mathbb{A}^2; f(r,s) = 0 \text{ e } r,s \in \mathbb{Z}\}.$$

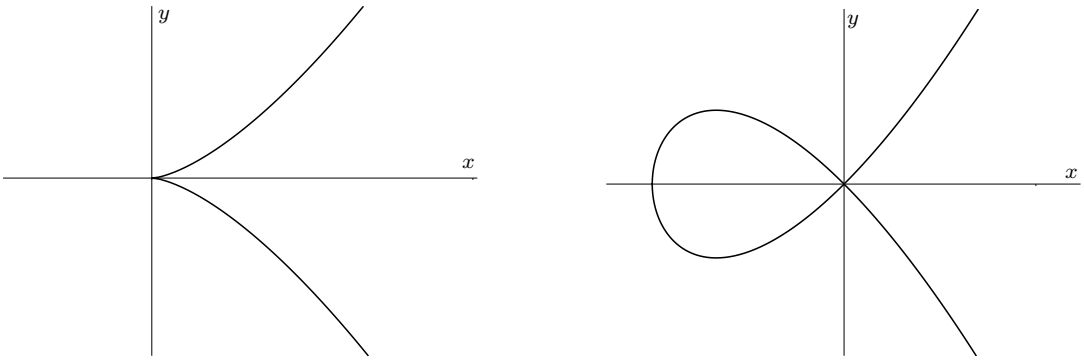
Sejam $a,b,c \in \mathbb{Q}$, como $[a:b:c] = [ta:tb:tc]$ para todo $t \neq 0$, tomando t igual ao mínimo múltiplo comum dos denominadores de a, b e c, podemos concluir que pontos racionais no plano projetivo podem ser representados por coordenadas homogêneas inteiras. Portanto, o conjunto de pontos inteiros de uma curva projetiva coincide com o conjunto dos pontos racionais.

Uma das questões fundamentais respondida pelo cálculo diferencial, é como encontrar a reta tangente à uma curva. Mais especificamente, se $C_0 : f(x,y) = 0$ é uma curva afim e $P = (r,s)$ é um ponto de C_0, então a equação da reta tangente à C_0 em P é dada pela equação

$$\frac{\partial f}{\partial x}(r,s)(x-r) + \frac{\partial f}{\partial y}(r,y)(y-s) = 0.$$

Note que se ambas as derivadas parciais de f forem nulas em P, a reta tangente não está bem definida em P. Por exemplo, isso acontece para cada uma das curvas $C_1 : y^2 = x^3$ e $C_2 : y^2 = x^3 + x^2$, no ponto $P = (0,0)$, (veja Figura 1.4). Em particular, a curva C_2 tem uma auto-interseção no ponto P, portanto, temos ambiguidade para definir tangente à curva neste ponto. A curva C_1, por outro lado, nos daria como reta limite das secantes passando por P, a reta $y = 0$.

Tais comportamentos são exemplos do conceito abaixo.



(a) Curva $C_1 : y^2 = x^3$. (b) Curva $C_2 : y^2 = x^3 + x^2$.

Figura 1.4: Curvas singulares.

Definição 1.7. Sejam $C : f(x,y) = 0$ uma curva afim e $P \in C$. Dizemos que P é um *ponto singular* de C se

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

caso contrário $P \in C$ é chamado *não singular* ou *regular*. Uma curva C é dita *regular* ou *não singular*, se todo ponto $P \in C$ é regular.

Outro conceito importante no estudo das curvas algébricas é definido a seguir:

Definição 1.8. Diremos que uma curva afim $C : f(x,y) = 0$ é *irredutível (redutível)*, se o polinômio f for irredutível (redutível) em $\mathbb{C}[x,y]$.

Definição 1.9. Se $C : f(x,y) = 0$ é uma curva afim e $f = f_1 f_2 \cdots f_n$ é uma decomposição em fatores irredutíveis em $\mathbb{C}[x,y]$, então diremos que as curvas $C_i : f_i(x,y) = 0$ são *componentes irredutíveis* de C.

Segue da definição, que se uma curva C tem componentes irredutíveis $C_1, C_2, \ldots, C_n$, então

$$C(\mathbb{Q}) = C_1(\mathbb{Q}) \cup \cdots \cup C_n(\mathbb{Q}).$$

Por conta disso, basta determinarmos os pontos racionais em curvas irredutíveis para determinarmos os pontos racionais de curvas gerais. Portanto, teremos as curvas irredutíveis como foco principal.

Para uma curva projetiva $C : F(X,Y,Z) = 0$ as definições de ponto singular, regular, reta tangentes e componentes irredutíveis são análogas. Em particular, a equação da reta tangente à C no ponto $P = [X_0 : Y_0 : Z_0]$ é dada por

$$F_X(P)(X - X_0) + F_Y(P)(Y - Y_0) + F_Z(P)(Z - Z_0) = 0.$$

Pela Identidade de Euler (1.3), temos que

$$0 = \delta(F) F(P) = X_0 F_X(P) + Y_0 F_Y(P) + Z_0 F_Z(P),$$

portanto, a reta tangente à C em P se resume a

$$T_P C : F_X(P) X + F_Y(P) Y + F_Z(P) Z = 0.$$

Quando consideramos curvas definidas por uma equação polinomial, é natural fazer uma mudança de variáveis para simplificar tal equação.

Dados[2] $T_1 \in GL_2(\mathbb{Q})$ e $T_2 \in \mathbb{Q}^2$, a transformação invertível, de $\mathbb{Q}^2$ em $\mathbb{Q}^2$, que associa $\mathrm{x} \in \mathbb{Q}^2$ em $T_1\mathrm{x} + T_2$ é chamada *transformação afim racional*.

No caso projetivo podemos fazer o mesmo usando as coordenadas homogêneas. Entretanto, para uma tal transformação estar bem definida no plano projetivo $\mathbb{P}^2$, devemos considerar somente a parte linear, ou seja, devemos considerar somente as transformações que associam $\mathrm{x} \in \mathbb{P}^2$ a $M\mathrm{x} \in \mathbb{P}^2$, com $M = (m_{ij})_{1\leq i,j\leq 3} \in GL_3(\mathbb{Q})$. Esta transformação nos dá a substituição

$$\begin{aligned} X &= m_{11}X' + m_{12}Y' + m_{13}Z', \\ Y &= m_{21}X' + m_{22}Y' + m_{23}Z', \\ Z &= m_{31}X' + m_{32}Y' + m_{33}Z'. \end{aligned} \tag{1.6}$$

Portanto, dada uma curva $C : F(X, Y, Z) = 0$, ao realizarmos a substituição (1.6) obtemos uma nova curva C' dada pela equação $F'(X', Y', Z') = 0$, com

$$\begin{aligned} F'(X', Y', Z') = F(&m_{11}X' + m_{12}Y' + m_{13}Z', \\ &m_{21}X' + m_{22}Y' + m_{23}Z', m_{31}X' + m_{32}Y' + m_{33}Z'). \end{aligned}$$

Vale observar que F' é a composição das aplicações homogêneas F e M. Assim, F' também é homogênea e como M é invertível e linear, então F' tem o mesmo grau de F.

A mudança de coordenadas (1.6) induz uma aplicação de C' para C, isto é, dado um ponto $[a' : b' : c'] \in C'$, substituímos $X' = a'$, $Y' = b'$ e $Z' = c'$ em (1.6) para obter um ponto $[a : b : c] \in C$. Além disso, a aplicação $M|_{C'} : C' \to C$ admite inversa, pois M é invertível, mais precisamente, se $M^{-1} = (n_{ij})_{1\leq i,j\leq 3}$, então a aplicação

$$\begin{aligned} X' &= n_{11}X + n_{12}Y + n_{13}Z, \\ Y' &= n_{21}X + n_{22}Y + n_{23}Z, \\ Z' &= n_{31}X + n_{32}Y + n_{33}Z, \end{aligned}$$

que associa pontos de C a pontos de C', é a aplicação inversa de M. Chamaremos uma mudança de coordenadas no plano projetivo $\mathbb{P}^2$, dada por uma matriz invertível 3×3, de *transformação projetiva racional*. Observamos que uma transformação projetiva racional nos dá uma bijeção entre $C(\mathbb{Q})$ e $C'(\mathbb{Q})$, ou seja, o problema de encontrar os pontos racionais na curva C é equivalente a encontrar os pontos racionais na curva C'.

[2] $GL_n(\mathbb{Q})$ denotando o grupo multiplicativo das matrizes invertíveis $n \times n$ com entradas racionais.

1.3 Interseção de Curvas Projetivas

Na Seção 1.1, ilustramos um modo de apresentar o plano projetivo de modo a garantir que duas retas projetivas distintas se intersectem em exatamente um ponto. Nesta seção, estudaremos a interseção entre curvas projetivas de maior grau. Vale notar, que mesmo que nosso interesse inicial seja estudar uma curva afim, adicionando apenas uma quantidade finita de pontos no infinito a esta curva obtemos seu fecho projetivo.

Iniciemos analisando a interseção, sobre $\mathbb{C}$, entre a reta $C : Y = 0$ e a curva dada por $D : F(X, Z) - YZ^{d-1} = 0$ em que $[X : Y : Z] \in \mathbb{P}^2$ e $F \in \mathbb{C}[X, Z]$ é homogêneo de grau $d > 1$. Pode-se verificar que $[X : Y : Z] \in C \cap D$ se, e somente se, $Y = 0$ e $F(X, Z) = 0$, portanto, o número de pontos na interseção de C com D é igual ao número de raízes de F, que pelo Teorema Fundamental da Álgebra, é exatamente d se considerarmos a multiplicidade das raízes de F.

Exemplo 1.10. Consideremos as curvas projetivas

$$C : Y = 0, \qquad D_1 : X^2 + Z^2 - YZ \qquad e \qquad D_2 : X^2 - YZ.$$

Temos que $C \cap D_1 = \{[\pm i : 0 : 1]\}$ e $C \cap D_2 = \{[0 : 0 : 1]\}$.

Os exemplos apresentados acima indicam que quando trabalhamos com curvas de maior grau, o plano projetivo não é o suficiente, precisamos também que o corpo seja algebricamente fechado e estender a noção de multiplicidade das raízes de polinômios em uma variável para interseção de curvas projetivas, em geral.

Nos casos apresentados acima, observarmos que a projeção $[X : Y : Z] \to [X : Z]$ induz uma bijeção entre os pontos do plano projetivo que estão na interseção das curvas $C : Y = 0$ e $D : F(X, Z) - YZ^{d-1} = 0$ e os pontos da reta projetiva que são raízes do polinômio F. Veremos que a ideia de projetar bijetivamente os pontos de interseção de duas curvas no conjunto de raízes de um polinômio F também será crucial no caso geral. Ao obtermos tal projeção, para recuperar o ponto na interseção, projetado na raiz $[X_0 : Z_0]$ de F, precisamos analisar os pontos nas interseções das curvas com a reta parametrizada por $\varphi(u, v) = [uX_0 : v : uZ_0]$ o que, em geral, é mais fácil de analisar.

Lema 1.11. *Sejam $C : F(X, Y, Z) = 0$ uma curva projetiva de grau d e L uma reta projetiva com parametrização $\varphi(u, v)$. Então $F(\varphi(u, v))$ é identicamente nulo ou homogêneo de grau d. Além disso, o ponto $\varphi(u_0, v_0) \in C \cap L$ se, e somente se, $F(\varphi(u_0, v_0)) = 0$.*

Demonstração. Seja $t \in \mathbb{C}^*$. Como φ é a parametrização de uma reta projetiva, então $\varphi(u,v) = [\alpha(u,v) : \beta(u,v) : \gamma(u,v)]$ com α, β e γ homogêneos de grau um, logo

$$\varphi(tu,tv) = [t\alpha(u,v) : t\beta(u,v) : t\gamma(u,v)].$$

Como F é homogêneo de grau d, então $F(tX,tY,tZ) = t^d F(X,Y,Z)$ para todo $[X:Y:Z] \in \mathbb{P}^2$, portanto

$$F(\varphi(tu,tv)) = F(t\alpha(u,v), t\beta(u,v), t\gamma(u,v)) = t^d F(\varphi(u,v)).$$

Logo, podemos concluir que $F(\varphi(u,v))$ é identicamente nulo ou homogêneo de grau d.

A última afirmação do lema, segue do fato de φ ser uma parametrização de L. □

Corolário 1.12. *Sejam C e L como no Lema 1.11. Então existe um ponto $[u_0 : v_0]$, tal que $F(\varphi(u_0,v_0)) = 0$.*

Demonstração. Pelo Lema 1.11, temos que $f(u,v) = F(\varphi(u,v))$ é identicamente nulo ou homogêneo de grau d.

Se $f(u,v)$ é identicamente nulo, podemos tomar $[u_0 : v_0] = [0:1]$. Caso contrário, pelo Teorema Fundamental da Álgebra, temos que

$$f(u,v) = \prod_{i=1}^{d} (\alpha_i u - \beta_i v),$$

com, $[\alpha_i : \beta_i] \in \mathbb{P}^1$ para cada $1 \leq i \leq d$. Sendo assim podemos tomar $[u_0 : v_0] = [\beta_1 : \alpha_1]$. □

Segue do Lema 1.11 que temos uma bijeção entre os parâmetros que anulam $f = F(\varphi)$ e os pontos da interseção entre a curva e a reta, portanto a multiplicidade de uma raiz de f induz uma noção de multiplicidade para o ponto de interseção correspondente.

Definição 1.13. Sejam $C : F = 0$ uma curva projetiva e L uma reta projetiva que não é componente de C. Sejam $\varphi(u,v)$ uma parametrização de L e $P_0 = \varphi(u_0,v_0) \in L$. Definimos o *número de interseção* $I(C \cap L, P_0)$ como sendo a multiplicidade de $[u_0 : v_0]$ como raiz de $F(\varphi(u,v)) = 0$.

Na Definição 1.13, consideramos uma parametrização de uma reta e definimos o número de interseção que estende a noção de multiplicidade de uma raiz, que temos quando

estudamos o gráfico de uma função polinomial, para a interseção entre uma curva e uma reta projetiva. Nos resultados seguintes observamos que essa definição independe da escolha da parametrização e é invariante sobre transformação projetiva.

Lema 1.14. *O número de interseção $I(C \cap L, P)$ depende somente de C, L e de P, ou seja, não depende da parametrização de L. Além disso, o número de interseção é invariante sobre transformação projetiva*

Demonstração. Ver demonstração em [Gib98, Lema 10.3 e Lema 11.7]. □

Uma vez que temos definido o número de interseção entre uma curva e reta projetiva, estamos em posição de apresentar os seguintes resultados:

Proposição 1.15. *Seja $C : F(X, Y, Z) = 0$ uma curva projetiva regular. Então temos que $I(C \cap L, P) > 1$ se, e somente se, L é a reta tangente à C no ponto P.*

Demonstração. Sejam $P \in C$, $Q \in \mathbb{P}^2 - \{P\}$ e $L = \overline{PQ}$. Então a reta L é parametrizada por $\varphi(s,t) = sP + tQ$.

Consideremos a equação de interseção, entre $C \cap L$, dada por $\psi(s,t) = F(\varphi(s,t))$. Por hipótese $P \in C \cap L$, portanto, $\psi(s,t) = t\gamma(s,t)$ para algum $\gamma \in \mathbb{C}[s,t]$ homogêneo não nulo.

Note que $\psi_t(s,t) = \nabla F(\varphi(s,t)) \cdot \varphi_t(s,t) = \nabla F(\varphi(s,t)) \cdot Q$, isto é, o produto escalar do gradiente de F por Q. Além disso, $I(C \cap L, P) > 1$ se, e somente se, t divide γ, ou seja, $(1,0)$ é uma raiz de γ. Como

$$\psi_t(1,0) = (\gamma + t\gamma_t)(1,0) = \gamma(1,0) = \nabla F(P) \cdot Q,$$

temos que $I(C \cap L, P) > 1$ se, e somente se, $\nabla F(P) \cdot Q = 0$, isto é, $Q \in T_P C$, com $T_P C$ denotando a reta tangente à C no ponto P.

Uma vez que $P \in T_P C$, podemos concluir que $I(C \cap L, P) > 1$ se, e somente se, $L = \overline{PQ} = T_P C$. □

Considerando C uma curva algébrica regular, $P \in C$ e $T_P C$ a reta tangente à C no ponto P. A Proposição 1.15 garante que $I(C \cap T_P C, P) > 1$. Entretanto, há pontos em que $I(C \cap T_P, P) > 2$, o que nos leva à seguinte definição:

Definição 1.16. Sejam P um ponto regular em uma curva projetiva C e T_PC a reta tangente à C no ponto P. Dizemos que P é *ponto de inflexão*, se $I\left(C \cap T_PC, P\right) > 2$.

Exemplo 1.17. Consideremos C uma curva projetiva regular na forma

$$C : Y^2Z - \left(X^3 + aX^2Z + bXZ^2 + cZ^3\right) = 0.$$

Então $\mathcal{O} = [0 : 1 : 0]$ é um ponto de inflexão de C.

De fato, claramente $\mathcal{O} \in C$ e como $\nabla\left(C\right)\left(\mathcal{O}\right) = [0 : 0 : 1]$, então a reta tangente à C no ponto $\mathcal{O}$ é a reta $T_{\mathcal{O}} : Z = 0$. Como $T_{\mathcal{O}}$ tem parametrização $\varphi\left(s, t\right) = [s : t : 0]$, então a equação de interseção de $T_{\mathcal{O}}$ e C é $s^3 = 0$. Portanto,

$$3 = I\left(C \cap T_{\mathcal{O}}, \varphi\left(0, 1\right)\right) = I\left(C \cap T_{\mathcal{O}}, \mathcal{O}\right),$$

o que nos permite concluir que $\mathcal{O}$ é um ponto de inflexão.

Teorema 1.18 (Teorema de Bézout - Caso curva e reta)**.** *Sejam C uma curva projetiva definida por um polinômio de grau n e L uma reta projetiva que não é componente de C. Então*

$$\sum_{P_i \in C \cap L} I\left(C \cap L, P_i\right) = n.$$

Demonstração. Sejam $\varphi\left(u, v\right)$ uma parametrização de L e $P_1, \ldots, P_l \in C \cap L$ o conjunto dos pontos de interseção dois a dois distintos, com $\varphi\left(u_i, v_i\right) = P_i$ para todo $1 \leq i \leq l$. Pelo Lema 1.11, temos que $\left\{[u_i : v_i]\,; 1 \leq i \leq l\right\}$ é o conjunto das raízes do polinômio $F\left(\varphi\left(u, v\right)\right)$ de grau n. Sendo m_i a multiplicidade da raiz $[u_i : v_i]$, temos que

$$n = \sum_{1 \leq i \leq l} m_i = \sum_{1 \leq i \leq l} I\left(C \cap L, P_i\right).$$

□

O Teorema de Bézout, que provamos acima no caso de uma das curvas ser uma reta, mostra que o número de pontos de interseção (se contados adequadamente) depende somente dos graus das curvas.

O resultado anterior pode ser estendido ao caso geral, para tanto, precisamos determinar algum polinômio definido sob a reta projetiva, tal que suas raízes são projeções dos pontos na interseção. Um modo de verificar a existência de tal polinômio, é determinarmos se existe alguma combinação não nula dos polinômios que definem as curvas que elimina uma das variáveis.

Apesar de nosso interesse ser em verificar se alguma combinação dos polinômios $F, G \in \mathbb{C}[X, Y, Z]$ elimina uma das variáveis, consideraremos um contexto mais geral que será útil mais adiante: Sendo $\mathbb{D}$ um domínio de fatoração única e $F, G \in \mathbb{D}[Y]$ não ambos constantes, verificaremos que existem $A, B \in \mathbb{D}[Y]$, tais que $AF + BG \in \mathbb{D}$ é não nulo.

Observação 1.19. Podemos supor que a condição de $F, G \in \mathbb{D}[Y]$ serem não ambos constantes é sempre satisfeita, trocando Y por X ou Z se necessário.

Primeiramente, observamos que existem $A', B' \in \mathbb{D}[Y]$ satisfazendo $A'F + B'G \in \mathbb{D} - \{0\}$ se, e somente se, existem $A, B \in Frac(\mathbb{D})[Y]$ satisfazendo $AF + BG \in Frac(\mathbb{D})^*$, com $Frac(\mathbb{D})$ sendo o corpo de frações de $\mathbb{D}$.

Por trabalharmos com $Frac(\mathbb{D})$ ao invés de $\mathbb{D}$, temos a vantagem de que $Frac(\mathbb{D})[Y]$ é um Domínio Euclidiano, ou seja, o algoritmo da divisão de Euclides é válido em $Frac(\mathbb{D})[Y]$. Além disso, se existem $A, B \in Frac(\mathbb{D})[Y]$ que satisfazem $AF + BG \in Frac(\mathbb{D})^*$, então podemos supor sem perda de generalidade que $\delta(A) < \delta(G)$ e $\delta(B) < \delta(F)$. De fato, como $Frac(\mathbb{D})[Y]$ é um Domínio Euclidiano e $\delta(F) > 0$, então existem $Q, R \in Frac(\mathbb{D})[Y]$, tais que $B = QF + R$ e $\delta(R) < \delta(F)$, logo

$$\begin{aligned} AF + BG &= AF + (QF + R)G \\ &= (A + QG)F + RG. \end{aligned}$$

Como $AF + BG \in Frac(\mathbb{D})^*$ então $0 = \delta(AF + BG) = \delta((A + QG)F + RG)$, portanto, $\delta(RG) = \delta((A + QG)F)$. Como $Frac(\mathbb{D})[Y]$ é domínio podemos concluir que

$$\begin{aligned} \delta(G) &= \delta(RG) - \delta(R) \\ &> \delta((A + QG)F) - \delta(F) \\ &= \delta(A + QG), \end{aligned}$$

sendo assim, tomando $A' = (A + QG)$ e $B' = R$, temos que $A'F + B'G \in Frac(\mathbb{D})^*$ com $\delta(A') < \delta(G)$ e $\delta(B') < \delta(F)$.

Portanto, basta procurarmos por $A, B \in Frac(\mathbb{D})[Y]$ com $\delta(A) < \delta(G)$, $\delta(B) < \delta(F)$ que satisfazem $AF + BG \in Frac(\mathbb{D})^*$.

Se considerarmos o anel $Frac(\mathbb{D})[Y]$ como o $Frac(\mathbb{D})$-espaço vetorial gerado pela base canônica $\{1, Y, Y^2, Y^3, \dots\}$, então provar a existência de $A, B \in Frac(\mathbb{D})[Y]$ que

satisfazem as condições desejadas é equivalente a provar que o $Frac(\mathbb{D})$-subespaço vetorial gerado por

$$\beta = \{F, YF, Y^2F, \ldots, Y^{\delta(G)-1}F, G, YG, Y^2G, \ldots, Y^{\delta(F)-1}G\} \tag{1.7}$$

contém 1.

Proposição 1.20. *Sejam $F, G \in Frac(\mathbb{D})[Y]$ não ambos constantes. Então F e G não têm fator comum em $Frac(\mathbb{D})[Y]$ se, e somente se, o conjunto β apresentado acima é linearmente independente.*

Demonstração. Podemos supor sem perda de generalidade que F é não constante.

($\Rightarrow$) Suponha por absurdo que β seja linearmente dependente. Então existem

$$A_0, A_1, \ldots, A_{\delta(G)-1}, B_0, B_1, \ldots, B_{\delta(F)-1} \in Frac(\mathbb{D}),$$

não todos nulos, tais que

$$\left(\sum_{i=0}^{\delta(G)-1} A_i Y^i\right) F + \left(\sum_{i=0}^{\delta(F)-1} B_i Y^i\right) G = 0.$$

Definindo

$$A = \sum_{i=0}^{\delta(G)-1} A_i Y^i \qquad e \qquad B = \sum_{i=0}^{\delta(F)-1} B_i Y^i,$$

temos que A e B são não nulos, pois nem todos os A_i's e B_i's são nulos e $AF+BG = 0$. Logo, BG é não nulo e divisível por F. Como $Frac(\mathbb{D})[Y]$ é domínio de fatoração única e $\delta(B) < \delta(F)$, então nem todos os fatores irredutíveis de F dividem B simultaneamente, ou seja, algum fator irredutível de F divide G. Logo F e G têm um fator comum, mas isso contradiz a hipótese deles não terem fator comum.

Podemos então concluir que β é um conjunto linearmente independente.

($\Leftarrow$) Suponha por absurdo que $H \in Frac(\mathbb{D})[Y]$ seja um fator, não constante, comum de F e G. Então existem $\widetilde{F}, \widetilde{G} \in Frac(\mathbb{D})[Y]$, tais que

$$F = H\widetilde{F} \qquad \text{e} \qquad G = H\widetilde{G}.$$

Como estamos em um domínio de integridade e $\delta(H) > 0$, então $\delta\left(\widetilde{F}\right) < \delta(F)$ e $\delta\left(\widetilde{G}\right) < \delta(G)$. Além disso, como $H \neq 0$ e

$$\begin{aligned} 0 &= GF - GF \\ &= \left(H\widetilde{G}\right)F - G\left(H\widetilde{F}\right) \\ &= H\left(\widetilde{G}F - G\widetilde{F}\right), \end{aligned}$$

temos que $\widetilde{G}F - G\widetilde{F} = 0$. Sendo $\widetilde{F}_i, \widetilde{G}_i \in Frac(\mathbb{D})$, tais que $\widetilde{F} = \sum_{i=0}^{\delta\left(\widetilde{F}\right)} \widetilde{F}_i Y^i$ e $\widetilde{G} = \sum_{i=0}^{\delta\left(\widetilde{G}\right)} \widetilde{G}_i Y^i$, então

$$\left(\sum_{i=0}^{\delta\left(\widetilde{G}\right)} \widetilde{G}_i Y^i\right) F + \left(\sum_{i=0}^{\delta\left(\widetilde{F}\right)} \widetilde{F}_i Y^i\right) G = 0$$

e como $\widetilde{F}$ e $\widetilde{G}$ são não nulos, então nem todos os $\widetilde{F}_i$'s e $\widetilde{G}_i$'s são nulos. Como $\delta\left(\widetilde{F}\right) < \delta(F)$ e $\delta\left(\widetilde{G}\right) < \delta(G)$, podemos concluir que β é linearmente dependente, o que é um absurdo.

Portanto, F e G não têm fator comum. □

Sendo $F_0, F_1, \ldots, F_{\delta(F)}, G_0, G_1, \ldots, G_{\delta(G)} \in \mathbb{D}$, tais que

$$F = F_0 + F_1 Y + \cdots + F_{\delta(F)} Y^{\delta(F)} \qquad e \qquad G = G_0 + G_1 Y + \cdots + G_{\delta(G)} Y^{\delta(G)},$$

então o conjunto β é linearmente independente se, e somente se, a matriz

$$R_{F,G} = \begin{bmatrix} F_0 & F_1 & F_2 & \cdots & F_{\delta(F)} & & 0 \\ & F_0 & F_1 & F_2 & \cdots & F_{\delta(F)} & \\ & \ddots & \ddots & \ddots & & \ddots & \\ 0 & & & F_0 & F_1 & F_2 & \cdots & F_{\delta(F)} \\ G_0 & G_1 & G_2 & \cdots & G_{\delta(G)} & & 0 \\ & G_0 & G_1 & G_2 & \cdots & G_{\delta(G)} & \\ & \ddots & \ddots & \ddots & & \ddots & \\ 0 & & & G_0 & G_1 & G_2 & \cdots & G_{\delta(G)} \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} \delta(G) \text{ linhas} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} \delta(F) \text{ linhas} \end{matrix}$$

tem determinante não nulo.

Observação 1.21. Considerando $A_0, \ldots, A_{\delta(G)-1}, B_0, \ldots, B_{\delta(F)-1} \in \mathbb{D}$, então

$$\begin{bmatrix} A_0 & A_1 & \ldots & A_{\delta(G)-1} & B_0 & B_1 & \ldots & B_{\delta(F)-1} \end{bmatrix} R_{F,G}$$

é igual a representação de $\left(\sum_{i=0}^{\delta(G)-1} A_i Y^i\right) F + \left(\sum_{i=0}^{\delta(F)-1} B_i Y^i\right) G$ na base canônica.

Definição 1.22. Chamaremos o determinante da matriz $R_{F,G}$ de *resultante* de F e G e o denotaremos por $Res_Y(F,G)$, ou simplesmente por $Res(F,G)$, quando não houver confusão de qual é a variável em que estamos expandindo os polinômios.

Uma vez que $R_{F,G}$ tem entradas em $\mathbb{D}$, então $Res(F,G) \in \mathbb{D}$. Além disso, se $F,G \in \mathbb{D}[x_1,\ldots,x_{n-1}][x_n]$ são homogêneos e não ambos constantes, então $Res_{x_n}(F,G) \in \mathbb{D}[x_1,\ldots,x_{n-1}]$ é identicamente nulo ou homogêneo de grau $\delta(F)\,\delta(G)$. Para verificar a homogeneidade basta seguir as indicações em [Gib98, Lema 14.3].

Pelo Lema de Gauss, temos que F e G têm fator comum não constante em $\mathbb{D}[Y]$ se, e somente se, eles têm fator comum em $Frac(\mathbb{D})[Y]$.

Como consequência temos:

Corolário 1.23. *Sejam $F,G \in \mathbb{D}[Y]$ não ambos constantes. Então $Res(F,G)=0$ se, e somente se, F e G têm um fator comum em $\mathbb{D}[Y]-\mathbb{D}$.*

Demonstração. Como os elementos de β (dado em (1.7)), expressos na base canônica, são as linhas da matriz $R_{F,G}$, então β é linearmente dependente se, e somente se, $Res(F,G)=0$. Pela Proposição 1.20, obtemos que $Res(F,G)=0$ se, e somente se, F e G têm fator comum em $Frac(\mathbb{D})[Y]$. Como F e G têm um fator em $Frac(\mathbb{D})[Y]$ se, e somente se, têm um fator comum em $\mathbb{D}[Y]-\mathbb{D}$, então podemos concluir que $Res(F,G)=0$ se, e somente se, F e G têm fator comum em $\mathbb{D}[Y]-\mathbb{D}$. □

Temos agora as ferramentas para demonstrar o seguinte resultado.

