Pontifícia Universidade Católica
do Rio de Janeiro

Eduardo Vieira de Oliveira Aguiar

Uma introdução às curvas elípticas sobre corpos finitos

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Matemática pelo Programa de Pós-graduação em Matemática, do Departamento de Matemática da PUC-Rio.

Orientador: Prof. Nicolau Corção Saldanha

Rio de Janeiro
Julho de 2021

Pontifícia Universidade Católica
do Rio de Janeiro

Eduardo Vieira de Oliveira Aguiar

Uma introdução às curvas elípticas sobre corpos finitos

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-Graduação em Matemática da PUC-Rio. Aprovada pela Comissão Examinadora abaixo:

Prof. Nicolau Corção Saldanha
Orientador
Departamento de Matemática – PUC-Rio

Prof. Carlos Gustavo Tamm de Araújo Moreira
Instituto de Matemática Pura e Aplicada

Prof.ª Christine Sertã Costa
Departamento de Matemática – PUC-Rio

Prof.ª Emília Carolina Santana Teixeira Alves
Departamento de Matemática Aplicada – UFF

Prof.ª Renata Martins Rosa
Departamento de Matemática – PUC-Rio

Rio de Janeiro, 02 de Julho de 2021

Eduardo Vieira de Oliveira Aguiar

Graduou-se em Engenharia de Computação pelo Instituto Tecnológico de Aeronáutica (ITA) em 2008.

Ficha Catalográfica

Aguiar, Eduardo Vieira de Oliveira

Uma introdução às curvas elípticas sobre corpos finitos / Eduardo Vieira de Oliveira Aguiar ; orientador: Nicolau Corção Saldanha. – 2021.
76 f. : il. color. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Matemática, 2021.
Inclui bibliografia

1. Matemática – Teses. 2. Curva elíptica. 3. Curva algébrica. 4. Corpo finito. I. Saldanha, Nicolau Corção. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Matemática. III. Título.

CDD: 510

Aos meus filhos Rayka, Beatriz e Andrew.

Agradecimentos

À minha esposa, Meryane, por todo o seu apoio e compreensão para que eu pudesse realizar o mestrado.

Aos meus pais, Nanci e Wilson, por terem me ensinado a importância dos estudos e terem me dado todo suporte ao longo da minha vida.

Ao meu orientador, Nicolau, que se dispôs a estar comigo durante todo o processo de produção deste trabalho, orientando e ensinando com muita dedicação.

A todos os professores e professoras que transmitiram seus conhecimentos durante o curso.

A todos os meus colegas de turma pelo apoio e parceria.

À PUC-Rio pela oportunidade.

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

Resumo

Aguiar, Eduardo Vieira de Oliveira; Saldanha, Nicolau Corção. **Uma introdução às curvas elípticas sobre corpos finitos**. Rio de Janeiro, 2021. 76 p. Dissertação de Mestrado - Departamento de Matemática, Pontifícia Universidade Católica do Rio de Janeiro.

Curvas elípticas são objeto de estudo pelos matemáticos há mais de 200 anos. Por si só, é uma teoria bastante interessante por estar relacionada com diversas áreas da matemática: álgebra, equações diofantinas e geometria algébrica, dentre outras. Recentemente, diversos pesquisadores sugeriram o uso de curvas elípticas para resolver problemas práticos; como exemplos, podemos citar a criptografia, algoritmos para fatoração de números inteiros e testes de primalidade. Uma curva elíptica é definida sobre um corpo (no sentido algébrico). Essa dissertação tem por objetivo apresentar os primeiros elementos da teoria das curvas elípticas sobre corpos finitos. Como veremos, o desenvolvimento do tema aborda diversos tópicos da educação básica. Para isso, iniciaremos o trabalho com uma introdução utilizando o corpo dos números reais e, em seguida, incluiremos a teoria mais geral sobre essas curvas algébricas. Concluiremos então com algumas propriedades e resultados de curvas elípticas sobre corpos finitos, incluindo alguns exemplos e a interpretação geométrica da soma de dois pontos de curvas sobre corpos finitos específicos.

Palavras-chave

Curva Elíptica; Curva Algébrica; Corpo Finito.

Abstract

Aguiar, Eduardo Vieira de Oliveira; Saldanha, Nicolau Corção. **An introduction to elliptic curves over finite fields**. Rio de Janeiro, 2021. 76 p. Dissertação de Mestrado - Departamento de Matemática, Pontifícia Universidade Católica do Rio de Janeiro.

Elliptic curves have been studied by mathematicians for over 200 years. By itself, it is a remarkably interesting theory as it is related to several areas of mathematics: algebra, Diophantine equations and algebraic geometry, among others. Recently, several researchers have suggested the use of elliptic curves to solve practical problems; as examples, we can mention cryptography, integer factorization algorithms and primality tests. An elliptic curve is defined over a field (in algebraic sense). This dissertation aims to present the first elements in the theory of elliptic curves on finite fields. As we will see, the development of the subject addresses a number of topics covered in basic education. In order to accomplish this, we will start the work with an introduction using the field of real numbers and then we will include the more general theory about these algebraic curves. Finally, we will present some properties and results on elliptic curves over finite fields, including some examples and a geometric interpretation of the sum of two points over specific finite fields.

Keywords

Elliptic Curve; Algebraic Curve; Finite Field.

Sumário

Lista de Tabelas

Lista de Figuras

1
INTRODUÇÃO

A teoria de curvas elípticas vem sendo desenvolvida desde o século XVIII, sua origem remonta o cálculo do comprimento de arcos de elipses através de integrais elípticas (ASH; GROSS, 2012). Inclusive, essa conexão histórica com elipses é o que fez com que tais curvas fossem batizadas com o nome "curvas elípticas", no entanto as curvas elípticas não são nada parecidas com elipses.

Apesar de possuir uma longa história, o estudo de curvas elípticas sempre esteve restrito à matemática pura por não se conhecer aplicações práticas (DOOLEY, 2018). No entanto, nas últimas décadas, o interesse no tema foi revitalizado devido a uma ampla variedade de aplicações teóricas e práticas, na matemática e na computação.

Pelo lado teórico, destacamos o papel central (e até surpreendente) na prova do Último Teorema de Fermat, que estabelece que, para todo natural $n \geq 3$, não existem inteiros não-nulos x, y, z tais que $x^n + y^n = z^n$. Já pelo lado prático, ressaltamos o uso em sistemas criptográficos de chave pública, em testes de primalidade e em algoritmos de fatoração (CRANDALL; POMERANCE, 2005).

Esse trabalho tem como objetivo, de forma geral, introduzir os conceitos e as principais propriedades das curvas elípticas: curvas cujas equações são da forma $y^2 = x^3 + Ax + B$ (a Figura 1 mostra o gráfico da curva elíptica $y^2 = x^3 - 4x + 1$ sobre $\mathbb{R}$). Mais especificamente, o foco principal é mostrar o que são curvas elípticas sobre corpos finitos. Como veremos, isso foge um pouco da intuição geométrica utilizada quando definimos uma curva elíptica sobre o corpo dos números reais.

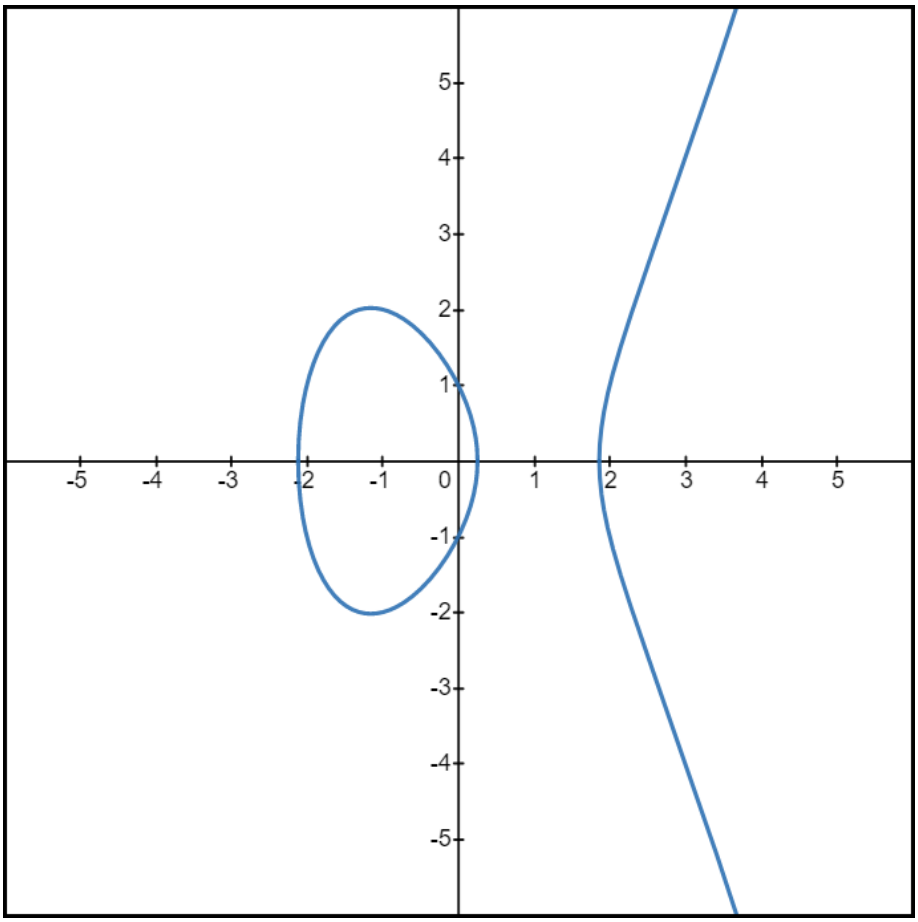

Figura 1: Curva elíptica sobre o conjunto dos reais

É interessante notar que o desenvolvimento inicial da teoria de curvas elípticas contém elementos presentes por toda educação básica: conjunto dos números reais, equação da reta, polinômios, dentre outros. Dessa forma, esse texto pode contribuir tanto para a educação continuada do professor da educação básica quanto para alunos do ensino médio interessados em assuntos um pouco mais avançados.

Para facilitar o acompanhamento e estabelecer uma sequência lógica dos assuntos necessários à compreensão da dissertação, dividimos o trabalho em capítulos. Os capítulos 2 e 3 contêm a teoria matemática mínima necessária para introdução adequada ao tema: álgebra e curvas algébricas planas, respectivamente. Cabe observar que, sempre que razoável, tentou-se fornecer as demonstrações dos teoremas apresentados. No entanto, devido ao tamanho e/ou à complexidade, optou-se por omitir algumas demonstrações: nesses casos um livro-texto que contenha a respectiva demonstração foi indicado junto ao enunciado. O capítulo 4 apresenta curvas elípticas sobre o corpo $\mathbb{R}$ com o objetivo de prover uma

introdução “amigável” sobre o assunto. No capítulo 5, generalizamos o conceito de curva elíptica para qualquer corpo. Já o capítulo 6 foca exclusivamente em curvas elípticas sobre corpos finitos, apresentando alguns resultados específicos para tais curvas e uma forma de plotar o gráfico para algumas delas. Por fim, o capítulo 7 contém as considerações finais do trabalho.

2
TÓPICOS DE ÁLGEBRA

Alguns conceitos de álgebra são essenciais para a compreensão da teoria de curvas elípticas. Esse capítulo apresenta as estruturas algébricas necessárias, algumas propriedades e resultados de interesse. Cabe observar que o objetivo desse capítulo é expor somente o mínimo de conteúdo para compreensão dos capítulos seguintes e que, em caso de necessidade, qualquer livro de Álgebra pode ser consultado, como Lang (2008).

2.1
Grupos

Considere um conjunto G que possui uma lei de composição, isto é, uma operação que para cada par ordenado (a, b) em $G \times G$ determina um elemento $a * b$ de G. Nessas condições, G munido da lei de composição $*$ é um *grupo* se satisfaz:

(g.1) Associatividade

Para todo $a, b, c \in G$, $a * (b * c) = (a * b) * c$

(g.2) Existência do elemento neutro

Existe $e \in G$ tal que, para todo $a \in G$, $e * a = a * e = a$

(g.3) Todo elemento possui elemento inverso

Para todo $a \in G$, existe $b \in G$ tal que $a * b = b * a = e$

Além disso, um grupo G é dito *abeliano* ou comutativo se satisfaz ainda

(g.4) Comutatividade

Para todo $a, b \in G$, $a * b = b * a$

O grupo G com operação $*$ é denotado por $(G,*)$. No entanto, quando a operação $*$ está implícita, esta pode ser omitida. Muitas vezes a operação $*$ do grupo G é chamada "soma" (usa-se o símbolo $+$) ou "produto" (símbolo $\times$ ou $\cdot$), sendo que não necessariamente as regras usuais de soma e produto são usadas. No caso do grupo $(G, +)$, costuma-se denotar o elemento neutro por 0 (zero) e o inverso aditivo de a por $-a$. Para o grupo $(G,\times)$, chamamos o elemento neutro de identidade, podendo ser denotado por e ou 1, e o inverso multiplicativo de a é denotado por a^{-1}.

Proposição 2.1 Seja $(G,*)$ um grupo, então

(i) O elemento neutro de G é único.

(ii) Para todo $a \in G$, o inverso de a é único.

Demonstração

(i) Suponha que G tenha elementos neutros e e e' satisfazendo a propriedade (g.2). Então, $e = e * e' = e' * e$ pois e' é um elemento neutro. Usando o mesmo argumento, temos $e' = e' * e = e * e'$. Logo, $e = e'$.

(ii) Sejam $b, b' \in G$ elementos inversos de a. Então, usando as propriedades (g.1), (g.2) e (g.3), temos $b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$.

■

Exemplo 2.2

a) $(\mathbb{Z}, +)$ é um grupo abeliano infinito, cujo elemento neutro é o 0. O inverso de $a \in \mathbb{Z}$ é o inteiro $-a$.

b) Denotando por $\mathbb{Z}/n\mathbb{Z}$ as classes de congruência módulo n, temos que $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ é um grupo abeliano finito com n elementos. O símbolo $\oplus$ denota a operação soma sobre elementos de $\mathbb{Z}/n\mathbb{Z}$, ou seja, $\bar{a} \oplus \bar{b} = \overline{a+b}$, onde $\bar{a}$ denota a classe de congruência de $a \in \mathbb{Z}$. O elemento neutro desse grupo é a classe de congruência $\bar{0}$.

c) Sejam G e G' grupos aditivos com elementos neutros e_G e $e_{G'}$, respectivamente. Considere o conjunto $G \times G'$ de todos os pares (a, a') em que $a \in G$ e $a' \in G'$. Se definirmos a operação soma para conjunto $G \times G'$ como $(a, a') + (b, b') = (a + b, a' + b')$, então o conjunto munido dessa operação é um grupo. O elemento neutro é $(e_G, e_{G'})$ e o inverso de (a, a') é $(-a, -a')$, onde $-a$ é o inverso de a em G e $-a'$ é o inverso de a' em G'. O grupo $G \times G'$ é chamado de produto direto de G e G'.

Considere agora um grupo $(G,*)$ com elemento neutro e e denote o inverso de a em $(G,*)$ por a^{-1}. Um subconjunto não-vazio H de G é um *subgrupo* de G quando ambas as condições seguintes são satisfeitas:

a) $e \in H$

b) Para quaisquer $a, b \in H$, $a * b \in H$ e $a^{-1} \in H$

A definição acima implica que H munido da operação $*$ é um grupo.

Vamos olhar agora a "exponenciação" em um grupo $(G,*)$. Inicialmente, se tomarmos $a \in G$, definimos $a^0 = e$, $a^t = a * a^{t-1}$ e $a^{-t} = (a^t)^{-1}$, para qualquer $t \in \mathbb{Z}$. A partir dessa definição, pode-se mostrar que, para todo $a \in G$ e $t, v \in \mathbb{Z}$, temos $a^t * a^v = a^{t+v}$ e $(a^t)^v = a^{tv}$.

Observação 2.3 A definição acima pode ser generalizada para qualquer grupo, usamos a notação de exponenciação somente por conveniência. Por exemplo, em um grupo aditivo $(G,+)$, definimos $0a = 0$, $ta = a + (t-1)a$ e $-ta = -(ta)$, onde $a \in G$ e $t \in \mathbb{Z}$. Com essa notação, os resultados abaixo continuam válidos.

Dado $a \in G$, podemos gerar um subconjunto de G tomando as potências a^t, onde $t \in \mathbb{Z}$. Esse conjunto será denotado por $\langle a \rangle$. Vamos provar que $\langle a \rangle$ é um subgrupo de G e, neste caso, dizemos que é um subgrupo gerado por a.

Proposição 2.4 Sejam $(G,*)$ um grupo e $a \in G$. O conjunto $\langle a \rangle = \{a^t | t \in \mathbb{Z}\}$ é um subgrupo de G.

Demonstração

Primeiro, como $a^0 = e$, temos que $e \in \langle a \rangle$. Seja $g \in \langle a \rangle$, então $g = a^t$, para algum $t \in \mathbb{Z}$. O inverso de g é $g^{-1} = (a^t)^{-1} = a^{-t}$, que pertence a $\langle a \rangle$. Por fim, sejam $g, h \in \langle a \rangle$, então existem $t_1, t_2 \in \mathbb{Z}$ tais que $g = a^{t_1}$ e $h = a^{t_2}$. Nesse caso, $g * h = a^{t_1} * a^{t_2} = a^{t_1+t_2} \in \langle a \rangle$.

Portanto, $\langle a \rangle$ é um subgrupo de G. ■

É possível que o subgrupo gerado por algum $a \in G$ seja o próprio G, ou seja, $G = \langle a \rangle$. Neste caso, dizemos que G é um *grupo cíclico* e a é um gerador de G. Observe que, nessas condições, G é um grupo abeliano (comutativo), pois temos $a^t * a^v = a^v * a^t = a^{t+v}$.

Exemplo 2.5 O conjunto dos inteiros $\mathbb{Z}$ munido da operação $+$ é um grupo cíclico, pois $\mathbb{Z} = \langle 1 \rangle$.

No exemplo acima, $(\mathbb{Z},+)$ é um grupo com infinitos elementos. Por outro lado, o grupo $\mathbb{Z}/n\mathbb{Z}$, definido no exemplo 2.2.b, é um grupo finito com n

elementos. O número de elementos de um grupo G é chamado de *ordem* do grupo e será denotado por $|G|$. A ordem de $a \in G$ é o número de elementos de $\langle a \rangle$.

Proposição 2.6 Sejam G um grupo, $a \in G$ e $\langle a \rangle$ o subgrupo gerado por a. Então a ordem de $\langle a \rangle$ é finita se e somente se existe $t \geq 1$ tal que $a^t = e$. Neste caso, denotando por n a ordem de a, temos que $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ e que se $a^t = e$, então $t = kn$, onde $k \in \mathbb{Z}$.

Demonstração

($\Longrightarrow$) Seja n a ordem finita de $\langle a \rangle$. Como $\mathbb{Z}$ é infinito, existem $t_1, t_2 \in \mathbb{Z}$, com $t_1 \neq t_2$, tais que $a^{t_1} = a^{t_2}$ (caso contrário, a ordem de $\langle a \rangle$ teria de ser infinita). Sem perda de generalidade, suponha que $t_2 > t_1$. Então podemos escrever $t_2 = t_1 + k$, onde $k \geq 1$ é inteiro.

Portanto, $e = (a^{t_1})^{-1} * a^{t_1} = a^{-t_1} * a^{t_2} = a^{t_2 - t_1} = a^k$. Ou seja, existe $k \geq 1$ tal que $a^k = e$.

($\Longleftarrow$) Existe $t \geq 1$ tal que $a^t = e$. Seja n o menor inteiro positivo tal que $a^n = e$. Para qualquer inteiro k, podemos escrever $k = qn + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < n$.

Então, $a^k = a^{qn+r} = a^{qn} * a^r = (a^n)^q * a^r = e^q * a^r = a^r$. Portanto, a^k pode assumir somente valores em $\{e, a, a^2, \dots, a^{n-1}\}$, que é um conjunto finito. Daí, conclui-se que $\langle a \rangle$ é um conjunto finito.

Ainda, dois elementos do conjunto $\{e, a, a^2, \dots, a^{n-1}\}$ devem ser diferentes. Caso contrário, teríamos $a^t = a^v$ para algum par de inteiros t e v satisfazendo $0 \leq t < v < n$. Assim, $a^v = a^{t+(v-t)} = a^t * a^{v-t} = a^v * a^{v-t} \Rightarrow a^{v-t} = e$ e $v - t \geq 1$, contradizendo a escolha de n. Logo, $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$.

Por fim, temos $a^k = a^{qn+r} = a^r$. Ou seja, $a^k = e \Leftrightarrow a^r = e \Leftrightarrow r = 0 \Leftrightarrow k = qn$. ■

Considere agora o conjunto de números inteiros k tal que $a^k = e$ para todo $a \in G$. Não é difícil verificar que esse conjunto é um subgrupo de $\mathbb{Z}$ e, portanto, existe o menor elemento não-negativo do conjunto (0 pode ser único elemento do conjunto), denotado por m. Definimos m como o *expoente* do grupo G.

Exemplo 2.7

a) O grupo aditivo $\mathbb{Z}$ tem expoente 0.

b) O grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ tem expoente n.

Para enunciar e provar o Teorema de Lagrange, precisamos fazer algumas considerações. Sejam G um grupo e H um subgrupo de G. Dados dois elementos $x, y \in G$, dizemos que $x \equiv y \ (mod\ H)$ se e somente se $xy^{-1} \in H$.