Teorema 1.24. *Sejam $F,G \in \mathbb{D}[Y]$ não ambos constantes. Então existem $A,B \in \mathbb{D}[Y]$ não ambos nulos, tais que*

$$AF+BG = Res(F,G),$$

com $\delta(A)<\delta(G)$ e $\delta(B)<\delta(F)$.

Demonstração. Se $Res(F,G)=0$, pelo Corolário 1.23, F e G têm fator comum $H \in \mathbb{D}[Y]$ não constante, ou seja, existem $\widetilde{F},\widetilde{G} \in \mathbb{D}[Y]$ tais que $F=H\widetilde{F}$ e $G=H\widetilde{G}$. Logo,

$$\begin{aligned} 0 &= FG - FG \\ &= \left(H\widetilde{F}\right)G - F\left(H\widetilde{G}\right) \\ &= H\left(\widetilde{F}G - F\widetilde{G}\right), \end{aligned}$$

como $H \neq 0$, então $\widetilde{F}G - F\widetilde{G} = 0$. Tomando $A = -\widetilde{G}$ e $B = \widetilde{F}$, temos o resultado desejado no caso $Res\,(F,G) = 0$.

Se $Res\,(F,G) \neq 0$, então a matriz $R_{F,G} \in Mat_{(\delta(F)+\delta(G))}\,(Frac\,(\mathbb{D}))$ é invertível.

Dado que $Res\,(F,G) \in \mathbb{D}$, pela Observação 1.21, existem $A = \sum_{i=0}^{\delta(G)-1} A_i Y^i$ e $B = \sum_{i=0}^{\delta(F)-1} B_i Y^i$ que satisfazem $AF + BG = Res\,(F,G)$ se, e somente se, o sistema

$$\begin{bmatrix} A_0 & \dots & A_{\delta(G)-1} & B_0 & \dots & B_{\delta(F)-1} \end{bmatrix} R_{F,G} = \begin{bmatrix} Res\,(F,G) & 0 & \cdots & 0 \end{bmatrix} \tag{1.8}$$

é satisfeito.

Como $R_{F,G}$ é uma matriz com entradas em $\mathbb{D}$, então sua matriz adjunta $adj\,(R_{F,G})$ também tem entradas em $\mathbb{D}$. Uma vez que

$$R_{F,G}^{-1} = \frac{1}{Res\,(F,G)} adj\,(R_{F,G})$$

temos que o sistema (1.8) tem solução em $Frac\,(\mathbb{D})$ dada por

$$\begin{aligned} \begin{bmatrix} A_0 & \dots & A_{\delta(G)-1} & B_0 & \dots & B_{\delta(F)-1} \end{bmatrix} &= \begin{bmatrix} Res\,(F,G) & 0 & \cdots & 0 \end{bmatrix} R_{F,G}^{-1} \\ &= \frac{1}{Res\,(F,G)} \begin{bmatrix} Res\,(F,G) & 0 & \cdots & 0 \end{bmatrix} adj\,(R_{F,G}) \\ &= \begin{bmatrix} 1 & 0 & \cdots & 0 \end{bmatrix} adj\,(R_{F,G})\,, \end{aligned}$$

ou seja, a solução na verdade tem entradas em $\mathbb{D}$. Portanto, definindo

$$A = \sum_{i=0}^{\delta(G)-1} A_i Y^i \qquad e \qquad B = \sum_{i=0}^{\delta(F)-1} B_i Y^i,$$

temos que $A, B \in \mathbb{D}\,[Y]$ e, pela Observação 1.21, $AF + BG = Res\,(F,G)$.

Pela forma que definimos os polinômios A e B em cada um dos casos, segue que $\delta\,(A) < \delta\,(G)$ e $\delta\,(B) < \delta\,(F)$. □

Observação 1.25. Se $Res\,(F,G) \neq 0$ e os elementos da primeira linha da matriz adjunta $adj\,(R_{F,G})$ são divisíveis por um elemento M em $\mathbb{D}$, então por cálculos análogos aos feitos na demonstração do Teorema 1.24, podemos encontrar $A, B \in \mathbb{D}\,[Y]$ com $\delta\,(A) < \delta\,(G)$ e $\delta\,(B) < \delta\,(F)$, tais que $AF + BG = \frac{Res(F,G)}{M} \in \mathbb{D}$.

Retomando ao estudo das curvas, pelo Teorema 1.24, sempre conseguimos uma combinação entre F e G que elimina uma certa variável, desde que F e G não sejam ambos constantes em relação à variável que estamos eliminando, o que pela Observação 1.19 sempre se pode assumir.

Um fato que pode ocorrer é termos infinitos pontos na interseção. Por exemplo, as curvas projetivas $C_1 : Y = 0$ e $C_2 : XY = 0$ têm como interseção toda a curva C_1. Isso ocorre quando os polinômios que definem as curvas têm um fator em comum em $\mathbb{C}[X, Y, Z]$. A proposição a seguir mostra que se os polinômios não têm fator comum, então a interseção é finita.

Proposição 1.26. *Sejam $C_1 : F_1(X, Y, Z) = 0$ e $C_2 : F_2(X, Y, Z) = 0$ duas curvas projetivas. Então $C_1 \cap C_2$ tem uma quantidade finita de pontos se, e somente se, F_1 e F_2 não têm fator comum em $\mathbb{C}[X, Y, Z]$.*

Demonstração. ($\Rightarrow$) Suponhamos por absurdo que $H \in \mathbb{C}[X, Y, Z]$ é um fator comum de F_1 e F_2. Como

$$H(X_0, Y_0, Z_0) = 0 \quad \Longrightarrow \quad [X_0 : Y_0 : Z_0] \in C_1 \cap C_2,$$

basta mostrarmos que existem infinitos pontos que anulam H para chegarmos a uma contradição.

Seja $P_0 = [X_0 : Y_0 : Z_0] \in \mathbb{P}^2$, tal que $H(P_0) \neq 0$. Sem perda de generalidade podemos supor que $X_0 \neq 0$. Para cada $K \in \mathbb{C}$ tomamos $P_K = [0 : K : 1]$. Como $X_0 \neq 0$, então temos que $P_0 \neq P_K$, portanto, podemos definir a reta projetiva $L_K = \overline{P_0 P_K}$ com parametrização dada por $\varphi_K(u, v) = [X_0 u : Y_0 u + Kv : Z_0 u + v]$.

Como $P_{K_1} \in L_{K_2}$ se, e somente se, $K_1 = K_2$, então temos que $L_{K_1} \neq L_{K_2}$ sempre que $K_1 \neq K_2$. Além disso, para todo $K \in \mathbb{C}$ temos que $P_0 \in L_K$, portanto esse sempre é o ponto de interseção entre duas retas L_K's distintas.

Pelo Corolário 1.12, para cada $K \in \mathbb{C}$ existe $[u_K : v_K]$, tal que $H(\varphi_K(u_K, v_K)) = 0$, ou seja, existe um ponto $\varphi_K(u_K, v_K) \in L_K$ que anula H. Além disso, se $K_1 \neq K_2$ então $\varphi_{K_1}(u_{K_1}, v_{K_1}) \neq \varphi_{K_2}(u_{K_2}, v_{K_2})$, pois o único ponto que está na interseção entre L_{K_1} e L_{K_2} é o ponto P_0 que não anula H, portanto, o conjunto $S = \{\varphi_K(u_K, v_K) ; K \in \mathbb{C}\}$ está em bijeção com $\mathbb{C}$, ou seja, é infinito. Como cada um dos elementos do conjunto S anula H, temos que existem infinitos pontos que anulam H, o que é uma contradição.

Logo F_1 e F_2 não têm fator comum.

($\Leftarrow$) Consideremos coordenadas de modo que $Y = 0$ seja a reta no infinito e procedemos a desomogeneização F_{i*} de F_i em relação à variável Y.

Sejam $I_0 = C_1 \cap C_2 \cap \{Y = 0\}$ os pontos de interseção no infinito e $I_1 = C_1 \cap C_2 \cap \{Y = 1\}$ os pontos de interseção que são afins. Como $C_1 \cap C_2 = I_0 \cup I_1$, basta mostrarmos que I_0 e I_1 são finitos para mostrarmos que a interseção é finita.

Uma vez que F_1 e F_2 não têm fator comum, podemos supor sem perda de generalidade que F_1 não é divisível por Y. Logo, pela homogeneidade de F_1, temos que $F_1(X, Z) := F_1(X, 0, Z)$ é homogêneo não nulo em $\mathbb{C}[X, Z]$. Pelo Teorema Fundamental da Álgebra, existe no máximo $\delta(F_1)$ raízes de $F_1(X, Z)$. Como

$$I_0 \subset \{[X : 0 : Z]\,; F_1(X, Z) = 0\},$$

podemos concluir que I_0 é um conjunto finito.

Se F_{1*} ou F_{2*} são constantes, então $I_1 = \varnothing$.

Se F_{1*} e F_{2*} são não constantes em $\mathbb{C}[X, Z]$, mostraremos que existe uma quantidade finita de candidatos para as coordenadas X e Z dos pontos em I_1.

Coordenada X: Se F_{1*} (ou F_{2*}) pertence a $\mathbb{C}[X]$, então F_{1*} (ou F_{2*}) tem uma quantidade finita de raízes, o que limita as possíveis coordenadas X dos pontos de I_1 a um conjunto finito.

Caso F_{1*} e F_{2*} pertençam a $\mathbb{C}[X][Z] - \mathbb{C}[X]$, pelo Teorema 1.24, existem $A, B \in \mathbb{C}[X][Z]$ tais que $AF_{1*} + BF_{2*} = Res_Z(F_{1*}, F_{2*})$. Como F_1 e F_2 não têm fator comum em $\mathbb{C}[X, Y, Z]$, então F_{1*} e F_{2*} não têm fator comum em $\mathbb{C}[X, Z]$, portanto, pelo Corolário 1.23, $Res_Z(F_{1*}, F_{2*})$ é um elemento não nulo de $\mathbb{C}[X]$. Uma vez que os pontos de $\{(X, Z)\,; [X : 1 : Z] \in I_1\}$ anulam F_{1*} e F_{2*}, temos que as coordenadas X dos pontos de I_1 são raízes de $Res_Z(F_{1*}, F_{2*})$, o que nos permite limitar as coordenadas X dos pontos de I_1 a um conjunto finito.

Coordenada Z: De modo análogo, podemos limitar as possibilidades para a coordenada Z dos pontos de I_1 a um conjunto finito.

Como as coordenadas dos pontos de I_1 se resumem a um conjunto finito, então I_1 é um conjunto finito.

Portanto, podemos concluir que a interseção $C_1 \cap C_2 = I_1 \cup I_2$ é finita. □

No que segue, nos concentraremos em interseções entre curvas definidas por polinômios sem fatores em comum, o que será suficiente para nossos interesses.

Proposição 1.27. *Sejam $C_1 : F_1 = 0$ e $C_2 : F_2 = 0$ curvas projetivas sem componentes em comum. Se*

(i) $[0 : 1 : 0] \notin C_1 \cap C_2$;

(ii) para todo $P_1, P_2 \in C_1 \cap C_2$ *distintos, temos que* $[0 : 1 : 0] \notin \overline{P_1P_2}$.

(iii) existem $A_1, A_2 \in \mathbb{C}[X, Y, Z]$, *tais que* $R = A_1F_1 + A_2F_2 \in \mathbb{C}[X, Z]$ *é não nulo.*

Então a aplicação $\varphi : C_1 \cap C_2 \to R^{-1}(0) \subset \mathbb{P}^1$, *definida por* $\varphi(X, Y, Z) = (X : Z)$, *é bijetora.*

Demonstração. Como $[0 : 1 : 0] \notin C_1 \cap C_2$, então φ não leva pontos de $C_1 \cap C_2$ na origem, ou seja, $\varphi(C_1 \cap C_2) \subset \mathbb{P}^1$. Além disso, se $P \in C_1 \cap C_2$, então $F_1(P) = F_2(P) = 0$, logo $R(\varphi(P)) = A_1(P) F_1(P) + A_2(P) F_2(P) = 0$, ou seja, $\varphi(C_1 \cap C_2) \subset R^{-1}(0)$. Sendo assim, $\varphi : C_1 \cap C_2 \to R^{-1}(0)$ é uma função bem definida.

Sejam $[X_0 : Z_0] \in R^{-1}(0) \subset \mathbb{P}^1$. Para mostrarmos que φ é sobrejetora, basta garantir que existe $Y_0 \in \mathbb{C}$, tal que $[X_0 : Y_0 : Z_0] \in C_1 \cap C_2$. Consideremos a reta passando por $[0 : 1 : 0]$ e $[X_0 : 0 : Z_0]$, com parametrização dada por $\psi(s, t) = [sX_0 : t : sZ_0]$. Sejam $f_1(s, t) = F_1(\psi(s, t))$ e $f_2(s, t) = F_2(\psi(s, t))$. Como $R(\psi(s, t)) = R(sX_0, sZ_0) = 0$, então

$$0 = a_1f_1 + a_2f_2,$$

com a_1 e a_2 definidos por $a_i(s, t) = A_i(\psi(s, t))$.

Uma vez que $\psi(0, 1) = [0 : 1 : 0] \notin C_1 \cap C_2$, então f_1 e f_2 não podem ser simultaneamente identicamente nulos.

Se f_1 e f_2 estão no ideal gerado por t, então eles têm a forma $f_i = tg_i$, com $g_1, g_2 \in \mathbb{C}[s, t]$. Podemos concluir, nesse caso, que f_1 e f_2 se anulam em $[1 : 0]$. Portanto, $\psi(1, 0) = [X_0 : 0 : Z_0] \in C_1 \cap C_2$, ou seja, $[X_0 : Z_0]$ está na imagem de φ.

Agora consideremos o caso em que f_1 ou f_2 não está no ideal gerado por t. Sem perda de generalidade, podemos supor que f_1 não está no ideal gerado por t, ou seja, $\delta_s(f_1) = \delta(f_1) > 0$. Sejam $\widetilde{f}_1, \widetilde{f}_2, \widetilde{a}_1, \widetilde{a}_2 \in \mathbb{C}[s]$ definidos por $\widetilde{f}_i(s) = f_i(s, 1)$ e $\widetilde{a}_i(s) = a_i(s, 1)$,

então

$$0 = \widetilde{a_1}\widetilde{f_1} + \widetilde{a_2}\widetilde{f_2}.$$

Como $\widetilde{f_1} \in \mathbb{C}[s]$ e $\delta\left(\widetilde{f_1}\right) = \delta_s(f_1) > 0$, então existem $q, r \in \mathbb{C}[s]$ com $\delta(r) < \delta\left(\widetilde{f_1}\right)$, tais que $\widetilde{a_2} = q\widetilde{f_1} + r$. Portanto,

$$\begin{aligned} 0 &= \widetilde{a_1}\widetilde{f_1} + \widetilde{a_2}\widetilde{f_2} \\ &= \widetilde{a_1}\widetilde{f_1} + \left(q\widetilde{f_1} + r\right)\widetilde{f_2} \\ &= \left(\widetilde{a_1} + q\widetilde{f_2}\right)\widetilde{f_1} + r\widetilde{f_2}, \end{aligned}$$

obtemos então que $\widetilde{f_1}$ divide $r\widetilde{f_2}$ e como $\delta(r) < \delta\left(\widetilde{f_1}\right)$, podemos concluir que $\widetilde{f_1}$ e $\widetilde{f_2}$ têm fator comum em $\mathbb{C}[s]$. Logo, existe $s_0 \in \mathbb{C}$, tal que $\widetilde{f_1}(s_0) = \widetilde{f_2}(s_0) = 0$, ou seja, $f_1(s_0, 1) = f_2(s_0, 1) = 0$, consequentemente, $\psi(s_0, 1) = [s_0X_0 : 1 : s_0Z_0] \in C_1 \cap C_2$. Como $[0:1:0] \notin C_1 \cap C_2$, então $s_0 \neq 0$, logo $[X_0 : Z_0] = [s_0X_0 : s_0Z_0] = \varphi(\psi(s_0, 1))$, ou seja, $[X_0 : Z_0]$ está na imagem de φ.

Portanto, podemos concluir que φ é sobrejetora.

Agora sejam $P_1, P_2 \in C_1 \cap C_2$, tais que $\varphi(P_1) = \varphi(P_2)$. Então existem $X_0, Y_1, Y_2, Z_0 \in \mathbb{C}$, tais que $P_1 = [X_0 : Y_1 : Z_0]$ e $P_2 = [X_0 : Y_2 : Z_0]$. Suponhamos por absurdo que $P_1 \neq P_2$, então a reta $\overline{P_1P_2}$ é definida pela equação $Z_0X - X_0Z = 0$. Daí, teríamos que $[0:1:0] \in \overline{P_1P_2}$, o que contradiz a condição (ii). Portanto, temos que $P_1 = P_2$, o que nos permite concluir que φ é injetora. □

Como estamos considerando duas curvas projetivas que não têm componentes em comum, pela Proposição 1.26, temos interseção finita. Logo a menos de mudança de coordenadas, as condições (i) e (ii) da Proposição 1.27 são satisfeitas. Além disso, pelo Teorema 1.24, existem $A, B \in \mathbb{C}[X, Y, Z]$ tais que $AF + BG = Res(F, G) \in \mathbb{C}[X, Z]$ é não nulo, portanto, a condição (iii) também é satisfeita.

Sendo assim, a menos de mudança de coordenadas, tomando $R = Res(F, G)$ na Proposição 1.27, temos que a aplicação φ é uma bijeção entre $C_1 \cap C_2$ e $R^{-1}(0)$. Logo, a multiplicidade das raízes de R induz uma noção de multiplicidade para pontos de $C_1 \cap C_2$.

Definição 1.28. Sendo $C_1 : F_1 = 0$ e $C_2 : F_2 = 0$ curvas projetivas sem componentes em comum, podemos escolher coordenadas tais que as condições da Proposição 1.27 sejam satisfeitas, com $R = Res_Y(F_1, F_2)$. Se $P = [X_0 : Y_0 : Z_0] \in C_1 \cap C_2$, então definimos o

número de interseção $I(C_1 \cap C_2, P)$ como sendo a multiplicidade de $[X_0 : Z_0]$ como uma raiz de $Res_Y(F_1, F_2)$.

Lema 1.29. *O número de interseção* $I(C_1 \cap C_2, P)$*, introduzido na Definição 1.28, é invariante por transformações projetivas.*

Demonstração. A demonstração foge ao escopo deste trabalho, mas pode ser encontrada em [Gib98, Lema 14.11]. □

Na Definição 1.13, introduzimos a noção de número de interseção de uma curva e uma reta em um ponto P. No resultado abaixo mostramos que a Definição 1.13 e a Definição 1.28 coincidem se uma das curvas é uma reta.

Proposição 1.30. *Sejam* $C : F = 0$ *uma curva projetiva de grau* d*,* L *uma reta que não é componente de* C *e* $P \in C \cap L$*. Então os números de interseção* $I(C \cap L, P)$ *dados nas Definições 1.13 e 1.28 coincidem.*

Demonstração. Como os números de interseção são independentes do sistema de coordenadas, podemos supor $P = [1 : 0 : 0]$ e que L é a reta $Y = 0$, consequentemente, as condições da Proposição 1.27 são satisfeitas com $R = Res_Y(F, L)$.

Escrevendo $F(X, Y, Z) = F_d(X, Z) + F_{d-1}(X, Z)\,Y + \cdots + F_0(X, Z)\,Y^d$, com F_k sendo homogêneo de grau k, temos que o resultante $Res_Y(F, L)$ é o determinante da matriz

$$\begin{bmatrix} F_d & F_{d-1} & \cdots & F_1 & F_0 \\ & 1 & & & 0 \\ & & \ddots & & \\ & 0 & & 1 & \\ & & & & 1 \end{bmatrix}.$$

Portanto, $Res_Z(F, L) = F_d(X, Y)$ e pela Definição 1.28, $I(C \cap L, P)$ é a multiplicidade de $[1 : 0]$ como raiz de $F_d(X, Y)$.

Considerando a parametrização $\varphi(s, t) = [s : 0 : t]$ para a reta L, temos que $P = \varphi(1, 0)$ e que $F(\varphi(s, t)) = F_d(s, t)$. Portanto, pela Definição 1.13 temos que $I(C \cap L, P)$ é a multiplicidade de $[1 : 0]$ como raiz de $F_d(s, t) = F(\varphi(s, t))$.

Logo, podemos concluir que os números de interseção introduzidos nas duas definições coincidem no caso em que uma das curvas é uma reta. □

Como consequência do que apresentamos, temos o caso geral do Teorema 1.18.

Teorema 1.31 (Teorema de Bézout)**.** *Sejam $C_1 : F_1 = 0$ e $C_2 : F_2 = 0$ curvas projetivas sem componentes em comum. Então*

$$\sum_{P_i \in C_1 \cap C_2} I\left(C_1 \cap C_2, P_i\right) = \delta\left(C_1\right)\delta\left(C_2\right).$$

Demonstração. Segue da Definição 1.28 e do fato que $\delta\left(Res_Y\left(F_1, F_2\right)\right) = \delta\left(F_1\right)\delta\left(F_2\right)$. □

O Teorema de Bézout permite obtermos várias conclusões. Dedicamos o final desta seção para a apresentação de alguns deles que serão utilizados no decorrer do trabalho.

Lema 1.32. *Sejam $C : F\left(X, Y, Z\right) = 0$ uma curva projetiva de grau $d > 1$ e L uma reta que não é componente de C, ambas definidas sobre os racionais. Se $d-1$ dos pontos da interseção de C e L são racionais (considerando multiplicidade), então o ponto restante da interseção também é racional.*

Demonstração. Sejam $P_1, P_2, \ldots, P_d \in C \cap L$ com $P_1, \ldots, P_{d-1}$ pontos racionais.

Consideremos $\varphi\left(s,t\right)$ uma parametrização racional[3] para L e $\left[s_1 : t_1\right], \ldots, \left[s_d : t_d\right] \in \mathbb{P}^1$, tais que $P_i = \varphi\left(s_i, t_i\right)$ para cada $1 \leq i \leq d$. Sem perda de generalidade, podemos supor que $s_i, t_i \in \mathbb{Q}$, para cada $1 \leq i < d$. Como

$$f\left(s,t\right) = F\left(\varphi\left(s,t\right)\right) = \lambda \prod_{i=1}^{d} \left(t_i s - s_i t\right) \in \mathbb{Q}\left[s,t\right]$$

para algum $\lambda \in \mathbb{C}^*$, então

$$f = \lambda G\left(s,t\right)\left(t_d s - s_d t\right)$$

com $G \in \mathbb{Q}\left[s,t\right] - \{0\}$ homogêneo.

Se $s_d t_d = 0$, então $P_d \in \{[0:1], [1:0]\}$, ou seja, P_d também é um ponto racional.

Se $s_d t_d \neq 0$, então $\left[s_d : t_d\right] = \left[\frac{s_d}{t_d} : 1\right]$. Denotando o coeficiente líder do polinômio f em relação à variável s por $cl_s\left(f\right)$, temos que $cl_s\left(f\left(s,1\right)\right) = \lambda cl_s\left(G\left(s,1\right)\right) t_d$, $cl_t\left(f\left(1,t\right)\right) = -\lambda cl_t\left(G\left(1,t\right)\right) s_d$ e como $f, G \in \mathbb{Q}\left[s,t\right] - \{0\}$, então

$$\frac{s_d}{t_d} = -\frac{cl_t\left(f\left(1,t\right)\right)/cl_t\left(G\left(1,t\right)\right)}{cl_s\left(f\left(s,1\right)\right)/cl_s\left(G\left(s,1\right)\right)} \in \mathbb{Q}.$$

Logo, temos que $\left[s_d : t_d\right] = \left[\frac{s_d}{t_d} : 1\right]$ é um ponto racional, o que nos permite concluir que $P_d = \varphi\left(s_d, t_d\right)$ também é racional. □

[3] A parametrização $\varphi\left(s,t\right)$ ser racional significa que as suas coordenadas pertencem a $\mathbb{Q}\left[s,t\right]$. Obtemos tal parametrização pois $L = \overline{P_1 P_2}$ ou L é a reta tangente à C no ponto P_1.

No caso de cúbicas irredutíveis singulares temos o seguinte resultado.

Proposição 1.33. *Seja $C : F = 0$ uma curva projetiva cúbica irredutível e $P \in C$ um ponto singular. Então para toda reta L passando por P temos que $I(C \cap L, P) \geq 2$. Além disso, para no máximo duas dessas retas, temos que $I(C \cap L, P) = 3$.*

Demonstração. A menos de uma transformação projetiva (que como vimos não altera $I(C \cap L, P)$), podemos supor que $P = [0 : 0 : 1]$. Como $F(P) = 0$, então $F = F_0 + F_1 Z + F_2 Z^2$, com $F_0, F_1, F_2 \in \mathbb{C}[X, Y]$ identicamente nulos ou homogêneos de graus três, dois e um, respectivamente. Logo $F_{0X}, F_{0Y}, F_{1X}, F_{1Y} \in \langle x, y \rangle \subset \mathbb{C}[X, Y]$, ou seja, se anulam em P. Além disso, F_{2X} e F_{2Y} são constantes.

Uma vez que

$$\begin{cases} F_X &= F_{0X} + F_{1X} Z + F_{2X} Z^2 \\ F_Y &= F_{0Y} + F_{1Y} Z + F_{2Y} Z^2, \end{cases}$$

e P é um ponto de singularidade de C, então podemos concluir que $F_{2X}(P) = F_{2Y}(P) = 0$, portanto pela Identidade de Euler, $F_2 = F_{2X} X + F_{2Y} Y = 0$, ou seja,

$$F = F_0 + F_1 Z.$$

Pelo fato de $[0 : 0 : 1] \in L$, podemos parametrizar L por $\varphi(s, t) = [as : bs : t]$, com $[a : b] \in \mathbb{P}^1$. Substituindo a parametrização φ no polinômio F, obtemos

$$\begin{aligned} f(s, t) &= F(as, bs, t) \\ &= F_0(as, bs) + F_1(as, bs)\, t \\ &= F_0(a, b)\, s^3 + F_1(a, b)\, s^2 t \\ &= s^2 (F_0(a, b)\, s + F_1(a, b)\, t). \end{aligned}$$

Pela Definição 1.13, temos que $I(C \cap L, P) \geq 2$, pois $\varphi(0, 1) = P$ e s divide $f(s, t)$ com multiplicidade pelo menos dois. Além disso, $I(C \cap L, P) = 3$ se, e somente se, $F_1(a, b) = 0$. Como F_1 é homogêneo de grau dois, então existem no máximo dois pontos $[a : b] \in \mathbb{P}^1$ que anulam F_1. Portanto, podemos concluir que existem no máximo duas retas passando por P, tais que $I(C \cap L, P) = 3$. □

Como consequência temos o seguinte resultado.

Corolário 1.34. *Uma curva cúbica irredutível e singular C tem um único ponto de singularidade.*

Demonstração. Suponhamos por absurdo que existam pontos P_1 e P_2, distintos e singulares de C.

Consideremos a reta $L = \overline{P_1P_2}$. Como $P_1, P_2 \in C \cap L$, então pela Proposição 1.33, temos que $I(C \cap L, P_1) \geq 2$ e $I(C \cap L, P_2) \geq 2$. Por outro lado, como C é irredutível, então C e L não têm componente em comum. Portanto, pelo Teorema de Bézout 1.31, temos que

$$3 = \sum_{P_i \in C \cap L} I(C \cap L, P_i) \geq \sum_{i=1}^{2} I(C \cap L, P_i) \geq 4,$$

o que é um absurdo.

Logo, podemos concluir que C tem um único ponto de singularidade. □

Uma outra conclusão obtida pelo Teorema de Bézout diz respeito a existência de singularidades para curvas redutíveis.

Proposição 1.35. *Seja $C : F(X, Y, Z) = 0$ uma curva projetiva redutível. Então C é singular.*

Demonstração. Como C é redutível, existem $F_1, F_2 \in \mathbb{C}[X, Y, Z]$ homogêneos, tais que $F = F_1F_2$. Consideremos as curvas projetivas $C_1 : F_1 = 0$ e $C_2 : F_2 = 0$.

Se C_1 e C_2 têm alguma componente C_0 em comum, então podemos tomar $P_0 \in C_0 \subset C_1 \cap C_2$. Se C_1 e C_2 não têm componente em comum, pelo Teorema de Bézout 1.31, as curvas $C_1 : F_1 = 0$ e $C_2 : F_2 = 0$ se intersectam em algum ponto P_0. Em ambos os casos, existe $P_0 \in C_1 \cap C_2 \subset C$.

Como $F_W = F_{1W}F_2 + F_1F_{2W}$, para $W \in \{X, Y, Z\}$, temos que

$$F_W(P_0) = F_{1W}(P_0) F_2(P_0) + F_1(P_0) F_{2W}(P_0) = 0.$$

Segue assim que P_0 é um ponto de singularidade de C, ou seja, C é uma curva singular. □

Capítulo 2

2.1 Pontos Racionais em Cônicas

Como mencionamos na introdução deste trabalho, as interseções entre retas e as curvas quadráticas têm um papel importante para determinar os pontos racionais dessas curvas.

Na Seção 1.3, vimos o Teorema de Bézout 1.31 o qual garante que a interseção entre uma curva projetiva quadrática irredutível C e uma reta projetiva L terá exatamente dois pontos no plano projetivo (considerando a multiplicidade). Em geral, esses dois pontos não serão racionais, mas pelo Lema 1.32, se um dos pontos for racional o outro também será.

Sendo assim, se conhecermos um ponto racional $\mathcal{O} \in C$, cada uma das retas projetivas racionais (isto é, definidas sobre os racionais) passando por $\mathcal{O}$ intersectará C em um "segundo" ponto racional. Se a reta em questão for a reta tangente de C passando por $\mathcal{O}$, o ponto obtido é o próprio $\mathcal{O}$. Por outro lado, se $P \in C$ é um ponto racional diferente de $\mathcal{O}$, então a reta $\overline{\mathcal{O}P}$ tem equação dada por

$$\langle (X, Y, Z), (P \times \mathcal{O}) \rangle = 0,$$

em que identificamos um ponto de $\mathbb{P}^2$ com um vetor de $\mathbb{R}^3$ e $\times$ é o produto vetorial, ou seja, essa é uma reta projetiva racional. Portanto, existe uma bijeção entre as retas racionais passando por $\mathcal{O}$ e os pontos racionais em C.

Logo, para obtermos todos os pontos racionais de C basta tomarmos as suas interseções com as retas racionais passando por $\mathcal{O}$. Um modo de obtermos as retas passando por $\mathcal{O}$ é tomarmos uma reta L_0 que não passe por $\mathcal{O}$ e considerarmos as retas que passam por $\mathcal{O}$ e os pontos racionais $Q \in L_0$, os quais podem ser facilmente parametrizados. Obviamente essas retas estarão contidas no conjunto das retas racionais que passam por $\mathcal{O}$. Por outro

lado, como estamos no plano projetivo, pelo Lema 1.32, uma reta racional que passa por $\mathcal{O}$ intersecta L_0 em exatamente um ponto racional Q. Sendo assim, existe uma bijeção entre retas racionais passando por $\mathcal{O}$ e pontos racionais em L_0.

Exemplo 2.1. Consideremos a curva projetiva quadrática C definida pela equação

$$X^2 + Y^2 - Z^2 = 0. \tag{2.1}$$

Podemos constatar facilmente que $[1:0:1]$ é um ponto racional de C. Seguindo o que descrevemos anteriormente, podemos fixar $\mathcal{O} = [1:0:1]$ e $L_0 : X = 0$. Tomando a parametrização de L_0 dada por

$$\varphi(m,n) = [0:m:n],$$

temos que a reta $L_{s,t} = \overline{\varphi(m,n)\,\mathcal{O}}$ tem parametrização dada por $\psi(s,t) = [t : ms : ns + t]$. Logo, os pontos em $L_{s,t} \cap C$ satisfazem a equação

$$\begin{aligned} t^2 + (ms)^2 - (ns+t)^2 &= 0 \\ m^2s^2 - n^2s^2 - 2nst &= 0 \\ s\left(m^2s - n^2s - 2nt\right) &= 0. \end{aligned}$$

A raiz $s = 0$ corresponde ao ponto $\psi(0,1) = \mathcal{O}$ e quando $(m^2 - n^2)\,s - 2nt = 0$ o ponto correspondente é

$$\psi\left(2n, \left(m^2 - n^2\right)\right) = \left[\left(m^2 - n^2\right) : 2mn : \left(m^2 + n^2\right)\right]. \tag{2.2}$$

Portanto, os pontos racionais de C são parametrizados por (2.2).

Além disso, a parametrização (2.2) também parametriza os ternos pitagóricos[1], isso ocorre pois todo terno pitagórico está associado (a menos de equivalência de triângulos) a um triângulo retângulo inscrito ao círculo unitário que tem o diâmetro como medida da hipotenusa [ver Figura 2.1].

Em resumo, se tivermos um ponto racional em uma curva projetiva quadrática definida sobre os racionais, conseguimos parametrizar todos os pontos racionais desta curva.

No exemplo acima conseguimos apresentar um ponto racional facilmente, mas nem sempre isso ocorre, como constataremos no exemplo a seguir, existem curvas quadráticas que não têm pontos racionais.

[1] Um terno pitagórico é uma tripla de números inteiros (a,b,c) que satisfaz $a^2 + b^2 = c^2$.

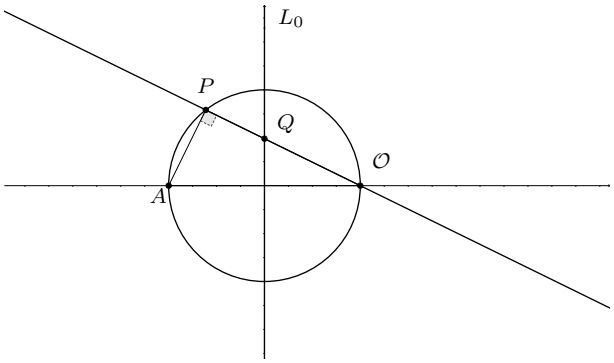


Figura 2.1: Projetando cônica em reta por $\mathcal{O}$.

Exemplo 2.2. Consideremos a curva projetiva quadrática C definida pela equação

$$X^2 + Y^2 - 3Z^2 = 0. \tag{2.3}$$

Suponhamos por absurdo que exista $[X_0 : Y_0 : Z_0] \in C(\mathbb{Q})$, podemos supor que X_0, Y_0 e Z_0 são inteiros que não têm fator comum. Se X_0 for divisível por 3, então 3 divide $Y_0^2 = 3Z_0^2 - X_0^2$, consequentemente, 3 divide Y_0. Como 3 divide X_0 e Y_0, então 9 divide $X_0^2 + Y_0^2 = 3Z_0^2$, portanto, 3 divide Z_0, o que contradiz o fato de X_0, Y_0 e Z_0 não terem fator comum. Logo, 3 não divide X_0.

De modo análogo podemos mostrar que 3 não divide Y_0.

Como X_0 e Y_0 não são divisíveis por 3, temos que

$$X_0 \equiv \pm 1 \pmod 3 \qquad \text{e} \qquad Y_0 \equiv \pm 1 \pmod 3.$$

Portanto,

$$X_0^2 + Y_0^2 \equiv 2 \pmod 3.$$

Entretanto, temos que

$$X_0^2 + Y_0^2 = 3Z_0^2 \equiv 0 \pmod 3,$$

o que é uma contradição.

Logo, podemos concluir que não existem pontos em $C(\mathbb{Q})$. Outra interpretação deste resultado é que não podemos escrever 3 como soma de quadrados de dois números racionais.

Algo que facilitou muito concluir que a curva C, no Exemplo 2.2, não tem pontos racionais é o fato da curva estar na forma

$$aX^2 + bY^2 + cZ^2 = 0.$$

As curvas com tal forma são ditas *diagonais*. Veremos agora que com transformações projetivas adequadas podemos transformar uma curva quadrática definida sobre os racionais em uma curva quadrática na foma diagonal definida sobre os racionais.

De fato, consideremos uma curva projetiva C definida por

$$aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ = 0,$$

com $a, b, c, d, e, f \in \mathbb{Q}$ não todos nulos.

Se $a = b = c = 0$, então pelo menos um entre d, e, f é não nulo. Sem perda de generalidade podemos supor que $d \neq 0$, assim ao substituirmos Y por $X + Y$ obteremos uma nova equação onde o coeficiente correspondente à X^2 é não nulo. Portanto, podemos supor que $a \neq 0$.

Se $a \neq 0$ (os casos $b, c \neq 0$ são análogos), podemos substituir X por $X - \frac{d}{2a}Y$ e assim eliminar o termo XY. Analogamente, podemos eliminar o termo XZ ao substituirmos X por $X - \frac{e}{2a}Z$, observamos que essa última mudança de coordenada não altera os coeficientes dos termos múltiplos de Y, ou seja, o termo XY não é reintroduzido.

Se $f \neq 0$ e $b = 0$, substituímos Z por $Y + Z$ e obtemos uma equação com o coeficiente correspondente a Y^2 não nulo, portanto, podemos supor que $b \neq 0$. Uma vez que $b \neq 0$, podemos substituir Y por $Y - \frac{f}{2b}Z$ e eliminar o termo YZ, pelo fato dessas duas últimas mudanças não alterarem os termos múltiplos de X, temos que os termos XY e XZ não são reintroduzidos, ou seja, obtemos a forma diagonal.

Pode-se observar que cada uma das substituições que fizemos correspondem a uma transformação projetiva racional, portanto ela induz uma bijeção entre os pontos racionais da cônica original e de sua forma diagonal.

Sendo assim, basta determinarmos quando uma curva quadrática diagonal $C : aX^2 + bY^2 + cZ^2 = 0$ tem ou não pontos racionais, e quando tiver algum ponto, como podemos determiná-lo. Os dois teoremas a seguir respondem essas duas questões.

Note que se os coeficientes a, b e c têm o mesmo sinal, então a curva C não têm ponto real, em particular $C(\mathbb{Q}) = \varnothing$. Se os coeficientes a, b e c têm um fator comum, então eliminamos este fator ao dividirmos a equação $aX^2 + bY^2 + cZ^2 = 0$ por este fator. Além disso se, por exemplo, $a = a'k^2$, então $0 = aX^2 + bY^2 + cZ^2 = a'(kX)^2 + bY^2 + cZ^2 = a'W^2 + bY^2 + cZ^2$, com $W = kX$. Deste modo, podemos assumir que $a, b, c \in \mathbb{Z}$ são livres de quadrados, dois a dois coprimos e nem todos com o mesmo sinal.

Teorema 2.3 (Legendre). *Sejam a, b, c números inteiros livres de quadrados, dois a dois coprimos e nem todos com o mesmo sinal. Então a equação $aX^2 + bY^2 + cZ^2 = 0$ tem uma solução racional se, e somente se, existem $r, s, t \in \mathbb{Z}$, tais que as congruências*

$$r^2 \equiv -bc \pmod{a}, \qquad s^2 \equiv -ac \pmod{b}, \qquad t^2 \equiv -ab \pmod{c},$$

são simultaneamente satisfeitas.

Demonstração. Ver em [IR90, Proposição 17.3.1]. □

Note que aplicando o Teorema de Legendre à curva do Exemplo 2.2, também concluímos que ela não tem ponto racional, pois $t^2 \equiv -1 \pmod{3}$ não tem solução.

Observação 2.4. Uma importante consequência do Teorema de Legendre é que o *Princípio de Hasse* vale para curvas quadráticas.

O Princípio de Hasse afirma que *solubilidade local* implica em *solubilidade global*. Por solubilidade local queremos dizer que a equação que estamos estudando tem solução não trivial módulo p^m para todo primo p e todo inteiro positivo m, bem como soluções reais. Enquanto solubilidade global se refere a ter soluções inteiras.

Apesar do Princípio de Hasse ser válido para curvas quadráticas, em geral, ele não vale para curvas de maior grau.

Teorema 2.5 (Holzer). *Sejam a, b, c números inteiros livres de quadrados e dois a dois coprimos, tais que a equação $aX^2 + bY^2 + cZ^2 = 0$ tem uma solução racional. Então existe uma solução inteira $[X_0 : Y_0 : Z_0]$ com*

$$|X_0| \leq \sqrt{|bc|}, \qquad |Y_0| \leq \sqrt{|ac|}, \qquad |Z_0| \leq \sqrt{|ab|}.$$

Demonstração. Uma demonstração mais acessível, em relação à apresentada por Holzer, é encontrada em [CM98]. □

2.2 Cúbicas Singulares

Antes de darmos continuidade ao nosso principal objetivo, estudaremos as cúbicas irredutíveis singulares e verificaremos que elas têm um comportamento semelhante as cônicas.

Seja C uma cúbica irredutível com singularidade racional P_0.

Pelo Teorema de Bézout e pela Proposição 1.33, para cada $P \in C(\mathbb{Q}) - \{P_0\}$ temos que a reta racional $\overline{PP_0}$ intersecta C somente em P e P_0, logo se $P' \in C(\mathbb{Q}) - \{P_0, P\}$, temos que $\overline{PP_0} \neq \overline{P'P_0}$. Portanto, a função $\varphi : C(\mathbb{Q}) - \{P_0\} \to \{$ retas racionais por $P_0\}$ definida por $\varphi(P) = \overline{PP_0}$ é injetora.

Por outro lado, toda reta racional $\overline{QP_0}$ irá intersectar C em um terceiro ponto P (que poder ser igual a P_0). Pelo Lema 1.32, P é um ponto racional. Portanto, temos uma função que leva retas racionais por P_0 nos pontos $C(\mathbb{Q})$.

As funções descritas acima estabelecem uma bijeção entre os pontos de $C(\mathbb{Q}) - \{P_0\}$ e as retas racionais que passam por P_0 com multiplicidade exatamente dois. As retas racionais que passam por P_0 com multiplicidade três estão relacionadas ao ponto P_0.

Na Seção 2.1, construímos uma bijeção entre os pontos racionais de uma cônica e o feixe de retas que passavam por algum ponto racional fixado nessa cônica. No caso das cúbicas singulares, em geral, não conseguimos uma tal bijeção, pois o ponto de singularidade P_0 é associado às retas racionais que passam por P_0 com multiplicidade três. Como vimos na Proposição 1.33, podem haver no máximo duas destas retas, sendo que sobre os racionais podemos ter nenhuma, uma ou as duas dessas retas (como as curvas representadas na Figura 2.2 , Figura 1.4a e Figura 1.4b, respectivamente).

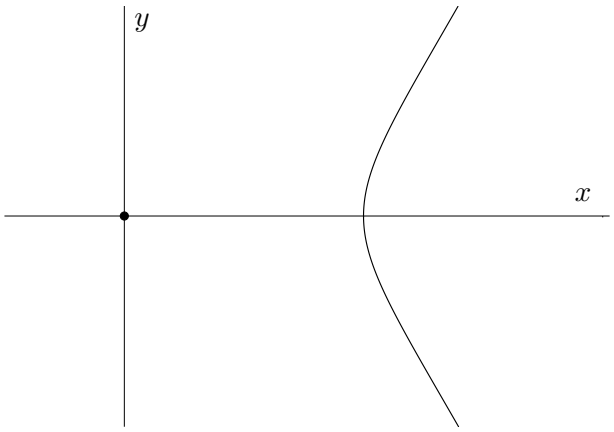


Figura 2.2: Curva $C : y^2 = x^2 - x^2$.

Começamos a análise das cúbicas singulares considerando que a singularidade é racional. Isto não é uma restrição, uma vez que mostraremos na Proposição 2.7 que esse é sempre o caso. Para tanto, utilizaremos dois resultados relacionados com extensões de corpos e cuja demonstração pode ser encontrada na referência indicada.

Lema 2.6. *Seja $\mathbb{L}$ o corpo de decomposição de algum polinômio sobre $\mathbb{K}$. Se $\alpha, \beta \in \mathbb{L}$ são raízes de um mesmo polinômio irredutível sobre $\mathbb{K}$, então existe um $\mathbb{K}$-automorfismo σ de $\mathbb{L}$, tal que $\sigma(\alpha) = \beta$.*

Demonstração. Veja [Ste15, Teorema 9.9 e Teorema 11.4] □

Proposição 2.7. *Seja $C : F(X, Y, Z) = 0$ uma cúbica definida sobre os racionais, irredutível e singular. Então o ponto de singularidade é racional.*

Demonstração. Como C é irredutível, pelo Corolário 1.34, ela tem um único ponto de singularidade. Seja $P = [X_0 : Y_0 : Z_0]$ o ponto de singularidade de C, sem perda de generalidade podemos supor que $Z_0 = 1$. Logo

$$F(X_0, Y_0, 1) = F_X(X_0, Y_0, 1) = F_Y(X_0, Y_0, 1) = F_Z(X_0, Y_0, 1) = 0. \tag{2.4}$$

Afirmamos que a derivada F_X não pertence a $\mathbb{C}[Z]$. De fato, se $F_X \in \mathbb{C}[Z]$, então como F é homogêneo de grau três, F_X teria a forma kZ^2. Portanto, $0 = F_X(X_0, Y_0, 1) = k$, ou seja, $F_X = 0$. Dado que $F_X = 0$, temos que $F \in \mathbb{C}[Y, Z]$. Pelo fato de F ser homogêneo de grau três e pertencer a $\mathbb{C}[Y, Z]$, o Teorema Fundamental da Álgebra assegura que $F = \prod_{i=1}^{3}(a_i Y - b_i Z)$, o que contradiz a irredutibilidade de F.

Como F é irredutível, pelo Lema 1.4-(ii) a desomogeneização de F em relação à variável Z, a qual denotaremos por F_*, é irredutível e não constante em $\mathbb{C}[x, y]$. Uma vez que $F_X \notin \mathbb{C}[Z]$, então F_{X*} não é constante em $\mathbb{C}[x, y]$. Pela irredutibilidade de F_* temos que F_* e F_{X*} não têm fator comum em $\mathbb{C}[x, y]$. Sendo $\mathbb{C}[x]$ um domínio de integridade, pelo Corolário 1.23, temos que

$$r(x) = Res_y(F_*, F_{X*}) \neq 0.$$

Uma vez que $F(X_0, Y_0, 1) = F_X(X_0, Y_0, 1) = 0$, então $F_*(X_0, Y_0) = F_{X*}(X_0, Y_0) = 0$.

Por hipótese, F tem coeficientes racionais, o mesmo ocorrendo com F_* e F_{X*}. Portanto, pelo Teorema 1.24, existem $A, B \in \mathbb{Q}[x][y]$ tais que $AF_* + BF_{X*} = r(x) \in \mathbb{Q}[x]$. Consequentemente, X_0 é uma raiz do polinômio com coeficientes racionais r, ou seja, podemos concluir que X_0 é um número algébrico.

De modo análogo, podemos mostrar que Y_0 é algébrico.

Suponhamos por absurdo que $X_0 \notin \mathbb{Q}$ ou $Y_0 \notin \mathbb{Q}$. Sem perda de generalidade, podemos supor que $X_0 \notin \mathbb{Q}$. Sejam $m_{X_0}, m_{Y_0} \in \mathbb{Q}[t]$ os polinômios minimais de X_0 e Y_0, respectivamente, e $\mathbb{L}$ o corpo de decomposição de $m_{X_0} m_{Y_0}$.

Como $X_0 \notin \mathbb{Q}$, temos que m_{X_0} tem grau maior que 1. Seja $X' \neq X_0$ raiz de m_{X_0}, pelo Lema 2.6, existe um $\mathbb{Q}$-automorfismo σ de $\mathbb{L}$ tal que

$$\sigma(X_0) = X'.$$

Aplicando o $\mathbb{Q}$-automorfismo σ nas igualdades (2.4), temos que

$$F(X', \sigma(Y_0), 1) = F_X(X', \sigma(Y_0), 1) = F_Y(X', \sigma(Y_0), 1) = F_Z(X', \sigma(Y_0), 1) = 0,$$

ou seja, $[X' : \sigma(Y_0) : 1]$ é um ponto de singularidade de C. Como $X' \neq X_0$ então

$$[X' : \sigma(Y_0) : 1] \neq [X_0 : Y_0 : 1],$$

o que é um absurdo pois, segundo o Corolário 1.34, C tem um único ponto singular.

Logo, temos que $X_0, Y_0 \in \mathbb{Q}$, o que nos permite concluir que $P \in C(\mathbb{Q})$. □

Sendo assim, de modo análogo ao caso das cônicas, podemos parametrizar o feixe de retas racionais que passam pelo ponto de singularidade de uma cúbica e descrever o terceiro ponto da interseção da reta com a cúbica em termos dos parâmetros que estamos considerando. Pelo que comentamos no início da seção, todos os pontos racionais da cúbica são representados por esta parametrização de maneira injetiva, com exceção de no máximo dois dos parâmetros os quais são levados em P_0.

Capítulo 3

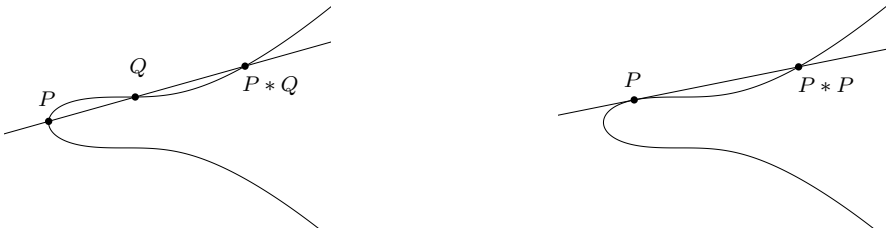
3.1 A Geometria das Curvas Cúbicas

No restante deste trabalho, estudaremos as cúbicas regulares[1]. Para tais cúbicas não podemos usar diretamente a mesma ideia geométrica que adotamos para curvas quadráticas, pois uma reta intersecta uma cúbica em "três" pontos; então se tivermos um ponto racional P_0 na curva cúbica, uma reta racional passando por P_0, irá intersectar a cúbica em mais "dois" pontos que podem não ser racionais. Portanto, o artifício de considerar as interseções do feixe de retas racionais passando por P_0 não será útil, como foi no caso das curvas quadráticas e das cúbicas singulares, que estudamos nas Seções 2.1 e 2.2, respectivamente.

Entretanto, se a curva cúbica tiver dois pontos racionais conhecidos, ao considerarmos sua interseção com a reta passando por esses dois pontos, pelo Lema 1.32, obtemos um "terceiro" ponto que também será racional. Esse procedimento nos dará, como veremos, uma lei de composição: começando com dois pontos P e Q, obteremos um terceiro ponto na interseção da curva cúbica com a reta $\overline{PQ}$, denotaremos este terceiro ponto por $P * Q$ (veja representação da construção de $P * Q$ na Figura 3.1a).

Pela regularidade da cúbica temos que uma reta tangente está bem definida em cada ponto. Portanto, mesmo se tivermos somente um ponto racional P conhecido, podemos obter um novo ponto ao considerarmos a interseção entre a cúbica e sua tangente por P (podemos pensar que este é o caso particular de quando temos dois pontos com $Q = P$), nesse caso, denotaremos este novo ponto por $P * P$. Portanto, se começarmos com alguns pontos racionais, ao aplicarmos a operação de composição $*$ nesses pontos , possivelmente,

[1] Pela Proposição 1.35, a regularidade de uma curva implica na irredutibilidade.



(a) Composição de pontos distintos. (b) Composição de pontos iguais.

Figura 3.1: Composição de pontos.

obteremos novos pontos racionais; ver representação da construção de $P*P$ na Figura 3.1b.

Observação 3.1. Pelo fato de transformações projetivas levarem retas em retas e preservarem o número de interseção, então elas também preservam a operação $*$, ou seja, sendo C uma cúbica regular, T uma transformação projetiva e $P_1, P_2 \in C$ temos que $T(P_1 * P_2) = T(P_1) * T(P_2)$, consequentemente, transformações projetivas levam pontos de inflexão em pontos de inflexão.

O nosso principal objetivo é demonstrar o Teorema de Mordell (1922), o qual afirma que, se C é uma cúbica regular definida sobre os racionais, então existe um conjunto finito de pontos racionais, tal que todos os outros pontos racionais podem ser obtidos por meio de traçar repetidamente certas retas e tomar as suas interseções com a cúbica.

Provaremos o Teorema de Mordell para uma classe de curvas cúbicas trabalhando somente sobre os racionais. A ideia da prova no caso geral continua válida, mas requer o uso de extensões algébricas merecendo assim um cuidado adicional.

Visando obter uma formulação algébrica para o Teorema de Mordell, podemos nos perguntar se a lei de composição $*$ nos dá alguma estrutura algébrica. Entretanto, antes mesmo de pensar em colocar alguma estrutura no conjunto dos pontos racionais de uma cúbica, precisamos nos perguntar se esse conjunto é não vazio.

Ao contrário do que acontecia com as curvas quadráticas, não se conhece um método que nos dê a garantia de determinar, em um número finito de passos, quando uma curva cúbica definida sobre os racionais tem um ponto racional.

A dificuldade em determinar a existência de pontos racionais em curvas de grau maior que dois, é que o Princípio de Hasse não é válido para curvas em geral, ou seja, existem

curvas com solubilidade local, mas não solubilidade global. A cúbica definida pela equação

$$3X^3 + 4Y^3 + 5Z^3 = 0, \tag{3.1}$$

é um contraexemplo para o Princípio de Hasse em curvas cúbicas, apresentado por Selmer em 1951 [Sel51]. Uma abordagem mais simples para verificar que a cúbica (3.1) não tem solubilidade global, pode ser encontrada em [Cas91, Capítulo 18].

Colocaremos esta dificuldade de lado e assumiremos, daqui em diante, que nossa cúbica tem um ponto racional, o qual denotaremos por $\mathcal{O}$.

Apesar de estarmos interessados em introduzir uma estrutura de grupo no conjunto dos pontos racionais $C(\mathbb{Q})$, é conveniente que esta estrutura possa ser estendida, de maneira natural, para $C(\mathbb{C})$.

A operação $*$ se estende naturalmente para $C(\mathbb{C})$. Entretanto, ela não admite elemento neutro, e consequentemente, não induz uma estrutura de grupo em $C(\mathbb{C})$.

De fato, suponhamos por absurdo que $\mathcal{O}$ seja o elemento neutro para a operação $*$.

Como $\mathcal{O}$ é elemento neutro da operação $*$, então $P * \mathcal{O} = P$, para todo $P \in C(\mathbb{C})$, ou seja, $P * (P * \mathcal{O}) = P * P$. Por outro lado, veremos no Lema 3.2, que $P * (P * \mathcal{O}) = \mathcal{O}$. Portanto, $\mathcal{O} = P * P$ para todo $P \in C(\mathbb{C})$. Em particular, $\mathcal{O} = \mathcal{O} * \mathcal{O}$, ou seja, $\mathcal{O}$ é um ponto de inflexão.

Uma cúbica regular tem nove pontos de inflexão distintos (veja [Gib98, Lema 15.3]). Consideremos P_0 um ponto de inflexão, distinto de $\mathcal{O}$. Portanto, $P_0 * P_0 = P_0 \neq \mathcal{O}$, o que contradiz $\mathcal{O} = P * P$ para todo $C(\mathbb{C})$.

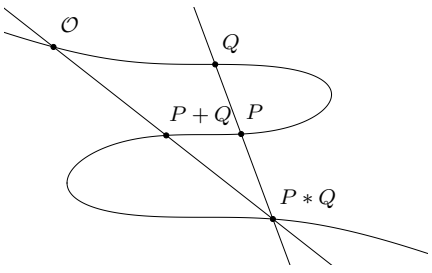


Figura 3.2: Descrição geométrica da operação $+$.

Sendo assim, a operação $*$, em geral, não induz uma estrutura de grupo no conjunto $C(\mathbb{Q})$. Entretanto, podemos definir a operação $+_{\mathcal{O}}$, a qual denotaremos simplesmente por $+$, quando não houver confusão, por

$$P + Q := \mathcal{O} * (P * Q). \tag{3.2}$$

Veremos adiante que a operação $+$ dá uma estrutura de grupo no conjunto $C(\mathbb{Q})$, tendo $\mathcal{O}$ como elemento neutro. Para tal, precisaremos apresentar alguns resultados técnicos.

Lema 3.2. *Sejam P e Q pontos de uma cúbica regular, então*

$$Q = P * (P * Q).$$

Demonstração. Como os pontos P, Q e $(P * Q)$ são colineares, então a reta definida por dois deles é sempre a mesma, e intersecta a cúbica nesses mesmos três pontos. Em particular, a reta que passa por P e $(P * Q)$ intersectará a cúbica no ponto Q. □

Proposição 3.3. *Se $P_1, P_2, \ldots, P_5$ são pontos distintos do plano projetivo, então existe uma cônica que contém $P_1, P_2, \ldots, P_5$. Além disso, se quaisquer quatro desses pontos não são colineares, então a cônica é única.*

Demonstração. Se $P_i = [X_i : Y_i : Z_i]$ e $v_i = (X_i^2, X_iY_i, X_iZ_i, Y_i^2, Y_iZ_i, Z_i^2) \in \mathbb{C}^6$, então P_i pertence à cônica

$$Q : aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2 = 0$$

se, e somente se, $\langle v_i, (a, b, c, d, e, f)\rangle = 0$. Logo, $P_1, P_2, \ldots, P_5 \in Q$ se, e somente se, (a, b, c, d, e, f) está no espaço ortogonal $V^\perp$ ao $\mathbb{C}$-espaço V gerado por $v_1, v_2, \ldots, v_5$. Como V tem dimensão no máximo cinco e está contido em um espaço de dimensão seis, então $V^\perp$ tem dimensão pelo menos um. Portanto, existe vetor não nulo $(a, b, c, d, e, f) \in V^\perp$, o que garante a existência da cônica contendo os cinco pontos.

Suponha agora que quaisquer quatro desses pontos não são colineares e suponha que Q_1 e Q_2 são cônicas passando por $P_1, P_2, \ldots, P_5$. Pelo Teorema de Bézout 1.31, temos que Q_1 e Q_2 têm componente em comum, ou seja, $Q_1 = Q_2$ ou existem retas L_0, L_1 e L_2 tais que[2]

$$Q_1 = L_0L_1 \qquad e \qquad Q_2 = L_0L_2.$$

Suponhamos $Q_1 = L_0L_1$ e $Q_2 = L_0L_2$. Como não podemos ter quatro pontos colineares, então a reta L_0 contém no máximo três dos cinco pontos, ou seja, pelo menos dois dos pontos, digamos P_1 e P_2, não estão em L_0. Uma vez que $P_1, P_2 \in Q_1 \cap Q_2$ e

[2]Sendo $C_1 : F_1 = 0$ e $C_2 : F_2 = 0$ duas curvas projetivas, denotaremos por C_1C_2 a curva definida pela equação $F_1F_2 = 0$.

$P_1, P_2 \notin L_0$, então P_1 e P_2 estão contidos nas retas L_1 e L_2. Pelo fato de P_1 e P_2 serem pontos distintos, temos que $L_1 = \overline{P_1P_2} = L_2$. Portanto, $Q_1 = Q_2$.

Podemos então concluir que se quaisquer quatro dos pontos não são colineares, então existe uma única cônica passando pelos cinco pontos. □

Proposição 3.4. *Se C_1 e C_2 são cúbicas sem componentes em comum e $P_1, P_2, \ldots, P_8$ são pontos distintos contidos em $C_1 \cap C_2$, então existe uma cúbica redutível que contém $P_1, P_2, \ldots, P_7$, mas não contém P_8.*

Demonstração. Primeiramente mostraremos a seguinte afirmação:

> Dentre os oito pontos, quatro não podem ser colineares e sete não podem estar contidos em uma mesma cônica. (▲)

De fato, suponhamos por absurdo que quatro dos pontos estejam contidos em uma reta L, então $C_1 \cap L$ e $C_2 \cap L$ têm pelo menos quatro pontos, pelo Teorema de Bézout 1.31 e a irredutibilidade de L, L é componente de C_1 e C_2 o que contradiz a hipótese de C_1 e C_2 não terem componentes em comum. Logo, não podemos ter quatro pontos colineares.