Proposição 2.8 A relação $\cdot \equiv \cdot \ (mod\ H)$ é uma relação de equivalência em G, i.e., para todo $x, y, z \in G$:

(i) $x \equiv x \ (mod\ H)$

(ii) $x \equiv y \ (mod\ H) \implies y \equiv x \ (mod\ H)$

(iii) $x \equiv y \ (mod\ H)$ e $y \equiv z \ (mod\ H) \implies x \equiv z \ (mod\ H)$

Demonstração

(i) $xx^{-1} = e \in H$. Logo $x \equiv x \ (mod\ H)$

(ii) $x \equiv y \ (mod\ H) \implies xy^{-1} \in H$. Como H é subgrupo de G, temos que $(xy^{-1})^{-1} \in H$. Observe que $(xy^{-1})(yx^{-1}) = x\big(y^{-1}(yx^{-1})\big) = x(y^{-1}y)x^{-1} = xex^{-1} = xx^{-1} = e$, portanto $yx^{-1} = (xy^{-1})^{-1} \in H$. Logo, $y \equiv x \ (mod\ H)$.

(iii) $x \equiv y \ (mod\ H)$ e $y \equiv z \ (mod\ H) \implies xy^{-1} \in H$ e $yz^{-1} \in H \implies (xy^{-1})(yz^{-1}) \in H$. Usando a associatividade, temos que $(xy^{-1})(yz^{-1}) = x\big(y^{-1}(yz^{-1})\big) = x(y^{-1}y)z^{-1} = xez^{-1} = xz^{-1} \in H$, ou seja, $x \equiv z \ (mod\ H)$. ■

Denotamos por $[a]_H$ a classe de equivalência de a, ou seja, o conjunto dos elementos $x \in G$ tal que $x \equiv a \ (mod\ H)$. Pela definição, $x \equiv a \ (mod\ H) \Leftrightarrow xa^{-1} = h \in H \Leftrightarrow x = ah$, para algum $h \in H$. Daí, $[a]_H = \{ah : h \in H\} = aH$. Observe que $a \in [a]_H$, pois $a = ae$ e $e \in H$.

Lema 2.9 Sejam G um grupo, H um subgrupo de G e $a, b \in G$. Considere a relação $\cdot \equiv \cdot \ (mod\ H)$. Se $a \in [b]_H$, então $[a]_H = [b]_H$.

Demonstração

Inicialmente, temos $a \in [b]_H \Leftrightarrow a \equiv b \ (mod\ H) \Leftrightarrow b \equiv a \ (mod\ H)$. Vamos provar que $[b]_H \subset [a]_H$ e $[a]_H \subset [b]_H$.

• $c \in [b]_H \Longrightarrow c \equiv b\ (mod\ H)$. Como $b \equiv a\ (mod\ H)$, pelo teorema 2.8(c), temos $c \equiv a(mod\ H) \Longrightarrow c \in [a]_H \Longrightarrow [b]_H \subset [a]_H$.

• $c \in [a]_H \Longrightarrow c \equiv a\ (mod\ H)$. Como $a \equiv b\ (mod\ H)$, pelo teorema 2.8(c), temos $c \equiv b(mod\ H) \Longrightarrow c \in [b]_H \Longrightarrow [a]_H \subset [b]_H$.

De (i) e (ii), $[a]_H = [b]_H$. ■

O lema acima implica que um elemento qualquer de G pertence a uma única classe de equivalência. Dessa forma, as classes de equivalência da relação $\cdot \equiv \cdot\ (mod\ H)$ formam uma partição de G.

Lema 2.10 Sejam G um grupo e H um subgrupo de G. Para quaisquer $a, b \in G$, a cardinalidade de $[a]_H$ é igual a cardinalidade de $[b]_H$. Ainda, como $[e]_H = \{eh : h \in H\} = H$, temos que a cardinalidade de uma classe qualquer é igual à $|H|$, que é ordem de H.

Demonstração

Considere $a, b \in G$. Seja $x \in [a]_H$, então existe $h \in H$ tal que $x = ah$. Multiplicando à esquerda por ba^{-1} ambos os lados da equação, temos $ba^{-1}x = ba^{-1}ah = bh$. Isso significa, pela definição, que $ba^{-1}x \in [b]_H$.

Seja a função

$$f: [a]_H \to [b]_H$$
$$x \mapsto ba^{-1}x$$

Vamos mostrar que f é uma bijeção (injetiva e sobrejetiva), o que conclui a demonstração.

• $f(x) = f(x') \Longrightarrow ba^{-1}x = ba^{-1}x' \Longrightarrow x = x'$. Logo, f é injetiva.

• $y \in [b]_H \Longrightarrow y = bh, h \in H \Longrightarrow ab^{-1}(y) = ab^{-1}(bh) = ah \in [a]_h$.

Daí, $f(ab^{-1}y) = ba^{-1}(ab^{-1}y) = b(a^{-1}a)b^{-1}y = bb^{-1}y = y$. Logo, f é sobrejetiva. ■

Finalmente, podemos enunciar o Teorema de Lagrange.

Teorema 2.11 (Teorema de Lagrange) Seja G um grupo finito e H um subgrupo de G. Então a ordem de H divide a ordem de G.

Demonstração

Suponha que a relação $\cdot \equiv \cdot \ (mod\ H)$ particione G em k classes disjuntas (lema 2.9) denotadas por $[a_1]_H, [a_2]_H, \dots, [a_k]_H$. Então, $|G| = |[a_1]_H| + |[a_2]_H| + \cdots + |[a_k]_H|$. Pelo lema 2.10, cada uma das classes tem $|H|$ elementos. Portanto, $|G| = k\,|H|$, provando o teorema. ■

Corolário 2.12 Seja G um grupo finito e seja $a \in G$. Então a ordem de a divide a ordem de G.

Demonstração

Aplicação direta do Teorema 2.11, pois $\langle a \rangle$ é um subgrupo de G. ■

Corolário 2.13 Seja G um grupo de ordem prima. Então G é cíclico.

Demonstração

Suponha $|G| = p$ e p um número primo. Considere $a \in G$, $a \neq e$ e o subgrupo gerado por a: $\langle a \rangle = \{e, a, \dots\}$. Como $e \in \langle a \rangle$ e $a \in \langle a \rangle$, $|\langle a \rangle| \geq 2$ e, pelo Corolário 2.12, $|\langle a \rangle|$ divide p. Logo, $|\langle a \rangle| = p$. Ou seja, $G = \langle a \rangle$ é cíclico. ■

Para alcançarmos o objetivo final dessa seção, que é apresentar o resultado sobre a estrutura de grupos abelianos finitos, necessitamos definir alguns novos conceitos. Comecemos abordando homomorfismos e isomorfismos de grupos.

Considere dois grupos G e G'. Um *homomorfismo de grupo* é uma aplicação $f: G \to G'$ que satisfaz $f(a * b) = f(a) * f(b)$ para todo $a, b \in G$. Observe que usamos por conveniência a notação $*$ para ambos os grupos, mas que $a * b$ é uma operação em G e $f(a) * f(b)$ é uma operação em G'.

Exemplo 2.14 Seja G um grupo abeliano multiplicativo. A aplicação $f: G \to G$ definida por $f(a) = a^{-1}$ é um homomorfismo. Para ver tal fato, observe que $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = f(b)f(a) = f(a)f(b)$.

Dado um homomorfismo $f: G \to G'$, definimos a *imagem* de f como o conjunto $Im(f) = \{f(a) : a \in G\}$, que é um subconjunto de G'. Já o *núcleo* de f

é conjunto $N(f) = \{a \in G : f(a) = e_{G'}\}$, onde $e_{G'}$ é o elemento neutro de G'. Dizemos ainda que f é um monomorfismo se f *injetiva* (ou seja, $f(a) = f(b) \Longrightarrow a = b$) e que f é um epimorfismo se f *sobrejetiva* ($Im(f) = G'$).

Proposição 2.15 Sejam G e G' grupos com elementos neutros e_G e $e_{G'}$, respectivamente, e a aplicação $f: G \to G'$ um homomorfismo de grupos. Então,

(i) $f(e_G) = e_{G'}$

(ii) $f(a^{-1}) = f(a)^{-1}$

(iii) f é injetiva se e somente se $N(f) = \{e_G\}$

Demonstração

(i) Usando a notação multiplicativa, $f(e_G) = f(e_G \times e_G) = f(e_G) \times f(e_G)$. Multiplicando ambos os lados por $f(e_G)^{-1}$, obtemos $e_{G'} = f(e_G) \times f(e_G)^{-1} = f(e_G)$.

(ii) $e_{G'} = f(e_G) = f(aa^{-1}) = f(a)f(a^{-1}) \Rightarrow f(a^{-1}) = f(a)^{-1}$.

(iii) ($\Longrightarrow$) f é injetiva. Como $f(e_G) = e_{G'}$, $f(a) = e_{G'} = f(e_G) \Rightarrow a = e_G$. Logo, $N(f) = \{e_G\}$.

($\Longleftarrow$) $N(f) = \{e_G\}$. $f(a) = f(b) \Rightarrow f(a)f(b)^{-1} = e_{G'} \Rightarrow f(ab^{-1}) = e'_G \Rightarrow ab^{-1} = e_G \Rightarrow a = b$. Logo, f é injetiva. ■

Considere agora um homomorfismo de grupos $f: G \to G'$. Se f é injetiva e sobrejetiva (ou seja, f é bijetiva), dizemos que f é um *isomorfismo de grupos*. Quando tal f existe, G é dito isomorfo a G', denotado por $G \cong G'$. Se $G = G'$, então f é chamado de um *automorfismo de grupos* sobre G.

Considere um grupo abeliano $(G, +)$. Dados H_1 e H_2 subgrupos de G tais que $H_1 \cap H_2 = \{e_G\}$, pode-se provar facilmente que o conjunto

$$H_1 \oplus H_2 = \{a_1 + a_2 \in G : a_1 \in H_1 \, e \, a_2 \in H_2\}$$

é um subgrupo de G e, a partir dele, podemos definir um isomorfismo de grupos.

Proposição 2.16 Seja G um grupo abeliano com subgrupos H_1 e H_2, onde $H_1 \cap H_2 = \{e_G\}$. Então temos um isomorfismo de grupos $H_1 \times H_2 \cong H_1 \oplus H_2$ dado pelo mapeamento

$$f: H_1 \times H_2 \to H_1 \oplus H_2$$
$$f(a_1, a_2) = a_1 + a_2$$

Demonstração

Primeiramente, verifiquemos o núcleo de f. Dados $a_1 \in H_1$ e $a_2 \in H_2$, suponhamos que $(a_1, a_2) \in N(f)$, i.e., $f(a_1, a_2) = e_G$. Temos, então, que

$$f(a_1, a_2) = a_1 + a_2 = e_G \Longrightarrow a_2 = -a_1 \in H_1.$$

Como $H_1 \cap H_2 = \{e_G\}$, a única possibilidade é $a_2 = a_1 = e_G$, ou seja, $N(f) = \{(e_G, e_G)\}$, o que implica que f é injetiva pela proposição 2.15.

Para ver que f é sobrejetiva, basta ver que qualquer elemento a de $H_1 \oplus H_2$ pode ser escrito como $a_1 + a_2$, em que $a_1 \in H_1$ e $a_2 \in H_2$. Então, $a = a_1 + a_2 = f(a_1, a_2)$.

Portanto, f é bijetiva e, então, um isomorfismo. ■

O conjunto $H_1 \oplus H_2$ definido acima é chamado de *soma direta* de H_1 e H_2. Pode-se generalizar o conceito de soma direta para k subgrupos de G disjuntos dois a dois e teríamos um isomorfismo $H_1 \times H_2 \times \ldots \times H_k \cong H_1 \oplus H_2 \oplus \ldots \oplus H_k$ equivalente ao da proposição 2.16.

Com todos os elementos definidos, podemos enunciar o Teorema Fundamental dos Grupos Abelianos Finitos. Uma prova para teorema pode ser encontrada em Shoup (2009, p. 163-164).

Teorema 2.17 (Teorema Fundamental dos Grupos Abelianos Finitos) Um grupo abeliano finito (com mais de um elemento) é isomorfo a uma soma direta de grupos cíclicos

$$\mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{e_r}}$$

em que todos os p_i são primos (não necessariamente distintos) e os expoentes e_i são inteiros positivos. Essa soma direta é única a não ser pela ordem dos fatores.

Exemplo 2.18 O grupo aditivo $\mathbb{Z}_{20} = \{0,1,2,3,\ldots,19\}$ pode ser visto como a soma direta de dois grupos cíclicos: $(0,4,8,12,16) \oplus (0,5,10,15)$. Logo, $\mathbb{Z}_{20} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5$.

O Teorema Fundamental dos Grupos Abelianos Finitos (teorema 2.17) pode ser reescrito de uma maneira alternativa:

Teorema 2.19 Um grupo abeliano finito (com mais de um elemento) é isomorfo a uma soma direta de grupos cíclicos

$$\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_t}$$

em que cada m_i é um inteiro positivo determinado de forma única e $m_i \mid m_{i+1}$ para todo $i = 1, \ldots, t-1$. Além disso, m_t é o expoente do grupo.

2.2
Anéis

Considere $\mathbb{A}$ um conjunto com duas leis de composição, denotadas por $+$ e $\times$. Essas operações costumam ser chamadas *adição* e *multiplicação*, respectivamente. O conjunto $\mathbb{A}$ é um anel ou anel comutativo, que será denotado por $(\mathbb{A}, +, \times)$, se satisfaz:

(a.1) $(\mathbb{A}, +)$ é um grupo abeliano

- O elemento neutro da adição é denotado por 0
- O inverso aditivo de $a \in \mathbb{A}$ é denotado $-a$

(a.2) A operação $\times$ é associativa em $\mathbb{A}$

Para todo $a, b, c \in \mathbb{A}$, $a \times (b \times c) = (a \times b) \times c$

(a.3) A operação $\times$ é comutativa em $\mathbb{A}$

Para todo $a, b \in \mathbb{A}$, $a \times b = b \times a$

(a.4) Existe o elemento neutro da multiplicação

Para todo $a \in \mathbb{A}$, existe $1 \in \mathbb{A}$ tal que $1 \times a = a \times 1 = a$

(a.5) A adição é distributiva em relação à multiplicação

Para todo $a, b, c \in \mathbb{A}$, $a \times (b + c) = (a \times b) + (a \times c)$

Adicionalmente, se o anel $\mathbb{A}$ satisfaz a propriedade (a.6), dizemos que $\mathbb{A}$ é um domínio de integridade.

(a.6) Anel sem divisores de zero

Para todo $a, b \in \mathbb{A}$, $a \times b = 0 \Longrightarrow a = 0$ ou $b = 0$

Proposição 2.20 Seja $(\mathbb{A}, +, \times)$ um anel com elementos neutros 0 (adição) e 1 (multiplicação). Então,

(i) O elemento neutro da multiplicação é único

(ii) $a \times 0 = 0 \times a = 0, \forall a \in \mathbb{A}$

(iii) $a \times (-b) = (-a) \times b = -(a \times b), \forall a, b \in \mathbb{A}$

Demonstração

(i) Sejam 1 e e elementos neutros da multiplicação. Então, $1 = 1 \times e = e \times 1 = e$.

(ii) $a \times 0 = a \times (0 + 0) = a \times 0 + a \times 0$. Somando $-(a \times 0)$ a ambos os lados, temos $0 = a \times 0$.

(iii) $0 = a \times 0 = a \times \big(b + (-b)\big) = a \times b + a \times (-b)$. Somando a ambos os lados $-(a \times b)$, temos $a \times (-b) = -(a \times b)$. ■

Exemplo 2.21 $(\mathbb{Z}, +, \times)$ é um anel comutativo.

Da mesma maneira como foi feita com grupos, podemos definir homomorfismos de anéis. Sejam $\mathbb{A}_1$ e $\mathbb{A}_2$ anéis e $f: \mathbb{A}_1 \to \mathbb{A}_2$ um mapeamento que toma um elemento de $\mathbb{A}_1$ e nos dá um elemento de $\mathbb{A}_2$. Dizemos que f é um homomorfismo de $\mathbb{A}_1$ em $\mathbb{A}_2$ se, para todo $a, b \in \mathbb{A}_1$, $f(a + b) = f(a) + f(b)$ e $f(a \times b) = f(a) \times f(b)$. As definições de isomorfismos e automorfismos são idênticas, assim como o núcleo e a imagem de f.

2.3
Corpos

Diremos que um anel $(\mathbb{K}, +, \times)$ é um *corpo* se satisfaz

(c.1) Todo elemento não-nulo possui elemento inverso relativo à multiplicação

Para todo $a \in \mathbb{K}\backslash\{0\}$, existe $b \in \mathbb{K}$ tal que $a \times b = b \times a = 1$

Observação 2.22 Quando as operações de um corpo ou de anel estão bem definidas, podemos omiti-las para facilitar a notação. Por exemplo, $(\mathbb{K}, +, \times)$ pode ser representado somente por $\mathbb{K}$.

Proposição 2.23 Seja $\mathbb{K}$ um corpo e seja $a \in \mathbb{K}\backslash\{0\}$. Denote o inverso multiplicativo de a por a^{-1}, então a^{-1} é único.

Demonstração

Basta observar que $(\mathbb{K}\backslash\{0\}, \times)$ é um grupo abeliano. Logo, pela proposição 2.1, o inverso de a é único. ■

Como observado na demonstração acima, os elementos não-nulos de um corpo $\mathbb{K}$ munidos somente com a operação de multiplicação formam um grupo abeliano. Esse grupo é chamado grupo multiplicativo do corpo $\mathbb{K}$ e denotado por $\mathbb{K}^*$.

Exemplo 2.24 $(\mathbb{R}, +, \times)$ é um corpo com elemento neutro aditivo 0 e elemento neutro multiplicativo 1.

Proposição 2.25 Seja $\mathbb{K}$ um corpo. Para todo $a, b \in \mathbb{K}$, temos

$$a \times b = 0 \Leftrightarrow a = 0 \text{ ou } b = 0.$$

Demonstração

Suponha $a \neq 0$, então existe o inverso multiplicativo de a denotado por $a^{-1} \neq 0$. Dessa forma, $b = (a^{-1} \times a) \times b = a^{-1} \times (a \times b) = a^{-1} \times 0 = 0$. Ou seja, $b = 0$.

Analogamente, supondo $b \neq 0$, obteremos $a = 0$. ■

Observação 2.26 O resultado da proposição 2.25 estabelece que todo corpo é um domínio de integridade, ou seja, não possui divisores de zero.

Seja $\mathbb{K}$ um corpo. Define-se uma operação que toma $a \in \mathbb{K}$ e $n \in \mathbb{Z}$ e nos dá um elemento de $\mathbb{K}$, denotado por na. Essa definição é feita indutivamente da seguinte maneira:

a) $0a = 0$;

b) $(k+1)a = ka + a$ para todo inteiro $k \geq 0$;

c) $(-k)a = -(ka)$ para todo inteiro $k > 0$.

Esses elementos na são chamados múltiplos inteiros de a.

Seja $\mathbb{K}$ um corpo. Denotando por 0 o elemento neutro aditivo e por 1 o elemento neutro multiplicativo de $\mathbb{K}$, considere o conjunto $A_{\mathbb{K}} = \{n \in \mathbb{Z} \,|n1 = 0\}$. Se $A_{\mathbb{K}} = \{0\}$, então dizemos que $\mathbb{K}$ tem característica 0. Caso contrário, existe um menor inteiro positivo em $A_{\mathbb{K}}$, denotado por p. Nesse caso, dizemos que $\mathbb{K}$ tem característica p.

Proposição 2.27 Seja $\mathbb{K}$ um corpo de característica p. Então $A_{\mathbb{K}}$ consiste somente dos múltiplos inteiros de p e p é um número primo.

Demonstração

Primeiramente, seja $m \in A_{\mathbb{K}}$. Podemos escrever $m = pq + r,\ 0 \leq r < p$. Então, $0 = m1 = (pq + r)1 = q(p1) + r1 = q0 + r1 = r1$. Ou seja, $r \in A_{\mathbb{K}}$. Se $r \neq 0$, como $r < p$, teríamos que p não é o menor inteiro positivo em $A_{\mathbb{K}}$, o que é falso. Logo, $r = 0$ e, portanto, m é múltiplo de p.

Suponha agora que $p = mn$ é um número composto (ou seja, $1 < m < p$ e $1 < n < p$). Temos, então, $(mn)1 = 0 \Longrightarrow (m1)(n1) = 0$. Pela proposição 2.25, devemos ter $m1 = 0$ ou $n1 = 0$. Logo, p não é o menor inteiro positivo em $A_{\mathbb{K}}$, o que é falso. Portanto, p deve ser primo. ■

O próximo resultado fornece informação sobre a quantidade de elementos em um corpo de característica p. A demonstração será omitida pois seria necessário um maior desenvolvimento teórico, o que foge um pouco do escopo do trabalho. Lang (2008) e Shoup (2009) são boas referências para o assunto.

Proposição 2.28 Seja $\mathbb{K}$ um corpo finito de característica p. Então o número de elementos de $\mathbb{K}$ é igual a p^m, onde m é um inteiro positivo.

2.4
Polinômios

Seja $\mathbb{A}$ um anel com elemento identidade 1. Denote por $P(\mathbb{A})$ o conjunto das infinitas seqüências $(a_0, a_1, \dots, a_n, \dots)$ de elementos de $\mathbb{A}$ em que cada seqüência tenha um número finito de elementos não-nulos, ou seja, para cada seqüência $a = (a_0, a_1, \dots, a_n, \dots)$ em $P(\mathbb{A})$, existe um inteiro N_a tal que $a_i = 0$ para todo $i > N_a$. Defina duas operações em $P(\mathbb{A})$:

- $(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$
- $(a_0, a_1, a_2, \dots) \times (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$ com $c_n = \sum_{i=0}^{n} a_i b_{n-i}$

Desta forma, $P(\mathbb{A})$ com essas operações é um anel denominado anel de polinômios com coeficientes em $\mathbb{A}$.