Suponhamos por absurdo que sete dos pontos estejam em uma cônica Q. Se $Q = LL'$, então uma componente de Q contém pelo menos quatro pontos, o que contradiz o que provamos acima. Logo, Q deve ser irredutível. Como $Q \cap C_1$ e $Q \cap C_2$ têm pelo menos sete pontos em comum, pelo Teorema de Bézout e a irredutibilidade de Q, temos que Q é uma componente em comum de C_1 e C_2, o que é um absurdo. Logo, sete pontos não podem estar em uma mesma cônica.

Consideremos $L_{ij} = \overline{P_iP_j}$, para $i \neq j$.

Mostremos a afirmação do enunciado da proposição, analisando os três casos:

(i) Se entre os sete pontos, seis estão contidos em uma cônica Q que não contém P_8, então podemos tomar uma reta L que passa pelo sétimo ponto, mas não por P_8. Portanto, a cúbica redutível definida por QL satisfaz a condição requerida.

(ii) Se entre os sete pontos, três são colineares, então sem perda de generalidade, podemos supor que os pontos P_1, P_2 e P_3 são tais pontos, ou seja, estão contidos na reta L_{12}. Pela Afirmação (▲) temos que $P_8 \notin L_{12}$.

Consideremos as retas

$$\{L_{45},\ L_{46},\ L_{47},\ L_{56},\ L_{57},\ L_{67}\}. \tag{3.3}$$

Se P_8 não está nas retas listadas em (3.3), então a cúbica redutível $L_{12}L_{45}L_{67}$, contém os pontos $P_1, \ldots, P_7$, mas não contém P_8.

Caso contrário, podemos supor sem perda de generalidade que $P_8 \in L_{47}$, logo

$$P_8 \in L_{47} \Longrightarrow \begin{cases} P_7 \in L_{48} \overset{(\blacktriangle)}{\Longrightarrow} P_5 \notin L_{48} \Longrightarrow P_8 \notin L_{45}, \\ P_4 \in L_{78} \overset{(\blacktriangle)}{\Longrightarrow} P_6 \notin L_{78} \Longrightarrow P_8 \notin L_{67}. \end{cases}$$

Consequentemente, a cúbica redutível definida por $L_{12}L_{45}L_{67}$, contém os pontos $P_1, \ldots, P_7$, mas não contém P_8.

(iii) Suponha que os casos anteriores não ocorram, ou seja, entre os sete pontos, seis não estão numa mesma cônica que não contenha P_8 e três não são colineares.

Provaremos a seguinte afirmação:

> Se duas cônicas são definidas por cinco dos sete pontos e têm quatro desses cinco pontos em comum, então pelo menos uma dessas cônicas não contém P_8. (▲▲)

Suponhamos por absurdo que (▲▲) seja falsa, ou seja, que existam cônicas Q_1 e Q_2 definidas por cinco dos sete pontos e têm quatro desses cinco pontos em comum juntamente com P_8. Sem perda de generalidade, podemos supor que Q_1 é a cônica passando por P_1, P_2, P_3, P_4 e P_5, que Q_2 é a cônica passando por P_1, P_2, P_3, P_4 e P_6 e que $P_8 \in Q_1 \cap Q_2$.

Como $\{P_1, P_2, P_3, P_4, P_8\} \subset Q_1 \cap Q_2$, pela Afirmação (▲) e Proposição 3.3, existe uma única cônica passando por P_1, P_2, P_3, P_4 e P_8. Portanto, $Q_1 = Q_2$. Logo, $P_1, P_2, \ldots, P_6$ e P_8 estão contidos em Q_1, o que contradiz a Afirmação (▲).

Portanto, a Afirmação (▲▲) é verdadeira e consideramos dois subcasos:

(A) P_8 não está nas retas ligando os pontos em $\{P_1, \ldots, P_7\}$.

Sejam Q_1 a cônica que contém P_1, P_2, P_3, P_4 e P_5, e Q_2 a cônica que contém P_1, P_2, P_3, P_4 e P_6, pela Afirmação (▲▲), podemos supor sem perda de generalidade que $P_8 \notin Q_1$. Como $P_8 \notin L_{67}$, então a cúbica redutível definida por Q_1L_{67} satisfaz as condições desejadas.

(B) P_8 está contido em uma das retas que ligam dois dos demais sete pontos.

Podemos supor sem perda de generalidade que $P_8 \in L_{12}$, então temos que

$$P_1 \in L_{28} \overset{(\blacktriangle)}{\Longrightarrow} P_3, \ldots, P_7 \notin L_{28} \Longrightarrow P_8 \notin L_{23}, \ldots, L_{27}.$$

Sejam Q_1 a cônica contendo P_1, P_3, P_4, P_5 e P_6, e Q_2 a cônica contendo P_1, P_3, P_4, P_5 e P_7. Pela Afirmação (▲▲), $P_8 \notin Q_1$ ou $P_8 \notin Q_2$. Se $P_8 \notin Q_1$, tomamos a cúbica Q_1L_{27}. Se $P_8 \notin Q_2$, tomamos a cúbica Q_2L_{26}. □

Teorema 3.5. *Sejam $C_1 : F_1 = 0$ e $C_2 : F_2 = 0$ cúbicas distintas sem componentes em comum que se intersectam em $P_1, P_2, \ldots, P_9$ distintos. Então toda cúbica $C : F = 0$ que contém $P_1, P_2, \ldots, P_8$ também contém P_9.*

Demonstração. Para cada $1 \leq l \leq 8$ consideramos $P_l = [X_l : Y_l : Z_l]$,

$$v_l = \left(X_l^3, X_l^2Y_l, X_l^2Z_l, X_lY_l^2, X_lY_lZ_l, X_lZ_l^2, Y_l^3, Y_l^2Z_l, Y_lZ_l^2, Z_l^3\right) \in \mathbb{C}^{10}$$

e V o espaço vetorial gerado por $v_1, \ldots, v_8$. Seja

$$C : F = aX^3 + bX^2Y + cX^2Z + dXY^2 + eXYZ + fXZ^2 + gY^3 + hY^2Z + iYZ^2 + jZ^3 = 0$$

uma cúbica arbitrária. Temos que

$$P_l \in C \Longleftrightarrow \langle v_l, (a, b, c, d, e, f, g, h, i, j)\rangle = 0. \tag{3.4}$$

Portanto, $P_1, \ldots, P_8 \in C$ se, e somente se, $(a, b, c, d, e, f, g, h, i, j) \in V^{\perp} - \{0\}$.

Mostraremos que V tem dimensão oito. Para tal, suporemos por absurdo que o conjunto $\{v_1, \ldots, v_8\}$ é linearmente dependente. Sem perda de generalidade, podemos supor que existem $\lambda_1, \ldots, \lambda_7 \in \mathbb{C}$, não todos nulos, tais que

$$v_8 = \sum_{l=1}^{7} \lambda_l v_l.$$

Tal igualdade, juntamente com a equivalência (3.4), nos dá que toda cúbica que contém $P_1, \ldots, P_7$ também contém P_8. Entretanto, pela Proposição 3.4, existe uma cúbica que contém $P_1, \ldots, P_7$, mas não contém P_8, o que é uma contradição. Logo, $\{v_1, \ldots, v_8\}$ é linearmente independente, ou seja, V tem dimensão oito.

Como V está contido em um espaço de dimensão dez, temos que a dimensão de $V^{\perp}$ é dois.

Veremos agora que C_1 e C_2 "geram" $V^{\perp}$. Consideremos os monômios das equações de C_1 e C_2 ordenados lexicograficamente. Consideremos w_1 e w_2 os vetores dos coeficientes das equações que definem C_1 e C_2, respectivamente. Além disso, note que w_1 e w_2 estão bem definidos a menos de multiplicação por escalar não nulo. Assim, temos que w_1 e w_2 são linearmente independentes, pois caso contrário, existiria $\lambda \in \mathbb{C}$ tal que $w_2 = \lambda w_1$ e neste caso, teríamos que as equações que definem C_1 e C_2 são múltiplas uma da outra, o que seria um absurdo, pois C_1 e C_2 são distintas.

Como $P_1, \ldots, P_8 \in C_1 \cap C_2$ pela equivalência (3.4), temos que

$$\langle v_l, w_1 \rangle = \langle v_l, w_2 \rangle = 0, \ \forall \ 1 \leq l \leq 8,$$

consequentemente, $w_1, w_2 \in V^{\perp}$ e como w_1 e w_2 são linearmente independentes, temos que eles geram $V^{\perp}$. Logo, considerando uma cúbica $C : F = 0$, temos

$$\begin{aligned} P_1, \ldots, P_8 \in C &\iff (a,b,c,d,e,f,g,h,i,j) \in V^{\perp} - \{0\} \\ &\iff (a,b,c,d,e,f,g,h,i,j) = \gamma_1 w_1 + \gamma_2 w_2 \\ &\iff F = \gamma_1 F_1 + \gamma_2 F_2 \\ &\implies F(P_9) = 0 \\ &\iff P_9 \in C, \end{aligned}$$

ou seja, toda cúbica que contém $P_1, \ldots, P_8$, também contém P_9. □

Os resultados auxiliares apresentados anteriormente, permite avançarmos no estudo dos pontos racionais de uma cúbica regular.

Teorema 3.6. *Seja C uma cúbica regular com um ponto racional $\mathcal{O}$, então $(C(\mathbb{Q}), +)$ é um grupo abeliano.*

Demonstração. Sejam P, Q e R pontos racionais quaisquer de C. Como já observamos, $P * Q \in C(\mathbb{Q})$ e assim $P + Q = \mathcal{O} * (P * Q) \in C(\mathbb{Q})$ e $+ : C(\mathbb{Q}) \times C(\mathbb{Q}) \to C(\mathbb{Q})$ está bem definida.

- (Comutatividade) Como a reta passando por P e Q é a mesma que passa por Q e P, temos que $P * Q = Q * P$, daí segue que

  $$P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P,$$

  ou seja, a operação $+$ é comutativa.

- ($\mathcal{O}$ é elemento neutro) Basta aplicar o Lema 3.2 para concluir que

$$\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P) = P$$

e pela comutatividade temos que $P + \mathcal{O} = P$.

- (Elemento inverso) Suponhamos que P' seja o elemento inverso de P. Então

$$\mathcal{O} = P + P' = \mathcal{O} * (P * P'),$$

consequentemente, a reta passando por $\mathcal{O}$ e $(P * P')$ passa por $\mathcal{O}$ com multiplicidade pelo menos dois, ou seja, essa é a reta tangente passando por $\mathcal{O}$, logo

$$P * P' = \mathcal{O} * \mathcal{O}.$$

Pelo Lema 3.2, temos que

$$P' = P * (P * P') = P * (\mathcal{O} * \mathcal{O}).$$

Sendo assim, o ponto $P * (\mathcal{O} * \mathcal{O})$ é o candidato a ser o elemento inverso de P. De fato, seja $-P := P * (\mathcal{O} * \mathcal{O})$, então

$$P + (-P) = P + (P * (\mathcal{O} * \mathcal{O})) = \mathcal{O} * (P * (P * (\mathcal{O} * \mathcal{O}))),$$

pelo Lema 3.2,

$$\mathcal{O} * (P * (P * (\mathcal{O} * \mathcal{O}))) = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O} + \mathcal{O} = \mathcal{O}.$$

Logo, podemos concluir que $P + (-P) = \mathcal{O}$, ou seja, todo $P \in C(\mathbb{Q})$ admite elemento inverso dado por

$$-P = P * (\mathcal{O} * \mathcal{O}). \tag{3.5}$$

- (Associatividade): A associatividade é de longe a maior dificuldade em provar que a operação nos dá uma estrutura de grupo. Daremos aqui uma demonstração que é válida em quase todos os casos.

Sejam P, Q e R três pontos racionais na curva C. Queremos mostrar que

$$(P + Q) + R = P + (Q + R).$$

Como $(P+Q)+R$ é o terceiro ponto da interseção da reta passando por $\mathcal{O}$ e $(P+Q)*R$, e $P+(Q+R)$ é o terceiro ponto da interseção da reta passando por $\mathcal{O}$ e $P*(Q+R)$, então basta mostrarmos que

$$(P+Q)*R = P*(Q+R)\,.$$

Na construção de $(P+Q)*R$, utilizamos as retas

$$L_1 = \overline{PQ}, \qquad L_2 = \overline{(P*Q)\,\mathcal{O}} \qquad \text{e} \qquad L_3 = \overline{(P+Q)\,R},$$

também observamos que

$$\begin{cases} \{P,\ Q,\ P*Q\} = L_1 \cap C, \\ \{P*Q,\ \mathcal{O},\ P+Q\} = L_2 \cap C, \\ \{P+Q,\ R,\ (P+Q)*R\} = L_3 \cap C. \end{cases}$$

Na construção de $P*(Q+R)$, utilizamos as retas

$$M_1 = \overline{QR}, \qquad M_2 = \overline{(Q*R)\,\mathcal{O}} \qquad \text{e} \qquad M_3 = \overline{(Q+R)\,P},$$

também observamos que

$$\begin{cases} \{Q,\ R,\ Q*R\} = M_1 \cap C, \\ \{Q*R,\ \mathcal{O},\ Q+R\} = M_2 \cap C, \\ \{Q+R,\ P,\ P*(Q+R)\} = M_3 \cap C. \end{cases}$$

Sendo assim, ao considerarmos as cúbicas

$$D_1 = L_1M_2L_3 \qquad \text{e} \qquad D_2 = M_1L_2M_3,$$

temos que

$$\begin{cases} C \cap D_1 = \{P,\ Q,\ R,\ \mathcal{O},\ P*Q,\ P+Q,\ Q*R,\ Q+R,\ (P+Q)*R\} \quad \text{e} \\ C \cap D_2 = \{P,\ Q,\ R,\ \mathcal{O},\ P*Q,\ P+Q,\ Q*R,\ Q+R,\ P*(Q+R)\}. \end{cases}$$

Como C é irredutível, as retas L_i's e M_i's não são componentes de C. Portanto, C e D_1 não têm componentes em comum.

Vamos supor que os pontos de $C \cap D_1$ ou $C \cap D_2$ sejam distintos.

Se os pontos

$$P,\ Q,\ R,\ \mathcal{O},\ P*Q,\ P+Q,\ Q*R,\ Q+R \ \text{ e } \ (P+Q)*R \tag{3.6}$$

são distintos, podemos usar o Teorema 3.5 para concluir que D_2 também contém o ponto $(P+Q)*R$. Pelo fato dos pontos em (3.6) serem distintos, temos que

$$(P+Q)*R \ \notin \ \{P,\ Q,\ R,\ \mathcal{O},\ P*Q,\ P+Q,\ Q*R,\ Q+R\},$$

como $(P+Q)*R \in C \cap D_2$ e pelo Teorema de Bézout $\#\left(C \cap D_2\right) = 9$, devemos ter que

$$(P+Q)*R = P*(Q+R),$$

o que nos permite concluir que a associatividade da operação é válida quando os pontos em (3.6) são distintos, bem como, com um argumento análogo, quando os pontos de $C \cap D_2$ são distintos.

Nos casos em que os pontos em (3.6) não são todos distintos, o resultado continua válido mas demandaria muitos resultados auxiliares e particulares, o leitor pode encontrar uma apresentação em [Ful08, Capítulo 5]. □

O teorema anterior assegura que $\left(C\left(\mathbb{Q}\right),+\right)$ é um grupo abeliano, com elemento neutro sendo um ponto racional $\mathcal{O}$ fixado, tal que $P+Q = \mathcal{O}*(P*Q)$. Se escolhermos um outro ponto racional $\mathcal{O}'$, e considerarmos $P \oplus Q := \mathcal{O}'*(P*Q)$, temos que $\left(C\left(\mathbb{Q}\right),\oplus\right)$ é também um grupo abeliano e a aplicação

$$\begin{aligned} \varphi : \left(C\left(\mathbb{Q}\right),+\right) &\longrightarrow \left(C\left(\mathbb{Q}\right),\oplus\right) \\ P &\longmapsto P+\mathcal{O}' \end{aligned}$$

é um isomorfismo de grupos. De fato, como

$$\begin{aligned}
\varphi(P+Q) &= (P+Q)+\mathcal{O}' \\
&= (P+Q)+\mathcal{O}'+(\mathcal{O}'-\mathcal{O}') \\
&= (P+\mathcal{O}')+(Q+\mathcal{O}')-\mathcal{O}' \\
&= (\mathcal{O}*[(P+\mathcal{O}')*(Q+\mathcal{O}')])-\mathcal{O}' \\
&= (\mathcal{O}*[\mathcal{O}'*(\mathcal{O}'*((P+\mathcal{O}')*(Q+\mathcal{O}')))])-\mathcal{O}' \\
&= (\mathcal{O}*[\mathcal{O}'*((P+\mathcal{O}')\oplus(Q+\mathcal{O}'))])-\mathcal{O}' \\
&= (\mathcal{O}'+((P+\mathcal{O}')\oplus(Q+\mathcal{O}')))-\mathcal{O}' \\
&= (P+\mathcal{O}')\oplus(Q+\mathcal{O}') \\
&= \varphi(P)\oplus\varphi(Q),
\end{aligned}$$

então φ é um homomorfismo de grupos. Como

$$P\in\ker\varphi \iff P+\mathcal{O}'=\mathcal{O}' \iff P=\mathcal{O},$$

então φ é injetora. Além disso, φ é sobrejetora pois $\varphi(P-\mathcal{O}')=P$.

3.2 Forma Normal de Weierstrass

Para provar o Teorema de Mordell, utilizaremos fórmulas explícitas para a lei de grupo. De modo a fazer com que estas fórmulas sejam mais simples, transformaremos uma cúbica regular arbitrária racional

$$C: aX^3+bX^2Y+cX^2Z+dXY^2+eXYZ+fXZ^2+gY^3+hY^2Z+iYZ^2+jZ^3=0,$$

com um ponto racional $P=[p_1:p_2:p_3]$, em uma cúbica com coeficientes inteiros na forma

$$E: Y^2Z=X^3+\alpha XZ^2+\beta Z^3. \tag{3.7}$$

Tal forma é conhecida como *forma de Weierstrass* ou *forma curta de Weierstrass*, nós utilizaremos a sua versão mais geral

$$E: Y^2Z=X^3+pX^2Z+qXZ^2+rZ^3 \tag{3.8}$$

e para nós, essa ou sua desomogeneização com respeito a Z, será a forma de Weierstrass a qual também chamaremos *curva elíptica*.

Independentemente dos coeficientes p, q e r, uma curva elíptica contém o ponto $\mathcal{O} = [0:1:0]$. Pelo Exemplo 1.17, o ponto $\mathcal{O}$ é um ponto de inflexão de uma curva elíptica e, pela Observação 3.1, transformações projetivas levam pontos de inflexão em pontos de inflexão. Portanto, quando P não é ponto de inflexão, não existe transformação projetiva que transforme C em uma cúbica na forma de Weierstrass e que leve P em $\mathcal{O}$.

Logo, começaremos a desenvolver dois casos separadamente, considerando um ponto $P = [p_1 : p_2 : p_3] \in C(\mathbb{Q})$.

- P é ponto de inflexão:

  Sendo $n_1 = (n_{11}, n_{12}, n_{13})$ e $n_2 = (n_{21}, n_{22}, n_{23})$ vetores geradores do $\mathbb{Q}$-espaço ortogonal ao espaço gerado por (p_1, p_2, p_3)[3], então

  $$T_1 = \begin{bmatrix} n_{11} & p_1 & n_{21} \\ n_{12} & p_2 & n_{22} \\ n_{13} & p_3 & n_{23} \end{bmatrix}$$

  é uma transformação projetiva racional, tal que $T_1(\mathcal{O}) = P$. Definindo $C_1 = C(T_1(X, Y, Z))$, temos que T_1 é uma transformação que leva pontos racionais de C_1 em pontos racionais de C, em particular, como mencionamos o ponto $\mathcal{O}$ é levado no ponto P. Como $\mathcal{O} \in C_1$, então C_1 tem a forma

  $$C_1 : aX^3 + bX^2Y + cX^2Z + dXY^2 + eXYZ + fXZ^2 + hY^2Z + iYZ^2 + jZ^3 = 0.$$

  Além disso, pela regularidade de C_1 e a Identidade de Euler (1.3), temos que o vetor $\nabla C_1(0, 1, 0) = (d, 0, h)$ é não nulo e ortogonal a $(0, 1, 0)$. Portanto, podemos definir a transformação projetiva racional

  $$T_2 = \begin{bmatrix} h & 0 & d \\ 0 & 1 & 0 \\ -d & 0 & h \end{bmatrix},$$

  tal que, $T_2(\mathcal{O}) = \mathcal{O}$ e $T_2(0, 0, 1) = [d, 0, h]$[4].

  Definindo $C_2 = C_1(T_2(X, Y, Z))$, temos que $\mathcal{O} \in C_2$ e, pela regra da cadeia,

  $$\nabla C_2(\mathcal{O}) = [\nabla C_1(T_2(\mathcal{O}))]\,[(DT_2)(\mathcal{O})] = \nabla C_1(\mathcal{O})\,T_2 = \left(0, 0, d^2 + h^2\right),$$

[3] Observamos que esse espaço independe das coordenadas homogêneas de P.

[4] Pela Identidade de Euler (1.3), temos que $\nabla C(p_1, p_2, p_3)$ é ortogonal a (p_1, p_2, p_3). Portanto, podemos tomar $n_2 = \nabla C(p_1, p_2, p_3)$ na definição de T_1, tornando assim a transformação T_2 desnecessária, pois neste caso, já teríamos que $T_1(\mathcal{O}) = P$ e $T_1(0, 0, 1) = \nabla C(P)$.

com DT_2 denotando a diferencial de T_2. Uma vez que $[0:0:d^2+h^2] = [0:0:1]$, temos que a reta tangente à C_2 no ponto $\mathcal{O}$ é dada pela equação $(Z=0)$, consequentemente, a curva C_2 tem a forma

$$C_2 : aX^3 + bX^2Y + cX^2Z + eXYZ + fXZ^2 + hY^2Z + iYZ^2 + jZ^3 = 0,$$

com $h \neq 0$. Uma vez que transformações projetivas levam ponto de inflexão em ponto de inflexão e P é ponto de inflexão de C. Temos que $\mathcal{O}$ é um ponto de inflexão de C_2, ou seja, a curva C_2 intersecta a reta $(Z=0)$ com multiplicidade três em $\mathcal{O}$. Portanto, $b=0$.

Pela irredutibilidade de C_2 temos que $a \neq 0$. Logo, C_2 tem a forma

$$C_2 : hY^2Z + (eX + iZ)YZ + \left(aX^3 + cX^2Z + fXZ^2 + jZ^3\right) = 0, \quad \text{com } ah \neq 0. \tag{3.9}$$

Retomaremos às curvas na forma (3.9) posteriormente.

- P não é ponto de inflexão:

  Sejam $P' = [p_1' : p_2' : p_3'] = P * P$ e $P'' = [p_1'' : p_2'' : p_3''] = P' * P'$. Se P' ou P'' forem pontos de inflexão podemos considerar o caso anterior. Caso contrário, temos que $P' \neq P$ e $P'' \neq P'$. Além disso, como

  $$C \cap \overline{PP'} = \{P, P, P'\} \qquad \text{e} \qquad C \cap \overline{P''P'} = \{P', P', P''\},$$

  temos $P \neq P''$. Portanto, os pontos P, P' e P'' são não colineares e a transformação

  $$T_1 = \begin{bmatrix} p_1 & p_1' & p_1'' \\ p_2 & p_2' & p_2'' \\ p_3 & p_3' & p_3'' \end{bmatrix},$$

  é uma transformação projetiva racional tal que

  $$T_1(1,0,0) = P, \quad T_1(0,1,0) = P' \quad \text{e} \quad T_1(0,0,1) = P''.$$

  Definindo $C_1 = C(T_1(X,Y,Z))$, temos que $\{[1:0:0], [0:1:0], [0:0:1]\} \subset C_1$, ou seja, a curva C_1 tem a forma

  $$C_1 : bX^2Y + cX^2Z + dXY^2 + eXYZ + fXZ^2 + hY^2Z + iYZ^2 = 0.$$

Como transformações projetivas levam retas em retas, preservam a lei de composição $*$, e as retas tangentes à C nos pontos P e P' são, respectivamente, $\overline{PP'}$ e $\overline{P'P''}$, então as retas tangentes à C_1 nos pontos $[1:0:0]$ e $[0:1:0]$ são, respectivamente, $\overline{[1:0:0]\,[0:1:0]}$ e $\overline{[0:1:0]\,[0:0:1]}$, ou seja, as retas $Z=0$ e $X=0$.

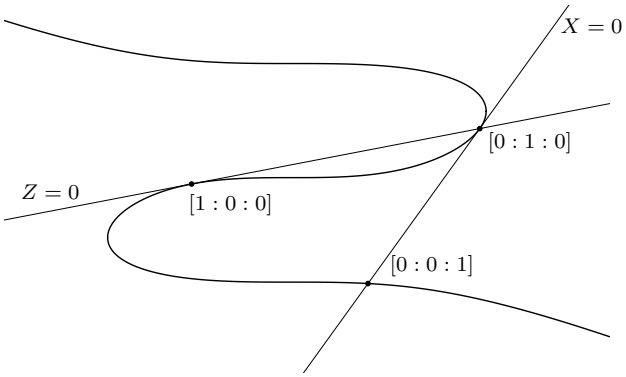


Figura 3.3: Representação das tangentes à C_1 nas novas coordenadas.

Por outro lado,

$$\nabla C_1\,(1,0,0) = (0,b,c) \qquad \text{e} \qquad \nabla C_1\,(0,1,0) = (d,0,h)\,.$$

Podemos então concluir que $b=h=0$ e $cd\neq 0$, consequentemente, C_1 se resume a uma curva na forma

$$C_1 : cX^2Z + dXY^2 + eXYZ + fXZ^2 + iYZ^2 = 0, \qquad \text{com } cd\neq 0. \tag{3.10}$$

Realizando a transformação quadrática

$$\varphi\,(X,Y,Z) = \left[X^2 : YZ : XZ\right] \tag{3.11}$$

na Equação (3.10), obtemos a equação

$$cX^5Z + dX^2Y^2Z^2 + eX^3YZ^2 + fX^4Z^2 + iX^2YZ^3 = 0, \qquad \text{com } cd\neq 0,$$

dividindo por X^2Z obtemos a cúbica

$$C_2 : dY^2Z + (eX+iZ)\,YZ + \left(cX^3 + fX^2Z\right) = 0, \quad \text{com } cd\neq 0. \tag{3.12}$$

Observação 3.7. A mudança de coordenada quadrática (3.11), foi apresentada por Nagell em 1928-29 (mais detalhes em [Mil06, pag. 48]).

Diferente de quando consideramos transformações projetivas, não é claro que a estrutura de grupo é preservada quando consideramos a transformação quadrática (3.11). Pode-se provar que a estrutura do grupo dos pontos racionais é preservada, mas precisaríamos de alguns resultados adicionais que não serão tratados neste trabalho.

Entretanto, se $\mathbb{QP}^2$ denota o plano projetivo definido sobre os racionais, então considerando $V = \{[X : Y : Z] \in \mathbb{QP}^2;\ XZ = 0\}$, temos que φ induz uma bijeção em $\mathbb{QP}^2 - V$, com inversa dada por

$$\varphi^{-1}(X, Y, Z) = \left[XZ : XY : Z^2\right].$$

Em particular, φ induz uma bijeção entre $C_1(\mathbb{Q}) - \{[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1]\}$ e $C_2(\mathbb{Q}) - \{[0 : 1 : 0], [0 : 0 : 1], [0 : i : -d]\}$. Portanto, determinando os pontos racionais de C_2, determinamos os pontos racionais de C_1.

Assim, independente de P ser ou não ponto de inflexão, obtemos as cúbicas (3.9) e (3.12), que têm a forma

$$C_2 : hY^2Z + (eX + iZ)YZ + \left(aX^3 + cX^2Z + fXZ^2 + jZ^3\right) = 0, \quad \text{com } ah \neq 0.$$

Como $h \neq 0$, podemos supor sem perda de generalidade que $h = 1$. Portanto, a equação definindo C_2 pode ser reescrita como

$$Y^2Z + (eX + iZ)YZ + \left(aX^3 + cX^2Z + fXZ^2 + jZ^3\right) = 0, \quad \text{com } a \neq 0$$

$$\Updownarrow$$

$$\left[Y + \frac{eX + iZ}{2}\right]^2 Z - \frac{(eX + iZ)^2}{4}Z = -aX^3 - cX^2Z - fXZ^2 - jZ^3, \quad \text{com } a \neq 0$$

$$\Updownarrow$$

$$\left[Y + \frac{eX + iZ}{2}\right]^2 Z = -aX^3 + \left(\frac{e^2}{4} - c\right)X^2Z + \left(\frac{ei}{2} - f\right)XZ^2 + \left(\frac{i^2}{4} - j\right)Z^3, \quad \text{com } a \neq 0.$$

Consideremos a transformação projetiva racional

$$T_3 = \begin{bmatrix} 1 & 0 & 0 \\ -\frac{e}{2} & 1 & -\frac{i}{2} \\ 0 & 0 & 1 \end{bmatrix}.$$

Definindo $C_3 = C_2(T_3(X, Y, Z))$, temos que a curva C_3 tem a forma

$$C_3 : Y^2Z = -aX^3 + \left(\frac{e^2}{4} - c\right)X^2Z + \left(\frac{ei}{2} - f\right)XZ^2 + \left(\frac{i^2}{4} - j\right)Z^3, \quad \text{com } a \neq 0. \quad (3.13)$$

Como $a \neq 0$ a aplicação

$$T_4 = \begin{bmatrix} -a & 0 & 0 \\ 0 & a^2 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

é uma transformação projetiva racional, tal que a curva $C_4 = C_3\left(T_4\left(X, Y, Z\right)\right)$ está na forma

$$C_4 : Y^2Z = X^3 + pX^2Z + qXZ^2 + rZ^3.$$

Podemos ainda aplicar uma transformação projetiva racional de modo que a equação obtida tenha coeficientes inteiros. Seja δ o mínimo múltiplo comum dos denominadores de p, q e r. Ao aplicarmos a transformação

$$T_5 = \begin{bmatrix} \frac{1}{\delta^2} & 0 & 0 \\ 0 & \frac{1}{\delta^3} & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

obtemos que $C_5 = C_4\left(T_5\left(X, Y, Z\right)\right)$ é uma curva na forma de Weierstrass com coeficientes inteiros

$$Y^2Z = X^3 + \delta^2 pX^2Z + \delta^4 qXZ^2 + \delta^6 rZ^3.$$

Sendo assim, compondo as transformações racionais definidas em cada um dos passos obteremos uma transformação que estabelece, com exceção de alguns pontos previamente determinados, uma bijeção entre os pontos racionais da curva C original e os pontos racionais de cúbica C_5 na forma de Weierstrass com coeficientes inteiros. Dizemos neste caso que C_5 é *birracionalmente* equivalente à C.

Exemplo 3.8. Encontremos uma cúbica na forma de Weierstrass que é birracional à curva $C : X^3 + Y^3 + cZ^3 = 0$, com $c \neq 0$.

Como o vetor gradiente $\nabla C = (3X^2, 3Y^2, 3cZ^2)$ não se anula em ponto algum do plano projetivo, temos que C é cúbica regular.

É fácil ver que $P_0 = [1 : -1 : 0] \in C\left(\mathbb{Q}\right)$ e como $\nabla C\left(P_0\right) = [1 : 1 : 0]$, então a reta tangente à curva C no ponto P_0 é dada pela equação $T_{P_0} : X + Y = 0$. Portanto, T_{P_0} admite parametrização $\varphi\left(s, t\right) = [s : -s : t]$. Sendo assim, a equação da interseção entre a curva C e a reta tangente T_{P_0} é

$$\psi\left(s, t\right) = s^3 - s^3 + ct^3 = ct^3.$$

Logo, $I\left(C \cap T_{P_0}, P_0\right) = 3$ o que nos permite concluir que P_0 é um ponto de inflexão de C.

O $\mathbb{Q}$-espaço ortogonal a P_0 é gerado por $(0,0,1)$ e $(1,1,0)$. Sendo

$$T_1 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{bmatrix},$$

ou seja, $T_1(X,Y,Z) = (Y+Z, Z-Y, X)$, definindo $C_1 = C\left(T_1(X,Y,Z)\right)$ temos

$$C_1 : (Y+Z)^3 + (Z-Y)^3 + cX^3 = 0 \Longleftrightarrow C_1 : cX^3 + 6Y^2Z + 2Z^3 = 0.$$

Dividindo a equação acima por 6, chegamos na forma (3.13). Aplicando a transformação

$$T_4 = \begin{bmatrix} -\frac{c}{6} & 0 & 0 \\ 0 & \frac{c^2}{36} & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

chegamos à equação

$$\left(\frac{c}{6}\right)^4 Y^2Z = \left(\frac{c}{6}\right)^4 X^3 - \frac{1}{3}Z^3,$$

dividindo por $\left(\frac{c}{6}\right)^4$ e desomogeneizando em relação à variável Z, obtemos a forma de Weierstrass

$$y^2 = x^3 - \frac{432}{c^4},$$

que é obtida ao aplicarmos a transformação

$$T_1T_4 = \begin{bmatrix} 0 & \frac{c^2}{36} & 1 \\ 0 & -\frac{c^2}{36} & 1 \\ -\frac{c}{6} & 0 & 0 \end{bmatrix},$$

na equação da curva C. Caso $\frac{432}{c^4}$ não seja inteiro, podemos realizar mais uma transformação projetiva para tornar os coeficientes inteiros.

Antes de considerarmos o estudo da operação $+$, apresentaremos uma fórmula que nos dará a informação sobre a regularidade de uma cúbica na forma de Weierstrass

$$E : y^2 - f(x) = 0, \quad \text{com } f(x) = x^3 + ax^2 + bx + c.$$

Primeiramente, observamos que $\mathcal{O}\,[0:1:0]$ não é um ponto de singularidade. Se (x_0, y_0) é um ponto de singularidade de E, então $y_0^2 = f(x_0)$ e $2y_0 = f'(x_0) = 0$. Como

$2y_0 = 0$, então $0 = y_0^2 = f(x_0)$, ou seja, f e f' têm $x - x_0$ como fator comum, portanto, $Res_x(f, f') = 0$.

Por outro lado, se $Res_x(f, f') = 0$, então f e f' têm um fator comum. Logo, existe $x_0 \in \mathbb{C}$ tal que $x - x_0$ divide f e f', daí podemos concluir que $(x_0, 0)$ é um ponto de singularidade de E.

Sendo assim, E é regular se, e somente se, $Res_x(f, f') \neq 0$. Dada a importância desse valor para o estudo das curvas elípticas, o destacamos na seguinte definição.

Definição 3.9. Se $E : y^2 = f(x) = x^3+ax^2+bx+c$ é uma cúbica na forma de Weierstrass, definimos o *discriminante* de E como

$$\Delta(E) = -Res_x(f, f') = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2.$$

3.3 Fórmulas Explícitas para a Lei de Grupo

Analisaremos com mais detalhes a operação + em uma curva elíptica.

Considerando a forma de Weierstrass temos que essas curvas têm somente o ponto $\mathcal{O} = [0 : 1 : 0]$ no infinito e, no Exemplo 1.17, observamos que esse é um ponto de inflexão, sendo $Z = 0$ sua respectiva reta tangente. Uma vez que $\mathcal{O}$ é um ponto racional que pertence a todas curvas elípticas, faz sentido tomá-lo como o elemento neutro do nosso grupo. Além disso, tendo em conta que somente o ponto $\mathcal{O}$ está no infinito, podemos por simplicidade, considerar a equação da curva na sua forma afim dada por

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c, \quad \text{com } \Delta(E) \neq 0,$$

com a qual trabalharemos daqui em diante. Além disso, pelo que discutimos no final da seção anterior, podemos supor que a, b e c são inteiros.

Como $\mathcal{O}$ está no infinito, precisamos analisar separadamente quais são as retas afins que passam por $\mathcal{O}$. Uma reta com parte afim tem equação homogênea da forma

$$\alpha X + \beta Y + \gamma Z = 0, \quad \text{com } [\alpha : \beta : \gamma] \neq [0 : 0 : 1].$$

Consequentemente, uma reta afim (não trivial) tem o ponto $\mathcal{O}$ como o ponto no infinito se, e somente se, ela tem a forma

$$\alpha X + \gamma Z = 0, \quad \alpha \neq 0,$$

ou equivalentemente, sua parte afim é uma reta vertical no plano afim.

Proposição 3.10. *Seja P um ponto de uma curva elíptica, então $-P = P * \mathcal{O}$. Em particular, se $P = (x_0, y_0)$, então $-P = (x_0, -y_0)$.*

Demonstração. Na demonstração da Teorema 3.6, provamos a igualdade (3.5)

$$-P = P * (\mathcal{O} * \mathcal{O}) .$$

Como $\mathcal{O}$ é um ponto de inflexão, ou seja, $\mathcal{O} = \mathcal{O} * \mathcal{O}$, temos $-P = P * \mathcal{O}$.

Se $P = (x_0, y_0)$, então P não é o ponto no infinito $\mathcal{O}$. Consequentemente, o ponto $-P$ também não é o ponto no infinito, ou seja, $-P$ é um ponto afim. Portanto, $-P$ é o "segundo" ponto afim na interseção da curva elíptica com a reta vertical que passa por P. Pela simetria das curvas elípticas em relação ao eixo x, podemos concluir que $-P = (x_0, -y_0)$. □

Como consequência, temos o seguinte resultado.

Corolário 3.11. *Sejam P e Q pontos em uma curva elíptica, então $P + Q = -(P * Q)$.*

Demonstração. Pela definição apresentada em (3.2), temos que $P + Q = \mathcal{O} * (P * Q)$. Portanto, pela Proposição 3.10 podemos concluir que $P + Q = -(P * Q)$. □

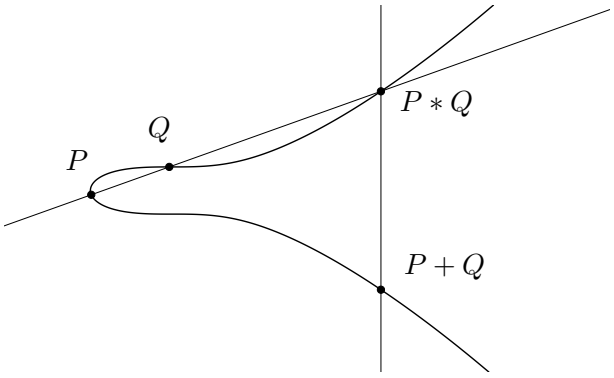


Figura 3.4: Representação da adição de dois pontos em uma curva elíptica.

Com base na Proposição 3.10 e no Corolário 3.11, basta determinarmos $P_1 * P_2$ para podermos apresentar as fórmulas explícitas para $P_1 + P_2$.

Quando P_1 ou P_2 é o elemento neutro $\mathcal{O}$, a operação de adição $+$ é imediata. Sendo assim, vamos nos concentrar nos casos em que P_1 e P_2 são distintos de $\mathcal{O}$, o que nos

permitirá representá-los por suas coordenadas afins

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

Outra consequência do Corolário 3.11 é que $P_1 * P_2 = \mathcal{O}$ se, e somente se,

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

Nos demais casos, teremos $P_2 \neq -P_1$, ou seja, $P_1 * P_2 \neq \mathcal{O}$. Portanto, podemos usar as coordenadas afins $P_1 * P_2 = (x_3, y_3)$.

Uma vez que

$$P_1 + P_2 = -\left(P_1 * P_2\right) = (x_3, -y_3)\,,$$

teremos como objetivo representar x_3 e y_3 em função das coordenadas de P_1 e P_2.

- Caso $P_2 \neq \pm P_1$:

  Nesse caso, temos que $x_1 \neq x_2$. Portanto, a equação da reta $\overline{P_1P_2}$ é dada por

  $$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}\left(x - x_1\right).$$

  Definindo $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ e $\nu = y_1 - \lambda x_1$ a equação da reta $\overline{P_1P_2}$ pode ser escrita como

  $$y = \lambda x + \nu. \tag{3.14}$$

  Assim, a coordenada x dos pontos na interseção da curva elíptica com a reta $\overline{P_1P_2}$ satisfazem

  $$\left(\lambda x + \nu\right)^2 = x^3 + ax^2 + bx + c \iff x^3 + \left(a - \lambda^2\right)x^2 + \left(b - 2\lambda\nu\right)x + \left(c - \nu^2\right) = 0.$$

  Como os pontos de interseção são exatamente P_1, P_2 e $P_1 * P_2$, então x_1, x_2 e x_3 são as raízes da equação de grau três acima, ou seja,

  $$x^3 + \left(a - \lambda^2\right)x^2 + \left(b - 2\lambda\nu\right)x + \left(c - \nu^2\right) = \left(x - x_1\right)\left(x - x_2\right)\left(x - x_3\right).$$

  Igualando os coeficientes de x^2 obtemos que $a - \lambda^2 = -x_1 - x_2 - x_3$, portanto,

  $$x_3 = \lambda^2 - a - x_1 - x_2,$$

  substituindo x_3 na Equação (3.14), podemos concluir que

  $$y_3 = \lambda x_3 + \nu.$$

- Caso $P_1 = P_2$ e $y_1 \neq 0$:

  Nesse caso, a reta $\overline{P_1P_2}$ é a reta tangente à curva elíptica no ponto P_1. Como $\nabla E = (f'(x), -2y)$, então a reta tangente no ponto P_1 é dada por

  $$f'(x_1)(x - x_1) - 2y_1(y - y_1) = 0.$$

  Uma vez que $y_1 \neq 0$, podemos definir $\lambda = \frac{f'(x_1)}{2y_1}$ e $\nu = y_1 - \lambda x_1$. Sendo assim, a equação da reta tangente pode ser escrita como

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

  Com cálculos análogos ao caso anterior, obtemos que

  $$x_3 = \lambda^2 - a - 2x_1 \qquad \text{e} \qquad y_3 = \lambda x_3 + \nu.$$

Resumimos os resultados obtidos acima na seguinte proposição.

Proposição 3.12. *Sejam $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ pontos não nulos de uma curva elíptica, temos que:*

- *Se $(x_2, y_2) = (x_1, -y_1)$, então $P_1 + P_2 = \mathcal{O}$.*
- *Caso contrário, $P_1 + P_2 = \left(\lambda^2 - a - x_1 - x_2,\ -(\lambda(\lambda^2 - a - x_1 - x_2) + \nu)\right)$, com*

$$\lambda = \begin{cases} \frac{f'(x_1)}{2y_1}, & \text{se } x_1 = x_2 \text{ e } y_1 = y_2 \neq 0 \\ \frac{y_2 - y_1}{x_2 - x_1}, & \text{se } x_2 \neq x_1 \end{cases} \qquad \text{e} \qquad \nu = y_1 - \lambda x_1.$$

Denotaremos as coordenadas x e y de um ponto P por $\mathbf{x}(P)$ e $\mathbf{y}(P)$, respectivamente.

Corolário 3.13. *Seja P um ponto em uma curva elíptica, tal que $2P \neq \mathcal{O}$ e $x = \mathbf{x}(P)$. Então*

$$\mathbf{x}(2P) = \frac{x^4 - 2bx^2 - 8cx + (b^2 - 4ac)}{4x^3 + 4ax^2 + 4bx + 4c},$$

que é conhecida como fórmula de duplicação.

Observamos que a fórmula de duplicação de Bachet (1), apresentada na introdução, é um caso particular da fórmula de duplicação dada no corolário anterior.

Capítulo 4

Na Seção 3.2, mostramos que estudar pontos racionais em cúbicas regulares, se resume a estudar as curvas elípticas com coeficientes inteiros, ou seja, cúbicas que são dadas por

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c, \quad \text{com } \Delta(E) \neq 0.$$

Na Seção 3.3, apresentamos fórmulas explícitas para a operação com pontos racionais de uma curva elíptica e, neste capítulo, as utilizaremos para estudar os pontos racionais de ordem finita.

Se m é um número inteiro positivo e P um elemento do grupo aditivo $E(\mathbb{Q})$, então P tem ordem m se

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ parcelas}} = \mathcal{O},$$

mas $m'P \neq \mathcal{O}$ para todo inteiro $1 \leq m' < m$. Se tal inteiro m existir, então o denotaremos por $|P|$ e diremos que P tem *ordem finita*. Caso contrário, diremos que P tem *ordem infinita* e indicaremos $|P| = \infty$. Além disso, definimos

$$E_{tor}(\mathbb{Q}) = \{P \in E(\mathbb{Q}) ; |P| < \infty\}.$$

Vale observar que $E_{tor}(\mathbb{Q})$ é um subgrupo de $E(\mathbb{Q})$, chamado de subgrupo de torção de $E(\mathbb{Q})$.

4.1 Pontos de Ordem Dois e Três

Um ponto P em uma curva elíptica tem ordem dois quando $P \neq \mathcal{O}$ e $2P = \mathcal{O}$, ou seja, é um ponto não nulo, tal que $P = -P$. Como $-(x, y) = (x, -y)$, podemos concluir que P tem ordem dois se, e somente se, o ponto P tem a forma $(\alpha, 0)$ com α sendo uma raiz racional de $f(x)$. A regularidade da curva garante que f tem raízes distintas, então

podemos ter zero, um ou três pontos de ordem dois. Além disso, o subgrupo gerado por esses pontos são isomorfos a $\{\mathcal{O}\}$, $\mathbb{Z}/2\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$, respectivamente.

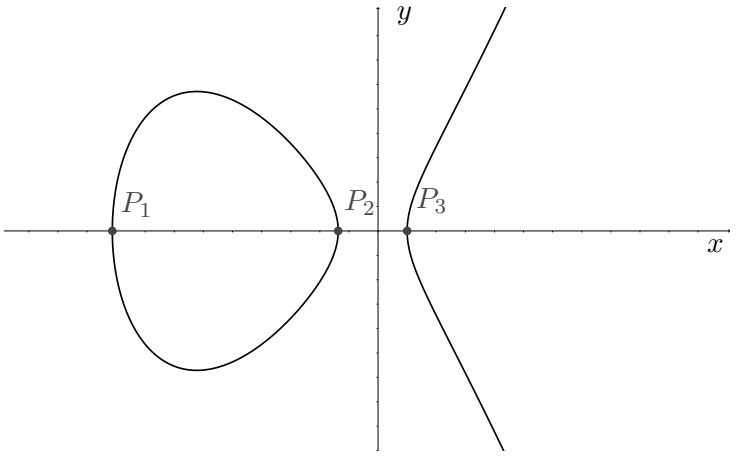


Figura 4.1: Representação dos pontos de ordem dois em uma curva elíptica dada por $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ com $\alpha_1 \neq \alpha_2 \neq \alpha_3 \neq \alpha_1$.

Para pontos de ordem três, podemos reescrever a equação $3P = \mathcal{O}$ como $2P = -P$, portanto, um ponto de ordem três irá satisfazer $\mathbf{x}(2P) = \mathbf{x}(-P) = \mathbf{x}(P)$. Reciprocamente, se $P \neq \mathcal{O}$ satisfaz $\mathbf{x}(2P) = \mathbf{x}(P)$, então $2P = \pm P$. Uma vez que $P \neq \mathcal{O}$ temos que $3P = \mathcal{O}$. Sendo assim, um ponto P não nulo tem ordem três se, e somente se, satisfaz $\mathbf{x}(2P) = \mathbf{x}(P)$.

Para encontrar os pontos não nulos que satisfazem a condição desejada, utilizaremos a fórmula de duplicação apresentada no Corolário 3.13, ou seja, se $\mathbf{x}(P) = x$ então

$$\mathbf{x}(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c},$$

igualando essa expressão a x obtemos a equação:

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0.$$

Portanto, um ponto não nulo tem ordem três se, e somente se, a sua coordenada x é raiz de ψ_3.

Lembremos de um resultado que nos será útil.

Lema 4.1. *Seja $f(x)$ um polinômio com raízes reais α_1 e α_2, com $\alpha_1 < \alpha_2$, tais que $f'(\alpha_1)$ e $f'(\alpha_2)$ são positivos. Então f tem uma raiz real no intervalo (α_1, α_2).*

Demonstração. Identificando f com uma função polinomial, como $f'(\alpha_1)$ e $f'(\alpha_2)$ são positivos, então f é crescente em α_1 e α_2. Portanto, existem $\alpha_1 < \alpha_1' < \alpha_2' < \alpha_2$ tais que

$$f(\alpha_2') < f(\alpha_2) = 0 = f(\alpha_1) < f(\alpha_1').$$

Como f é contínua, pelo Teorema do Valor Intermediário, f admite raiz real

$$\alpha_0 \in (\alpha_1', \alpha_2') \subset (\alpha_1, \alpha_2).$$

□

Destaquemos propriedades dos pontos de ordem dois e três.

Teorema 4.2 (Pontos de Ordem Dois e Três)**.** *Seja E uma curva elíptica definida por*

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

(i) Um ponto $P = (x, y) \neq \mathcal{O}$ em $E(\mathbb{Q})$ tem ordem dois se, e somente se, $y = 0$.

(ii) O subgrupo gerado pelos pontos de ordem dois é o grupo trivial, isomorfo a $\mathbb{Z}/2\mathbb{Z}$ ou a $(\mathbb{Z}/2\mathbb{Z})^2$.

(iii) Um ponto $P = (x, y) \neq \mathcal{O}$ em $E(\mathbb{Q})$ tem ordem três se, e somente se, x é uma raiz racional de

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

(iv) O subgrupo gerado pelos pontos de ordem três é trivial ou isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

Demonstração. Os itens *(i), (ii)* e *(iii)* seguem dos comentários do início deste capítulo.

(iv) Se $P = (x, y)$ é um ponto de ordem três, isto é, $|P| = 3 \neq 2$, então $y \neq 0$ e

$$\psi_3'(x) = 12f(x) = 12y^2 > 0,$$

portanto, a coordenada x dos pontos de ordem três é raiz de ψ_3 em que a derivada é positiva.

Como ψ_3 tem grau quatro, pelo Lema 4.1, existem no máximo duas raízes reais distintas de ψ_3 com derivadas positivas. Uma vez que cada raiz de ψ_3 é a coordenada x de exatamente dois pontos de ordem três em $E(\mathbb{C})$, então podem existir no máximo quatro pontos de ordem três em $E(\mathbb{Q})$. Logo, o grupo gerado pelos pontos racionais de ordem

três é finitamente gerado. Portanto, isomorfo a $(\mathbb{Z}/3\mathbb{Z})^m$, para algum m inteiro positivo. Além disso, todos seus elementos, não nulos, têm ordem três. Como existem no máximo quatro elementos de ordem três, podemos concluir que $m < 2$, ou seja, o subgrupo gerado pelos elementos de ordem três é trivial ou isomorfo a $\mathbb{Z}/3\mathbb{Z}$. □

Corolário 4.3. *Pontos de ordem dois em $E(\mathbb{Q})$ têm coordenadas inteiras.*

Demonstração. Pelo Teorema 4.2, pontos de ordem dois em $E(\mathbb{Q})$ têm a forma $(\alpha, 0)$, com α sendo uma raiz de $f = x^3 + ax^2 + bx + c$. Como f é um polinômio mônico e tem coeficientes inteiros, então α é um número inteiro. □

Na proposição a seguir observamos que os pontos que satisfazem $3P = \mathcal{O}$ têm a propriedade geométrica de serem pontos de inflexão.

Proposição 4.4. *Se P é um ponto racional em uma curva elíptica. Então $3P = \mathcal{O}$ se, e somente se, P é ponto de inflexão.*

Demonstração. De fato, $3P = \mathcal{O}$ se, e somente se, $2P = -P$, que pelo Corolário 3.11, é equivalente a afirmar que $-P = 2P = -(P * P)$. Podemos então concluir que $3P = \mathcal{O}$ se, e somente se, $P = P * P$, ou seja , P é um ponto de inflexão. □

4.2 Pontos de Ordem Finita têm Coordenadas Inteiras

No Corolário 4.3 observamos que os pontos de ordem dois têm coordenadas inteiras. Nesta seção mostraremos que essa característica não é exclusividade dos pontos de ordem dois, mas comum a todos os pontos de ordem finita. Nossa estratégia será demonstrar que os denominadores das coordenadas de um ponto de torção não são divisíveis por nenhum número primo.

Como antes, consideramos uma curva elíptica E dada por

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Lema 4.5. *Se $P \in E(\mathbb{Q}) - \{\mathcal{O}\}$, então existem $\phi, \omega, \psi \in \mathbb{Z}$ com $MDC(\phi\omega, \psi) = 1$ e $\psi > 0$, tais que*

$$P = \left(\frac{\phi}{\psi^2}, \frac{\omega}{\psi^3}\right).$$

Demonstração. Se uma das coordenadas de P é zero, então a outra coordenada é raiz de $y^2 - c = 0$ ou de $f(x) = x^3 + ax^2 + bx + c$; como ambos são polinômios mônicos com coeficientes inteiros, temos que qualquer raiz racional é inteira e o lema é válido ao tomarmos $\psi = 1$.

Seja $P = \left(\frac{\phi}{\rho}, \frac{\omega}{\sigma}\right)$ com ϕ e ω não nulos, ρ e σ positivos e $MDC(\phi, \rho) = MDC(\omega, \sigma) = 1$. Substituindo P na equação que define E e eliminando os denominadores, temos que

$$\omega^2\rho^3 = \sigma^2\left(\phi^3 + a\phi^2\rho + b\phi\rho^2 + c\rho^3\right). \tag{4.1}$$

Como todos os valores envolvidos são inteiros segue que σ^2 divide $\omega^2\rho^3$. Além disso, por ω e σ serem coprimos, temos que σ^2 divide ρ^3. Por outro lado, ρ^3 divide o lado direito da Equação (4.1) e dado que $MDC(\phi, \rho) = 1$ implica em $MDC(\phi^3 + a\phi^2\rho + b\phi\rho^2 + c\rho^3, \rho) = 1$, ou seja, ρ^3 divide σ^2.

Pelo fato de ρ ser positivo, então $\rho^3 = \sigma^2$, consequentemente, $\rho = \left(\frac{\sigma}{\rho}\right)^2$ e $\sigma = \left(\frac{\sigma}{\rho}\right)^3$. Denotando o inteiro positivo

$$\psi = \frac{\sigma}{\rho},$$

temos que $\rho = \psi^2$ e $\sigma = \psi^3$.

Como ϕ e ρ são coprimos, temos que ϕ e ψ são coprimos. Analogamente, por ω e σ serem coprimos temos que ω e ψ são coprimos. Portanto, $MDC(\phi\omega, \psi) = 1$. □

Observação 4.6. Uma consequência importante do Lema 4.5 é que um número primo p divide o denominador de $\mathbf{x}(P)$ se, e somente se, p divide o denominador de $\mathbf{y}(P)$, portanto, se uma das coordenadas de $P \in E(\mathbb{Q}) - \{\mathcal{O}\}$ é inteira a outra também é inteira.

Notação: Sendo P um ponto racional em uma curva elíptica, denotaremos os valores ϕ, ω e ψ apresentados no Lema 4.5 por $\boldsymbol{\phi}(P)$, $\boldsymbol{\omega}(P)$ e $\boldsymbol{\psi}(P)$ respectivamente. Quando não houver confusão quanto ao ponto que estamos considerando, utilizaremos simplesmente ϕ, ω e ψ.

Definição 4.7. Sejam E uma curva elíptica, p um número primo e v um número inteiro positivo. Definimos o conjunto $E(p^v)$ como:

$$E(p^v) = \{P \in E(\mathbb{Q}) ; p^v \text{ divide } \boldsymbol{\psi}(P)\} \cup \{\mathcal{O}\}.$$

Segue da definição que

$$E(\mathbb{Q}) \supset E(p) \supset E\left(p^2\right) \supset E\left(p^3\right) \supset \cdots$$

além disso,

$$\mathcal{O} = \bigcap_{v>0} E\left(p^v\right).$$

Para mostrarmos que pontos de torção têm coordenadas inteiras basta mostrarmos que, para todo número primo p, o conjunto $E(p)$ não contém pontos de torção além de $\mathcal{O}$. Primeiramente mostraremos que $E\left(p^v\right)$ é um subgrupo de $E(\mathbb{Q})$.

Consideremos $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$ a homogeneização da equação que define E. Desomogeneizando em relação a Y obtemos a equação:

$$s = t^3 + at^2s + bts^2 + cs^3, \tag{4.2}$$

com as variáveis t e s satisfazendo

$$t = \frac{X}{Y} \qquad \text{e} \qquad s = \frac{Z}{Y}.$$

Sendo v um número inteiro positivo e p um número primo, os únicos pontos de E que estão na reta projetiva $Y = 0$ são os pontos de ordem dois, que pelo Lema 4.5, têm coordenadas inteiras. Portanto, todos os pontos de $E\left(p^v\right)$ podem ser representados no sistema de coordenadas afim (t, s). Em particular, o elemento neutro $\mathcal{O}$ pode ser representado por $(0, 0)$ nas coordenadas (t, s) e um ponto não nulo $(x, y) \in E(\mathbb{Q})$ com $y \neq 0$ é representado, nas coordenadas (t, s) por $\left(\frac{x}{y}, \frac{1}{y}\right)$. Desse modo, podemos recuperar as coordenadas originais por $x = \frac{t}{s}$ e $y = \frac{1}{s}$.

Essa mudança de coordenadas não muda como os pontos se relacionam, pois estamos apenas homogeneizando nossa equação afim original e desomogeneizando em uma outra direção. Desse modo, as operações ficam preservadas. Logo, mostrar que $E\left(p^v\right)$ é subgrupo utilizando as coordenadas (x, y) é equivalente a mostrar que $E\left(p^v\right)$ é subgrupo nas coordenadas (t, s).

Primeiramente, vamos dar uma caracterização do conjunto $E\left(p^v\right)$ em termos das coordenadas (t, s). Para isso consideramos o anel

$$R_p = \left\{ \frac{u}{w} \in \mathbb{Q};\ p \text{ não divide } w \right\}.$$

Observamos que R_p é um subanel de $\mathbb{Q}$, pois se α e β são números racionais com denominadores coprimos a p, então $\alpha \pm \beta$ e $\alpha\beta$ também têm denominadores coprimos a p. Além disso, o conjunto dos elementos invertíveis de R_p é o conjunto dos números racionais tais que o numerador e o denominador são coprimos a p, denotaremos tal conjunto por $R_p{}^*$.

Um ponto não nulo $P \in E(p^v)$ se, e somente se, p^v divide $\boldsymbol{\psi}(P)$. Como $\mathbf{x}(P) = \frac{\phi}{\psi^2}$ e $\mathbf{y}(P) = \frac{\omega}{\psi^3}$, então as coordenadas t e s correspondentes ao ponto P são

$$t = \frac{\frac{\phi}{\psi^2}}{\frac{\omega}{\psi^3}} = \frac{\phi\psi}{\omega} \qquad \text{e} \qquad s = \frac{1}{\frac{\omega}{\psi^3}} = \frac{\psi^3}{\omega}. \tag{4.3}$$

Portanto, o ponto $P = (t, s) \in E(p^v)$ se, e somente se, p^v divide o numerador de t e p^{3v} divide o numerador de s, ou seja, $t \in p^v R_p$ e $s \in p^{3v} R_p$.

Agora que temos uma caracterização dos pontos de $E(p^v)$ em termos do sistema de coordenadas (t, s), podemos demonstrar que $E(p^v)$ é um subgrupo de $E(\mathbb{Q})$.