Considere o mapeamento $\kappa: \mathbb{A} \to P(\mathbb{A})$ definido por $\kappa(a_0) = (a_0, 0, 0, \dots)$, para todo $a_0 \in \mathbb{A}$. O mapeamento κ é um monomorfismo, denominado

monomorfismo canônico de $\mathbb{A}$ em $P(\mathbb{A})$. Dessa forma, vamos identificar a_0 com $\kappa(a_0) = (a_0, 0,0, \dots)$. Além disso, definimos $X = (0,1,0, \dots) \in P(\mathbb{A})$.

Observação 2.29 Escolhemos a letra X para representar o polinômio $(0,1,0, \dots)$. No entanto, qualquer símbolo poderia ter sido escolhido.

Seja n um inteiro não-negativo, definimos X^n recursivamente da seguinte maneira: $X^0 = (1,0,0, \dots)$ e $X^t = X \times X^{t-1}$ para todo $t > 0$. Para todo inteiro não-negativo, é fácil provar por indução que:

(i) $X^n = (x_0, x_1, \dots, x_n, \dots)$ com $x_n = 1$ e, para todo $i \neq n$, $x_i = 0$

(ii) $\kappa(a)X^n = (a_0, a_1, \dots, a_n, \dots)$ com $a_n = a$ e, para todo $i \neq n$, $a_i = 0$.

Dessa maneira, se $f = (a_0, a_1, \dots, a_n, 0,0, \dots) \in P(\mathbb{A})$, então podemos escrever $f = \kappa(a_0) + \kappa(a_1)X + \cdots + \kappa(a_n)X^n$. Como identificamos $\kappa(\mathbb{A})$ por $\mathbb{A}$, podemos reescrever o polinômio como $f = a_0 + a_1X + \cdots + a_nX^n$ e diremos que f é um polinômio na variável X. Com essa notação, o anel de polinômios na variável X costuma ser denotado por $\mathbb{A}[X]$.

Seja $f = a_0 + a_1X + \cdots + a_nX^n$ um polinômio em $\mathbb{A}[X]$. O *grau* de f é definido como o maior inteiro n tal que $a_n \neq 0$. Denotamos o grau de f por ∂f. Dizemos que a_n é o coeficiente principal de f. Se $a_n = 1$, dizemos que o polinômio é mônico.

Observação 2.30 O grau do polinômio nulo $(0,0,0, \dots)$ é definido como sendo $-\infty$.

Exemplo 2.31 O polinômio definido por $f(x) = 2 + x^2 + x^5$ tem grau 5.

Considere agora um corpo $\mathbb{K}$. Como $\mathbb{K}$ não possui divisores de zero (proposição 2.25), é fácil mostrar que o anel de polinômios $P(\mathbb{K})$ é um domínio de integridade (LANG, 2008, p. 159). Dizemos que o polinômio f em $P(\mathbb{K})$ é divisível por um polinômio g se existe um polinômio q tal que $f = g \times q$. Nesse caso dizemos que f é múltiplo de g ou que g é um fator de f. Ainda, dizemos que f é irredutível se f não possui fator g tal que $0 < \partial g < \partial f$. O próximo teorema é conhecido como algoritmo euclidiano (similar ao algoritmo euclidiano para

números inteiros), sua demonstração pode ser encontrada em Lang (2008, p. 159-161).

Teorema 2.32 Sejam $\mathbb{K}$ um corpo, f um polinômio em $P(\mathbb{K})$ e d um polinômio não-nulo em $P(\mathbb{K})$. Então, existe um único par de polinômios q e r com coeficientes em $\mathbb{K}$ tal que $f = q \times d + r$ e $\partial r < \partial d$.

Considere o corpo $\mathbb{K}$ e $\alpha \in \mathbb{K}$. Dado o polinômio $f = a_0 + a_1X + \cdots + a_nX^n$ em $\mathbb{K}[X]$, definimos $\sigma_\alpha: \mathbb{K}[X] \to \mathbb{K}$ como $\sigma_\alpha(f) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$. Denota-se por $\mathbb{K}[\alpha]$ o conjunto $\sigma_\alpha(P(\mathbb{K}))$. Dizemos que α é uma raiz de f em $\mathbb{K}$ se $\sigma_\alpha(f) = 0$, nesse caso escrevemos $f(\alpha) = 0$.

Proposição 2.33 Seja f um polinômio em $\mathbb{K}[X]$ e $\alpha \in \mathbb{K}$. Denotando o polinômio $X - \alpha$ por l_α, temos que α é raiz de f se e somente se l_α é um fator de f em $\mathbb{K}[X]$.

Demonstração

Pelo teorema 2.32, existem polinômios q e r em $\mathbb{K}[X]$ tais que $f = q \times l_\alpha + r$, onde $\partial r < \partial l_\alpha$. Sendo $\partial l_\alpha = 1$, devemos ter $\partial r = 0$ e, portanto, r é uma constante.

Temos também que α é raiz de $f \Leftrightarrow f(\alpha) = 0 = q(\alpha) \times l_\alpha(\alpha) + r(\alpha) = r(\alpha)$. Logo, como r é constante, $r = 0$ e l_α é um fator de f. ■

Considere uma raiz $\alpha \in \mathbb{K}$ do polinômio $f \in \mathbb{K}[X]$. Pela proposição 2.33, sabemos que $X - \alpha$ é um fator de f. Seja m o maior número inteiro positivo tal que $(X - \alpha)^m$ é um fator de f. Dizemos, então, que α é uma raiz de f com multiplicidade m ou que m é a multiplicidade da raiz α em f. Se $m = 1$, dizemos que α é uma raiz simples de f.

Corolário 2.34 Seja f um polinômio não-nulo em $P(\mathbb{K})$ com grau $\partial f = n \geq 0$. Então f tem, no máximo, n raízes em $\mathbb{K}$, contando com multiplicidades.

Demonstração

Por contradição, suponha que f tenha pelo menos $n+1$ raízes em $\mathbb{K}$: $\alpha_1, \dots, \alpha_{n+1}$. Pela proposição 2.33, cada polinômio $X-\alpha_i$ é um fator de f, ou seja, $f = (X-\alpha_1) \dots (X-\alpha_{n+1})q(X)$, onde q é um polinômio com grau ≥ 0.

Pela definição de produtos de polinômios, o produto

$(X-\alpha_1) \dots (X-\alpha_{n+1}) = X^{n+1} + a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$

é um polinômio de grau $n+1$ e, portanto, o grau de f deveria ser maior do que ou igual a $n+1$, o que é falso. Logo, f tem, no máximo, n raízes em $\mathbb{K}$. ■

Por fim, para dar sentido ao conceito de derivada de um polinômio sobre um corpo $\mathbb{K}$ qualquer mantendo a consistência com os resultados obtidos em $\mathbb{R}$, define-se que a derivada do polinômio $f(x) = a_0 + a_1 x + a_2 x^2 \dots + a_d x^d$ é dada por $f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + d a_d x^{d-1}$. Observe que se $\partial f = d \geq 1$, então f' é não-nulo e $\partial f' = d-1$.

É interessante notar que, a partir da definição, pode-se provar propriedades das derivadas já conhecidas para o corpo dos reais: $(f \pm g)'(x) = f'(x) \pm g'(x)$ e $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.

Proposição 2.35 Seja f um polinômio em $P(\mathbb{K})$ com grau $\partial f = n \geq 1$ e $\alpha \in \mathbb{K}$ uma raiz de f com multiplicidade m. Então $m > 1$ se e somente se $f'(\alpha) = 0$.

Demonstração

Como α é raiz de f com multiplicidade m, podemos escrever o polinômio f como $f(X) = (X-\alpha)^m q(X)$, onde $q(X) \in P(\mathbb{K})$ e $q(\alpha) \neq 0$.

Derivando f, obtemos $f'(X) = m(X-\alpha)^{m-1}q(X) + (X-\alpha)^m q'(X)$.

($\Longrightarrow$) Suponha $m > 1$. Então $m-1 > 0$. Fazendo $X = \alpha$ em $f'(X)$, temos $f'(\alpha) = 0$.

($\Longleftarrow$) Suponha $f'(\alpha) = 0$. Se $m = 1$, teremos $f'(X) = q(X) + (X-\alpha)q \Rightarrow f'(\alpha) = q(\alpha) \neq 0$, contradizendo a hipótese. Logo, $m > 1$. ■

2.5
Extensões de Corpos

Nessa seção, trataremos brevemente o conceito de extensões de corpos. O objetivo é somente apresentar as definições e os resultados que nos permitem definir o fecho algébrico de um corpo. As demonstrações podem ser encontradas na bibliografia recomendada no início do capítulo.

Dado um corpo $\mathbb{K}$, uma extensão de $\mathbb{K}$ é o par $(\mathbb{L}, \iota)$ consistindo de um corpo $\mathbb{L}$ e de um monomorfismo ι de $\mathbb{K}$ em $\mathbb{L}$. Muitas vezes identificamos $\mathbb{K}$ com $\iota(\mathbb{K})$, considerando o próprio $\mathbb{K}$ um subcorpo de $\mathbb{L}$ e omitindo o monomorfismo ι.

Considere uma extensão $\mathbb{L}$ de um corpo $\mathbb{K}$. Um elemento $\alpha \in \mathbb{L}$ é dito algébrico sobre $\mathbb{K}$ se existir um polinômio não-nulo $f \in P(\mathbb{K})$ tal que $f(\alpha) = 0$. Se todo elemento de $\mathbb{L}$ é algébrico sobre $\mathbb{K}$, dizemos que $\mathbb{L}$ é *algébrico* sobre $\mathbb{K}$.

Proposição 2.36 Seja $\mathbb{K}$ um corpo finito com q elementos. Para cada inteiro positivo n, existe uma extensão algébrica de $\mathbb{K}$ com q^n elementos.

Um corpo $\mathbb{K}$ é dito algebricamente fechado quando todo polinômio em $P(\mathbb{K})$ de grau maior ou igual a 1 tem uma raiz em $\mathbb{K}$. Por fim, o fecho algébrico de $\mathbb{K}$ é um corpo algebricamente fechado e algébrico sobre $\mathbb{K}$.

Teorema 2.37 Seja $\mathbb{K}$ um corpo. Então existe um fecho algébrico de $\mathbb{K}$.

Usualmente, o fecho algébrico de $\mathbb{K}$ é denotado por $\overline{\mathbb{K}}$. Pode-se provar também que, excetuando isomorfismo natural, o fecho algébrico é único. Assim, por exemplo, o fecho algébrico de um corpo finito $\mathbb{F}_p$ é um corpo infinito enumerável $\overline{\mathbb{F}_p}$. Se q é uma potência de p, existe um único subcorpo com q elementos $\mathbb{F}_q \subset \overline{\mathbb{F}_p}$.

2.6
Polinômios em Várias Variáveis

Podemos expandir o conceito de polinômio visto na seção 2.4. Recordemos que, dado um corpo $\mathbb{K}$, podemos representar um polinômio na variável x sobre um corpo $\mathbb{K}$ pela fórmula $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$, onde os

coeficientes $a_i \in \mathbb{K}$. Cada $a_k x^k$, com $a_k \neq 0$, é um monômio de f e tem grau k. O grau do polinômio $f(x)$ é o maior grau dentre os monômios de f.

De maneira análoga, um polinômio nas variáveis $x_1, x_2, \dots, x_n$ sobre um corpo $\mathbb{K}$ é uma expressão finita da forma

$$f(x_1, x_2, \dots, x_n) = \sum_{i_1, i_2, \dots, i_n} a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n},$$

onde os coeficientes $a_{i_1 i_2 \dots i_n} \in \mathbb{K}$. Nesse caso, o grau do monômio $a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ é a soma $i_1 + i_2 + \cdots + i_n$ e o grau do polinômio $f(x_1, x_2, \dots, x_n)$ é o maior grau dos monômios que compõe o polinômio (com coeficientes $a_{i_1 i_2 \dots i_n} \neq 0$).

Exemplo 2.38 O polinômio $f(x, y, z) = x^3 y^2 z - x^2 z^2 + 3xy^2 z + z^2 + 3$ tem grau 6.

Da mesma forma como fizemos para polinômios em uma variável, podemos definir as derivadas parciais $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$, etc para polinômios em mais de uma variável sobre o corpo $\mathbb{K}$ (outra notação comum para derivadas parciais é f_x,f_y,etc). A mesma ideia é aplicada para obtermos derivadas de ordem mais alta.

Exemplo 2.39 Seja $f(x, y, z) = x^3 y^2 z - x^2 z^2 + 3xy^2 z + z^2 + 3$. Então $f_x(x, y, z) = 3x^2 y^2 z - 2xz^2 + 3y^2 z$, $f_y(x, y, z) = 2x^3 yz + 6xyz$ e $f_z(x, y, z) = x^3 y^2 - 2x^2 z + 3xy^2 + 2z$.

2.7
Polinômios Homogêneos

Considere um polinômio F de grau d nas variáveis $x_1, x_2, \dots, x_n$ sobre um corpo $\mathbb{K}$. Dizemos que F é um *polinômio homogêneo* se todo monômio de F tem grau d.

Exemplo 2.40 $F(x, y, z) = 4x^2 + 9y^2 - 3z^2$ é um polinômio homogêneo de grau 2.

Exemplo 2.41 $G(x, y) = x^4 - x^2 y^2 + xy^3$ é homogêneo de grau 4.

Um polinômio qualquer F de grau d pode ser escrito como a soma de polinômios homogêneos, i.e., $F = F_0 + F_1 + \cdots + F_d$, onde cada F_k é um polinômio homogêneo de grau k. Como exemplo, considere o polinômio $F(x, y, z) = x^3y^2z - x^2z^2 + 3xy^2z + z^2 + 3$. Tomando $F_6 = x^3y^2z$, $F_4 = -x^2z^2 + 3xy^2z$, $F_2 = z^2$ e $F_0 = 3$, temos que $F = F_6 + F_4 + F_2 + F_0$.

Proposição 2.42 Seja $F(x_1, x_2, \ldots, x_n)$ um polinômio de grau d sobre um corpo $\mathbb{K}$. Então F é um polinômio homogêneo se, e somente se, para todo $t \in \mathbb{K}$, temos

$$F(tx_1, tx_2, \ldots, tx_n) = t^d F(x_1, x_2, \ldots, x_n)$$

Demonstração

($\Longrightarrow$) Se F é um polinômio homogêneo de grau d, ao multiplicarmos as variáveis de F por t, o monômio $a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ de F torna-se $t^d a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$. Como $i_1 + i_2 + \cdots + i_n = d$ para todo monômio de F, temos que $F(tx_1, tx_2, \ldots, tx_n) = t^d F(x_1, x_2, \ldots, x_n)$.

($\Longleftarrow$) Suponha agora que $F(tx_1, tx_2, \ldots, tx_n) = t^d F(x_1, x_2, \ldots, x_n)$. Podemos escrever F como a soma de polinômios homogêneos:

$$F = F_0 + F_1 + \cdots + F_d.$$

Como F_k é homogêneo, temos que $F_k(tx_1, tx_2, \ldots, tx_n) = t^k F_k(x_1, x_2, \ldots, x_n)$. Então, podemos escrever

$$t^d F = F(tx_1, tx_2, \ldots, tx_n) = F_0 + tF_1 + \cdots + t^d F_d,$$

ou seja, temos que $F_0 + tF_1 + \cdots + t^d(F_d - F) = 0$. Podemos enxergar essa última equação como um polinômio na variável t sobre o domínio de integridade $\mathbb{K}[x_1, \ldots, x_n]$ com infinitos zeros, logo ele é o polinômio identicamente nulo. Daí, segue que $F = F_d$ e, portanto, F é um polinômio homogêneo. ■

3
CURVAS ALGÉBRICAS PLANAS E O PLANO PROJETIVO

O presente capítulo tem por finalidade apresentar a teoria básica de curvas algébricas planas, incluindo retas tangentes, espaço projetivo e coordenadas projetivas. Faremos uma breve introdução usando o conjunto dos reais e então generalizamos para corpos quaisquer. Os temas abordados são essenciais para uma melhor compreensão da teoria de curvas elípticas, pois é utilizado desde o princípio conceitos como "pontos no infinito". Além disso, o tema enriquece o estudo de outras curvas, como as cônicas, cujo estudo usualmente é iniciado sem o uso de pontos no infinito. Para uma discussão mais aprofundada sobre curvas algébricas planas sugerimos Gibson (1998).

3.1
Curvas Algébricas Planas

Como já estamos habituados com o plano afim $\mathbb{R}^2$, antes de proceder com a definição de curvas algébricas sobre corpos quaisquer, vamos verificar o que seria uma curva algébrica plana real. Uma curva algébrica plana real é representada por um polinômio não-nulo $f(x,y)$ sobre $\mathbb{R}$. O *traço* dessa curva é o conjunto de pontos $(x,y) \in \mathbb{R}^2$ satisfazendo $f(x,y) = 0$. Observe que multiplicar f por uma constante diferente de zero não altera o traço da curva nem o grau do polinômio, por isso diremos que $f(x,y)$ e $t \times f(x,y)$, $t \neq 0$, representam a mesma curva algébrica.

Observação 3.1 É comum usarmos o termo "curva" para nos referirmos ao seu traço, no entanto o contexto deve deixar claro quando estamos de fato falando sobre o traço $[f(x,y) = 0]$ ou sobre a curva $[f(x,y)]$. Essa distinção é importante porque duas curvas diferentes podem ter o mesmo traço como, por exemplo, as curvas reais $x^2 + y^2 = -1$ e $x^4 + y^4 = -1$.

Dada a definição acima, percebe-se que já estamos habituados a trabalhar com curvas algébricas planas reais. Por exemplo, uma reta em $\mathbb{R}^2$, cuja equação é

dada por $ax + by + c = 0$ onde os coeficientes são reais, é uma curva algébrica plana real. Além disso, temos as cônicas, cúbicas, dentre outras curvas.

Da mesma forma como fizemos com o corpo $\mathbb{R}$, definimos uma curva algébrica plana sobre o corpo $\mathbb{K}$ como um polinômio não-nulo $f(x, y)$ sobre $\mathbb{K}$, a menos da multiplicação por um escalar não nulo, ou seja, os polinômios $t \times f(x, y)$, $t \neq 0$, representam a mesma curva algébrica plana (ou, abreviando, curva). O *traço* da curva é o conjunto $\{(x, y) \in \mathbb{K}^2 \mid f(x, y) = 0\}$ e seu *grau* é o grau do polinômio.

Da mesma maneira que definimos uma curva real no plano $\mathbb{R}^2$, para tornar o conceito de curva algébrica sobre $\mathbb{K}$ consistente com $\mathbb{R}$ deveríamos abordar com mais detalhes o que torna $\mathbb{K}^2$ em um plano afim como $\mathbb{R}^2$. Sugerimos a bibliografia indicada para uma discussão mais aprofundada, mas o ponto principal é que, ao definirmos uma reta em $\mathbb{K}^2$ como o subconjunto de pontos

$$\{(x, y) \in \mathbb{K}^2 : ax + by + c = 0\}$$

em que a, b, $c \in \mathbb{K}$ e $a \neq 0$ ou $b \neq 0$, temos todas as "propriedades geométricas" que definem um plano afim:

a) existem pelo menos três pontos não colineares (por exemplo, $(0,0)$, $(1,0)$ e $(0,1)$);

b) dados dois pontos distintos P, Q de $\mathbb{K}^2$, existe uma única reta l em $\mathbb{K}^2$ que passa por P e Q; e

c) dados uma reta l e um ponto P em $\mathbb{K}^2$, existe uma única reta paralela a l passando por P.

Observação 3.2 Apesar de a definição ser coerente com aquelas utilizadas nos corpos mais comuns ($\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$), cabe observar que algumas propriedades geométricas são perdidas no processo de generalização. Por exemplo, não é claro como os conceitos geométricos de distância e ângulo seriam definidos de modo geral.

Exemplo 3.3 Considere $\mathbb{K}$ sendo o corpo (finito) $\mathbb{F}_3 = \{0,1,2\}$. Existem nove pontos em $\mathbb{K}^2$: $(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1)$ e $(2,2)$. Lembrando que ao multiplicar o polinômio por um escalar obtemos a mesma

curva, temos as seguintes retas $ax + by + c = 0$ em $\mathbb{K}^2$ ($a, b, c \in \mathbb{K}$ e a,b não se anulam simultaneamente):

$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	**Reta** $\boldsymbol{ax + by + c = 0}$	**Reta equivalente**
0	1	0	$y = 0$	$2y = 0$
0	1	1	$y + 1 = 0$	$2y + 2 = 0$
0	1	2	$y + 2 = 0$	$2y + 1 = 0$
1	0	0	$x = 0$	$2x = 0$
1	0	1	$x + 1 = 0$	$2x + 2 = 0$
1	0	2	$x + 2 = 0$	$2x + 1 = 0$
1	1	0	$x + y = 0$	$2x + 2y = 0$
1	1	1	$x + y + 1 = 0$	$2x + 2y + 2 = 0$
1	1	2	$x + y + 2 = 0$	$2x + 2y + 1 = 0$
1	2	0	$x + 2y = 0$	$2x + y = 0$
1	2	1	$x + 2y + 1 = 0$	$2x + y + 2 = 0$
1	2	2	$x + 2y + 2 = 0$	$2x + y + 1 = 0$

Tabela 1: Retas em $\mathbb{K}^2$, onde $\mathbb{K} = \mathbb{F}_3 = \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$

Observe que cada reta $ax + by + c = 0$ possui uma reta equivalente (mostrada na última coluna da tabela 1) obtida ao multiplicarmos a equação da reta pelo escalar 2 (por exemplo, $2 \times (x + 2y + 1) = 2x + y + 2$). Portanto, existem doze retas distintas em $\mathbb{K}^2$. Graficamente, enxergar essas retas foge um pouco da intuição. Por exemplo, considere a reta $x + 2y + 1 = 0$ (ou equivalentemente $2x + y + 2 = 0$). Os três pontos de $\mathbb{K}^2$ na reta são $P_1 = (0,1)$, $P_2 = (2,0)$ e $P_3 = (1,2)$. Em $\mathbb{R}^2$, claramente esses pontos são não colineares (ver figura 2), no entanto, se tomarmos as equações das retas que conectam esses três pontos dois-a-dois, temos de verificar que tais equações são equivalentes em $\mathbb{K}^2$:

$(r1)$ Reta P_1P_2: $x + 2y - 2 = 0$

$(r2)$ Reta P_1P_3: $x - y + 1 = 0$

$(r3)$ Reta P_2P_3: $2x + y - 4 = 0$

Para ver que as equações de $(r1)$, $(r2)$ e $(r3)$ são equivalentes, basta observar que, em $\mathbb{K} = \mathbb{F}_3$, temos $-2 = 1$ e $-4 = -1 = 2$. Assim, as equações tornam-se:

$(r1')$ Reta P_1P_2: $x + 2y + 1 = 0$

$(r2')$ Reta P_1P_3: $x + 2y + 1 = 0$

$(r3')$ Reta P_2P_3: $2x + y + 2 = 0$

E, conforme a tabela 1, essas retas são equivalentes em $\mathbb{K}^2$. No capítulo 6, discutiremos uma outra maneira de desenhar e interpretar gráficos de retas sobre corpos finitos.

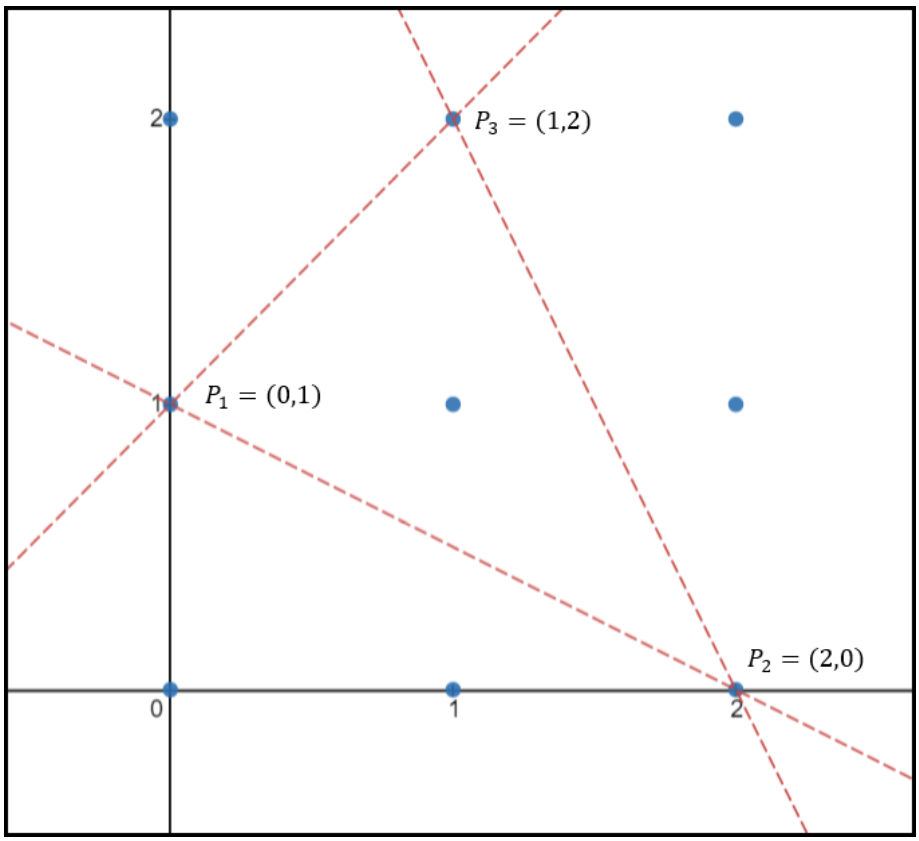

Figura 2: Pontos em $\mathbb{K}^2$, onde $\mathbb{K} = \mathbb{F}_3 = \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$

Em geometria diferencial, dizemos que a curva real de equação $f(x, y) = 0$ é real-suave quando não existe $(x, y) \in \mathbb{R}^2$ tal $f_x(x, y) = 0$ e $f_y(x, y) = 0$. Em geometria algébrica, entretanto, é muito importante considerar o fecho algébrico do corpo. Sabemos que o fecho algébrico de $\mathbb{R}$ é $\mathbb{C}$, conjuntos dos números complexos. Assim, diremos que a curva definida pela equação $f(x, y) = 0$ definida em $\mathbb{R}^2$ é *suave* (ou não-singular) se e somente se não existe $(x, y) \in \mathbb{C}^2$ tal que $f_x(x, y) = 0$ e $f_y(x, y) = 0$.

Da mesma maneira, quando a curva $f(x,y)=0$ está definida em $\mathbb{K}^2$, diremos que ela é suave se e somente se não existe $(x,y) \in \overline{\mathbb{K}}^2$ tal que $f_x(x,y)=0$ e $f_y(x,y)=0$, onde $\overline{\mathbb{K}}$ é o fecho algébrico de $\mathbb{K}$.

Os pontos $P=(a,b)$ de uma curva algébrica de equação $f(x,y)=0$ em que podemos traçar uma única reta tangente são ditos pontos simples ou pontos de multiplicidade 1 e a equação da reta tangente é dada por

$$(x-a)f_x(P)+(y-b)f_y(P)=0 \qquad (1)$$

em que f_x e f_y são as derivadas parciais de $f(x,y)$ com relação à x e à y, respectivamente. Lembre-se da seção 2.6 que as derivadas são definidas algebricamente. Observe que, de acordo com a equação (1), a reta só estará definida se $f_x(P) \neq 0$ ou $f_y(P) \neq 0$.

O objetivo desse trabalho é tratar sobre curvas elípticas, que são curvas algébricas descritas pela equação $f(x,y)=y^2-x^3-Ax-B=0$, em que os coeficientes A e B são elementos de um corpo. Uma propriedade requerida para as curvas de interesse é que seja possível traçar uma única reta tangente em cada ponto da curva, ou seja, a curva deve ser suave. Para curvas elípticas, a suavidade permite definir uma operação de grupo entre os pontos da curva.

Exemplo 3.4 Dada a curva $f(x,y)=y^2-x^3-Ax-B$, temos que $f_x(x,y)=-3x^2-A$ e $f_y(x,y)=2y$. Dessa forma, a reta tangente à curva no ponto (x_1,y_1) é dada pela equação $(x-x_1)(-3x_1^2-A)+(y-y_1)(2y_1)=0$, que, isolando a variável y, pode ser reescrita como $y=\frac{3x_1^2+A}{2y_1}x+(y_1-\frac{3x_1^2+A}{2y_1}x_1)$.

3.2
Plano Projetivo e Pontos no Infinito

Existem algumas maneiras de construir o Plano Projetivo, vamos descrever uma construção somente, no entanto pode-se provar que elas são equivalentes (SILVERMAN; TATE, 2015).

Começaremos o tópico com a noção de coordenadas homogêneas. Considere um corpo $\mathbb{K}$ e considere triplas $(x,y,z) \in \mathbb{K}^3$ não-nulas, ou seja, $(x,y,z) \neq (0,0,0)$. Diremos que duas triplas (x_1,y_1,z_1) e (x_2,y_2,z_2) são

equivalentes se existe $t \in \mathbb{K}, t \neq 0$, tal que $(x_1, y_1, z_1) = (tx_2, ty_2, tz_2)$. Nesse caso, escrevemos $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$.

Pode-se facilmente mostrar que a relação $\sim$ acima é uma relação de equivalência, isto é, reflexiva, simétrica e transitiva. Representamos a classe de equivalência que contém a tripla (x, y, z) por $(x: y: z)$.

Definimos, então, o plano projetivo $P\mathbb{K}^2$ como o conjunto das classes de equivalência de triplas $(x: y: z) \in \mathbb{K}^3 \backslash \{(0,0,0)\}$. Nesse contexto, a classe de equivalência $(x: y: z)$ é chamada de ponto.

Exemplo 3.5 Uma reta no plano projetivo $P\mathbb{K}^2$ é o conjunto de pontos $(a: b: c)$ em $P\mathbb{K}^2$ satisfazendo a equação $\alpha X + \beta Y + \gamma Z = 0$, em que $\alpha, \beta, \gamma \in \mathbb{K}$. Observe que, conforme esperado, se $(a: b: c)$ satisfaz a equação, então $(ta: tb: tc)$ também a satisfaz para qualquer $t \neq 0$. Portanto, qualquer representante da classe de equivalência pode ser utilizado para verificar se o ponto pertence à reta.

Conforme vimos na seção anterior, uma curva algébrica no plano afim $\mathbb{K}$ é dada pelo conjunto de soluções de uma equação polinomial em duas variáveis: $f(x, y) = 0$. Quando tratamos de curvas no plano projetivo, uma vez que seus pontos têm três coordenadas, é natural que sejam utilizados polinômios com três variáveis: $F(X, Y, Z) = 0$. Além disso, um ponto em $P\mathbb{K}^2$ é uma classe de equivalência, o que significa que qualquer representante da classe pode ser utilizado, por isso estamos interessados em polinômios com a seguinte propriedade: $F(X, Y, Z) = 0$ se, e somente se, $F(tX, tY, tZ) = 0$ para todo $t \neq 0$. Os polinômios homogêneos introduzidos na seção 2.7 satisfazem essa propriedade. Assim, uma curva algébrica no plano projetivo é dada pelo conjunto de soluções de uma equação polinomial $F(X, Y, Z) = 0$ em que F é um polinômio homogêneo.

Exemplo 3.6 Seja $\mathbb{K}$ um corpo e $P\mathbb{K}^2$ o plano projetivo associado à $\mathbb{K}$. A curva dada pela equação $Y^2Z - X^3 - AXZ^2 - BZ^3$ é um exemplo de curva algébrica em $P\mathbb{K}^2$.

Se $(X:Y:Z)$ é uma classe tal que $Z \neq 0$, então existe uma única tripla na forma $(x, y, 1)$ tal que $(X:Y:Z) \sim (x:y:1)$. Essa tripla é claramente dada por $(X/Z:Y/Z:1)$. As triplas em que $Z \neq 0$ são chamadas de "pontos finitos" em $P\mathbb{K}^2$. O conjunto dos pontos finitos em $P\mathbb{K}^2$ está em bijeção natural com o plano afim $\mathbb{K}^2$. Se, por outro lado, $Z = 0$, a divisão por Z resultaria em fazer X e/ou Y tender(em) ao infinito. Por isso, os pontos $(X:Y:0)$ são denominados "pontos no infinito" em $P\mathbb{K}^2$.

É interessante notar que também existe um mapeamento natural entre pontos de curvas algébricas em $\mathbb{K}^2$ e pontos finitos de curvas algébricas em $P\mathbb{K}^2$. Para isso, dada uma curva algébrica de equação $f(x, y) = 0$, basta "inserir" potências de z em seus termos de modo a transformar f em um polinômio homogêneo.

Exemplo 3.7 Seja $f(x, y) = y^2 - x^3 - 3xy + 2$, sua forma homogênea será $F(X, Y, Y) = Y^2Z - X^3 - 3XYZ + 2Z^3$.

De modo mais formal, a bijeção entre as curvas $f(x, y)$ em $\mathbb{K}^2$ e $F(X, Y, Z)$ em $P\mathbb{K}^2$ é dada pelas equações

$$F(X, Y, Z) = Z^{\mathrm{n}} f(\frac{X}{Z}, \frac{Y}{Z})$$

e

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

onde n é o grau do polinômio f.

Observação 3.8 O plano projetivo e os pontos no infinito tornam mais concretas algumas afirmações como "duas retas paralelas se encontram no infinito". Por exemplo, considere as duas retas paralelas dadas pelas equações abaixo:

$$(r1)\ y - 2x - 1 = 0$$
$$(r2)\ 2y - 4x + 3 = 0$$

Suas equações no plano projetivo são dadas por

$$(R1)\ Y - 2X - Z = 0$$
$$(R2)\ 2Y - 4X + 3Z = 0$$

Os pontos no infinito são aqueles em que $Z = 0$. Dessa forma, temos que, em $(R1)$, $Z = 0 \Longrightarrow Y - 2X = 0 \Longrightarrow Y = 2X$. Nesse caso, o ponto no infinito é dado

por $(X: 2X: 0)$ ou, como basta escolher qualquer representante da classe de equivalência, por $(1: 2: 0)$. Para $(R2)$, temos $Z = 0 \Longrightarrow 2Y - 4X = 0 \Longrightarrow Y = 2X$. Ou seja, o ponto no infinito em $(R2)$ também é dado por $(1: 2: 0)$. Logo, $(R1)$ e $(R2)$ se encontram no infinito.

4
CURVAS ELÍPTICAS REAIS

Esse capítulo tem por objetivo apresentar a noção de Curva Elíptica utilizando o corpo dos números reais. Optou-se por essa abordagem porque, no conjunto dos reais, é possível mostrar alguns conceitos com auxílio da geometria e cálculo, facilitando o desenvolvimento do tema. Nos capítulos seguintes, faremos generalizações da teoria para corpos quaisquer.

4.1
Curvas Elíptica sobre $\mathbb{R}$

Considere o conjunto dos números reais $\mathbb{R}$. Uma curva elíptica E sobre $\mathbb{R}$ é o conjunto de pontos que satisfazem a equação

$$y^2 = x^3 + Ax + B, \tag{2}$$

onde $x, y, A, B \in \mathbb{R}$. Por definição, a curva elíptica E contém um ponto adicional $\mathcal{O}$, denominado ponto no infinito, que será formalmente definido na seção 5.3.

Escrevemos $E(\mathbb{R})$ para representar os pontos da curva elíptica, que são pontos em $\mathbb{R}^2$ satisfazendo a equação (2) mais o ponto no infinito $\mathcal{O}$, i.e.,

$$E(\mathbb{R}) = \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + Ax + B\}.$$

Observação 4.1 Definiremos o ponto no infinito $\mathcal{O}$ no próximo capítulo. Ainda que tenhamos tal definição, veremos que, ao trabalharmos no plano afim, o ponto no infinito é uma entidade muita abstrata, de forma que a melhor maneira de o enxergar é como um símbolo que satisfaz algumas regras computacionais. Por exemplo, toda reta vertical no plano ($x = c$) intersecta a curva elíptica no ponto $\mathcal{O}$.

Diferentemente da maioria dos corpos, quando a curva elíptica está definida sobre $\mathbb{R}$, podemos visualizar o gráfico da curva. O gráfico de uma curva elíptica pode assumir algumas formas características dependendo das raízes do polinômio cúbico $Q(x) = x^3 + Ax + B$. A figura 4.1 contém um exemplo de cada um dos casos possíveis: (a) uma raiz real, (b) três raízes reais distintas, (c) duas raízes reais distintas sendo uma com multiplicidade dois e, por último, (d) uma raiz real com multiplicidade três.

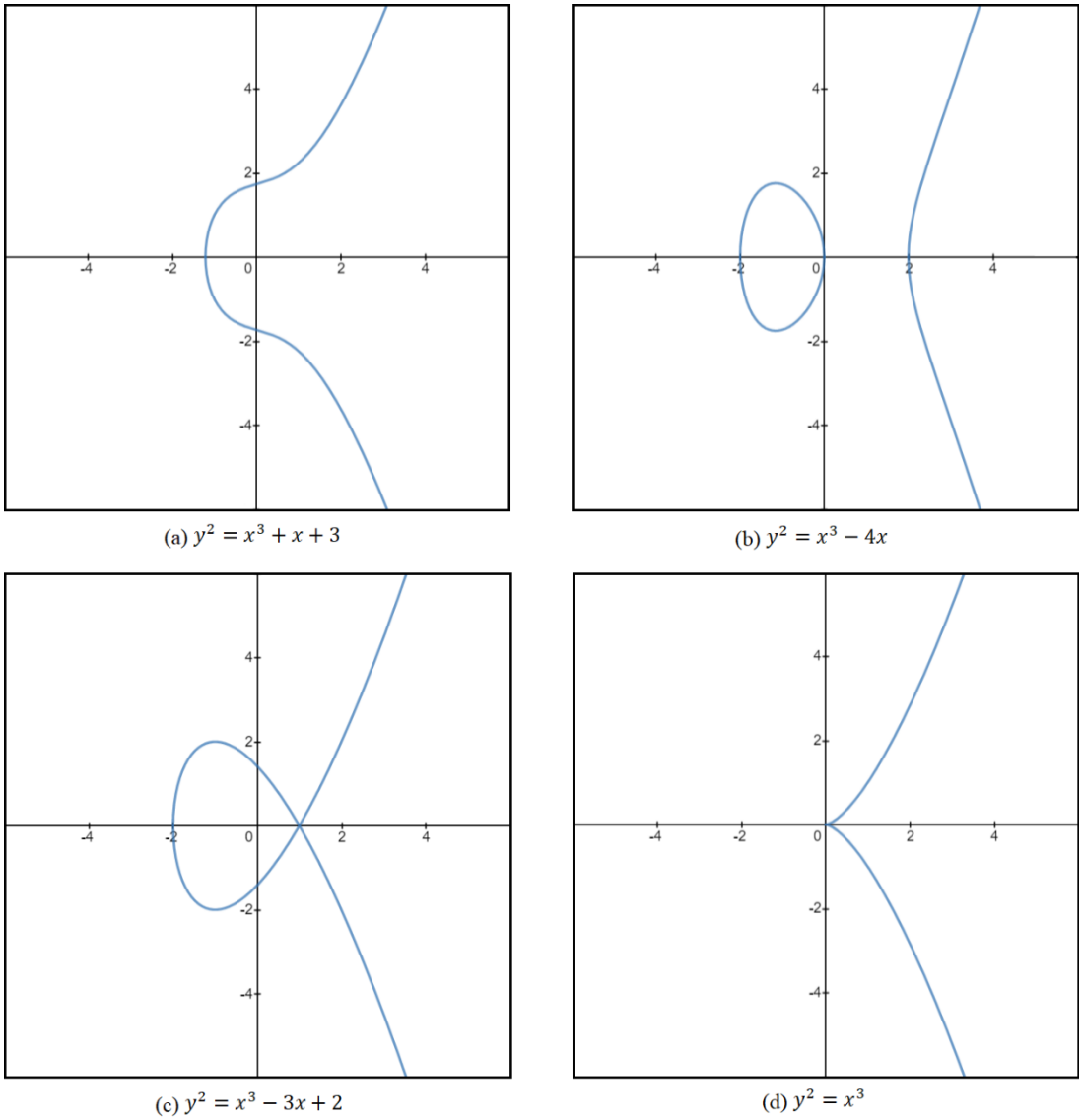

Figura 3: Gráfico de curvas elípticas sobre o conjunto dos números reais

Observe que o eixo x é um eixo de simetria da curva, isto é, se $(x, y) \in E$ então $(x, -y) \in E$.

4.2
Soma de Pontos em uma Curva Elíptica (Lei de Grupo)

Quando conhecemos alguns pontos da curva elíptica, podemos obter novos pontos utilizando um método geométrico. Para entender o processo, considere a curva elíptica sobre $\mathbb{R}$ dada pela equação $E: y^2 = x^3 - 4x$ e sejam $P_1 = (0,0)$ e $P_2 = (4,4\sqrt{3})$ pontos da curva. A reta r que passa por P_1 e P_2 é dada pela equação $y = x\sqrt{3}$.

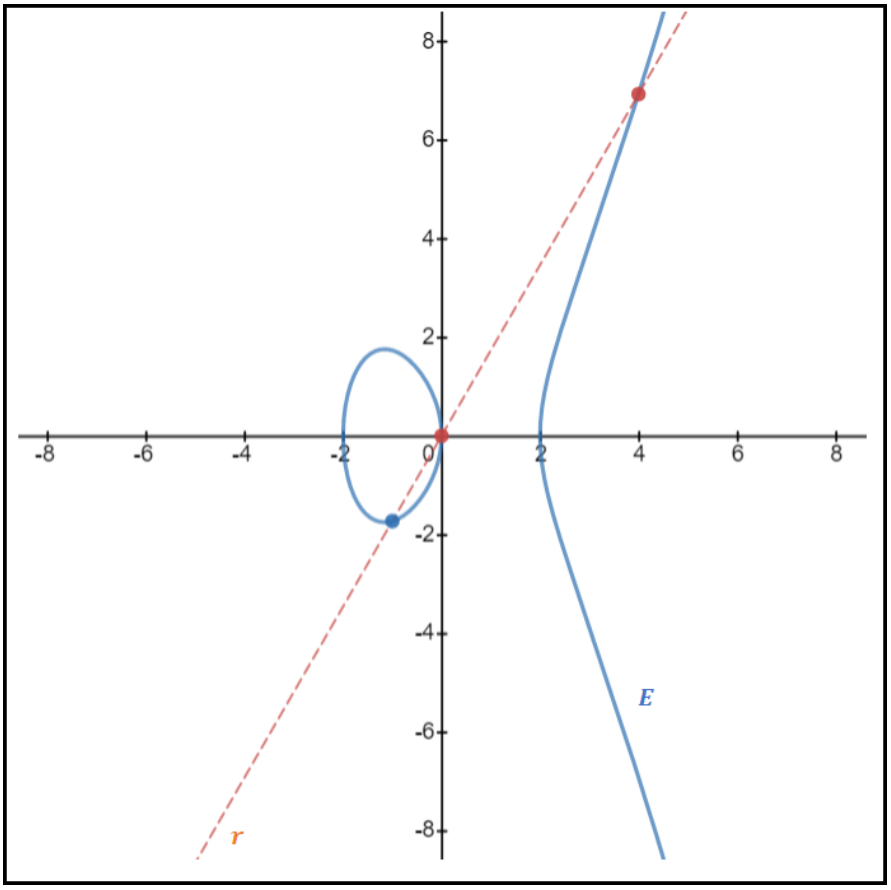

Figura 4: Interseção da Curva Elíptica $\boldsymbol{E}$ com a reta $\boldsymbol{r}$

Para encontrar todos os pontos que pertencem à interseção da curva elíptica E com a reta r (figura 4), substituímos a equação da reta r na equação de E:

$$\left(x\sqrt{3}\right)^2 = x^3 - 4x \Longrightarrow 3x^2 = x^3 - 4x \Longrightarrow x^3 - 3x^2 - 4x = 0$$

Apesar de ser um polinômio de grau 3, encontrar suas raízes é fácil pois já conhecemos dois pontos na interseção: P_1 e P_2. Logo, $x_1 = 0$ e $x_2 = 4$ são raízes do polinômio. Denotando por x_3 a última raiz, temos $x_1 + x_2 + x_3 = -(-3) = 3 \Longrightarrow 0 + 4 + x_3 = 3 \Longrightarrow x_3 = -1$. Substituindo x_3 na equação da reta r (ou da curva E), obtemos $y_3 = -\sqrt{3}$. Portanto, como a curva é simétrica em relação ao eixo x, encontramos dois novos pontos da curva elíptica: $(-1, \pm\sqrt{3})$. Com novos pontos conhecidos, poderíamos repetir o processo e obter mais pontos.