Proposição 4.8. *Se p é um número primo e v um número inteiro positivo, então o conjunto $E(p^v)$ é um subgrupo de $E(\mathbb{Q})$.*

Demonstração. Seja $P = (t, s) \in E(p^v)$ um ponto não nulo. Pelo Teorema 3.6,

$$-P = P * (\mathcal{O} * \mathcal{O}),$$

como $\mathcal{O}$ é um ponto de inflexão temos que $\mathcal{O} = \mathcal{O} * \mathcal{O}$, portanto

$$-P = P * \mathcal{O}.$$

O ponto $(-t, -s)$ é não nulo e também satisfaz a Equação (4.2), então ele é um ponto racional de E. Pelo fato de $\{(t, s), (0, 0), (-t, -s)\}$ serem três pontos colineares distintos temos que

$$-P = P * \mathcal{O} = (t, s) * (0, 0) = (-t, -s).$$

Portanto,

$$\begin{aligned}(t, s) \in E(p^v) &\Leftrightarrow t \in p^v R_p \quad e \quad s \in p^{3v} R_p \\ &\Leftrightarrow -t \in p^v R_p \quad e \quad -s \in p^{3v} R_p \\ &\Leftrightarrow -P = (-t, -s) \in E(p^v).\end{aligned}$$

Consideremos os pontos $P_1 = (t_1, s_1)$ e $P_2 = (t_2, s_2)$ em $E(p^v)$.

Observamos que se $t_1 = t_2$, então $s_1 = s_2$. De fato, suponhamos por absurdo que $s_1 \neq s_2$. Então $s_1 = t_1^3 + at_1^2 s_1 + bt_1 s_1^2 + cs_1^3$ e $s_2 = t_1^3 + at_1^2 s_2 + bt_1 s_2^2 + cs_2^3$. Subtraindo as duas equações temos que

$$s_2 - s_1 = at_1^2 (s_2 - s_1) + bt_1 \left(s_2^2 - s_1^2\right) + c \left(s_2^3 - s_1^3\right),$$

dividindo por $s_2 - s_1$ obtemos que

$$1 = at_1^2 + bt_1 (s_2 + s_1) + c \left(s_2^2 + s_2 s_1 + s_1^2\right). \tag{4.4}$$

Como a, b e c são números inteiros, t_1, s_1 e s_2 são elementos de $p^v R_p$, então o lado direito da Equação (4.4) está em $p^v R_p$. Entretanto, isso é um absurdo pois 1 não é um elemento de $p^v R_p$. Portanto, devemos ter $s_1 = s_2$.

Sendo assim, temos dois possíveis casos para analisar:

- $t_1 \neq t_2$: Então a reta $\overline{P_1 P_2}$ não é uma reta vertical, ou seja, pode ser descrita por $s = \alpha t + \beta$. Além disso, o coeficiente angular α dessa reta é dado por

  $$\alpha = \frac{s_2 - s_1}{t_2 - t_1}.$$

  Como (t_1, s_1) e (t_2, s_2) satisfazem a Equação (4.2). Subtraindo as equações avaliadas no pontos P_2 e P_1, obtemos:

  $$\begin{aligned} s_2 - s_1 &= \left(t_2^3 - t_1^3\right) + a \left(t_2^2 s_2 - t_1^2 s_1\right) + b \left(t_2 s_2^2 - t_1 s_1^2\right) + c \left(s_2^3 - s_1^3\right) \\ &= \left(t_2^3 - t_1^3\right) + a \left(\left(t_2^2 - t_1^2\right) s_2 + t_1^2 (s_2 - s_1)\right) + b \left((t_2 - t_1) s_2^2 + t_1 \left(s_2^2 - s_1^2\right)\right) + \\ &\quad + c \left(s_2^3 - s_1^3\right), \end{aligned}$$

  agrupando os fatores $(t_2 - t_1)$ e $(s_2 - s_1)$ obtemos

  $$\begin{aligned} &(s_2 - s_1) \left(1 - at_1^2 - bt_1 (s_2 + s_1) - c \left(s_2^2 + s_1 s_2 + s_1^2\right)\right) \\ &\quad = (t_2 - t_1) \left(t_2^2 + t_1 t_2 + t_1^2 + a (t_2 + t_1) s_2 + bs_2^2\right), \end{aligned}$$

  como $-at_1^2 - bt_1 (s_2 + s_1) - c (s_2^2 + s_1 s_2 + s_1^2) \in p^v R_p$ então

  $$1 - at_1^2 - bt_1 (s_2 + s_1) - c \left(s_2^2 + s_1 s_2 + s_1^2\right) \in R_p^*,$$

  em particular, tal elemento é não nulo, portanto

  $$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a (t_2 + t_1) s_2 + bs_2^2}{1 - at_1^2 - bt_1 (s_2 + s_1) - c (s_2^2 + s_1 s_2 + s_1^2)}. \tag{4.5}$$

  Por um breve momento deixaremos esse caso de lado.

- $t_1 = t_2$, ou seja, $P_1 = P_2$: Como

$$\nabla E\left(t,s\right) = \left(3t^2 + 2ats + bs^2, at^2 + 2bts + 3cs^2 - 1\right),$$

então o coeficiente angular da reta tangente à E no ponto P_1 é

$$\alpha = \frac{3t_1^2 + 2at_1s_1 + bs_1^2}{1 - at_1^2 - 2bt_1s_1 - 3cs_1^2}.$$

Se substituirmos $t_2 = t_1$ e $s_2 = s_1$ no lado direito da Equação (4.5), obtemos esse mesmo coeficiente angular. Portanto, podemos utilizar a Equação (4.5) em ambos os casos.

Ao analisarmos a Equação (4.5), como t_1, t_2, s_1 e s_2 são elementos de p^vR_p, temos que o numerador de α

$$t_2^2 + t_1t_2 + t_1^2 + a\left(t_2 + t_1\right)s_2 + bs_2^2 \in p^{2v}R_p,$$

e, como observamos anteriormente, o denominador de α está em R_p^*, portanto, $\alpha \in p^{2v}R_p$.

O ponto P_1 satisfaz a equação $s = \alpha t + \beta$, logo

$$\beta = s_1 - \alpha t_1.$$

Como $t_1 \in p^vR_p$, $s_1 \in p^{3v}R_p$ e $\alpha \in p^{2v}R_p$, então $\beta \in p^{3v}R_p$.

Seja $P_3 = P_1 * P_2$. Substituindo $s = \alpha t + \beta$ na Equação (4.2) obtemos a equação de interseção

$$\left(\alpha t + \beta\right) = t^3 + at^2\left(\alpha t + \beta\right) + bt\left(\alpha t + \beta\right)^2 + c\left(\alpha t + \beta\right)^3,$$

expandindo e agrupando as potências de t obtemos

$$0 = \left(1 + a\alpha + b\alpha^2 + c\alpha^3\right)t^3 + \left(a\beta + 2b\alpha\beta + 3c\alpha^2\beta\right)t^2 + \left(b\beta^2 + 3c\alpha\beta^2 - \alpha\right)t + c\beta^3 - \beta,$$

como $\alpha \in p^{2v}R_p$, então $(1 + a\alpha + b\alpha^2 + c\alpha^3)$ está em R_p^*, consequentemente, ele é não nulo e a equação de interseção tem grau três. Como a equação de interseção tem grau três, então P_3 é um ponto afim e pode ser escrito na forma $P_3 = (t_3, s_3)$. Além disso, a equação de interseção tem raízes t_1, t_2 e t_3, portanto[1]

$$t_1 + t_2 + t_3 = -\frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}. \tag{4.6}$$

[1]Em geral, vale que a soma das raízes de uma equação cúbica na forma $a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ é igual a $-\frac{a_2}{a_3}$.

Finalmente, analisando a Equação (4.6), temos que o denominador de $t_1+t_2+t_3$ está em R_p^* e o numerador é múltiplo de β. Como $\beta \in p^{3v}R_p$, então $t_1+t_2+t_3 \in p^{3v}R_p$.

Uma vez que $t_1, t_2 \in p^vR_p$, então $t_3 \in p^vR_p$. Além disso, pelo fato de $\alpha \in p^{2v}R_p$, temos $s_3 = \alpha t_3 + \beta \in p^{3v}R_p$, o que implica em $P_3 \in E(p^v)$.

Como vimos, o inverso de qualquer elemento de $E(p^v)$ também pertence a $E(p^v)$, então podemos concluir que

$$P_1 + P_2 = -(P_1 * P_2) = -P_3 \in E(p^v).$$

□

Na demonstração do resultado anterior provamos que se $P_1, P_2 \in E(p^v)$, então

$$\boldsymbol{t}(P_1) + \boldsymbol{t}(P_2) - \boldsymbol{t}(P_1 + P_2) \in p^{3v}R_p,$$

com $\boldsymbol{t}(P)$ denotando a coordenada t correspondente ao ponto P. Podemos reescrever essa condição de uma maneira mais conveniente:

$$\boldsymbol{t}(P_1 + P_2) \equiv \boldsymbol{t}(P_1) + \boldsymbol{t}(P_2) \pmod{p^{3v}R_p}. \tag{4.7}$$

Continuemos com alguns resultados auxiliares.

Lema 4.9. *Sejam $v' \geq v > 0$ números inteiros e P um ponto não nulo de $E(p^v)$. Se $\boldsymbol{t}(P) \in p^{v'}R_p$, então $P \in E\left(p^{v'}\right)$.*

Demonstração. Uma vez que $P = (t, s)$ é um ponto não nulo, então $s \neq 0$, pois o único ponto que tem a coordenada s nula é o elemento neutro $(0, 0)$.

Se a coordenada t for nula, então a correspondente coordenada $x = \frac{t}{s}$ também é nula, portanto, a correspondente coordenada racional y é raiz do polinômio $y^2 - c$. Como esse polinômio é mônico e tem coeficientes inteiros, então suas raízes são inteiras. Daí podemos concluir que P tem coordenadas inteiras, o que contradiz a hipótese de P pertencer a $E(p^v)$, portanto, $t = \boldsymbol{t}(P) \neq 0$.

Pelo fato de $P \in E(p^v)$, segue que $\boldsymbol{\psi}(P) \in p^vR_p$. Uma vez que podemos escrever $\boldsymbol{t}(P)$ como $\frac{\phi\psi}{\omega}$, com $\phi\omega \neq 0$ e $MDC(\phi\omega, \psi) = 1$ (veja Lema 4.5 e (4.3)), temos que ϕ e ω são coprimos a p.

Por hipótese $\boldsymbol{t}(P) = \frac{\phi\psi}{\omega} \in p^{v'}R_p$, além disso, os elementos ϕ e ω são invertíveis em R_p, segue assim que $\psi \in p^{v'}R_p$, o que nos permite concluir que $P \in E\left(p^{v'}\right)$. □

Lema 4.10. *Para todo número primo p, o grupo $E(p)$ não contêm pontos de ordem finita além de $\mathcal{O}$.*

Demonstração. Sejam p um número primo e $P \in E(\mathbb{Q})$ um ponto de ordem $m > 1$. Suponhamos por absurdo que $P \in E(p)$.

Como P tem ordem $m > 1$, ou seja, não é o elemento neutro, então $P \notin \bigcap_{v>0} E(p^v)$, portanto, existe $v > 0$ tal que $P \in E(p^v)$ e $P \notin E(p^{v+1})$. Temos três possíveis casos:

(i) m é par:

Temos que $m = 2k$ para algum inteiro positivo k. Portanto, o subgrupo de $E(\mathbb{Q})$ gerado por P contém o elemento de ordem dois kP. Como $P \in E(p^v)$, pela Proposição 4.8 temos que $kP \in E(p^v)$, mas isso contradiz o Corolário 4.3, o qual garante que pontos de ordem dois têm coordenadas inteiras.

(ii) m é ímpar e coprimo a p:

Ao considerarmos a relação (4.7) sucessivas vezes, temos que

$$\boldsymbol{t}(mP) \equiv m\boldsymbol{t}(P) \pmod{p^{3v}R_p}.$$

Uma vez que $mP = \mathcal{O}$ e $\boldsymbol{t}(\mathcal{O}) = 0$, segue que $0 \equiv m\boldsymbol{t}(P) \pmod{p^{3v}R_p}$, pelo fato de p e m serem coprimos, temos que m é invertível em R_p, portanto

$$0 \equiv \boldsymbol{t}(P) \pmod{p^{3v}R_p}.$$

Temos $3v > v + 1 > v$, assim pelo Lema 4.9, podemos concluir que $P \in E(p^{3v}) \subset E(p^{v+1})$, mas isso contradiz a hipótese de que $P \notin E(p^{v+1})$.

(iii) Se m é ímpar e divisível por p:

Sendo m divisível p, então $m = pn$ para algum inteiro positivo n. Seja $P' = nP$, então P' tem ordem p. Pelo fato de $E(p^v)$ ser um subgrupo que contém P, temos que $P' \in E(p^v)$. Consideremos o número inteiro $v' \geq v$, tal que $P' \in E\left(p^{v'}\right)$ e $P' \notin E\left(p^{v'+1}\right)$. De modo análogo ao segundo caso obtemos que

$$0 = \boldsymbol{t}(\mathcal{O}) = \boldsymbol{t}(pP') \equiv p\boldsymbol{t}(P') \pmod{p^{3v'}R_p}.$$

Portanto,

$$\boldsymbol{t}(P') \equiv 0 \pmod{p^{3v'-1}R_p}.$$

Do fato $3v'-1 \geq v'+1 > v'$, e do Lema 4.9, podemos concluir que $P' \in E\left(p^{3v'-1}\right) \subseteq E\left(p^{v'+1}\right)$, mas isso contradiz o fato de que $P' \notin E\left(p^{v'+1}\right)$.

Pela arbitrariedade de p, podemos concluir que para todo número primo p, o grupo $E(p)$ não contém pontos de ordem finita além de $\mathcal{O}$. □

Os resultados anteriores, permitem obter o seguinte teorema:

Teorema 4.11. *Os pontos de torção de $E(\mathbb{Q})$ têm coordenadas inteiras.*

Demonstração. Seja $P \neq \mathcal{O}$ um ponto de ordem finita em $E(\mathbb{Q})$. Se P não tem coordenadas inteiras, então expressando $P = \left(\frac{\phi}{\psi^2}, \frac{\omega}{\psi^3}\right)$ como no Lema 4.5, existe um número primo p que divide $\boldsymbol{\psi}(P)$. Portanto, $P \in E(p)$, mas isso contradiz o Lema 4.10.

Logo, podemos concluir que P tem coordenadas inteiras. □

4.3 O Teorema de Nagell-Lutz

Se $P = (x_0, y_0) \in E(\mathbb{Q})$ é um ponto de torção, então $2P$ também é um ponto de torção. Pelo Teorema 4.11, os pontos de torção de $E(\mathbb{Q})$ têm coordenadas inteiras, consequentemente, se P é um ponto de torção então P e $2P$ têm coordenadas inteiras.

O lema a seguir estabelece um critério que permite determinar os pontos $P \in E(\mathbb{Q})$, tais que P e $2P$ têm coordenadas inteiras. Em particular, permite determinar os pontos de torção.

Lema 4.12. *Seja $P = (x_0, y_0)$ um ponto racional não nulo de uma curva elíptica E, tal que P e $2P$ têm coordenadas inteiras. Então $y_0 = 0$ ou y_0^2 divide $\Delta(E)$.*

Demonstração. Se P é um ponto de ordem dois, então as condições de P e $2P$ terem coordenadas inteiras são satisfeitas e, pelo Teorema 4.2, temos que $y_0 = 0$. Logo, o lema é satisfeito para pontos de ordem dois.

Portanto, precisamos considerar somente os casos em que P tem ordem diferente de dois. Pela fórmula apresentada na Proposição 3.12, temos que

$$\mathbf{x}(2P) = \left(\frac{f'(x_0)}{2y_0}\right)^2 - a - 2x_0.$$

Os números x_0, y_0 e $\mathbf{x}(2P)$ são inteiros por hipótese e, pelo fato de $f(x) = x^3+ax^2+bx+c$ ter coeficientes inteiros, então a e $f'(x_0)$ também são inteiros, logo

$$\left(\frac{f'(x_0)}{2y_0}\right)^2 \in \mathbb{Z},$$

o que permite concluir y_0^2 divide $f'(x_0)^2$.

Como $P \in E(\mathbb{Q})$, ou seja, $y_0^2 = f(x_0)$, temos que y_0^2 divide $f(x_0)$.

Observamos que[2] $Res(f, f'^2) = \Delta(E)^2$ e, os elementos da primeira linha da matriz $adj(R_{f,f'^2})$ são divisíveis por $\Delta(E)$ (veja demonstração do Teorema 1.24). Portanto, pela Observação 1.25, existem $r, s \in \mathbb{Z}[x]$, tais que

$$rf + sf'^2 = \frac{\Delta(E)^2}{\Delta(E)} = \Delta(E).$$

Os polinômios r e s são dados explicitamente por[3]

$$r(x) = 27x^3 + 27ax^2 + 27bx - 4a^3 + 18ab - 27c \qquad \text{e} \qquad s(x) = -3x^2 - 2ax + a^2 - 4b.$$

Como y_0^2 divide $f(x_0)$ e $f'^2(x_0)$, e $r(x_0)$ e $s(x_0)$ são números inteiros, então podemos concluir que y_0^2 divide $\Delta(E)$. □

Reunindo os resultados desta seção podemos apresentar o seguinte teorema.

Teorema 4.13 (Nagell-Lutz). *Seja $P = (x, y)$ um ponto racional de ordem finita em uma curva elíptica E. Então*

(i) x e y são inteiros;

(ii) $y = 0$ ou y^2 divide $\Delta(E)$;

(iii) $E_{tor}(\mathbb{Q})$ é um subgrupo finito de $E(\mathbb{Q})$.

Demonstração. Dado que P tem ordem finita, temos que $2P$ também tem ordem finita, logo pela Proposição 4.11 os pontos P e $2P$ têm coordenadas inteiras, o que mostra o item *(i)*.

[2] Na verdade, essa igualdade segue da definição de $\Delta(E)$ e da propriedade de que se f, g e h são polinômios com variável x, então $Res_x(f, gh) = Res_x(f, g)\, Res_x(f, h)$ (veja [Kir92, Capítulo 3]).

[3] Fazer esses cálculos manualmente não é tarefa fácil, felizmente existem vários softwares que podem nos auxiliar em tais tarefas. Para esses cálculos utilizamos o SageMath que pode também ser acessado em sua versão online SageMathCell.

Como P e $2P$ têm coordenadas inteiras, pelo Lema 4.12, temos que $y = 0$ ou y^2 divide $\Delta(E)$ que nos dá o item *(ii)*.

Pelo que observamos ao final da Seção 3.2, temos que a regularidade de E implica em $\Delta(E) \neq 0$, portanto, existe uma quantidade finita de possibilidades para coordenada y dos pontos de torção. Para cada um dos candidatos à coordenada y existe no máximo três candidatos à coordenada x obtidos pela equação $y^2 = f(x)$. Podemos então concluir que $E_{tor}(\mathbb{Q})$ é um subgrupo finito de $E(\mathbb{Q})$. □

Exemplo 4.14. Consideremos a curva elíptica dada por $E : y^2 = x^3 + x^2 + x + 1$. Pela Definição 3.9, segue que $\Delta(E) = -16 = -2^4$, portanto, pelo Teorema de Nagell-Lutz os pontos de torção têm a coordenada y no conjunto $\{0, \pm 1, \pm 2, \pm 4\}$. Testando cada uma das possibilidades encontramos os pontos

$$(-1, 0), (0, \pm 1), (1, \pm 2).$$

Como a coordenada y do ponto $(-1, 0)$ é nula, então esse é um ponto de ordem dois. Usando a fórmula de duplicação

$$\mathbf{x}(2P) = \frac{x^4 - 2bx^2 - 8cx + (b^2 - 4ac)}{4x^3 + 4ax^2 + 4bx + 4c},$$

podemos verificar que o dobro dos pontos $(0, \pm 1)$ e $(1, \pm 2)$ não têm coordenadas inteiras, ou seja, esses pontos não têm ordem finita. Existem ainda os pontos de coordenadas inteiras $(7, \pm 20)$[4], como 20^2 não divide $\Delta(E)$ esse ponto tem ordem infinita.

O Teorema de Nagell-Lutz tem grande importância, pois além de dar um modo de encontrar os pontos de ordem finita, ele garante que existe somente uma quantidade finita de tais pontos e como consequência, que $E_{tor}(\mathbb{Q})$ é finitamente gerado.

Uma limitação do Teorema de Nagell-Lutz é que ele não nos diz quais são as possíveis ordens de um elemento de torção e nem quantos geradores o subgrupo de torção pode ter. Na verdade, a lista de possíveis estruturas de $E_{tor}(\mathbb{Q})$, a menos de isomorfismo, é bem restrita e totalmente descrita pelo teorema enunciado a seguir.

Teorema 4.15 (Teorema de Mazur). *Seja E uma curva elíptica. Então $E_{tor}(\mathbb{Q})$ é isomorfo a um dos seguinte grupos*

[4]Este ponto pode ser obtido usando o método da descida que será descrito no Capítulo 5. Entretanto, para exemplos mais simples, podemos consultar o banco de dados [LMF22] que contém várias informações de milhões de curvas elípticas.

(i) $\mathbb{Z}/N\mathbb{Z}$, *com* $1 \leq N \leq 10$ *ou* $N = 12$.

(ii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, *com* $1 \leq N \leq 4$.

Apesar do enunciado simples, o Teorema de Mazur é um resultado muito difícil de demonstrar, como observado por diversos autores [ST15, Teorema 2.7] ou [Hus04, Teorema 5.3].

Observação 4.16. Para cada um dos grupos apresentados no Teorema de Mazur existe uma curva elíptica que tem tal grupo como subgrupo de torção. Uma lista de curvas elípticas cobrindo todos os possíveis subgrupos de torção, sobre o corpo dos números racionais, pode ser encontrada em [ST15, Exercício 2.12].

Capítulo 5

Neste capítulo demonstraremos o Teorema de Mordell o qual garante que o grupo dos pontos racionais $E(\mathbb{Q})$ de uma curva elíptica é finitamente gerado. Nossa abordagem será, primeiramente, estabelecer quais condições um grupo abeliano deve satisfazer para garantir que ele seja finitamente gerado, posteriormente, mostraremos que $E(\mathbb{Q})$ satisfaz tais condições.

5.1 Uma Caracterização para os Grupos Abelianos Finitamente Gerados

Em geral, explicitar os geradores de um grupo abeliano finitamente gerado não é fácil. Portanto, nesta seção, estabeleceremos alguns critérios que permitirão garantir que um grupo abeliano é finitamente gerado sem precisar explicitar seus geradores.

Como um grupo abeliano livre finitamente gerado, a menos de isomorfismo, tem a forma $\mathbb{Z}^n$, então a norma em $\mathbb{Z}^n$ induzida por $\mathbb{R}^n$ induz, via isomorfismo, uma norma no grupo abeliano. Isso nos motiva a seguinte definição:

Definição 5.1. Uma *norma* em um grupo abeliano A é uma função $\| \ \| : A \to [0, +\infty)$, tal que:

(i) Para cada número real r o conjunto $\{P \in A; \|P\| \leq r\}$ é finito.

(ii) $\|mP\| = |m|\|P\|$ para todo $P \in A$ e número inteiro m.

(iii) $\|P + Q\| \leq \|P\| + \|Q\|$ para todo $P, Q \in A$.

Observação 5.2. Como observamos inicialmente, um grupo abeliano livre finitamente gerado tem uma norma que é a induzida de $\mathbb{Z}^n$. Outra classe de grupos abelianos que

admite uma norma é a dos grupos abelianos finitos. Para grupos abelianos finitos a norma deve ser necessariamente a norma nula, pois pela propriedade (ii) temos que $\|\mathcal{O}\| = \|2\mathcal{O}\| = 2\|\mathcal{O}\|$, logo $\|\mathcal{O}\| = 0$, em que $\mathcal{O}$ é o elemento neutro do grupo. Para qualquer elemento P com ordem $n > 0$, temos que $0 = \|\mathcal{O}\| = \|nP\| = n\|P\|$ o que implica em $\|P\| = 0$. Além disso, a norma nula é de fato uma norma para grupos finitos, pois satisfaz incondicionalmente as propriedades (ii) e (iii) e pelo fato do grupo ser finito também satisfaz a propriedade (i).

Lema 5.3. *Sejam $A_1, \ldots, A_n$ grupos abelianos com normas $\| \ \|_1, \ldots, \| \ \|_n$, respectivamente. Se $A = A_1 \oplus \cdots \oplus A_n$, então A admite uma norma dada por*

$$\| (P_1, \ldots, P_n) \| = \|P_1\|_1 + \cdots + \|P_n\|_n.$$

Demonstração. De fato, $\| \ \| : A \to [0, +\infty)$ é uma função bem definida e as propriedades (ii) e (iii) seguem diretamente da definição de $\| \ \|$. Para mostrarmos a propriedade (i), suponhamos que $(P_1, \ldots, P_n) \in A$ com $\| (P_1, \ldots, P_n) \| \leq r$, então $\|P_i\|_i \leq r$ para todo $1 \leq i \leq n$. Como $\| \ \|_i$ são normas, existe apenas uma quantidade finita de possibilidades para a coordenada P_i. Portanto, temos uma quantidade finita de possibilidades para $(P_1, \ldots, P_n)$, ou seja, a quantidade de elementos em A com imagem por $\| \ \|$ menor ou igual a r é finita.

Podemos então concluir que $\| \ \|$ é uma norma em A. □

Proposição 5.4. *Se A é um grupo abeliano finitamente gerado, então A admite uma norma.*

Demonstração. Uma vez que o grupo A é abeliano finitamente gerado, podemos expressar A como uma soma direta de sua parte livre A_{free} e sua parte de torção A_{tor}, ou seja, $A = A_{free} \oplus A_{tor}$. Dado que A_{free} e A_{tor} são subgrupos de A, então eles também são abelianos finitamente gerados, além disso, A_{tor} é finito.

Como A_{free} é um grupo abeliano livre finitamente gerado, ele admite a norma induzida pelo $\mathbb{Z}^n$. Pela Observação 5.2, a norma nula é uma norma para A_{tor}. Portanto, pelo Lema 5.3, podemos concluir que $A = A_{free} \oplus A_{tor}$ admite uma norma. □

O exemplo a seguir mostra que a recíproca do Proposição 5.4 não é verdadeira.

Exemplo 5.5. Seja $A \subset \mathbb{Z}[x]$ o grupo aditivo gerado por $\{f_i = (i+1)\, x^i; i \in \mathbb{N}\}$. Se $f = \sum_{0 \leq i \leq m} a_i x^i \in \mathbb{Z}\,[x]$, definimos $\|f\|_\infty = \max\{|a_i|; 0 \leq i \leq m\}$.

Pode-se provar que $\| \ \|_\infty$ é uma norma em A. Mostraremos somente que $\| \ \|_\infty$ satisfaz a propriedade (i). Sejam r um número real e N o maior inteiro menor ou igual a $|r|$, consideremos o conjunto $C_r = \{f \in A; \|f\|_\infty \leq r\}$, para demonstrar a Propriedade (i) basta mostrarmos que C_r é finito. Observamos que se $f \in C_r$, então f não contém nenhum dos monômios f_i com $i > N$, ou seja, podemos escrever $f = \sum_{1 \leq i \leq N} a_i f_i$, com os a_i's inteiros em $[-N, N]$. Sendo assim, existem no máximo $(2N+1)^N$ possibilidades para o polinômio f. Como f foi tomado arbitrariamente em C_r, podemos concluir que C_r é um conjunto finito.

Entretanto, A não é finitamente gerado, pois A contém polinômios com graus arbitrariamente grande.

Proposição 5.6. *Seja A um grupo abeliano finitamente gerado, então o índice $(A : mA)$ é finito para todo inteiro $m > 1$.*

Demonstração. Como o grupo A é finitamente gerado, então ele admite um conjunto finito de geradores $\{g_1, \ldots, g_n\}$. Além disso, $mA = \{mg; g \in A\}$ é obviamente um subgrupo (normal) de A. Mostraremos que o conjunto finito $\mathcal{C} = \left\{\sum_{1 \leq i \leq n} r_i g_i;\ 0 \leq r_i < m\right\}$ contém ao menos um representante de cada uma das classes laterais de $A/(mA)$.

De fato, seja g um elemento qualquer do grupo aditivo A, como os elementos g_i's geram o grupo abeliano A, então podemos escrever $g = m_1 g_1 + \cdots + m_n g_n$. Para cada $1 \leq i \leq n$ existem números inteiros q_i e $0 \leq r_i < m$, tais que $m_i = q_i m + r_i$, logo $g = \sum_{1 \leq i \leq n} (q_i m + r_i) g_i$. Consequentemente,

$$g - \sum_{1 \leq i \leq n} r_i g_i \in mA;$$

uma vez que $\sum_{1 \leq i \leq n} r_i g_i \in \mathcal{C}$ e g é um elemento arbitrário de A, temos que $\mathcal{C}$ contém representantes de cada uma das classes laterais.

Como $\mathcal{C}$ é um conjunto finito, podemos concluir que existe um número finito de classes laterais de mA em A, isto é, o índice $(A : mA)$ é finito. □

O exemplo a seguir mostra que a recíproca da Proposição 5.6 também não é verdadeira.

Exemplo 5.7. Se $A = (\mathbb{Q}, +)$ é o grupo aditivo dos números racionais, então para todo número inteiro $m > 1$ temos que $(A : mA) = 1$; entretanto, o grupo aditivo dos números racionais não é finitamente gerado.

Evidenciamos nos últimos exemplos que a recíproca das Proposições 5.4 e 5.6 não é válida. Entretanto, se a tese das duas proposições forem simultaneamente satisfeitas, então o grupo é finitamente gerado.