E se conhecêssemos somente um ponto $P = (x, y)$ da curva elíptica E? Nesse caso, podemos traçar a reta tangente à curva no ponto P. A diferença é que o ponto P seria uma interseção com "multiplicidade 2" e sua coordenada x seria uma raiz dupla do polinômio cúbico obtido.

O processo descrito acima para obtenção de novos pontos de uma curva elíptica nos dá a possibilidade de definirmos uma operação entre os pontos de uma curva elíptica E.

Seja $E(\mathbb{R})$ uma curva elíptica e considere dois pontos satisfazendo a equação da curva: $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$. A soma $P_1 + P_2$ é definida da seguinte maneira:

(i) Trace a reta que passa por P_1 e P_2. Essa reta encontrará a curva em um ponto $P_3' = (x_3', y_3')$;

(ii) Ache o ponto $P_3 = (x_3, y_3)$, simétrico a $P_3{}'$ em relação ao eixo de simetria da curva;

(iii) Defina $P_3 = P_1 + P_2$.

A figura 5 exemplifica graficamente a soma $P_3 = P_1 + P_2$. É importante deixar claro que, como vimos acima, essa operação não equivale a somar coordenadas.

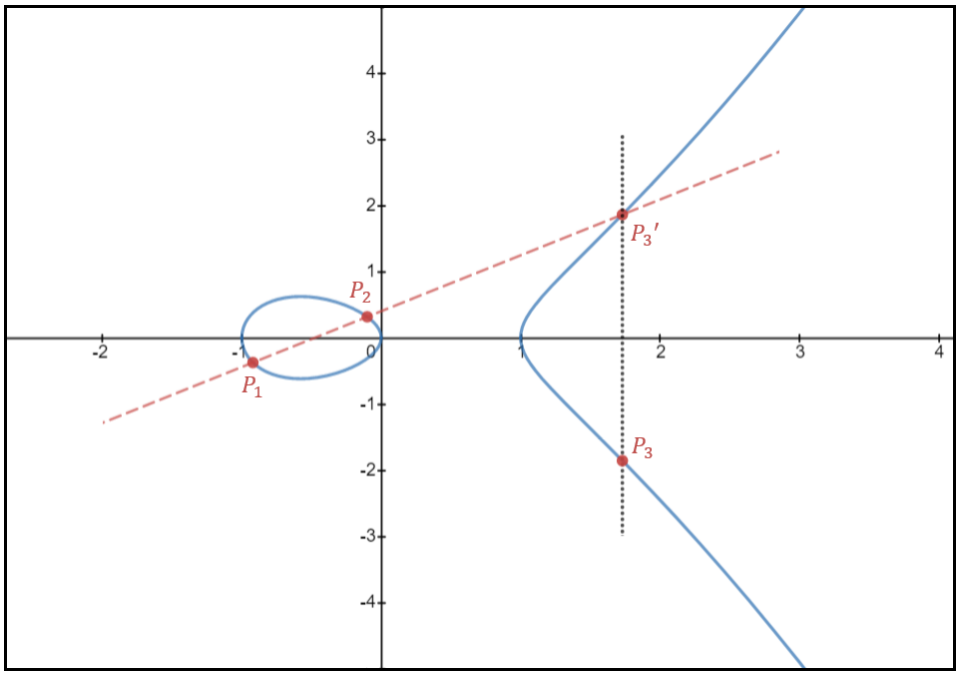

Figura 5: Soma de dois pontos distintos em uma curva elíptica

Agora tornaremos explícitos os cálculos realizados para somar os pontos de curvas elíptica sobre $\mathbb{R}$, dividindo a operação em casos para facilitar a compreensão. Lembremos que a equação da curva elíptica é dada por $y^2 = x^3 + Ax + B$ e que toda reta vertical $x = c$ intersecta a curva elíptica no ponto $\mathcal{O}$.

- Caso 1: $P_1, P_2 \neq \mathcal{O}$ e $P_1 \neq P_2$

  - Caso 1.1: $x_1 \neq x_2$ (figura 5)

  A reta r que passa por P_1 e P_2 tem coeficiente angular dado por

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

  Portanto, a equação da reta r será

$$r : y = m(x - x_1) + y_1$$

  Para encontrar a interseção entre a curva e a reta, substituímos a equação da reta r na equação da curva E, desta forma obteremos

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B \iff$$

$$x^3 - m^2x^2 + (A + 2m^2x_1 - 2m)x + (B - m^2x_1^2 + 2mx_1 - y_1^2) = 0$$

  Conhecemos duas raízes dessa equação (a saber, x_1 e x_2) e sabemos também que a soma das raízes é $-(-m^2)$. Logo,

$$x_1 + x_2 + x_3{}' = m^2 \iff x_3{}' = m^2 - x_1 - x_2;$$

  Substituindo $x_3{}'$ na equação da reta r:

$$y_3{}' = m(x_3{}' - x_1) + y_1.$$

  Refletindo o ponto $P_3{}' = (x_3', y_3')$ em relação ao eixo x, obtemos

$$P_3 = P_1 + P_2 = (x_3, y_3) \text{ com } \begin{cases} x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases}$$

  - Caso 1.2: $x_1 = x_2$

  Nesse caso, a reta que passa por P_1 e P_2 será vertical (reta $x = x_1$). Toda reta vertical cruza com a curva E no infinito, ou seja, no ponto $\mathcal{O}$. Refletindo o ponto $\mathcal{O}$ em relação ao eixo x, encontramos novamente o ponto $\mathcal{O}$. Portanto,

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

- Caso 2: $P_1 = P_2 \neq \mathcal{O}$

  Nesse caso, traçar a reta por P_1 e P_2 significa traçar a reta tangente ao ponto.

  Utilizando os conceitos de curvas algébricas desenvolvidos no capítulo 3, reescrevemos a equação da curva como $f(x, y) = y^2 - x^3 - Ax - B = 0$ e usamos a equação $f_y(x_1, y_1) \times (y - y_1) + f_x(x_1, y_1) \times (x - x_1) = 0$ para a reta tangente à curva no ponto $P_1 = (x_1, y_1)$.

Como $f_y(x_1, y_1) = 2y_1$ e $f_x(x_1, y_1) = -3x_1^2 - A$, a equação da reta tangente é dada por $2y_1(y - y_1) - (3x_1^2 + A)(x - x_1) = 0$.

Há dois a casos a serem considerados.

- Caso 2.1: $y_1 = 0$

Nesse caso, teremos $x = x_1$ (como veremos, $y_1 = 0 \Longrightarrow 3{x_1}^2 + A \neq 0$). Portanto, a reta tangente será vertical e teremos $P_1 + P_2 = 2P_1 = \mathcal{O}$.

- Caso 2.2: $y_1 \neq 0$ (figura 6)

Temos:

$$y = y_1 + \frac{3x_1^2 + A}{2y_1}(x - x_1) = mx + (y_1 - mx_1), \text{ onde } m = \frac{3x_1^2 + A}{2y_1}.$$

Uma sequência de cálculos similar ao caso 1.1 nos leva às seguintes equações

$$P_3 = P_1 + P_2 = (x_3, y_3) \text{ com } \begin{cases} x_3 = m^2 - 2x_1 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases}$$

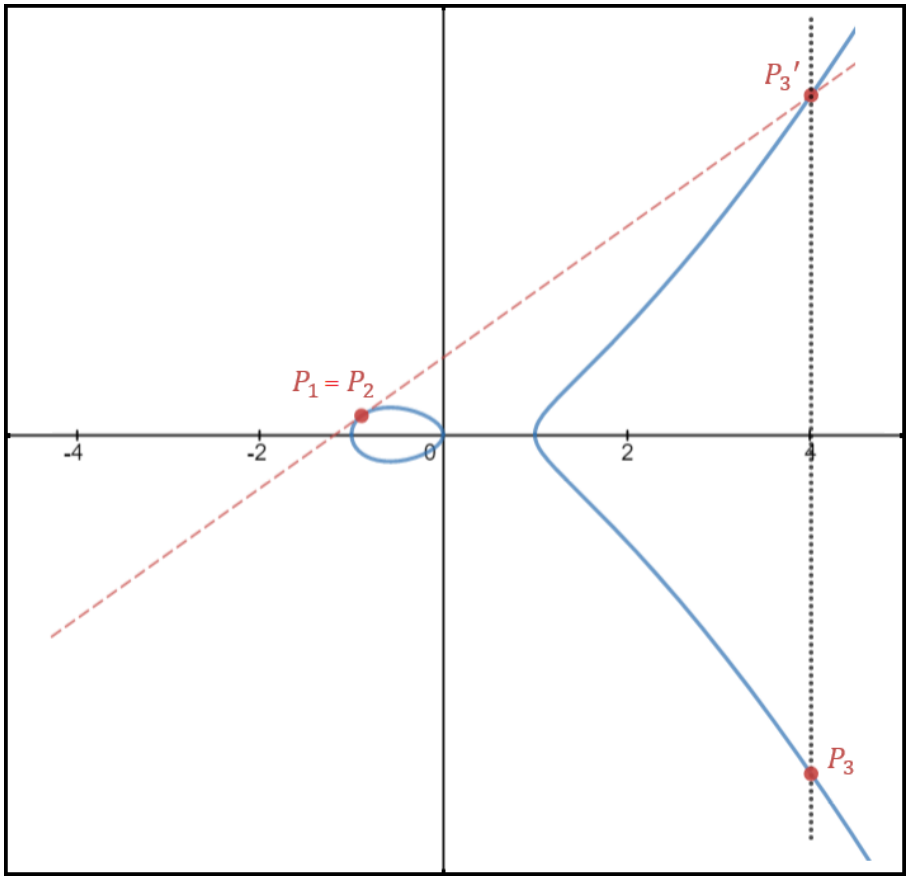

Figura 6: Soma de dois iguais pontos em uma curva elíptica

- Caso 3: $P_2 = \mathcal{O}$ (ou, equivalentemente, $P_1 = \mathcal{O}$)

A reta através de P_1 e $\mathcal{O}$ intersecta a curva E no ponto $-P_1$, o simétrico de P_1 em relação ao eixo x. Refletindo $-P_1$ em relação a x, encontramos o próprio ponto P_1. Portanto,

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

Por definição, esse resultado vale inclusive quando $P_1 = \mathcal{O}$, ou seja,

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

A tabela 2 sintetiza os resultados obtidos para a operação soma dos pontos $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ da curva elíptica $E(\mathbb{R})$: $y^2 = x^3 + Ax + B$.

Caso 1.1	$P_1 \neq \mathcal{O}$ $P_2 \neq \mathcal{O}$	$P_1 \neq P_2$	$x_1 \neq x_2$	$P_1 + P_2 = P_3(x_3, y_3)$: $\begin{cases} x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases}$ em que $m = \frac{y_2 - y_1}{x_2 - x_1}$
Caso 1.2	$P_1 \neq \mathcal{O}$ $P_2 \neq \mathcal{O}$	$P_1 \neq P_2$	$x_1 = x_2$	$P_1 + P_2 = \mathcal{O}$
Caso 2.1	$P_1 \neq \mathcal{O}$ $P_2 \neq \mathcal{O}$	$P_1 = P_2$	$y_1 = 0$	$P_1 + P_2 = \mathcal{O}$
Caso 2.2	$P_1 \neq \mathcal{O}$ $P_2 \neq \mathcal{O}$	$P_1 = P_2$	$y_1 \neq 0$	$P_1 + P_2 = P_3(x_3, y_3)$: $\begin{cases} x_3 = m^2 - 2x_1 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases}$ em que $m = \frac{3{x_1}^2 + A}{2y_1}$
Caso 3	$P_1 = \mathcal{O}$	-	-	$P_1 + P_2 = P_2$
	$P_2 = \mathcal{O}$	-	-	$P_1 + P_2 = P_1$

Tabela 2: Resumo da operação soma para pontos de curvas elípticas

Exemplo 4.2 Considere o exemplo dado no início da seção: curva elíptica real E dada pela equação $y^2 = x^3 - 4x$ e pontos da curva $P_1 = (0,0)$ e $P_2 = (4,4\sqrt{3})$. O ponto $P_3 = P_1 + P_2$ pode ser encontrado usando a fórmula do caso 1.1 da tabela 2 ($P_1 \neq \mathcal{O}$, $P_2 \neq \mathcal{O}$, $P_1 \neq P_2$ e $x_1 \neq x_2$):

- $m = (y_2 - y_1)/(x_2 - x_1) = 4\sqrt{3}/4 = \sqrt{3}$
- $x_3 = m^2 - x_1 - x_2 = \left(\sqrt{3}\right)^2 - 0 - 4 = -1$
- $y_3 = m(x_1 - x_3) - y_1 = \sqrt{3}\big(0 - (-1)\big) - 0 = \sqrt{3}$

Logo, $P_3 = P_1 + P_2 = (-1, \sqrt{3})$. A figura 7 mostra graficamente a soma realizada.

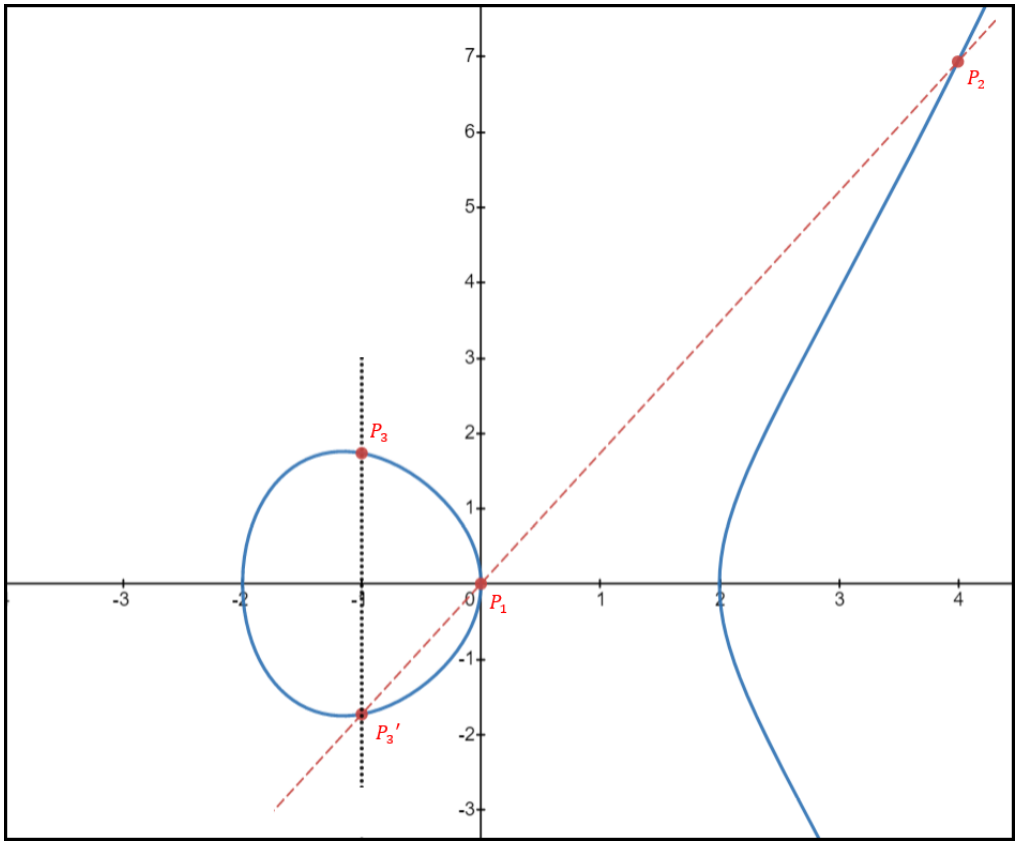

Figura 7: Soma $\boldsymbol{P_1 + P_2}$ na curva $\boldsymbol{E}(\mathbb{R})$: $\boldsymbol{y^2 = x^3 - 4x}$

Observe que se P_1 e P_2 são pontos da curva elíptica em $\mathbb{R}^2$, então o ponto $P_3 = (x_3, y_3)$ também terá coordenadas em $\mathbb{R}$, pois utilizamos somente operações que são fechadas em $\mathbb{R}$ (adição, inverso aditivo, multiplicação e inverso multiplicativo). Ou seja, $E(\mathbb{R})$ é fechado sobre a operação de adição de pontos. Com isso em mente, podemos mostrar que $E(\mathbb{R})$ munido da operação $+$ como definido acima é um grupo abeliano, conforme enunciado no teorema 4.3.

Teorema 4.3 O conjunto de pontos sobre uma curva elíptica $E(\mathbb{R})$ munido da operação de adição definida acima forma um grupo abeliano, ou seja, a adição de pontos sobre uma curva elíptica $E(\mathbb{R})$ satisfaz as seguintes propriedades:

(i) Associatividade

$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$, para todo $P_1, P_2, P_3 \in E(\mathbb{R})$

(ii) Existência do Elemento Neutro

$P + \mathcal{O} = P$, para todo $P \in E(\mathbb{R})$

(iii) Existência do Elemento Inverso

Para todo $P \in E(\mathbb{R})$, existe $P' \in E(\mathbb{R})$ tal que $P + P' = \mathcal{O}$

(iv) Comutatividade

$P_1 + P_2 = P_2 + P_1$, para todo $P_1, P_2 \in E(\mathbb{R})$

A prova das três primeiras propriedades é trivial (consequências da definição), por outro lado a prova da associatividade (usando as fórmulas da tabela 2) é muito trabalhosa em função dos diversos casos que devem ser analisados e, por este motivo, não será dada. Provas utilizando conceitos mais elaborados são dadas em Washington (2003) e Silverman (2009). Cabe destacar que o teorema nos dá uma informação interessante, pois a teoria de grupos abelianos está bastante desenvolvida.

A operação descrita acima é normalmente referida como Lei de Grupo para a Curva Elíptica. A partir da definição acima, uma questão natural é descobrir em quais curvas elípticas podemos usar a Lei de Grupo. No restante desse capítulo, mostraremos as condições necessárias para que os pontos de uma curva elíptica formem um grupo quando munidos da operação adição.

4.3
Discriminante de um Polinômio Cúbico

Inicialmente, devemos tecer algumas palavras sobre o discriminante de um polinômio cúbico $Q(x) = ax^3 + bx^2 + cx + d$, com $a \neq 0$. Vamos supor, inicialmente, que os coeficientes a, b, c e d são números reais.

Se denotarmos as raízes de $Q(x)$ por x_1, x_2 e x_3, o discriminante de $Q(x)$ é definido pela equação abaixo.

$$\Delta = a^4\,[(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2 \qquad (3)$$

Expandindo o lado direito da equação (3) e usando as relações de Girard para polinômios cúbicos[1], concluiremos facilmente que

$$\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2 \qquad (4)$$

Primeiramente, observe que se houver raízes iguais (multiplicidade 2 ou 3) então $\Delta = 0$. Além disso, o sinal do discriminante fornece informações sobre as raízes do polinômio. Se elas forem todas reais e distintas, teremos $\Delta > 0$ (o quadrado de um número real não nulo é positivo). Se somente uma raiz for real, denotando as raízes por $x_1 = \alpha + \beta i$, $x_2 = \alpha - \beta i$ e $x_3 = \gamma$, onde $\alpha, \beta, \gamma \in \mathbb{R}$, teremos

$$\Delta = [(2\beta i)(\alpha - \gamma + \beta i)(\alpha - \gamma - \beta i)]^2 \Longrightarrow$$
$$\Delta = (2\beta i)^2[(\alpha - \gamma)^2 - (\beta i)^2]^2 \Longrightarrow$$
$$\Delta = (-4\beta^2)[(\alpha - \gamma)^2 + \beta^2]^2 < 0$$

A tabela 3 mostra as conclusões obtidas para polinômios cúbicos com coeficientes em $\mathbb{R}$.

$\Delta < \mathbf{0}$	Uma raiz real e duas raízes complexas conjugadas
$\Delta = \mathbf{0}$	Três raízes reais, sendo uma com multiplicidade 2 ou 3
$\Delta > \mathbf{0}$	Três raízes reais distintas

Tabela 3: Análise do sinal do discriminante

Por fim, considerando uma curva elíptica de equação $y^2 = x^3 + Ax + B$, o discriminante do polinômio $Q(x) = x^3 + Ax + B$ pode ser trivialmente calculado a partir da equação (4). Após substituir $a = 1$, $b = 0$, $c = A$ e $d = B$, obteremos a equação (5).

$$\Delta = ((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2 = -(4A^3 + 27B^2) \qquad (5)$$

Observação 4.4 Um polinômio pode ter coeficientes em corpos diferentes de $\mathbb{R}$. Nesse caso, somente a análise do sinal do discriminante deve ser desconsiderada, pois, em outros corpos, a afirmação $\Delta > 0$ ou $\Delta < 0$ pode não fazer sentido. Observe que, ainda assim, permanece válida a conclusão de que $\Delta = 0$ quando polinômio tem raízes com multiplicidade 2 ou 3.