Teorema 5.8. *Seja A um grupo abeliano aditivo munido de uma norma $\| \ \|$, tal que o índice $(A : mA)$ é finito para algum $m > 1$. Então, A é finitamente gerado.*

Demonstração. Como o subgrupo mA tem índice finito em A, então existe um subconjunto finito $\mathcal{C} = \{Q_1, \ldots, Q_n\} \subset A$ de representantes das classes laterais em $A/(mA)$.

Seja $P_0 \in A$. Mostraremos que existe um subconjunto finito $\mathcal{C}' \subset A$, que não depende de P_0, tal que P_0 pertence ao subgrupo gerado por $\mathcal{C} \cup \mathcal{C}'$. Neste caso, uma vez que $\mathcal{C}'$ não depende de P_0, poderemos concluir que o conjunto $\mathcal{C} \cup \mathcal{C}'$ gera todo o grupo A.

Se P_0 está no subgrupo gerado por $\mathcal{C}$, então não há o que mostrar.

Se P_0 não está no subgrupo gerado por $\mathcal{C}$, consideremos $Q_{i_0} \in \mathcal{C}$ um representante da classe do elemento P_0, ou seja, existe um elemento $P_1 \in A$, tal que $P_0 - Q_{i_0} = mP_1$. Como P_0 não é um elemento do subgrupo gerado por $\mathcal{C}$, então P_1 também não é, portanto, podemos repetir o processo sucessivamente

$$P_0 - Q_{i_0} = mP_1$$

$$P_1 - Q_{i_1} = mP_2$$

$$P_2 - Q_{i_2} = mP_3$$

$$\vdots$$

$$P_{j-1} - Q_{i_{j-1}} = mP_j,$$

$$\vdots$$

com $\{Q_{i_0}, Q_{i_1}, Q_{i_2}, \ldots\} \subset \mathcal{C}$ e $\{P_0, P_1, P_2, \ldots\} \subset A$ sequências que continuam indefinidamente.

Para cada $j \geq 1$, temos $mP_j = P_{j-1} - Q_{i_{j-1}}$; pela Propriedade (ii) da norma que estamos assumindo que A admite, temos que $\|mP_j\| = m\|P_j\|$ e, pela Propriedade (iii) temos $\|P_{j-1} - Q_{i_{j-1}}\| \leq \|P_{j-1}\| + \| - Q_{i_{j-1}}\|$. Como $\mathcal{C}$ é um conjunto finito, existe $M = \max\{\| - Q_i\| \ ; \ Q_i \in \mathcal{C}\}$. Portanto,

$$m\|P_j\| = \|mP_j\| = \|P_{j-1} - Q_{i_{j-1}}\| \leq \|P_{j-1}\| + \| - Q_{i_{j-1}}\| \leq \|P_{j-1}\| + M,$$

daí obtemos que

$$\|P_j\| \leq \frac{1}{m}\|P_{j-1}\| + \frac{M}{m}. \tag{5.1}$$

Vale notar que M depende somente de $\mathcal{C}$.

Ao usarmos a Desigualdade (5.1) repetidamente, começando de P_j até P_0, temos que

$$\begin{aligned}
\|P_j\| &\leq \frac{1}{m}\|P_{j-1}\| + \frac{1}{m}M \\
&\leq \frac{1}{m^2}\|P_{j-2}\| + \left(\frac{1}{m} + \frac{1}{m^2}\right) M \\
&\leq \frac{1}{m^3}\|P_{j-3}\| + \left(\frac{1}{m} + \frac{1}{m^2} + \frac{1}{m^3}\right) M \\
&\vdots \\
&\leq \frac{1}{m^j}\|P_0\| + \left(\frac{1}{m} + \frac{1}{m^2} + \frac{1}{m^3} + \cdots + \frac{1}{m^j}\right) M \\
&< \frac{1}{m^j}\|P_0\| + \frac{1}{m-1}M.
\end{aligned}$$

Tomando j' suficientemente grande, obtemos que $\|P_{j'}\| < 1 + \frac{1}{m-1}M$, ou seja, a sequência sempre contém algum ponto $P_{j'}$ contido no subconjunto

$$\mathcal{C}' = \left\{ Q \in A; \|Q\| < 1 + \frac{1}{m-1}M \right\},$$

que é finito pela propriedade (i) da norma.

Além disso, pelo fato de

$$\begin{aligned}
P_0 &= Q_{i_0} + mP_1 \\
&= Q_{i_0} + mQ_{i_1} + m^2P_2 \\
&= Q_{i_0} + mQ_{i_1} + m^2Q_{i_2} + m^3P_3 \\
&\vdots \\
&= Q_{i_0} + mQ_{i_1} + m^2Q_{i_2} + m^3Q_{i_3} + \cdots + m^{j'-1}Q_{i_{j'-1}} + m^{j'}P_{j'},
\end{aligned}$$

segue que P_0 está no subgrupo gerado por $\mathcal{C} \cup \mathcal{C}'$.

Como P_0 é um elemento arbitrário de A, podemos concluir que A é gerado por $\mathcal{C} \cup \mathcal{C}'$ e consequentemente é também finitamente gerado, como desejado. □

Os pontos chaves para demonstrarmos o Teorema 5.8 foram a Desigualdade (5.1) e a Propriedade (i) da norma, enquanto as Propriedades (ii) e (iii) foram necessárias somente para obter a Desigualdade (5.1). Observaremos no Teorema 5.9, que podemos admitir

uma maior flexibilidade nas Propriedades (ii) e (iii) de modo a continuar obtendo uma versão análoga à Desigualdade (5.1), o que também nos permitirá concluir que o grupo é finitamente gerado.

Teorema 5.9 (Teorema da descida)**.** *Sejam A um grupo abeliano aditivo e $m > 1$ um número inteiro, tais que o índice $(A : mA)$ é finito. Suponha que exista uma função $h : A \longrightarrow [0, +\infty)$, tal que:*

(i) Para todo número real c_1, o conjunto $\{P \in A : h(P) \leq c_1\}$ é finito.

(ii) Dado $Q \in A$, existe uma constante positiva c_Q, tal que

$$h(P+Q) \leq mh(P) + c_Q \qquad \text{para todo } P \in A.$$

(iii) Existe uma constante positiva $c_m > 0$, tal que

$$h(mP) \geq m^2 h(P) - c_m, \qquad \text{para todo } P \in A.$$

Então A é um grupo finitamente gerado.

Demonstração. Como mA tem índice finito em A, então existe um subconjunto finito $\mathcal{C} = \{Q_1, \ldots, Q_n\} \subset A$ de representantes das classes laterais em $A/(mA)$.

Seja $P_0 \in A$. Do mesmo modo que realizamos no Teorema 5.9, apresentaremos um subconjunto finito $\mathcal{C}' \in A$, que não depende de P_0, tal que P_0 pertence ao subgrupo gerado por $\mathcal{C} \cup \mathcal{C}'$.

Se P_0 está no subgrupo gerado por $\mathcal{C}$, nada há que fazer.

Se P_0 não está no subgrupo gerado por $\mathcal{C}$, consideremos $Q_{i_0} \in \mathcal{C}$ um representante da classe lateral de P_0, ou seja, existe um elemento $P_1 \in A$, tal que $P_0 - Q_{i_0} = mP_1$. Como P_0 não está no subgrupo gerado por $\mathcal{C}$, então P_1 também não está, portanto, podemos repetir o processo sucessivamente

$$P_0 - Q_{i_0} = mP_1$$

$$P_1 - Q_{i_1} = mP_2$$

$$P_2 - Q_{i_2} = mP_3$$

$$\vdots$$

$$P_{j-1} - Q_{i_{j-1}} = mP_j,$$

$$\vdots$$

com $\{Q_{i_0}, Q_{i_1}, Q_{i_2}, \dots\} \subset \mathcal{C}$ e $\{P_0, P_1, P_2, \dots\} \subset A$ sequências que continuam indefinidamente.

Seja $j > 0$. Mostraremos que podemos obter desigualdade análoga a (5.1), ou seja, que existe uma constante M positiva dependendo somente de $\mathcal{C}$, tal que

$$h(P_j) \leq \frac{1}{m} h(P_{j-1}) + \frac{M}{m}. \tag{5.2}$$

Pela Propriedade (ii), temos que $h\left(P_{j-1} - Q_{i_{j-1}}\right) \leq mh(P_{j-1}) + c_{-Q_{i_{j-1}}}$. Além disso, pela Propriedade (iii), temos que $m^2 h(P_j) - c_m \leq h(mP_j)$. Como $P_{j-1} - Q_{i_{j-1}} = mP_j$, então $h\left(P_{j-1} - Q_{i_{j-1}}\right) = h(mP_j)$, e portanto

$$h(P_j) \leq \frac{1}{m} h(P_{j-1}) + \frac{c_{-Q_{i_{j-1}}} + c_m}{m^2}.$$

Tomando $M = \max\left\{\frac{c_{-Q}+c_m}{m};\ Q \in \mathcal{C}\right\}$, obtemos a Desigualdade (5.2).

Ao usarmos a Desigualdade (5.2) repetidamente, começando de P_j até P_0, temos que

$$\begin{aligned}
h(P_j) &\leq \frac{1}{m} h(P_{j-1}) + \frac{1}{m} M \\
&\leq \frac{1}{m^2} h(P_{j-2}) + \left(\frac{1}{m} + \frac{1}{m^2}\right) M \\
&\leq \frac{1}{m^3} h(P_{j-3}) + \left(\frac{1}{m} + \frac{1}{m^2} + \frac{1}{m^3}\right) M \\
&\vdots \\
&\leq \frac{1}{m^j} h(P_0) + \left(\frac{1}{m} + \frac{1}{m^2} + \frac{1}{m^3} + \cdots + \frac{1}{m^j}\right) M \\
&< \frac{1}{m^j} h(P_0) + \frac{1}{m-1} M.
\end{aligned}$$

Tomando j' suficientemente grande, temos que $h(P_{j'}) \leq 1 + \frac{1}{m-1} M$, ou seja, a sequência sempre contém algum ponto $P_{j'}$ contido no subconjunto

$$\mathcal{C}' = \left\{Q \in A; h(Q) \leq 1 + \frac{1}{m-1} M\right\},$$

que é finito pela Propriedade (i).

Além disso, pelo fato de

$$\begin{aligned} P_0 &= Q_{i_0} + mP_1 \\ &= Q_{i_0} + mQ_{i_1} + m^2P_2 \\ &= Q_{i_0} + mQ_{i_1} + m^2Q_{i_2} + m^3P_3 \\ &\vdots \\ &= Q_{i_0} + mQ_{i_1} + m^2Q_{i_2} + m^3Q_{i_3} + \cdots + m^{j'-1}Q_{i_{j'-1}} + m^{j'}P_{j'}, \end{aligned}$$

segue que P_0 está no subgrupo gerado por $\mathcal{C} \cup \mathcal{C}'$.

Como P_0 é um elemento arbitrário de A, podemos concluir que A é um grupo finitamente gerado. □

Definição 5.10. Seja A um grupo abeliano aditivo. Uma função $h : A \to [0, +\infty)$ que satisfaz as condições listadas no Teorema 5.9 é chamada *altura* em A.

5.2 Altura em $E(\mathbb{Q})$

Na Seção 5.1, apresentamos alguns critérios que permitem concluir que um grupo abeliano é finitamente gerado, sem a necessidade de explicitar seus geradores. Nesta seção, mostraremos que o grupo $E(\mathbb{Q})$ dos pontos racionais de uma curva elíptica com coeficientes inteiros dada por

$$E : y^2 = f(x), \qquad \text{com } f(x) = x^3 + ax^2 + bx + c$$

satisfaz uma dessas propriedades. Faremos isso utilizando uma função altura para $E(\mathbb{Q})$.

Definição 5.11. Seja $t = p/q \in \mathbb{Q} \setminus \{0\}$, com p e q inteiros coprimos. Definimos a *altura* de t, denotada por $H(t)$, por

$$H(t) = \max(|p|, |q|).$$

A função H está definida em $\mathbb{Q}$, entretanto, podemos defini-la em $E(\mathbb{Q})$, por $H(P) = H(\mathbf{x}(P))$ se $P \neq \mathcal{O}$ e $H(\mathcal{O}) = 0$. Observamos que ao definir $H(P)$ consideramos somente a coordenada x do ponto P; o motivo para isso é que a altura da coordenada y pode ser limitada em função de $H(\mathbf{x}(P))$.

De fato, pelo Lema 4.5, um ponto $P \in E(\mathbb{Q})$ pode ser expresso na forma $P = \left(\frac{\phi}{\psi^2}, \frac{\omega}{\psi^3}\right)$, com $MDC(\phi\omega, \psi) = 1$, logo

$$|\phi| \leq H(P) \qquad \text{e} \qquad |\psi| \leq H(P)^{1/2}.$$

Ao substituirmos $\left(\frac{\phi}{\psi^2}, \frac{\omega}{\psi^3}\right)$ na equação que define E e eliminarmos os denominadores obtemos

$$\omega^2 = \phi^3 + a\phi^2\psi^2 + b\phi\psi^4 + c\psi^6,$$

portanto,

$$\begin{aligned} |\omega^2| &= |\phi^3 + a\phi^2\psi^2 + b\phi\psi^4 + c\psi^6| \\ &\leq |\phi^3| + |a\phi^2\psi^2| + |b\phi\psi^4| + |c\psi^6| \\ &\leq (1 + |a| + |b| + |c|) \cdot H(P)^3. \end{aligned}$$

Definindo $K = \sqrt{1 + |a| + |b| + |c|}$, podemos concluir que

$$|\omega| \leq K \cdot H(P)^{3/2}.$$

Por conta disso, consideramos somente a coordenada $\mathbf{x}(P)$.

Nosso objetivo é justificar o seguinte resultado:

Teorema 5.12. *A função $h : E(\mathbb{Q}) \to [0, +\infty)$, dada por*

$$h(P) = \begin{cases} \ln(H(P)) & , \text{ se } P \neq \mathcal{O} \\ 1 & , \text{ se } P = \mathcal{O}, \end{cases}$$

é uma altura em $E(\mathbb{Q})$.

Como no caso da função H, algumas vezes adotaremos $h(\mathbf{x}(P))$ para indicar $h(P)$.

As demonstrações de que a função h satisfaz as condições (i), (ii) e (iii) (correspondentes a $m = 2$) do Teorema 5.9, serão feitas nos Lemas 5.13, 5.14 e 5.16, respectivamente.

Lema 5.13. *Para todo número real c_1, o conjunto $\{P \in E(\mathbb{Q});\ h(P) \leq c_1\}$ é finito.*

Demonstração. Sejam $\mathcal{A}_{c_1} = \{P \in E(\mathbb{Q}) - \{\mathcal{O}\};\ h(P) \leq c_1\}$ e $P \in \mathcal{A}_{c_1}$. Como a função exponencial é uma função crescente, então $H(P) \leq e^{c_1}$, ou seja, o numerador e o denominador de $\mathbf{x}(P)$ são números inteiros pertencentes a $[-e^{c_1}, e^{c_1}]$, portanto, existe uma

quantidade finita de possibilidades para $\mathbf{x}(P)$. Como em $E(\mathbb{Q})$, existem no máximo dois pontos com uma mesma coordenada x, o conjunto $\mathcal{B}_{c_1} = \left\{ (x,y) \in E(\mathbb{Q}) \,;\, x \in [-e^{c_1}, e^{c_1}] \right\}$ é finito e contém o ponto P.

Pelo fato de $\mathcal{B}_{c_1}$ não depender de P, temos que $\mathcal{A}_{c_1} \subset \mathcal{B}_{c_1}$, portanto, $\mathcal{A}_{c_1}$ é um conjunto finito e consequentemente $\{P \in E(\mathbb{Q}) \,;\, h(P) \leq c_1\}$ também será. □

Lema 5.14. *Seja $P_0 = (x_0, y_0) \in E(\mathbb{Q})$. Existe constante $c_{P_0} > 0$, tal que*

$$h(P + P_0) \leq 2h(P) + c_{P_0}, \quad \textit{para todo } P \in E(\mathbb{Q}).$$

Demonstração. Observamos que o lema é trivial para $P_0 = \mathcal{O}$, portanto, vamos supor que $P_0 \neq \mathcal{O}$ e tem coordenadas afim (x_0, y_0). Além disso, dado que a demonstração envolve manipular a coordenada x de $P + P_0$, é conveniente supormos que $P \notin \{\mathcal{O}, -P_0, P_0\}$, pois, neste caso, $\mathbf{x}(P + P_0)$ é dada pela fórmula geral da operação apresentada na Proposição 3.12. Isso não é uma restrição, pois como o conjunto $\{\mathcal{O}, -P_0, P_0\}$ é finito, podemos garantir que o lema é válido quando P é um desses três pontos, se tomarmos $c_{P_0} \geq \max\{h(P_0), 1, h(2P_0)\}$.

Sejam $(x,y) = P \notin \{\mathcal{O}, -P_0, P_0\}$ e $(\xi, \eta) = P + P_0$. Uma vez que $P \neq \pm P_0$, temos $x \neq x_0$, consequentemente,

$$\begin{aligned}
\xi &= \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0 - a \\
&= \frac{f(x) - 2yy_0 + f(x_0) - (x + x_0 + a)(x - x_0)^2}{(x - x_0)^2} \\
&= \frac{-2y_0 y + x_0 x^2 + (x_0^2 + 2x_0 a + b)\, x + (x_0 b + 2c)}{x^2 - 2x_0 x + x_0^2},
\end{aligned}$$

ou seja, podemos escrever

$$\xi = \frac{A_1 y + A_2 x^2 + A_3 x + A_4}{A_5 x^2 + A_6 x + A_7} \tag{5.3}$$

com $A_1, A_2, \ldots, A_7$ números racionais que podem ser expressos em termos de a, b, c, x_0 e y_0. Além disso, ao multiplicarmos o numerador e denominador de ξ pelo mínimo múltiplo comum dos denominadores de $A_1, A_2, \ldots, A_7$, podemos supor que eles são números inteiros que independem de x e y, pois os $A_1, A_2, \ldots, A_7$ originais não dependem de x e y.

Pelo Lema 4.5, podemos escrever $x = \frac{\phi}{\psi^2}$ e $y = \frac{\omega}{\psi^3}$, com $MDC(\phi\omega, \psi) = 1$, ao substituirmos essas identidades em (5.3) e eliminarmos os denominadores do numerador

e denominador de ξ, obtemos

$$\xi = \frac{A_1\omega\psi + A_2\phi^2 + A_3\phi\psi^2 + A_4\psi^4}{A_5\phi^2 + A_6\phi\psi^2 + A_7\psi^4}, \tag{5.4}$$

ou seja, expressamos ξ como quociente de dois números inteiros. O numerador e o denominador, apresentados na Equação (5.4), poderiam ter um fator em comum, mas ao eliminarmos este possível fator o valor absoluto do numerador e denominador de ξ diminuiriam. Portanto,

$$H(\xi) \leq \max\{|A_1\omega\psi + A_2\phi^2 + A_3\phi\psi^2 + A_4\psi^4|, |A_5\phi^2 + A_6\phi\psi^2 + A_7\psi^4|\}.$$

Observamos no início da seção que

$$|\psi| \leq H(P)^{1/2}, \qquad |\omega| \leq K \cdot H(P)^{3/2} \qquad \text{e} \qquad |\phi| \leq H(P),$$

sendo K uma constante positiva dependendo somente de E, consequentemente

$$\begin{aligned} |A_1\omega\psi + A_2\phi^2 + A_3\phi\psi^2 + A_4\psi^4| &\leq |A_1\omega\psi| + |A_2\phi^2| + |A_3\phi\psi^2| + |A_4\psi^4| \\ &\leq (|A_1K| + |A_2| + |A_3| + |A_4|) \cdot H(P)^2 \end{aligned}$$

e

$$\begin{aligned} |A_5\phi^2 + A_6\phi\psi^2 + A_7\psi^4| &\leq |A_5\phi^2| + |A_6\phi\psi^2| + |A_7\psi^4| \\ &\leq (|A_5| + |A_6| + |A_7|) \cdot H(P)^2. \end{aligned}$$

Portanto,

$$H(P + P_0) = H(\xi) \leq \max\left\{ (|A_1K| + |A_2| + |A_3| + |A_4|), (|A_5| + |A_6| + |A_7|) \right\} \cdot H(P)^2. \tag{5.5}$$

Tomando o logaritmo em ambos os lados da Desigualdade (5.5), temos que

$$h(P + P_0) \leq 2h(P) + c_0,$$

com

$$c_0 = \ln\left(\max\left\{ (|A_1K| + |A_2| + |A_3| + |A_4|), (|A_5| + |A_6| + |A_7|) \right\}\right)$$

dependendo somente de E e P_0, consequentemente, se tomarmos $c_{P_0} \geq c_0$, então o lema é satisfeito para todo $P \notin \{\mathcal{O}, \pm P_0\}$.

Finalmente, pelo que observamos inicialmente, a constante

$$c_{P_0} = \max\{c_0, h(P_0), 1, h(2P_0)\}$$

satisfaz o lema para todo $P \in E(\mathbb{Q})$. □

Para provar que h satisfaz a condição (iii) listada no Teorema 5.9, iniciaremos de modo análogo ao Lema 5.14, até chegarmos ao ponto em que escreveremos a coordenada $\mathbf{x}(2P)$ como o quociente de duas expressões, que nesse caso, dependerão somente da coordenada x do ponto P. Dado que no caso anterior estávamos interessados em estabelecer uma cota superior para $H(P+P_0)$ em função de $H(P)$, pudemos contornar a possibilidade do numerador e denominador terem um fator em comum, pois se este fosse o caso, o valor de $H(P+P_0)$ seria ainda menor em relação à cota obtida. Isto não pode ser feito na demonstração da Propriedade (iii), pois aqui estamos interessados em estabelecer uma cota inferior para $H(2P)$. Entretanto, como escreveremos $\mathbf{x}(2P) = g_1(x)/g_2(x)$, com $g_1, g_2 \in \mathbb{Z}[x]$ sem fator em comum, podemos tratar o caso mais geral que envolve comparar $H(x)$ com a imagem de H no quociente de duas funções polinomiais avaliadas em x.

Lema 5.15. *Sejam g_1 e g_2 polinômios não monomiais de $\mathbb{Z}[x]$ sem fatores em comum e d o máximo dos seus graus. Então existe uma constante $B > 0$ que depende somente de g_1 e g_2, tal que para todo x_0 racional que não é raiz de g_2, temos*

$$\left| h\left(\frac{g_1(x_0)}{g_2(x_0)}\right) - d \cdot h(x_0) \right| \leq B.$$

Demonstração. Sejam x_0 um número racional que não é raiz de g_2, e $p, q \in \mathbb{Z}$, tais que $x_0 = \frac{p}{q}$ com $q > 0$ e $MDC(p,q) = 1$. Uma vez que d é o máximo dos graus de g_1 e g_2, então $G_1(X,Y) = Y^d g_1\left(\frac{X}{Y}\right)$ e $G_2(X,Y) = Y^d g_2\left(\frac{X}{Y}\right)$ são polinômios homogêneos com coeficientes inteiros de grau d e

$$\xi = \frac{g_1(x_0)}{g_2(x_0)} = \frac{G_1(p,q)}{G_2(p,q)},$$

portanto, $H(\xi) = H\left(\frac{G_1(p,q)}{G_2(p,q)}\right)$.

Para estabelecer uma cota superior, como no Lema 5.14, não precisamos nos preocupar se haverá fatores em comum entre os números inteiros $G_1(p,q)$ e $G_2(p,q)$. Definindo $C = (d+1) \cdot \max\{|\alpha|;\ \alpha \text{ é coeficiente de } G_1 \text{ ou } G_2\}$, temos que

$$H(\xi) \leq \max\left\{|G_1(p,q)|, |G_2(p,q)|\right\} \leq C \cdot \max\left\{|p|, |q|\right\}^d = C \cdot H(x_0)^d. \tag{5.6}$$

Como ln é uma função crescente, de (5.6), obtemos

$$h\left(\frac{g_1(x_0)}{g_2(x_0)}\right) = h(\xi) \leq d \cdot h(x_0) + \ln(C),$$

uma vez que d e C dependem somente de g_1 e g_2, está demonstrado uma das desigualdades do lema, considerando $B \geq \ln(C)$.

Para garantir a existência de $B > 0$, tal que $-B \leq h(\xi) - d \cdot h(x_0)$, precisamos determinar uma cota inferior de $H(\xi)$, portanto, precisamos ter um cuidado maior quanto a possibilidade dos números inteiros $G_1(p,q)$ e $G_2(p,q)$ terem um fator k em comum. Entretanto, a hipótese dos polinômios g_1 e g_2 não terem fatores em comum em $\mathbb{Z}[x]$ permitirá limitar o quão grande este fator k pode ser, o que será suficiente para estabelecermos a cota inferior.

Como g_1 e g_2 não são monômios, então eles não são constantes, portanto, podemos considerar a resultante $R_1 = Res(g_1, g_2) \in \mathbb{Z}$. Uma vez que g_1 e g_2 não têm fatores em comum, pelo Corolário 1.23, R_1 é não nulo. Segue do Teorema 1.24, que existem $a_1, b_1 \in \mathbb{Z}[x]$ de graus menor que d, tais que

$$a_1 g_1 + b_1 g_2 = R_1. \tag{5.7}$$

Consideremos $A_1(X,Y) = Y^{d-1} a_1\left(\frac{X}{Y}\right)$ e $B_1(X,Y) = Y^{d-1} b_1\left(\frac{X}{Y}\right)$. Avaliando a Equação (5.7) em $\frac{X}{Y}$ e multiplicando a equação obtida por Y^{2d-1}, obtemos

$$A_1(X,Y)\, G_1(X,Y) + B_1(X,Y)\, G_2(X,Y) = R_1 Y^{2d-1}. \tag{5.8}$$

Além disso, como os graus de a_1 e b_1 são menores que d, então $A_1(X,Y)$ e $B_1(X,Y)$ são polinômios com coeficientes inteiros e homogêneos de grau $d-1$.

Observamos que os fatores irredutíveis de G_1 ou G_2 são: o polinômio Y ou as homogeneizações dos fatores irredutíveis de g_1 ou g_2. Pela hipótese de g_1 e g_2 serem coprimos, então o polinômio Y é o único candidato a ser fator comum entre G_1 e G_2. Entretanto, como $d = \max\{\delta(g_1), \delta(g_2)\}$ e $G_1 = g_1\left(\frac{X}{Y}\right) Y^d$ e $G_2 = g_2\left(\frac{X}{Y}\right) Y^d$, então Y não é um fator comum de G_1 e G_2, ou seja, G_1 e G_2 não têm fator em comum.

Consideremos $\widetilde{g_1}, \widetilde{g_2} \in \mathbb{Z}[y]$ as desomogeneizações, em relação a variável X, de G_1 e G_2, respectivamente. Pelo fato de g_1 e g_2 não serem monômios, temos que $\widetilde{g_1}$ e $\widetilde{g_2}$ não são constantes, portanto, podemos considerar a resultante $R_2 = Res(\widetilde{g_1}, \widetilde{g_2}) \in \mathbb{Z}$. Pelo fato de G_1 e G_2 não terem fatores em comum, então $\widetilde{g_1}$ e $\widetilde{g_2}$ não têm fatores em comum, portanto, $R_2 \neq 0$. Por argumento análogo ao que fizemos com R_1, existem polinômios homogêneos $A_2, B_2 \in \mathbb{Z}[X,Y]$ de grau $d-1$, tais que

$$A_2(X,Y)\, G_1(X,Y) + B_2(X,Y)\, G_2(X,Y) = R_2 X^{2d-1}. \tag{5.9}$$

Avaliando as igualdades (5.8) e (5.9) no ponto $[p:q] \in \mathbb{P}^1$, obtemos

$$\begin{aligned} A_1(p,q)\,G_1(p,q) + B_1(p,q)\,G_2(p,q) &= R_1 q^{2d-1}, \\ A_2(p,q)\,G_1(p,q) + B_2(p,q)\,G_2(p,q) &= R_2 p^{2d-1}. \end{aligned} \tag{5.10}$$

Das Equações (5.10), temos que $MDC\left(G_1(p,q), G_2(p,q)\right)$ divide $MDC\left(R_1 q^{2d-1}, R_2 p^{2d-1}\right)$. Como p e q são inteiros coprimos, então qualquer potência de um número primo que divide $MDC\left(R_1 q^{2d-1}, R_2 p^{2d-1}\right)$ divide R_1 ou R_2, portanto,

$$MDC\left(|G_1(p,q)|, |G_2(p,q)|\right) \quad \text{divide} \quad R_1 R_2. \tag{5.11}$$

Observamos que a Equação (5.11) permite limitar os possíveis cancelamentos de fatores que podem ocorrer em $\frac{G_1(p,q)}{G_2(p,q)}$.

Como os polinômios A_i's e B_i's têm graus $d-1$, por argumento análogo ao feito na demonstração da desigualdade (5.6), existe constante $C' > 0$, tal que

$$\max\{|A_1(p,q)|, |B_1(p,q)|, |A_2(p,q)|, |B_2(p,q)|\} \leq C' \cdot \max\{|p|,|q|\}^{d-1},$$

consequentemente, as Equações (5.10) permitem concluir que

$$2C' \cdot \max\{|p|,|q|\}^{d-1} \cdot \max\{|G_1(p,q)|, |G_2(p,q)|\} \geq \max\{|R_1||q|^{2d-1}, |R_2||p|^{2d-1}\},$$

com a Equação (5.11), obtemos

$$\begin{aligned} H(\xi) &= \frac{\max\{|G_1(p,q)|, |G_2(p,q)|\}}{MDC\left(|G_1(p,q)|, |G_2(p,q)|\right)} \\ &\geq \frac{1}{|R_1 R_2|} \max\{|G_1(p,q)|, |G_2(p,q)|\} \\ &\geq \frac{\max\{|R_1||q|^{2d-1}, |R_2||p|^{2d-1}\}}{2C' \cdot \max\{|p|,|q|\}^{d-1} \cdot |R_1 R_2|} \\ &\geq \frac{\max\{|q|^{2d-1}, |p|^{2d-1}\}}{2C' \cdot |R_1 R_2| \cdot \max\{|p|,|q|\}^{d-1}} \\ &\geq \frac{1}{2C' \cdot |R_1 R_2|} H(x_0)^d. \end{aligned}$$

Avaliando a função ln, obtemos

$$h(\xi) \geq d \cdot h(x_0) - \ln\left(2C' \cdot |R_1 R_2|\right).$$

Podemos então concluir que a constante $B = \max\{\ln(C), \ln\left(2C' \cdot |R_1 R_2|\right)\}$ satisfaz o lema, pois d, C, C', R_1 e R_2 dependem somente de g_1 e g_2. □

O lema anterior, permite concluir a propriedade (iii) do Teorema 5.9, que se traduz no seguinte resultado.