[1] $x_1 + x_2 + x_3 = -\frac{b}{a}$, $x_1x_2 + x_1x_3 + x_2x_3 = \frac{c}{a}$ e $x_1x_2x_3 = -\frac{d}{a}$

4.4
Curvas Suaves (ou Não-Singulares)

Na definição da Lei de Grupo para a curva elíptica, há um caso em que foi necessário calcular as derivadas parciais f_x e f_y em um ponto da curva com o objetivo de achar a reta tangente à curva. Como a operação soma deve estar definida para quaisquer dois pontos, a reta tangente à curva deve existir em cada ponto da curva elíptica.

Considere, então, uma curva elíptica E sobre o corpo $\mathbb{R}$ dada pela equação $y^2 = x^3 + Ax + B$. A equação de E pode ser reescrita como

$$f(x, y) = y^2 - x^3 - Ax - B = 0,$$

que é uma função definida em $\mathbb{R}^2$. Dado um ponto $P = (x_0, y_0) \in E$, se $f_x\,(x_0, y_0\,) \neq 0$ ou $f_y\,(x_0, y_0\,) \neq 0$, a reta tangente à curva E em P existe e sua equação é dada pela equação (1) conforme seção 3.1:

$$f_x(x_0, y_0) \times (x - x_0) + f_y(x_0, y_0) \times (y - y_0) = 0.$$

Como deve existir uma reta tangente à curva em todos os seus pontos, conclui-se que, para que possamos usar a Lei de Grupo, a curva elíptica deve ser suave. Assim, para qualquer ponto $P = (x_0, y_0) \in E$, devemos ter $f_x\,(x_0, y_0\,) \neq 0$ ou $f_y\,(x_0, y_0\,) \neq 0$. Ou seja, as derivadas parciais $f_x(x, y) = -(3x^2 + A)$ e $f_y(x, y) = 2y$ não podem se anular simultaneamente. Naturalmente, isso ocorre somente se

- $3x^2 + A = 0$; e
- $2y = 0 \iff y = 0 \iff y^2 = 0 \iff x^3 + Ax + B = 0$.

Portanto, o polinômio $Q(x) = x^3 + Ax + B$ não pode ter raízes duplas (se x é raiz dupla, então $Q(x) = Q'(x) = 0$). Note que, conforme mencionado no caso 2.1 da Lei de Grupo, em uma curva suave temos $y = 0 \Longrightarrow 3x^2 + A \neq 0$.

Sendo o discriminante do polinômio cúbico $Q(x) = x^3 + Ax + B$ com raízes x_1, x_2 e x_3 igual a

$$\Delta = a^4((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2 = -(4A^3 + 27B^2),$$

não ter raízes duplas é o mesmo que o $\Delta \neq 0$. Daí, para que a curva seja não-singular, devemos ter $4A^3 + 27B^2 \neq 0$.

Voltando aos exemplos dados na figura 3, as curvas elípticas sobre os reais (a) $y^2 = x^3 + x + 3$ e (b) $y^2 = x^3 - 4x$ são curvas não-singulares e, portanto, os conjuntos de seus pontos formam um grupo abeliano. Por outro lado, as duas

curvas (c) $y^2 = x^3 - 3x + 2$ e (d) $y^2 = x^3$ são singulares nos pontos $(1,0)$ e $(0,0)$, respectivamente, e não podemos usar a Lei de Grupo como definida na seção 4.2. Observe que os gráficos das curvas já fornecem elementos visuais das singularidades como auto interseções (4.1 (c)) e cúspides (4.1 (d)).

Observação 4.5 Considere os grupos multiplicativos $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ e $\{-1,1\}$. É possível mostrar que o grupo formado pelos pontos da curva $E(\mathbb{R}): y^2 = x^3 + x + 3$ é isormorfo a S^1 – na realidade, essa observação é válida para todas as curvas não-singulares em $\mathbb{R}$ cujo polinômio cúbico tem uma única raiz real. Analogamente, quando o polinômio cúbico possui três raízes reais distintas, o grupo formado pelos pontos da curva é isomorfo ao grupo $S^1 \times \{-1,1\}$, como é o caso da curva $E(\mathbb{R}): y^2 = x^3 - 4x$.

5
DEFINIÇÃO DE UMA CURVA ELÍPTICA

No capítulo anterior, introduzimos o conceito de curva elíptica e algumas de suas propriedades usando o conjunto dos números reais, aproveitando a familiaridade com o conjunto $\mathbb{R}$ e a intuição geométrica por trás da operação soma. Nesse capítulo, vamos generalizar a definição para que qualquer corpo $\mathbb{K}$ possa ser utilizado. Além disso, definiremos formalmente o ponto no infinito $\mathcal{O}$ e revisitaremos a Lei de Grupo para explorar algumas propriedades da operação.

5.1
A Equação de Weierstrass

Para a maioria dos corpos, assim como no caso do conjunto $\mathbb{R}$, podemos definir uma curva elíptica E sobre um corpo $\mathbb{K}$ como uma equação da forma

$$y^2 = x^3 + Ax + B, \tag{6}$$

onde $x, y, A, B \in \mathbb{K}$. Adicionamos o ponto no infinito $\mathcal{O}$ e exigimos que a condição $4A^3 + 27B^2 \neq 0$ seja satisfeita para que a curva seja suave.

Observação 5.1 Dadas as definições de curvas suaves e de retas tangentes (capítulo 3) e a restrição de existir a reta tangente em cada ponto da curva, os cálculos apresentados na seção 4.4 para $\mathbb{R}$ valem para qualquer corpo $\mathbb{K}$, ou seja, o discriminante deve ser não nulo para curva ser suave e podermos usar a Lei de Grupo.

Analogamente ao caso real, usa-se a notação $E(\mathbb{K})$ para representar os pontos da curva elíptica, que são pontos em $\mathbb{K} \times \mathbb{K}$ satisfazendo a equação (6) mais o ponto no infinito $\mathcal{O}$, i.e.,

$$E(\mathbb{K}) = \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid y^2 = x^3 + Ax + B\}$$

A equação $y^2 = x^3 + Ax + B$ é comumente chamada de *Equação de Weierstrass* para Curvas Elípticas.

5.2
A Equação Generalizada de Weierstrass

De um modo mais geral, podemos escrever a equação de uma curva elíptica $E(\mathbb{K})$, onde $\mathbb{K}$ é um corpo, na forma

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (7)$$

em que todas as variáveis e coeficientes são elementos do corpo $\mathbb{K}$. Essa equação é conhecida como *Equação Generalizada de Weierstrass*.

A equação generalizada costuma ser utilizada somente quando a característica do corpo $\mathbb{K}$ é igual a 2, pois, caso contrário, a mudança de variável $y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$ transforma a equação (7) em

$$y_1{}^2 = x^3 + a_2{}'x^2 + a_4{}'x + a_6{}', \quad (8)$$

para algumas constantes $a_2{}', a_4{}', a_6{}' \in \mathbb{K}$.

Ainda, se a característica de $\mathbb{K}$ não for 3, podemos fazer uma nova mudança de variáveis na equação (8): $x_1 = x + \frac{a_2{}'}{3}$. Essa nova mudança transforma a equação (8) na equação (6): $y^2 = x^3 + Ax + B$, onde $A, B \in \mathbb{K}$. Assim, obtemos a Equação de Weierstrass, conforme seção 5.1. Como a equação generalizada é usada somente em casos especiais, assumiremos que a característica do corpo $\mathbb{K}$ é diferente de 2 e 3 e utilizaremos somente a equação $y^2 = x^3 + Ax + B$ para curvas elípticas.

Como última observação, devemos notar que, ao utilizarmos a equação generalizada da curva elíptica $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, o eixo x deixa de ser um eixo de simetria da curva. Ainda assim, dado um ponto $P = (x, y)$ na curva, existe um $P' = (x, y')$ da curva que possui a mesma coordenada x. Nesse caso, é fácil mostrar que $y' = -a_1x - a_3 - y$. Para ver tal fato, basta observar que, dado $P = (x, y) \in E(\mathbb{K})$, o ponto $P' = (x, y')$ de mesma coordenada x pode ser encontrado através de uma equação de 2º grau em y cuja soma das raízes é $y + y' = -(a_1x + a_3)$. Ou seja, $y' = -a_1x - a_3 - y$. Essa observação é importante para realizar a soma de pontos da curva elíptica (Lei de Grupo) quando utilizamos a equação generalizada.

5.3
O Ponto no Infinito de uma Curva Elíptica

Agora tornaremos mais claro o conceito de ponto no infinito de uma curva elíptica. Sejam $\mathbb{K}$ um corpo, $E(\mathbb{K}) \subset \mathbb{K}^2$ uma curva elíptica definida pela equação $y^2 = x^3 + Ax + B$ e $P\mathbb{K}^2$ o espaço projetivo como definido no capítulo 3.

A curva algébrica equivalente a $E(\mathbb{K})$ em $P\mathbb{K}^2$ é o conjunto de pontos $(X:Y:Z) \in P\mathbb{K}^2$ satisfazendo o polinômio homogêneo $Y^2Z = X^3 + AXZ^2 + BZ^3$.

Os pontos da curva no infinito satisfazem $Z = 0$. Portanto, temos $X^3 = 0 \Leftrightarrow X = 0$. Como $(X, Y, Z) \neq (0,0,0)$, o único ponto em $P\mathbb{K}^2$ que satisfaz $X = Z = 0$ é o ponto $(0:1:0)$. Definimos $\mathcal{O} = (0:1:0)$, que é um ponto no infinito em $P\mathbb{K}^2$.

No capítulo 4, afirmamos que "toda reta vertical no plano intersecta a curva elíptica no ponto $\mathcal{O}$". Vamos provar essa afirmação. Considere a reta $x = c$ definida sobre um corpo $\mathbb{K}$. Sua equação no plano projetivo é dada pelo polinômio homogêneo $X = cZ$ cujo único ponto no infinito é $(0:1:0) = \mathcal{O}$, pois $Z = 0 \Longrightarrow X = 0$. Dessa forma, verificamos que $\mathcal{O}$ é o único ponto no infinito pertencente à reta $x = c$, ou seja, toda reta vertical $(x = c)$ intersecta a curva elíptica no ponto $\mathcal{O}$.

5.4
A Lei de Grupo Revisitada

No capítulo 4, definimos um procedimento geométrico para somar pontos de curvas elípticas no conjunto $\mathbb{R}$. Dada uma curva elíptica $E(\mathbb{R})$ e dois pontos da curva $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$, a soma $P_1 + P_2$ é definida pelo procedimento:

(i) Trace uma reta que passa por P_1 e P_2. Essa reta encontrará a curva em um ponto $P_3' = (x_3', y_3')$;

(ii) Ache o ponto $P_3 = (x_3, y_3)$, simétrico a $P_3{}'$ em relação ao eixo de simetria da curva;

(iii) Defina $P_3 = P_1 + P_2$.

Em um primeiro momento, pode-se pensar que, em geral, tal definição para soma de pontos não possa ser usada em curvas definidas sobre outros corpos. No entanto, como explicado no capítulo 3, os conceitos de planos, curvas algébricas, retas, tangentes, derivadas, dentre outros, podem ser generalizados para uso em qualquer corpo. Ainda, para que tais generalizações sejam consistentes com toda a

teoria desenvolvida sobre o conjunto $\mathbb{R}$, ao criarmos as definições para outros corpos partimos dos resultados obtidos em $\mathbb{R}$. Por exemplo, temos que a função $f(x) = x^3 + Ax + B$ definida sobre o corpo $\mathbb{K}$ possui como derivada a função $f'(x) = 3x^2 + A$. Se $\mathbb{K} = \mathbb{R}$, esse resultado é obtido através do cálculo do limite $f'(x) = \lim_{h \to 0} \frac{f(x+h)-f(x)}{h}$; por outro lado, se $\mathbb{K}$ é um corpo finito, por exemplo, esse resultado é obtido por definição.

Com isso em mente, percebemos então que o procedimento soma pode ser executado em qualquer corpo $\mathbb{K}$ sobre o qual a curva elíptica esteja definida. Ainda, observamos que as mesmas fórmulas usadas para uma curva $E(\mathbb{R})$ valem para a curva $E(\mathbb{K})$. Finalmente, as fórmulas obtidas contêm somente operações fechadas em um corpo (adição, inverso aditivo, multiplicação e inverso multiplicativo), ou seja, se P_1 e P_2 têm coordenadas em $\mathbb{K}$, então $P_3 = (x_3, y_3)$ também terá coordenadas no corpo $\mathbb{K}$.

Dessa forma, concluímos que a soma de pontos de uma curva elíptica $E(\mathbb{K})$ pode ser realizada usando o mesmo procedimento definido sobre $\mathbb{R}$ e que as fórmulas na tabela 2 valem, na realidade, para qualquer corpo $\mathbb{K}$.

Como última observação, o teorema 4.3, enunciado para curvas elípticas sobre $\mathbb{R}$, pode ser generalizado.

Teorema 5.1 O conjunto de pontos $E(\mathbb{K})$ de uma curva elíptica munido da operação de adição definida acima forma um grupo abeliano.

Exemplo 5.2 Considere a curva elíptica E sobre o corpo finito $\mathbb{F}_{13}$ definida pela equação $y^2 = x^3 - x$. Sejam $P_1 = (5,4)$ e $P_2 = (-5,-6)$ pontos de $E(\mathbb{F}_{13})$. Vamos calcular $P_1 + P_2$ (lembrando que todos os cálculos devem ser realizados em $\mathbb{F}_{13}$) usando a definição:

- O coeficiente angular da reta r que passa por P_1 e P_2 é

$$m = \frac{(-6) - 4}{(-5) - 5} = 3 \times 3^{-1} = 1$$

- A equação da reta r é

$$r: y = 1(x - 5) + 4 = x - 1$$

- Substituindo a equação da reta na equação da curva elíptica

$$(x - 1)^2 = x^3 - x \Leftrightarrow x^3 - x^2 + x - 1 = 0$$

- $x_1 = 5$ e $x_2 = -5$ são raízes da equação obtida, portanto podemos facilmente achar x_3

$$x_1 + x_2 + x_3 = 1 \Longrightarrow 5 + (-5) + x_3 = 1 \Longrightarrow x_3 = 1$$

- Se denotarmos $P_3 = (x_3, y_3) = P_1 + P_2$, temos

$$-y_3 = x_3 - 1 = 1 - 1 = 0 \Longrightarrow y_3 = 0$$

- Logo, $P_3 = (1,0) \in E(\mathbb{F}_{13})$.

5.5
Ordem do Grupo e Ordem de um Ponto

Considere uma curva elíptica suave $E(\mathbb{K})$: $y^2 = x^3 + Ax + B$. Já sabemos que $(E(\mathbb{K}), +)$ é um grupo abeliano. A ordem do grupo é o número de elementos do grupo, ou seja, a quantidade de pontos da curva elíptica, que pode ser finita ou infinita. A ordem da curva elíptica $E(\mathbb{K})$ será denotada por $\#E(\mathbb{K})$.

A ordem das curvas elípticas reais é sempre infinita. O problema de se obter a ordem de uma curva elíptica torna-se interessante quando ela está definida sobre outros corpos. Inclusive, de forma geral, este é um problema em aberto, no entanto existem diversos resultados muito interessantes sobre o tema.

Por exemplo, quando $\mathbb{K} = \mathbb{Q}$, conjunto dos números racionais, temos o Teorema de Mordell, que estabelece que, para toda curva elíptica não-singular $E(\mathbb{Q})$, o conjunto de pontos da curva forma um grupo abeliano finitamente gerado. Ou seja, existe um conjunto finito de pontos $P_1, P_2, \dots, P_k \in E(\mathbb{Q})$ tal que, para todo ponto $P \in E(\mathbb{Q})$, existem inteiros $m_1, m_2, \dots, m_k$ de forma que $P = m_1P_1 + m_2P_2 + \cdots + m_kP_k$.

Já quando o corpo $\mathbb{K}$ é finito, podemos ver facilmente que o conjunto $E(\mathbb{K})$ também o será. No próximo capítulo veremos com mais detalhes algumas propriedades específicas para tais curvas.

Da mesma maneira que definimos a ordem da curva, podemos definir a ordem de um ponto. Inicialmente, dado um ponto $P \in E(\mathbb{K})$, definimos a multiplicação de P por um inteiro t:

a) $0P = \mathcal{O}$;

b) $tP = P + (t-1)P$; e;

c) $(-t)P = -(tP)$

O conjunto $\langle P \rangle = \{tP \mid t \in \mathbb{Z}\}$ é um subgrupo de $E(\mathbb{K})$. Se a ordem desse subgrupo for finita, denotada por n, então temos que $nP = \mathcal{O}$ e $tP = \mathcal{O}$ se, e somente se, n divide t (ou seja, existe inteiro k tal que $t = kn$). Nesse caso, dizemos que o ponto P tem ordem n. Esses resultados são aplicações diretas das proposições 2.4 e 2.6.

Estamos interessados nos pontos de ordem finita, que são usualmente chamados Pontos de Torção. Vamos iniciar nossa análise pelos pontos P de ordem 2 em $E(\mathbb{K})$, i.e., pontos P tais que $2P = \mathcal{O}$. Inicialmente, podemos escrever:

$$2P = \mathcal{O} \Leftrightarrow P + P = \mathcal{O} \Leftrightarrow P = -P$$

Se $P = (x, y)$, então $-P = (x, -y)$. Daí, $P = -P \Leftrightarrow y = -y \Leftrightarrow y = 0$. Fazendo $y = 0$ na equação da curva, obtemos $x^3 + Ax + B = 0$. Como essa equação possui três raízes distintas (curva suave!), existem três pontos de ordem 2 na curva E: $P_1 = (x_1, 0)$, $P_2 = (x_2, 0)$ e $P = (x_3, 0)$, onde x_1, x_2 e x_3 são raízes do polinômio cúbico.

É interessante notar que é possível que alguma raiz do polinômio não esteja no corpo $\mathbb{K}$ (mas certamente estará em seu fecho algébrico $\overline{\mathbb{K}}$). Por exemplo, o polinômio cúbico da curva elíptica $E(\mathbb{R})$: $y^2 = x^3 - 2x - 4$ tem como única raiz real $x_1 = 2$, portanto seu único ponto de ordem 2 é $P_1 = (2,0)$. Se a curva estivesse definida sobre $\mathbb{C}$, teríamos três pontos de ordem 2: $P_1 = (2,0)$, $P_2 = (-1 + i, 0)$ e $P_3 = (-1 - i, 0)$.

Assim, podemos afirmar que uma curva elíptica $E(\overline{\mathbb{K}})$ tem três pontos de ordem 2. Se considerarmos todos os pontos tais que $2P = \mathcal{O}$, teremos o conjunto $\{\mathcal{O}, P_1, P_2, P_3\}$, que é um subgrupo de $E(\overline{\mathbb{K}})$. Observe ainda que esse subgrupo é a soma direta de dois subgrupos cíclicos de ordem 2 (por exemplo, $\{\mathcal{O}, P_1, P_2, P_3\} = \{\mathcal{O}, P_1\} \oplus \{\mathcal{O}, P_2\}$).

A discussão acima prova a proposição 5.3.

Proposição 5.3 Seja $E(\overline{\mathbb{K}})$ uma curva elíptica não-singular definida pela equação $y^2 = x^3 + Ax + B$. Então,

(i) $P = (x, y)$ é um ponto de ordem 2 se e somente se $y = 0$

(ii) A curva $E(\overline{\mathbb{K}})$ tem exatamente quatro pontos de ordem dividindo 2. Esses pontos formam um grupo que é a soma direta de dois grupos cíclicos de ordem 2.

Vamos analisar agora os pontos de ordem 3. Denotando por $x(P)$ a coordenada x do ponto P, buscamos pontos P tais que $3P = \mathcal{O}$ ou, equivalentemente, $2P = -P$. Se $P \neq \mathcal{O}$, temos $2P = -P \Longrightarrow x(2P) = x(-P) \Longrightarrow x(2P) = x(P)$. Por outro lado, $x(2P) = x(P) \Longrightarrow 2P = \pm P$. Como $P \neq \mathcal{O}$, temos somente a possibilidade $2P = -P$. Ou seja,

$$3P = \mathcal{O} \Leftrightarrow 2P = -P \Leftrightarrow x(2P) = x(P)$$

Usando os dados da tabela 2, temos $x = x(P)$ e $x(2P) = m^2 - 2x$, onde $m = \frac{3x^2+A}{2y}$. Expandindo a equação acima e usando que $y^2 = x^3 + Ax + B$, obteremos uma equação do 4º grau em x:

$$\rho(x) = 3x^4 + 6Ax^2 + 12Bx - A^2 = 0 \qquad (9)$$

Nosso objetivo é provar que o polinômio $\rho(x)$ não tem raízes duplas, pois isso nos daria quatro valores distintos de x. Inicialmente, vamos reescrever $\rho(x)$ em função de $Q(x) = x^3 + Ax + B$. Usando que $Q'(x) = 3x^2 + A$ e $Q''(x) = 6x$, temos que $x(2P) = \frac{Q'(x)^2}{4Q(x)} - 2x = \frac{Q'(x)^2}{4Q(x)} - \frac{Q''(x)}{3}$ e que $x(P) = x = \frac{Q''(x)}{6}$. Então, substituindo esses valores em $\rho(x) = x(P) - x(2P) = 0$, obtemos

$$\rho(x) = 2Q(x)Q''(x) - Q'(x)^2. \qquad (10)$$

A partir da equação (10), podemos calcular $\rho'(x)$:

$$\rho'(x) = 12Q(x). \qquad (11)$$

Para provar que $\rho(x)$ não tem raízes duplas, suponha, por absurdo, que a é uma raiz dupla de $\rho(x)$, então $\rho(a) = \rho'(a) = 0$. Da equação (11), temos que $\rho'(a) = 0 \Longrightarrow Q(a) = 0$. Da equação (10), $\rho(a) = 2Q(a)Q''(a) - Q'(a)^2$. Substituindo $\rho(a) = 0$ e $Q(a) = 0$, obtemos $0 = Q'(a)$, ou seja, a é uma raiz dupla de $Q(x)$, o que não é possível pois a curva é suave. Portanto, $\rho(x)$ não possui raízes duplas.