Lema 5.16. *Existe uma constante $c_2 > 0$, tal que*

$$h(2P) \geq 4h(P) - c_2, \text{ para todo } P \in E(\mathbb{Q}).$$

Demonstração. Seja $P \in E(\mathbb{Q})$. Nosso objetivo é estabelecer uma cota inferior para $h(2P)$ em termos de $h(P)$. Inicialmente, excluiremos os casos em que não podemos usar a fórmula de duplicação apresentada na Proposição 3.12, ou seja, consideraremos somente $P \in E(\mathbb{Q})$, tais que $2P \neq \mathcal{O}$, isto é, para os quais $h(2P) = 1$. Como o conjunto de pontos que estamos desconsiderando é finito, podemos garantir que o lema é satisfeito para estes pontos ao tomarmos $c_2 \geq \max\{4h(P);\ 2P = \mathcal{O}\}$.

Sejam $(x_0, y_0) = P \in E(\mathbb{Q})$, tal que $2P \neq \mathcal{O}$ e $(\xi, \eta) = 2P$. Dado que P é não nulo e não tem ordem dois, pelas fórmulas apresentadas na Proposição 3.12, temos que

$$\xi = \left(\frac{f'(x_0)}{2y_0}\right)^2 - 2x_0 - a = \frac{f'(x_0)^2 - 4(2x_0 + a) f(x_0)}{4f(x_0)},$$

ou seja, podemos escrever $\xi = \frac{g_1(x_0)}{g_2(x_0)}$, com $g_1, g_2 \in \mathbb{Z}[x]$ dados por $g_1 = f'(x)^2 - 4(2x + a) f(x)$ e $g_2 = 4f(x)$. Além disso, pela regularidade de E, temos que $\Delta(E) = -Res(f, f') \neq 0$, ou seja, f e f' não têm fator comum, portanto, g_1 e g_2 não têm fator comum. Sendo assim, os polinômios g_1 e g_2 satisfazem a hipótese do Lema 5.15 com $d = 4$, ou seja, existe uma constante $B > 0$, tal que

$$h\left(\frac{g_1(x)}{g_2(x)}\right) \geq 4h(x) - B,$$

para todo $x \in \mathbb{Q}$, tal que $f(x) \neq 0$, em particular $h(\xi) \geq 4h(x_0) - B$. Como P foi tomado arbitrariamente e a constante B não depende de P, se tomarmos $c_2 \geq B$, temos que o lema é satisfeito para todo elemento em $\{P \in E(\mathbb{Q}); 2P \neq \mathcal{O}\}$.

Podemos então concluir que a constante

$$c_2 = \max\left\{B, \max\{4h(P); 2P = \mathcal{O}\}\right\}$$

satisfaz o lema para todo $P \in E(\mathbb{Q})$. □

5.3 O Índice $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ é Finito

O último passo para provar o Teorema de Mordell é mostrar que o índice $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ é finito. Para isso, lembramos que, se G_1 e G_2 são grupos e $\rho : G_1 \to G_2$ é um homomor-

fismo, então $G_1/\ker\rho \cong \operatorname{Im}\rho$.

Se G_2 é abeliano e finitamente gerado, então todos seus subgrupos também são finitamente gerados, em particular, a imagem de ρ é um subgrupo finitamente gerado. Sendo assim, para mostrarmos que $E(\mathbb{Q})/2E(\mathbb{Q})$ é finitamente gerado, basta encontrarmos um grupo abeliano finitamente gerado G e um homomorfismo $\rho : E(\mathbb{Q}) \to G$, tais que $\ker\rho = 2E(\mathbb{Q})$.

Começamos analisando as curvas elípticas $E : y^2 = f(x)$ que têm pelo menos um ponto de ordem dois, ou seja, o polinômio f se decompõe como $(x-\alpha)\,g(x)$ em $\mathbb{Z}[x]$. Como a curva elíptica E é regular, então todas as raízes de f têm multiplicidade um, portanto, para cada $P_0 = (x_0, y_0) \in E(\mathbb{Q})$ temos que $(x_0 - \alpha) \neq 0$ ou $g(x_0) \neq 0$. Além disso, se $(x_0 - \alpha)$ e $g(x_0)$ são não nulos então eles representam a mesma classe em $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Consideremos a função $\rho_\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$, definida por $\rho_\alpha(\mathcal{O}) \equiv 1$ e se $(x,y) \in E(\mathbb{Q}) - \{\mathcal{O}\}$, então

$$\rho_\alpha(x,y) \equiv \begin{cases} (x-\alpha) & , \ se\ x \neq \alpha \\ g(\alpha) = f'(\alpha) & , \ se\ x = \alpha. \end{cases}$$

Mostraremos que ρ_α tem imagem finita e é um homomorfismo de grupos. Para tanto, lembremos do seguinte resultado:

Lema 5.17. *Sejam A e B números inteiros não nulos, tais que $AB \in \mathbb{Q}^{*2}$. Se B é livre de quadrados, então B divide A.*

Demonstração. Uma vez que B é livre de quadrados e $AB \in \mathbb{Q}^{*2}$, todo número primo que divide B também divide A. Pelo fato de B ser livre de quadrados e seus divisores primos dividirem A, podemos concluir que B divide A. □

O discriminante $\Delta(E)$ dado na Definição 3.9, nos auxilia na descrição de $\operatorname{Im}\rho_\alpha$, como mostra o resultado a seguir.

Proposição 5.18. *A imagem de ρ_α está contida no conjunto das classes dos divisores inteiros de $\Delta(E)$ em $\mathbb{Q}^*/\mathbb{Q}^{*2}$.*

Demonstração. A imagem de $\mathcal{O}$ está no conjunto das classes dos divisores de $\Delta(E)$, pois 1 divide $\Delta(E)$ e $\rho_\alpha(\mathcal{O}) \equiv 1$. Seja $P = (x_0, y_0) \in E(\mathbb{Q})$ um ponto não nulo. Pelo Lema 4.5, existem números inteiros ϕ, ω e ψ, tais que $P = \left(\frac{\phi}{\psi^2}, \frac{\omega}{\psi^3}\right)$ com $MDC(\phi\omega, \psi) = 1$.

Seja $g(x) = x^2 + Ax + B$. Como ψ é um inteiro não nulo, então

$$\left(\phi - \alpha\psi^2\right) = (x_0 - \alpha)\,\psi^2 \equiv (x_0 - \alpha)$$

e

$$\left(\phi^2 + A\phi\psi^2 + B\psi^4\right) = g(x_0)\,\psi^4 \equiv g(x_0).$$

Consideremos D o inteiro livre de quadrados, tal que $\rho_\alpha(P) \equiv D$. Pela definição da função ρ_α, temos que os números inteiros $(\phi - \alpha\psi^2)$ e $(\phi^2 + A\phi\psi^2 + B\psi^4)$ estão na classe $D\mathbb{Q}^{*2}$ ou são nulos (não simultaneamente). Pelo Lema 5.17, podemos concluir que $(\phi - \alpha\psi^2)$ e $(\phi^2 + A\phi\psi^2 + B\psi^4)$ são divisíveis por D.

Pelo Teorema 1.24, existem $h_1, h_2 \in \mathbb{Z}[x]$, tais que $\delta(h_1) < 2$, $\delta(h_2) < 3$ e

$$h_1 f + h_2 f' = \Delta(E). \tag{5.12}$$

Avaliando a Igualdade (5.12) em $\frac{\phi}{\psi^2}$ e eliminando os denominadores, temos que

$$\Delta(E)\,\psi^8 = h_1^*\left(\phi, \psi^2\right) \cdot f^*\left(\phi, \psi^2\right) + h_2^*\left(\phi, \psi^2\right) \cdot f'^*\left(\phi, \psi^2\right), \tag{5.13}$$

com f^* denotando a homogeneização do polinômio f. Uma vez que $(\phi^2 + A\phi\psi^2 + B\psi^4)$ e $(\phi - \alpha\psi^2)$ são divisíveis por D e

$$f'^*\left(\phi, \psi^2\right) = \left(\phi^2 + A\phi\psi^2 + B\psi^4\right) + \left(\phi - \alpha\psi^2\right) \cdot g^*\left(\phi, \psi^2\right),$$

então $f'^*(\phi, \psi^2)$ é divisível por D. Além disso, como

$$f^*\left(\phi, \psi^2\right) = \left(\phi - \alpha\psi^2\right)\left(\phi^2 + A\phi\psi^2 + B\psi^4\right),$$

então $f^*(\phi, \psi^2)$ é divisível por D. Logo, pela Equação (5.13), D divide $\Delta(E)\,\psi^8$.

Como $(\phi - \alpha\psi^2)$ ou $(\phi^2 + A\phi\psi^2 + B\psi^4)$ é não nulo e divisível por D e $MDC(\phi, \psi) = 1$, então $MDC(D, \psi) = 1$, portanto, podemos concluir que D divide $\Delta(E)$, ou seja, $\rho_\alpha(P)$ é representado em $\mathbb{Q}/\mathbb{Q}^{*2}$ por algum divisor de $\Delta(E)$. □

O conjunto dos divisores de $\Delta(E)$ é determinado pelos divisores primos de $\Delta(E)$ e -1. Denotaremos por $\mathbb{Q}(S, 2)$ o subgrupo de $\mathbb{Q}^*/\mathbb{Q}^{*2}$, gerado pelo conjunto

$$S = \{\text{divisores primos de } \Delta(E)\} \cup \{-1\}.$$

Mostremos agora que ρ_α é na verdade um homomorfismo de grupos.

Proposição 5.19. *A função ρ_α é homomorfismo de grupos.*

Demonstração. Seja $P \in E(\mathbb{Q})$. Se $P = \mathcal{O}$, temos que $\rho_\alpha(-\mathcal{O}) \equiv 1 \equiv \rho_\alpha(\mathcal{O})^{-1}$. Se $P \neq \mathcal{O}$, como $\mathbf{x}(P) = \mathbf{x}(-P)$ e, em pontos não nulos, ρ_α é definida por uma função polinomial da coordenada x do ponto, então $\rho_\alpha(-P) \equiv \rho_\alpha(P) \equiv \rho_\alpha(P)^{-1}$. Portanto, $\rho_\alpha(-P) = \rho_\alpha(P)^{-1}$ para todo $P \in E(\mathbb{Q})$.

Sejam $P_1, P_2 \in E(\mathbb{Q})$. Se um desses dois pontos é o elemento neutro ou $P_1 = -P_2$, segue que $\rho_\alpha(P_1 + P_2) = \rho_\alpha(P_1) \cdot \rho_\alpha(P_2)$.

Se $P_1, P_2 \neq \mathcal{O}$ e $P_1 \neq -P_2$, temos que

$$\begin{aligned}\rho_\alpha(P_1 + P_2) \equiv \rho_\alpha(P_1) \cdot \rho_\alpha(P_2) &\iff \rho_\alpha(P_1) \cdot \rho_\alpha(P_2) \cdot \rho_\alpha(P_1 + P_2) \equiv 1 \\ &\iff \rho_\alpha(P_1) \cdot \rho_\alpha(P_2) \cdot \rho_\alpha(-(P_1 + P_2)) \equiv 1 \\ &\iff \rho_\alpha(P_1) \cdot \rho_\alpha(P_2) \cdot \rho_\alpha(P_1 * P_2) \equiv 1,\end{aligned}$$

em que a última equivalência segue do Corolário 3.11. Logo, para mostrarmos que ρ_α é homomorfismo, basta mostrarmos que

$$\rho_\alpha(P_1) \cdot \rho_\alpha(P_2) \cdot \rho_\alpha(P_1 * P_2) \equiv 1.$$

Como $P_1, P_2 \neq \mathcal{O}$ e $P_1 \neq -P_2$, então a reta passando pelo pontos P_1 e P_2 não contém $\mathcal{O}$, ou seja, não é uma reta vertical, portanto, existem números racionais λ e ν, tais que a reta L passando por P_1, P_2 e $P_3 = P_1 * P_2$ tem equação dada por $y = \lambda x + \nu$.

Sejam x_1, x_2 e x_3 as coordenadas dos pontos P_1, P_2 e P_3, respectivamente.

Se x_1, x_2 ou x_3 é igual a α, podemos supor sem perda de generalidade que $x_1 = \alpha$, então $P_1 = (\alpha, 0)$ e $P_2, P_3 \neq P_1$, pois caso contrário teríamos que a reta $\overline{P_1P_2}$ seria vertical. Assim, temos

$$\rho_\alpha(P_1) \cdot \rho_\alpha(P_2) \cdot \rho_\alpha(P_3) \equiv f'(\alpha)(x_2 - \alpha)(x_3 - \alpha). \tag{5.14}$$

Substituindo a equação da reta L na equação da curva elíptica, obtemos o polinômio cujas raízes determinam as abcissas de P_1, P_2 e P_3. Assim, temos que

$$f(x) - (\lambda x + \nu)^2 = (x - \alpha)(x - x_2)(x - x_3). \tag{5.15}$$

Como $(x - \alpha)$ divide o lado direito da Equação (5.15) e também divide $f(x)$, então $(x - \alpha)$ divide $(\lambda x + \nu)^2$, portanto, $(\lambda x + \nu)^2 = \lambda^2 (x - \alpha)^2$. Substituindo a última igualdade na Equação (5.15) e eliminando o fator $(x - \alpha)$, obtemos que $g(x) - \lambda^2 (x - \alpha) =$

$(x-x_2)(x-x_3)$, ao avaliarmos em $x=\alpha$, temos que

$$f'(\alpha) = g(\alpha) = (\alpha - x_2)(\alpha - x_3). \tag{5.16}$$

Pelas igualdades (5.14) e (5.16), temos

$$\rho_\alpha(P_1) \cdot \rho_\alpha(P_2) \cdot \rho_\alpha(P_3) \equiv f'(\alpha)(x_2-\alpha)(x_3-\alpha) \equiv 1,$$

o que nos permite concluir que $\rho_\alpha(P_1+P_2) = \rho_\alpha(P_1)\cdot\rho_\alpha(P_2)$, se x_1, x_2 ou x_3 é igual α.

Se x_1, x_2 e x_3 são diferentes de α, então

$$\rho_\alpha(P_1) \cdot \rho_\alpha(P_2) \cdot \rho_\alpha(P_3) \equiv (x_1-\alpha)(x_2-\alpha)(x_3-\alpha). \tag{5.17}$$

Substituindo a equação da reta L na equação da curva elíptica, temos que $f(x) - (\lambda x+\nu)^2 = (x-x_1)(x-x_2)(x-x_3)$, ao avaliarmos em $x=\alpha$, temos que

$$-(\lambda\alpha+\nu)^2 = (\alpha-x_1)(\alpha-x_2)(\alpha-x_3). \tag{5.18}$$

Pelas igualdades (5.17) e (5.18), temos

$$\rho_\alpha(P_1) \cdot \rho_\alpha(P_2) \cdot \rho_\alpha(P_3) \equiv (x_1-\alpha)(x_2-\alpha)(x_3-\alpha) \equiv 1.$$

Portanto, $\rho_\alpha(P_1+P_2) = \rho_\alpha(P_1)\cdot\rho_\alpha(P_2)$, se x_1, x_2 e x_3 são diferentes de α. □

Agora passemos a descrever o núcleo de ρ_α.

Corolário 5.20. *Temos que* $2E(\mathbb{Q}) \subset \ker\rho_\alpha$.

Demonstração. Segue diretamente do fato de ρ_α ser homomorfismo de grupos e os elementos da sua imagem terem ordem dois. □

Os últimos resultados apresentados mostram que $\rho_\alpha : E(\mathbb{Q}) \to \mathbb{Q}(S,2)$ é um homomorfismo de grupos com $\mathbb{Q}(S,2)$ abeliano e finitamente gerado. Também mostramos que $2E(\mathbb{Q}) \subset \ker\rho_\alpha$, entretanto, o exemplo abaixo mostra que a inclusão contrária nem sempre é válida.

Exemplo 5.21. Consideremos a curva elíptica $E: y^2 = x^3+x$, $\alpha = 0$ e $P=(0,0)$. Como $\Delta(E) = -4$, ao aplicarmos o Teorema de Nagell-Lutz, concluímos que P é o único ponto de torção, além de $\mathcal{O} = [0:1:0]$. Portanto, $E_{tor}(\mathbb{Q}) = \{\mathcal{O}, P\}$, e consequentemente, $P \notin 2E(\mathbb{Q})$.

Entretanto, $\rho_\alpha(P) = 1$, ou seja, $P \in \ker\rho_\alpha$.

O Exemplo 5.21 mostra que o homomorfismo ρ_α, em geral, não captura toda a estrutura de $E(\mathbb{Q})/2E(\mathbb{Q})$.

Denotaremos por $E[2]$ o subgrupo gerado pelos elementos de ordem dois em $E(\mathbb{C})$.

Se $E[2] \subset E(\mathbb{Q})$, então f se fatora totalmente em $\mathbb{Z}[x]$, ou seja, existem $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$, tais que

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3).$$

Consideremos[1] $\rho : E(\mathbb{Q}) \to \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ definida por

$$\rho(P) = (\rho_{\alpha_1}(P), \rho_{\alpha_2}(P)). \tag{5.19}$$

Dado que ρ_{α_1} e ρ_{α_2} são homomorfismos com imagens finitas e seus núcleos contêm $2E(\mathbb{Q})$, então ρ é um homomorfismo de imagem finita e $2E(\mathbb{Q}) \subset \ker\rho$.

Lema 5.22. *Sejam* $P = (x_0, y_0) \in E(\mathbb{Q})$ *e* $\mathbb{L} = \mathbb{Q}(\sqrt{x_0-\alpha_1}, \sqrt{x_0-\alpha_2}, \sqrt{x_0-\alpha_3})$. *Então existe* $Q \in E(\mathbb{L})$, *tal que* $2Q = P$.

Demonstração. Sem perda de generalidade, podemos supor que $x_0 - \alpha_1 \neq 0$. Podemos ainda supor que $\alpha_1 = 0$, pois caso contrário, basta realizarmos a mudança de coordenada $x' = x - \alpha_1$. Com essas convenções feitas, temos que $x_0 \neq 0$,

$$\mathbb{L} = \mathbb{Q}\left(\sqrt{x_0}, \sqrt{x_0-\alpha_2}, \sqrt{x_0-\alpha_3}\right) \qquad \text{e} \qquad f = x(x-\alpha_2)(x-\alpha_3) = x^3 + ax^2 + bx.$$

Observamos que $P = 2Q = -(Q*Q)$ se, e somente se, $Q*Q = -P$, portanto, basta mostrarmos que existe $Q \in E(\mathbb{L})$, tal que $Q*Q = -P = (x_0, -y_0)$. Consideremos $L_u : y = ux - (y_0 + ux_0)$ o feixe de retas complexas passando por $-P$. Uma vez que $y_0^2 = f(x_0)$, então a equação de interseção entre a curva elíptica E e a reta L_u pode ser expressa por

$$\begin{aligned}\psi_u(x) &= f(x) - (ux - y_0 - ux_0)^2 \\ &= (x-x_0)\left[x^2 + \left(a - u^2 + x_0\right)x + \left(b + 2uy_0 + x_0a + x_0^2 + u^2x_0\right)\right].\end{aligned} \tag{5.20}$$

Existe $Q \in E(\mathbb{L})$, tal que $Q*Q = -P$ se, e somente se, existe $u \in \mathbb{L}$, tal que o fator quadrático da Equação (5.20) é o quadrado de um fator linear em $\mathbb{L}[x]$, ou seja,

$$\left(a - u^2 + x_0\right)^2 - 4\left(b + 2uy_0 + x_0a + x_0^2 + u^2x_0\right) = 0, \tag{5.21}$$

[1] Observamos que $\rho_{\alpha_1}(P)\rho_{\alpha_2}(P)\rho_{\alpha_3}(P) \equiv 1$, portanto, podemos escrever $\rho_{\alpha_3}(P)$ em função de $\rho_{\alpha_1}(P)$ e $\rho_{\alpha_2}(P)$.

além disso, o correspondente ponto $Q_u \in E(\mathbb{L})$, tal que $Q_u * Q_u = -P$, tem a coordenada x dada por $-\frac{a-u^2+x_0}{2}$ e a coordenada y pode ser obtida da equação definindo L_u. Portanto, basta mostrarmos que existe $u \in \mathbb{L}$ satisfazendo a Equação (5.21).

A Equação (5.21) é satisfeita se, e somente se,

$$\begin{aligned}\left(a-u^2+x_0\right)^2 &= 4\left(b+2uy_0+x_0a+x_0^2+u^2x_0\right)\\ &= \frac{4}{x_0}\left(f(x_0)+2uy_0x_0+u^2x_0^2\right)\\ &= \frac{4}{x_0}\left(y_0+ux_0\right)^2. \end{aligned} \tag{5.22}$$

Por sua vez, a Equação (5.22) é satisfeita se, e somente se, a equação $a-u^2+x_0 = \zeta_1\frac{2}{\sqrt{x_0}}(y_0+ux_0)$ é satisfeita, com ζ_1 podendo assumir os valores ± 1. Além disso, podemos reescrever essa equação como

$$u^2+2\zeta_1\sqrt{x_0}u-\left(a+x_0-2\zeta_1\frac{y_0}{\sqrt{x_0}}\right)=0. \tag{5.23}$$

Da equação que define E, observamos que

$$a=-(\alpha_2+\alpha_3) \qquad \text{e} \qquad \frac{y_0}{\sqrt{x_0}} = \eta_0\sqrt{x_0-\alpha_2}\sqrt{x_0-\alpha_3},$$

com η_0 sendo uma constante que depende somente do ponto P e vale -1 ou 1. A Equação (5.23) é satisfeita se, e somente se,

$$\begin{aligned} u &= \frac{-2\zeta_1\sqrt{x_0}+\zeta_2\sqrt{4x_0+4\left(a+x_0-2\zeta_1\frac{y_0}{\sqrt{x_0}}\right)}}{2}\\ &= -\zeta_1\sqrt{x_0}+\zeta_2\sqrt{2x_0-(\alpha_2+\alpha_3)-2\zeta_1\eta_0\sqrt{x_0-\alpha_2}\sqrt{x_0-\alpha_3}}\\ &= -\zeta_1\sqrt{x_0}+\zeta_2\sqrt{\left(\sqrt{x_0-\alpha_2}-\zeta_1\eta_0\sqrt{x_0-\alpha_3}\right)^2}\\ &= -\zeta_1\sqrt{x_0}+\zeta_2\left(\sqrt{x_0-\alpha_2}-\zeta_1\eta_0\sqrt{x_0-\alpha_3}\right), \end{aligned} \tag{5.24}$$

com ζ_2 podendo assumir os valores ± 1. Como as Equações (5.24) e (5.21) são equivalentes, temos que a Equação (5.21) é satisfeita para

$$u=-\zeta_1\sqrt{x_0}+\zeta_2\left(\sqrt{x_0-\alpha_2}-\zeta_1\eta_0\sqrt{x_0-\alpha_3}\right)\in\mathbb{L},$$

o que nos permite concluir que existe um ponto $Q \in E(\mathbb{L})$, tal que $2Q = P$. □

Com a hipótese que estamos considerando, ou seja, que $E[2] \subset E(\mathbb{Q})$, temos a proposição a seguir.

Proposição 5.23. *Considerando o homomorfismo ρ definido anteriormente, temos que* $\ker \rho \subset 2E(\mathbb{Q})$.

Demonstração. Seja $P = (x_0, y_0) \in E(\mathbb{Q})$, tal que $\rho(P) = (1,1)$. Mostraremos que $P \in 2E(\mathbb{Q})$, ou seja, que existe $Q \in E(\mathbb{Q})$, tal que $P = 2Q$.

Dado que $\rho(P) = (1,1)$, então $x_0 - \alpha_1$, $x_0 - \alpha_2$ e $x_0 - \alpha_3$ são quadrados em $\mathbb{Q}$, logo $\mathbb{Q}(\sqrt{x_0 - \alpha_1}, \sqrt{x_0 - \alpha_2}, \sqrt{x_0 - \alpha_3}) = \mathbb{Q}$. Pelo Lema 5.22, existe $Q \in E(\mathbb{Q})$, tal que $2Q = P$, portanto, o ponto P pertence a $2E(\mathbb{Q})$.

Como P foi tomado arbitrariamente em $\ker \rho$, podemos concluir que $\ker \rho \subset 2E(\mathbb{Q})$. □

Considerando os resultados apresentados, estamos em posição de apresentar o principal resultado deste trabalho.

Teorema 5.24 (Teorema de Mordell)**.** *Caso $E[2] \subset E(\mathbb{Q})$:*

O grupo dos pontos racionais de uma curva elíptica E é finitamente gerado.

Demonstração. Na Seção 5.2, apresentamos uma função altura para $E(\mathbb{Q})$ (veja Teorema 5.12).

Pelo Corolário 5.20 e Proposição 5.23, temos que $\ker \rho = 2E(\mathbb{Q})$. Pela Proposição 5.18 as imagens das ρ_{α_i}'s são finitas, logo $\operatorname{Im}\rho = \operatorname{Im}\rho_{\alpha_1} \times \operatorname{Im}\rho_{\alpha_2}$ é um grupo finito. Então $E(\mathbb{Q})/2E(\mathbb{Q}) \cong \operatorname{Im}\rho$ é um grupo finito, ou seja, o índice $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ é finito. Desse modo, pelo Teorema da Descida 5.9, podemos concluir que $E(\mathbb{Q})$ é finitamente gerado. □

Observação 5.25. No caso $E[2] \not\subset E(\mathbb{Q})$, observamos que se $\mathbb{K}$ é uma extensão algébrica de $\mathbb{Q}$, então $E(\mathbb{Q})$ é subgrupo de $E(\mathbb{K})$. Com exceção da Proposição 5.18 (a qual garante que $\operatorname{Im}\rho_\alpha$ é finita), podemos reproduzir os argumentos dessa seção considerando $\mathbb{K}$ ao invés de $\mathbb{Q}$. Portanto, a dificuldade fica em demonstrar que $\operatorname{Im}\rho$ é finita. Infelizmente, não estudaremos estes casos neste trabalho, mas indicamos a leitura de [Cas91, Capítulo 15] ou [Sim02] para tais situações.

O Teorema de Mordell garante que existe $r_E \in \mathbb{N}$, tal que

$$E(\mathbb{Q}) \cong E_{tor}(\mathbb{Q}) \oplus \mathbb{Z}^{r_E}.$$

O valor de r_E é chamado *rank* de $E(\mathbb{Q})$.

O rank máximo conhecido atualmente, exatamente determinado, é 20 (veja [EK20]). Entretanto, existem curvas com rank maior mas não exatamente determinado, sendo 28 a de maior estimativa inferior (veja Tabela 5.1 e [KSW19]).

Enquanto os subgrupos de torção são totalmente caracterizados pelo Teorema de Mazur, não se sabe quais valores o rank de uma curva elíptica pode assumir ou se ele é limitado. Resultados experimentais recentes [PPVW19], sugerem que existe uma quantidade finita de curvas elípticas com rank maior que 21. Mas, sem uma demonstração formal, a pergunta continua sem resposta.

rank $\geq$	ano	Autor
3	1938	Billing
4	1945	Wiman
6	1974	Penney - Pomerance
7	1975	Penney - Pomerance
8	1977	Grunewald - Zimmert
9	1977	Brumer - Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao - Kouya
22	1997	Fermigier
23	1998	Martin - McMillen
24	2000	Martin - McMillen
28	2006	Elkies

Tabela 5.1: Progresso dos recordes do rank de uma curva elíptica.

Referências Bibliográficas

[Cas91] John W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[CM98] Todd Cochrane and Patrick Mitchell. Small solutions of the Legendre equation. *J. Number Theory*, 70(1):62–66, 1998.

[CR03] John Cremona and David Rusin. Efficient solution of rational conics. *Math. Comp.*, 72(243):1417–1441, 2003.

[EK20] Noan D. Elkies and Zev Klagsbrun. New rank records for elliptic curves faving rational torsion. *Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, 4:233–250, 2020.

[Ful08] William Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. Fourth edition, 2008.

[Gib98] Christopher Gibson. *Elementary geometry of algebraic curves: an undergraduate introduction*. Cambridge University Press, Cambridge, 1998.

[Hus04] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Kir92] Frances Kirwan. *Complex Algebraic Curves*. London Mathematical Society Student Texts. Cambridge University Press, 1992.

[KSW19] Zev Klagsbrun, Travis Sherman, and James Weigandt. The Elkies curve has rank 28 subject only to GRH. *Math. Comp.*, 88(316):837–846, 2019.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2022. [Online; accessed 25 February 2022].

[Mil06] James S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[PPVW19] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood. A heuristic for boundedness of ranks of elliptic curves. *J. Eur. Math. Soc. (JEMS)*, 21(9):2859–2903, 2019.

[Sel51] Ernst S. Selmer. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85:203–362, 1951.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sim02] Denis Simon. Computing the rank of elliptic curves over number fields. *LMS J. Comput. Math.*, 5:7–17, 2002.

[ST15] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[Ste15] Ian Stewart. *Galois Theory*. Chapman and Hall/CRC, New York, fourth edition, 2015.

[The22] The Sage Developers. Sagemath, the Sage Mathematics Software System (Version 9.5). https://www.sagemath.org, 2022. [Online; accessed 25 February 2022].

[Vai17] Israel Vainsencher. *Introdução às Curvas Algébricas Planas*. Coleção Matemática Universitária. IMPA, 2017.