Uma vez que $\rho(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$ não tem raízes duplas e cada raiz x define dois pontos na curva elíptica $[(x, \pm y)]$, temos oito pontos distintos de ordem 3. Observe que temos necessariamente $y \neq 0$, pois, pela proposição 5.3, $y = 0$ só ocorre em pontos de ordem 2. Com o ponto no infinito $\mathcal{O}$, temos no total nove pontos tais que $3P = \mathcal{O}$. Assim como no caso de ordem 2, possivelmente as raízes de $\rho(x)$ não estão todas no corpo $\mathbb{K}$, por isso a afirmação acima vale para pontos em $E(\overline{\mathbb{K}})$.

Proposição 5.4 Seja $E(\overline{\mathbb{K}})$ uma curva elíptica não-singular definida pela equação $y^2 = x^3 + Ax + B$. Então,

(i) $P = (x, y)$ é um ponto de ordem 3 se e somente se x é raiz do polinômio $\rho(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$

(ii) A curva $E(\overline{\mathbb{K}})$ tem exatamente nove pontos de ordem dividindo 3. Esses pontos formam um grupo que é a soma direta de dois grupos cíclicos de ordem 3.

Os resultados acima valem para qualquer curva elíptica definida sobre um corpo de característica diferente de 2 e de 3. No entanto, podemos generalizar o resultado para quaisquer curvas elípticas e qualquer ordem n.

Para simplificar a notação, seja E uma curva elíptica definida sobre um corpo $\mathbb{K}$ e seja n um inteiro positivo. Definimos o conjunto $E[n]$:

$$E[n] = \{P \in E(\overline{\mathbb{K}}) : nP = \mathcal{O}\}$$

Observe que o conjunto $E[n]$ contém pontos com coordenadas em $\overline{\mathbb{K}}$, o fecho algébrico de $\mathbb{K}$, e não somente pontos com coordenadas em $\mathbb{K}$.

Teorema 5.5 Seja E uma curva elíptica sobre um corpo $\mathbb{K}$ e seja n um inteiro positivo.

(i) Se a característica de $\mathbb{K}$ não divide n ou é 0, então $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$.

(ii) Se a característica de $\mathbb{K}$ é $p > 0$ e $p|n$, escrevendo $n = p^r n'$ com $p \nmid n'$, então $E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ ou $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$.

A prova do teorema 5.5 é um pouco complicada e utiliza alguns conceitos que não serão abordados nesse texto e, por isso, ela será omitida. No entanto, ela pode ser encontrada em Washington (2003).

Os casos das proposições 5.3(ii) e 5.4(ii) são casos particulares do teorema 5.5(i). Uma consequência interessante do teorema 5.5 é que podemos afirmar que existem no máximo n^2 pontos de ordem dividindo n, para qualquer n.

6
CURVAS ELÍPTICAS SOBRE CORPOS FINITOS

Após os conceitos gerais apresentados nos últimos capítulos, buscaremos agora verificar algumas propriedades das curvas elípticas sobre corpos finitos. Estamos particularmente interessados nos resultados relacionados a ordem desse grupo, não somente por sua importância teórica, mas também pelos aspectos práticos associados a tais curvas.

6.1
Introdução às Curvas Elípticas sobre Corpos Finitos

Seja E uma curva elíptica sobre um corpo finito $\mathbb{F}$. Como $\mathbb{F}$ é finito, há um número finito de pares $(x, y) \in \mathbb{F} \times \mathbb{F}$ e, portanto, $E(\mathbb{F})$ é um grupo abeliano finito. Vamos começar nossa discussão do tema com um exemplo, mostrando algumas propriedades e como podemos construir graficamente a soma de pontos da curva quando o corpo é do tipo $\mathbb{F}_p$, onde p é primo.

Seja E a curva representada por $y^2 = x^3 + 1$ definida sobre o corpo finito $\mathbb{F}_7 = \{-3, -2, -1, 0, 1, 2, 3\}$. A tabela 4 mostra os inversos multiplicativos, os quadrados e os cubos dos elementos de $\mathbb{F}_7$, informação que auxiliará os cálculos no exemplo.

n	-3	-2	-1	0	1	2	3
n^{-1}	2	3	-1	$\times$	1	-3	-2
n^2	2	-3	1	0	1	-3	2
n^3	1	-1	-1	0	1	1	-1

Tabela 4: Inversos, quadrados e cubos dos elementos do corpo finito $\mathbb{F}_7$

Para encontrar os pontos finitos de $E(\mathbb{F}_7)$, como o corpo é relativamente pequeno, podemos usar o método da força bruta, i.e., testar todos os valores possíveis de x e verificar se existe um y correspondente.

Por exemplo, se tomarmos $x = 2$, teremos $y^2 = 2^3 + 1 = 1 + 1 = 2$. Consultando a tabela 4, $y^2 = 2 \Longrightarrow y = -3$ ou $y = 3$. Dessa forma, $(2, \pm 3)$ são pontos de $E(\mathbb{F}_7)$. Naturalmente, é possível que alguns valores x não tenham um y correspondente. A tabela 5 fornece os pontos da curva $E(\mathbb{F}_7)$.

x	$y^2 = x^3 + 1$	y	Pontos de $E(\mathbb{F}_7)$
-3	$(-3)^3 + 1 = 1 + 1 = 2$	$-3,3$	$(-3,-3), (-3,3)$
-2	$(-2)^3 + 1 = -1 + 1 = 0$	0	$(-2,0)$
-1	$(-1)^3 + 1 = -1 + 1 = 0$	0	$(-1,0)$
0	$0^3 + 1 = 0 + 1 = 1$	$-1,1$	$(0,-1), (0,1)$
1	$1^3 + 1 = 1 + 1 = 2$	$-3,3$	$(1,-3), (1,3)$
2	$2^3 + 1 = 1 + 1 = 2$	$-3,3$	$(2,-3), (2,3)$
3	$3^3 + 1 = -1 + 1 = 0$	0	$(3,0)$
$\mathcal{O}$	$-$	$\mathcal{O}$	$\mathcal{O}$

Tabela 5: Pontos da curva $y^2 = x^3 + 1$ sobre $\mathbb{F}_7$

Observe que a ordem de $E(\mathbb{F}_7)$ é igual a 12, i.e., $\#E(\mathbb{F}_7) = 12$. Além disso, pela proposição 5.3(i), os pontos $(-2,0)$, $(-1,0)$ e $(3,0)$ têm ordem 2 e, juntamente como o ponto $\mathcal{O}$, esses são todos os pontos de ordem dividindo 2 em $E(\mathbb{F}_7)$ – e em $E(\overline{\mathbb{F}_7})$! Esses quatro pontos formam um subgrupo de $E(\mathbb{F}_7)$ que é a soma direta de dois grupos cíclicos de ordem 2. Por exemplo, $\{\mathcal{O}, (-2,0), (-1,0), (3,0)\} = \{\mathcal{O}, (-2,0)\} \oplus \{\mathcal{O}, (-1,0)\}$.

De acordo com a proposição 5.4, os pontos $P = (x, y)$ de ordem 3 devem satisfazer a equação $3x^4 + 12x = 0$. O único valor possível para $x \in \mathbb{F}_7$ é $x = 0$. Logo, os pontos de ordem dividindo 3 em $E(\mathbb{F}_7)$ formam o grupo cíclico $\{\mathcal{O}, (0,-1), (0,1)\}$.

Como $\#E(\mathbb{F}_7) = 12$, não é difícil concluir que $E(\mathbb{F}_7) = \{\mathcal{O}, (-2,0)\} \oplus \{\mathcal{O}, (-1,0)\} \oplus \{\mathcal{O}, (0,-1), (0,1)\}$, ou seja, $E(\mathbb{F}_7) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Ainda, essa estrutura implica que a ordem dos outros pontos deve ser igual a 6. Assim, o expoente do grupo $E(\mathbb{F}_7)$ é 6 e, usando a versão alternativa do teorema fundamental dos grupos abelianos finitos, podemos escrever $E(\mathbb{F}_7) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6$.

O "gráfico" de $E(\mathbb{F}_7)$ é mostrado na figura 8 e, inicialmente, parece não haver muito sentido da construção desse gráfico. A única informação que visualizamos é a simetria da curva em relação ao eixo x e isso ocorre somente por causa dos elementos escolhidos para o corpo $\mathbb{F}_7$.

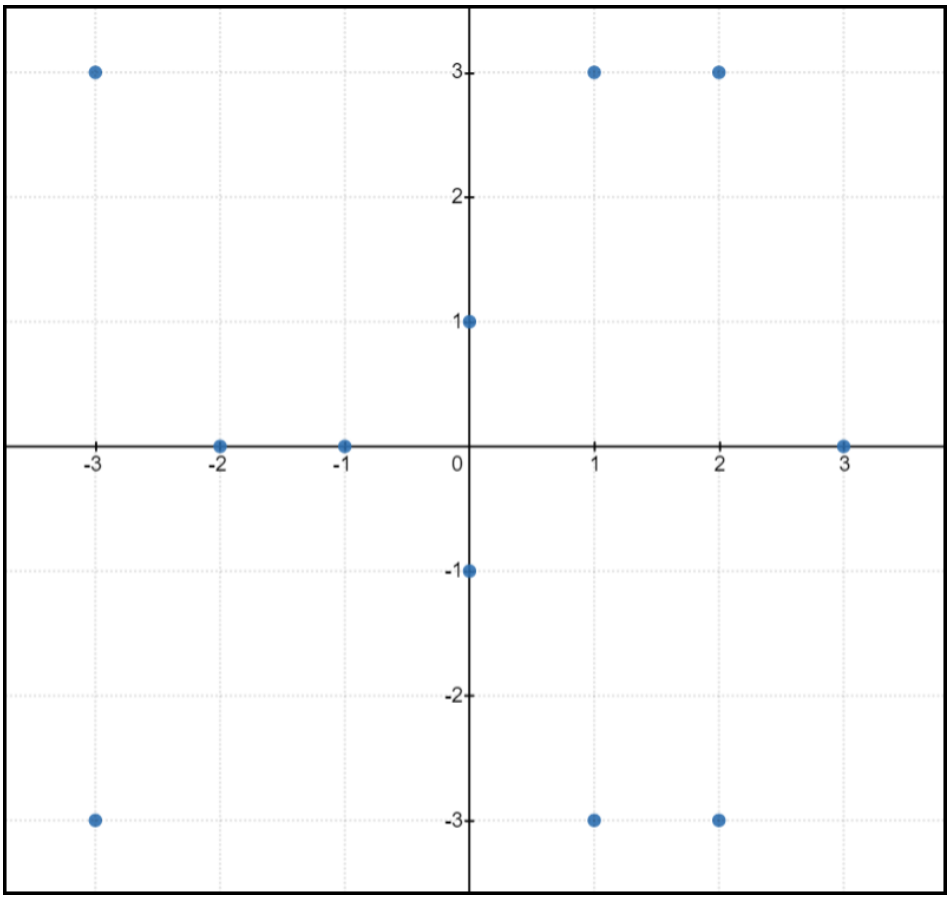

Figura 8: Gráfico da curva $\boldsymbol{y^2 = x^3 + 1}$ sobre $\mathbb{F}_7$

Vamos calcular agora a soma de pontos da curva elíptica $E(\mathbb{F}_7)$. Considere, por exemplo, os pontos $P_1 = (-3,3)$ e $P_2 = (2,-3)$. A soma $P_1 + P_2$ pode ser encontrada pela definição da Lei de Grupo:

- Coeficiente angular da reta que passa por P_1 e P_2:

$$m = \frac{3-(-3)}{(-3)-(2)} = (-1) \times 2^{-1} = 3$$

- Equação da reta por P_1 e P_2:

$$y = 3(x-(-3)) + 3 = 3x - 2$$

- Substituindo a equação da reta na equação da curva elíptica:

$$(3x-2)^2 = x^3 + 1 \Leftrightarrow x^3 - 2x^2 - 2x - 3 = 0$$

- $x_1 = -3$ e $x_2 = 2$ são raízes da equação obtida, portanto podemos facilmente achar x_3:

$$x_1 + x_2 + x_3 = -(-2) \Longrightarrow (-3) + 2 + x_3 = 2 \Longrightarrow x_3 = 3$$

- Se denotarmos $P_3 = (x_3, y_3) = P_1 + P_2$, temos $-P_3 = (x_3, -y_3)$:

$$(-y_3) = 3x_3 - 2 = 0 \Longrightarrow y_3 = 0$$

- Logo, $P_3 = (-3,3) + (2,-3) = (3,0) \in E(\mathbb{F}_7)$.

Podemos visualizar essa soma graficamente, no entanto a construção da figura não é intuitiva. Vamos analisar a figura 9 para entender a ideia por trás da construção gráfica. Observe que marcamos em vermelho os pontos $P_1 = (-3,3)$ e $P_2 = (2,-3)$. O ponto-chave dessa construção é que, ao invés de traçarmos a reta que passa por P_1 e P_2 como fazemos em $\mathbb{R}$ (e fizemos no exemplo da figura 2), vamos traçar um feixe de retas com o coeficiente angular calculado ($m = 3$) passando por P_1 e P_2.

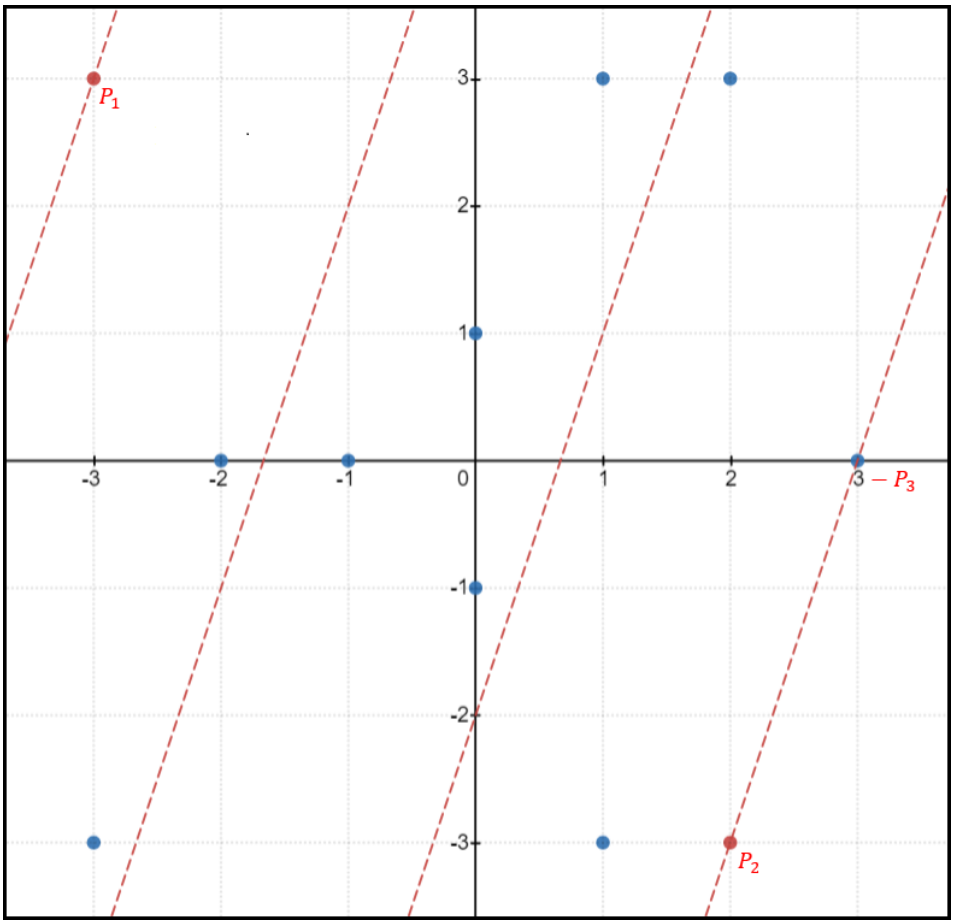

Figura 9: Gráfico da soma $(-\mathbf{3}, \mathbf{3}) + (\mathbf{2}, -\mathbf{3})$ em $\boldsymbol{E}(\mathbb{F}_7)$

Como consideramos $\mathbb{F}_7 = \{-3, -2, -1, 0, 1, 2, 3\}$, estamos interessados nos pontos com coordenadas nesse conjunto. No entanto, cada elemento de $\mathbb{F}_7$ pode ser visto como uma classe de equivalência módulo 7, ou seja, podemos escrever o 0 como qualquer elemento do conjunto $\{7k : k \in \mathbb{Z}\}$, o 1 pode ser representado por qualquer elemento de $\{7k + 1 : k \in \mathbb{Z}\}$, etc.

Com isso em mente, quando permitimos pontos de coordenadas inteiras, devemos enxergar, por exemplo, que os pontos $(-3,3)$, $(-3,-4)$ e $(4,3)$ são iguais, pois $-3 = 4$ e $3 = -4$ em $\mathbb{F}_7$. Então, considerando retas com um mesmo coeficiente angular, a reta passando por $(-3,3)$ é a "mesma" reta que passa por $(-3,-4)$. Se uma dessas retas tiver equação $y = mx + b$, as retas a serem desenhadas têm equação $y = mx + b + 7k,\ k \in \mathbb{Z}$. Por exemplo, considerando $m = 3$, a reta que passa por $P_1 = (-3,3)$ é dada pela equação $y = 3x + 12$. As outras retas são dadas pelas equações $y = 3x + 5$, $y = 3x - 2$, $y = 3x - 9$, etc.

Plotando esse feixe de retas passando pelos pontos equivalentes em $\mathbb{F}_7$ e usando como ponto inicial P_1 ou P_2, necessariamente essas retas terão três pontos em comum com $E(\mathbb{F}_7)$: P_1, P_2 e $-P_3$, conforme a definição de soma de pontos apresentada no 4. No exemplo da figura 9, as retas passam pelos pontos P_1, P_2 e $-P_3 = (3,0)$, cujo simétrico é o próprio ponto $(3,0)$. Portanto, $P_1 + P_2 = (3,0)$.

Vamos ver um outro exemplo para a mesma curva. Considere $P_1 = (-3,3)$ e $P_2 = (-2,0)$. O coeficiente angular em $\mathbb{F}_7$ é $m = \frac{3-0}{(-3)-(-2)} = \frac{3}{-1} = -3$. Devemos plotar retas com coeficiente angular $m = -3$ passando por P_1 e P_2. Observe, na figura 10, que as retas ainda passam pelo ponto $-P_3 = (0,1)$. Portanto, $P_3 = P_1 + P_2 = (0,-1)$.

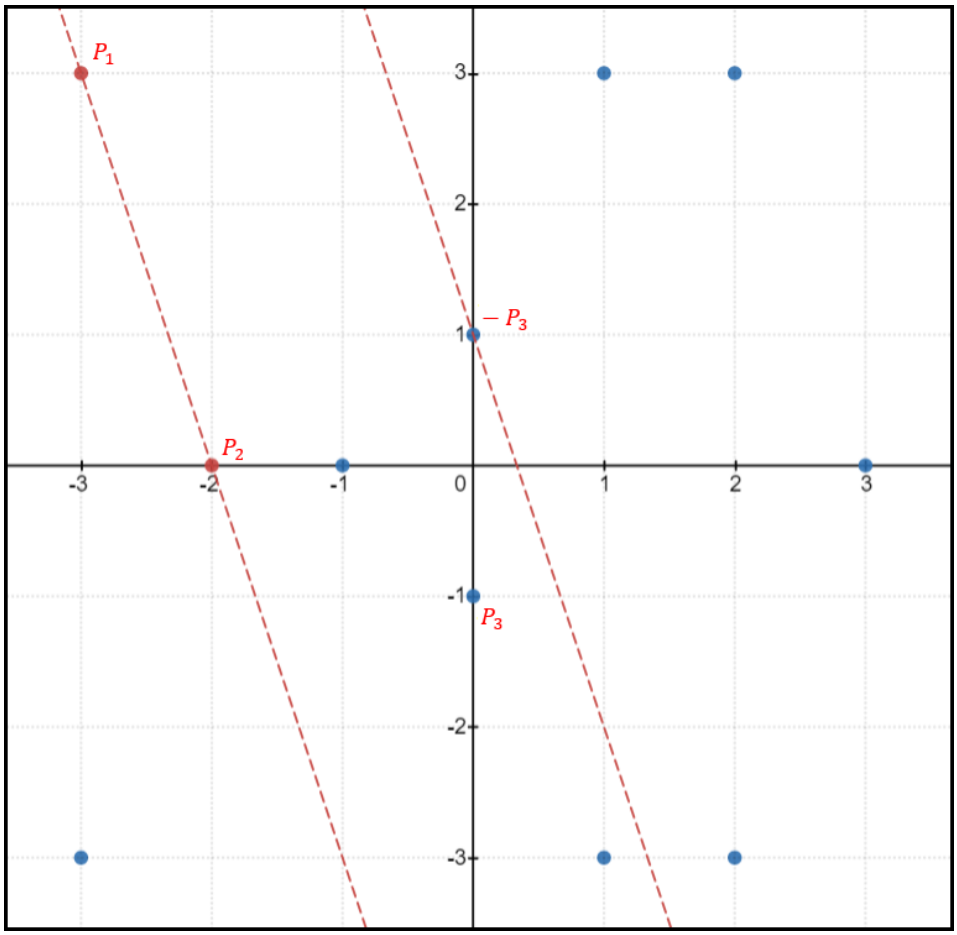

Figura 10: Gráfico da soma $(-\mathbf{3},\mathbf{3}) + (-\mathbf{2},\mathbf{0})$ em $\boldsymbol{E}(\mathbb{F}_7)$

Podemos calcular algebricamente a soma $(-3,3) + (-2,0)$ e verificar se o resultado é o mesmo:

- Coeficiente angular da reta: $m = \frac{3-0}{(-3)-(-2)} = \frac{3}{-1} = -3$
- Equação da reta por P_1 e P_2: $y = -3\big(x - (-3)\big) + 3 = -3x + 1$
- Substituindo a equação da reta na equação da curva elíptica

$$(-3x + 1)^2 = x^3 + 1 \Leftrightarrow x^3 - 2x^2 - x = 0$$

- $x_1 = -3$ e $x_2 = -2$ são raízes da equação obtida:

$$x_1 + x_2 + x_3 = -(-2) \Longrightarrow (-3) + (-2) + x_3 = 2 \Longrightarrow x_3 = 0$$

- Se denotarmos $P_3 = (x_3, y_3) = P_1 + P_2$, temos

$$(-y_3) = -3x_3 + 1 = 1 \Longrightarrow y_3 = -1$$

- Logo, $P_3 = (-3,3) + (2,-3) = (0,-1) \in E(\mathbb{F}_7)$.

A sequência de cálculos acima corrobora a interpretação geométrica dada na figura 10.

Observação 6.1 A interpretação geométrica dada para a soma dos pontos da curva $E(\mathbb{F}_7)$ pode ser aplicada a outras curvas elípticas sobre corpos finitos, desde que o corpo seja da forma $\mathbb{F}_p$, onde p é primo.

Fazendo os cálculos para todos os pares de pontos da curva elíptica usando as fórmulas da tabela 2, podemos obter a soma de todos os pontos da curva $E(\mathbb{F}_7)$. Para simplificar a apresentação dos dados, nomeamos os pontos da curva na tabela 6. A tabela 7 contém os resultados obtidos. Observe que os dados da tabela 7 nos permitem verificar facilmente a ordem de todos os pontos da curva.

$\mathcal{O}$	$(-3,-3)$	$(-3,3)$	$(-2,0)$	$(-1,0)$	$(0,-1)$	$(0,1)$	$(1,-3)$	$(1,3)$	$(2,-3)$	$(2,3)$	$(3,0)$
$\mathcal{O}$	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}

Tabela 6: Pontos da curva $\boldsymbol{E(\mathbb{F}_7)}$

$+$	$\mathcal{O}$	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
$\mathcal{O}$	$\mathcal{O}$	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
P_1	P_1	P_5	$\mathcal{O}$	P_6	P_7	P_3	P_2	P_{10}	P_4	P_8	P_{11}	P_9
P_2	P_2	$\mathcal{O}$	P_6	P_5	P_8	P_1	P_3	P_4	P_9	P_{11}	P_7	P_{10}
P_3	P_3	P_6	P_5	$\mathcal{O}$	P_{11}	P_2	P_1	P_9	P_{10}	P_7	P_8	P_4
P_4	P_4	P_7	P_8	P_{11}	$\mathcal{O}$	P_{10}	P_9	P_1	P_2	P_6	P_5	P_3
P_5	P_5	P_3	P_1	P_2	P_{10}	P_6	$\mathcal{O}$	P_{11}	P_7	P_4	P_9	P_8
P_6	P_6	P_2	P_3	P_1	P_9	$\mathcal{O}$	P_5	P_8	P_{11}	P_{10}	P_4	P_7
P_7	P_7	P_{10}	P_4	P_9	P_1	P_{11}	P_8	P_5	$\mathcal{O}$	P_2	P_3	P_6
P_8	P_8	P_4	P_9	P_{10}	P_2	P_7	P_{11}	$\mathcal{O}$	P_6	P_3	P_1	P_5
P_9	P_9	P_8	P_{11}	P_7	P_6	P_4	P_{10}	P_2	P_3	P_5	$\mathcal{O}$	P_1
P_{10}	P_{10}	P_{11}	P_7	P_8	P_5	P_9	P_4	P_3	P_1	$\mathcal{O}$	P_6	P_2
P_{11}	P_{11}	P_9	P_{10}	P_4	P_3	P_8	P_7	P_6	P_5	P_1	P_2	$\mathcal{O}$

Tabela 7: Soma dos pontos da curva $\boldsymbol{E(\mathbb{F}_7)}$: $\boldsymbol{y^2 = x^3 + 1}$

6.2
Ordem do Grupo $E(\mathbb{F}_{p^n})$

Seja E uma curva elíptica não-singular definida sobre um corpo finito $\mathbb{F}_{p^n}$. Sabemos que a ordem do grupo (ou ordem da curva), denotada por $\#E(\mathbb{F}_{p^n})$, é a quantidade de pontos dessa curva. Por exemplo, na seção anterior vimos por tentativa e erro que, para a curva $E: y^2 = x^3 + 1$ definida sobre o corpo $\mathbb{F}_7$, $\#E(\mathbb{F}_7) = 12$. Mas é possível como determinar essa ordem sem testar todos os elementos de $\mathbb{F}_{p^n}$? Veremos que não é uma tarefa trivial e que em geral os resultados dependem de algum conhecimento prévio sobre os pontos da curva. Importante destacar que, além do interesse teórico, essa informação é crucial em diversas aplicações de curvas elípticas, como a criptografia.

Vamos iniciar nossa discussão apresentando um teorema que impõe limites para o valor de $\#E(\mathbb{F}_{p^n})$: o Teorema de Hasse. Uma prova para esse teorema pode ser encontrada em Washington (2003) e em Silverman (2009).

Teorema 6.2 (Teorema de Hasse) Seja E uma curva elíptica sobre um corpo finito $\mathbb{F}_q$, onde $q = p^n$ e p é primo. Então a ordem de $E(\mathbb{F}_q)$ satisfaz

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

Apesar de somente estabelecer limites, esse teorema pode ser aplicado em conjunto com outros fatos que conhecemos sobre grupos. Por exemplo, pelo Teorema de Lagrange (teorema 2.11), a ordem de um ponto divide a ordem do grupo. Então, se conhecermos a ordem de um ponto, podemos restringir os valores $\#E(\mathbb{F}_q)$ usando o Teorema de Hasse.

Exemplo 6.3 Voltando ao exemplo da seção 6.1, considere a curva $E: y^2 = x^3 + 1$ definida sobre $E(\mathbb{F}_7)$. Aplicando o Teorema de Hasse, fazendo $q = 7$, temos $8 - 2\sqrt{7} \leq \#E(\mathbb{F}_7) \leq 8 + 2\sqrt{7}$. Como $\#E(\mathbb{F}_7)$ é um número inteiro, podemos escrever $3 \leq \#E(\mathbb{F}_7) \leq 13$. Com auxílio dos teoremas 5.3 e 5.4, encontramos pontos de ordem 2 e pontos de ordem 3 em $E(\mathbb{F}_7)$. Portanto, 2 e 3 dividem $\#E(\mathbb{F}_7)$, ou seja, 6 divide $\#E(\mathbb{F}_7)$. Juntando todas as informações, $\#E(\mathbb{F}_7)$ pode ser somente 6 ou 12. Mesmo procurando pontos pelo método da força bruta, após

encontrar o sétimo ponto já poderíamos concluir que $\#E(\mathbb{F}_7) = 12$ sem a necessidade de testar todos os pontos do corpo $\mathbb{F}_7$.

Em alguns casos, o Teorema de Hasse nos dá resultados precisos sobre a ordem da curva.

Exemplo 6.4 Considere a curva $E(\mathbb{F}_{31}): y^2 = x^3 + 7x + 1$. Se tomarmos o ponto $P = (0,1)$ e calcularmos nP para valores crescentes de n, descobriremos que a ordem de P é 26. Pelo Teorema de Hasse, $32 - 2\sqrt{31} \leq \#E(\mathbb{F}_{31}) \leq 32 + 2\sqrt{31}$, que pode ser reescrito como $21 \leq \#E(\mathbb{F}_{31}) \leq 43$, pois a ordem do grupo é um número inteiro. Como 26 divide $\#E(\mathbb{F}_{31})$, só temos a possibilidade $\#E(\mathbb{F}_{31}) = 26$. Podemos afirmar ainda que $E(\mathbb{F}_{31})$ é um grupo cíclico e que $P = (0,1)$ é um gerador do grupo.

O teorema a seguir nos dá o resultado exato da ordem de $E(\mathbb{F}_{q^n})$ desde que tenhamos de antemão a ordem de $E(\mathbb{F}_q)$. Em geral, $\mathbb{F}_q$ tem que ser um corpo relativamente pequeno para que possamos calcular sua ordem verificando todos os seus pontos ou a partir de algum outro método elementar.

Teorema 6.5 Seja E uma curva elíptica sobre um corpo finito $\mathbb{F}_q$, onde $q = p^n$ e p é primo. Suponha $\#E(\mathbb{F}_q) = q + 1 - a$ e escreva $X^2 - aX + q = (X - \alpha)(X - \beta)$. Então, $\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$.

Observe que o parâmetro a é um inteiro que depende somente da curva $E(\mathbb{F}_q)$ e que α e β são números complexos conjugados.

Exemplo 6.6 Mais uma vez, considere a curva $E: y^2 = x^3 + 1$ definida sobre $E(\mathbb{F}_7)$. Sabemos que $\#E(\mathbb{F}_7) = 12$. Primeiro, encontramos o parâmetro a:

$$12 = 7 + 1 - a \Longrightarrow a = -4$$

Temos, então, $X^2 + 4X + 7 = 0$. Resolvendo a equação, encontramos

$$\alpha = -2 + i\sqrt{3} \text{ e } \beta = -2 - i\sqrt{3}.$$

Com essas informações, vamos encontrar $\#E(\mathbb{F}_{7^2})$. Pelo teorema 6.5,

$$\#E(\mathbb{F}_{7^2}) = 7^2 + 1 - (\alpha^2 + \beta^2)$$

Como $\alpha^2 = \left(-2 + i\sqrt{3}\right)^2 = 1 - 4i\sqrt{3}$ e $\beta^2 = \left(-2 - i\sqrt{3}\right)^2 = 1 + 4i\sqrt{3}$, temos $\alpha^2 + \beta^2 = 2$. Logo,

$$\#E(\mathbb{F}_{7^2}) = 49 + 1 - 2 = 48$$

Observe que $\#E(\mathbb{F}_7)$ divide $\#E(\mathbb{F}_{7^2})$, o que é esperado pois $E(\mathbb{F}_7) \subset E(\mathbb{F}_{7^2})$. Na próxima seção, encontraremos os pontos de $E(\mathbb{F}_{7^2})$ e confirmaremos que $\#E(\mathbb{F}_{7^2}) = 48$.

Os resultados acima mostram que encontrar a ordem do grupo de uma curva elíptica é uma tarefa complicada, pois não há uma fórmula exata a não ser em casos especiais. No entanto, existem métodos computacionais eficientes que fornecem resultados precisos como, por exemplo, o Algoritmo de Schoof (SCHOOF, 1985).

6.3
Um Exemplo de Curva Elíptica sobre Extensões de Corpos

Considere o corpo $\mathbb{F}_7 = \{-3, -2, -1, 0, 1, 2, 3\}$ e seja $i = \sqrt{-1}$. É fácil verificar que não existe $a \in \mathbb{F}_7$ tal que $a^2 = -1$ e, portanto, $i \notin \mathbb{F}_7$. Então, $(\mathbb{F}_7)[i] = \{a + bi : a, b \in \mathbb{F}_7\}$ é um corpo com 49 elementos e podemos denotá-lo por $\mathbb{F}_{7^2}$ ou $\mathbb{F}_{49}$.

Na seção 6.1, tomamos a curva elíptica $E: y^2 = x^3 + 1$ e encontramos os pontos dessa curva sobre $\mathbb{F}_7$, que formam o conjunto $E(\mathbb{F}_7)$. Nessa seção, vamos encontrar os pontos da curva E sobre $\mathbb{F}_{49}$. Sendo os elementos do corpo $\mathbb{F}_{49}$ da forma $a + bi$, com $a, b \in \mathbb{F}_7$, para essa curva especificamente, já conhecemos todos os pontos $P = (x, y) \in E(\mathbb{F}_{49})$ em que $x = a \in \mathbb{F}_7$ (ou seja, $b = 0$), esses pontos são exatamente os pontos de $E(\mathbb{F}_7)$. Basta, portanto, procurar pontos cuja coordenada x é igual a $a + bi$ com $b \neq 0$.

Assim como no caso anterior, a ideia é escolher valores para $x \in \mathbb{F}_{49}$ e verificar se existe um $y \in \mathbb{F}_{49}$ tal que $y^2 = x^3 + 1$. A figura 11 mostra os quadrados dos elementos $z = a + bi \in \mathbb{F}_{49}$. Mostramos somente os pontos em que $b \geq 0$ pois $(-z)^2 = z^2$. Por exemplo, $(1 - i)^2 = (-1 + i)^2 = -2i$.

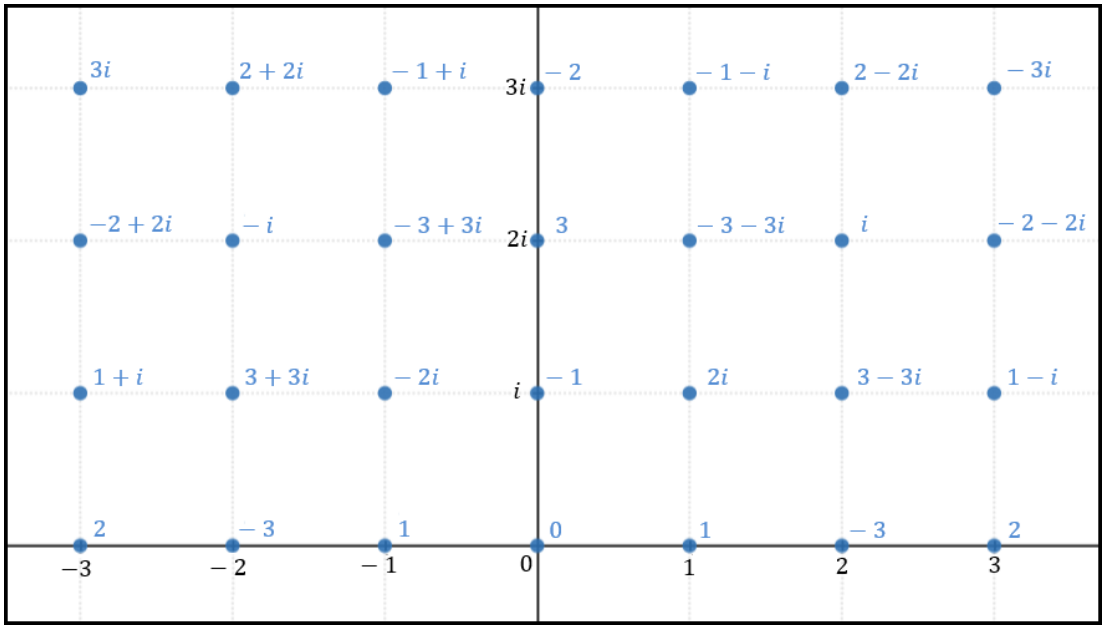

Figura 11: Quadrados dos elementos de $\mathbb{F}_{49}$

Para essa curva, podemos otimizar o cálculo de seus pontos ao observar que as raízes cúbicas de 1 em $\mathbb{F}_{49}$ são 1,2 e -3, logo $x^3 = (2x)^3 = (-3x)^3$ e, portanto, se (x, y) é um ponto da curva então $(2x, y)$ e $(-3x, y)$ também pertencem à curva. Por exemplo, $x = i \Longrightarrow y^2 = x^3 + 1 = 1 - i \Longrightarrow y = \pm(3 + i)$; logo, temos $\{(i, 3 + i), (i, -3 - i)\} \subset E(\mathbb{F}_{49})$. Pela observação anterior, a curva também contém os pontos $(2i, 3 + i)$, $(-3i, 3 + i)$, $(2i, -3 - i)$ e $(-3i, -3 - i)$. A tabela 8 sumariza os resultados encontrados.

$\boldsymbol{x}$	$\boldsymbol{2x}$	$\boldsymbol{-3x}$	$\boldsymbol{y^2 = x^3 + 1}$	**y**
$\boldsymbol{i}$	$2i$	$-3i$	$y^2 = i^3 + 1 = 1 - i$	$\pm(3 + i)$
$\boldsymbol{-i}$	$-2i$	$3i$	$y^2 = (-i)^3 + 1 = 1 + i$	$\pm(-3 + i)$
$\boldsymbol{1 + i}$	$2 + 2i$	$-3 - 3i$	$y^2 = (1 + i)^3 + 1 = -1 + 2i$	$-$
$\boldsymbol{1 - i}$	$2 - 2i$	$-3 + 3i$	$y^2 = (1 - i)^3 + 1 = -1 - 2i$	$-$
$\boldsymbol{2 + i}$	$-3 + 2i$	$1 - 3i$	$y^2 = (2 + i)^3 + 1 = 3 - 3i$	$\pm(2 + i)$
$\boldsymbol{2 - i}$	$-3 - 2i$	$1 + 3i$	$y^2 = (2 - i)^3 + 1 = 3 + 3i$	$\pm(-2 + i)$
$\boldsymbol{3 + i}$	$-1 + 2i$	$-2 - 3i$	$y^2 = (3 + i)^3 + 1 = -2 - 2i$	$\pm(3 + 2i)$
$\boldsymbol{3 - i}$	$-1 - 2i$	$-2 + 3i$	$y^2 = (3 - i)^3 + 1 = -2 + 2i$	$\pm(-3 + 2i)$
$\boldsymbol{1 + 2i}$	$2 - 3i$	$-3 + i$	$y^2 = (1 + 2i)^3 + 1 = -3 - 2i$	$-$
$\boldsymbol{1 - 2i}$	$2 + 3i$	$-3 - i$	$y^2 = (1 - 2i)^3 + 1 = -3 + 2i$	$-$
$\boldsymbol{3 + 2i}$	$-1 - 3i$	$-2 + i$	$y^2 = (3 + 2i)^3 + 1 = -1 - 3i$	$-$
$\boldsymbol{3 - 2i}$	$-1 + 3i$	$-2 - i$	$y^2 = (3 - 2i)^3 + 1 = -1 + 3i$	$-$
$\boldsymbol{3 + 3i}$	$-1 - i$	$-2 - 2i$	$y^2 = (3 + 3i)^3 + 1 = 3 - 2i$	$-$
$\boldsymbol{3 - 3i}$	$-1 + i$	$-2 + 2i$	$y^2 = (3 - 3i)^3 + 1 = 3 + 2i$	$-$

Tabela 8: Pontos da curva $\boldsymbol{y^2 = x^3 + 1}$ sobre $\mathbb{F}_{\mathbf{49}}$

Observe que para cada linha da tabela em que há um valor na coluna y, temos seis pontos da curva (três possíveis valores para x vezes dois possíveis valores para y). Portanto, além dos 12 pontos de $E(\mathbb{F}_7) \subset E(\mathbb{F}_{49})$ que já conhecíamos, obtemos mais 36 pontos em $E(\mathbb{F}_{49})$, totalizando os $\#E(\mathbb{F}_{49}) = 48$ pontos que esperávamos encontrar de acordo com o exemplo 6.6.

Por fim, vamos estabelecer a estrutura do grupo $E(\mathbb{F}_{49})$. Já conhecemos a ordem dos pontos em $E(\mathbb{F}_7)$, vamos escolher um ponto P da curva $E(\mathbb{F}_{49})$ tal que $P \notin E(\mathbb{F}_7)$ e e analisar $\langle P \rangle$, o subgrupo gerado por P. A tabela 9 contém os múltiplos do ponto $P = (i, 3 + i)$, de onde podemos concluir que a ordem de P é 12 (a coluna "Ordem de nP" foi preenchida somente após encontrarmos todos os elementos de $\langle P \rangle$).

$\boldsymbol{n}$	$\boldsymbol{nP}$	Ordem de $\boldsymbol{nP}$
1	$(i, 3+i)$	12
2	$(2,3)$	6
3	$(-1-2i, -3+2i)$	4
4	$(0,1)$	3
5	$(-3+2i, -2-i)$	12
6	$(-1,0)$	2
7	$(-3+2i, 2+i)$	12
8	$(0,-1)$	3
9	$(-1-2i, 3-2i)$	4
10	$(2,-3)$	6
11	$(i, -3-i)$	12
12	$\mathcal{O}$	–

Tabela 9: Múltiplos de $\boldsymbol{P = (i, 3+i)}$ em $\boldsymbol{E(\mathbb{F}_{49})}$

Esse é um grupo cíclico de ordem 12, portanto $\langle P \rangle \simeq \mathbb{Z}_{12}$. Podemos escrever também que $\langle P \rangle \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_4$. Por exemplo,

$\langle P \rangle \simeq \{\mathcal{O}, (0,1), (0,-1)\} \oplus \{\mathcal{O}, (-1-2i, -3+2i), (-1,0), (-1-2i, 3-2i)\}$.

Tomando o ponto $P_2 = (3+i, 3+2i)$, que não está em $\langle P \rangle$ e, fazendo um procedimento similar, obtemos que a ordem de P_2 é 4 (tabela 10).

$\boldsymbol{n}$	$\boldsymbol{nP_2}$	Ordem de $\boldsymbol{nP_2}$
1	$(3+i, 3+2i)$	4
2	$(3,0)$	2
3	$(3+i, -3-2i)$	4
4	$\mathcal{O}$	–

Tabela 10: Múltiplos de $\boldsymbol{P = (3+i, 3+2i)}$ em $\boldsymbol{E(\mathbb{F}_{49})}$

Daí, temos que $E(\mathbb{F}_{49}) \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$ ou $E(\mathbb{F}_{49}) \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

7
CONSIDERAÇÕES FINAIS

O objetivo do trabalho foi introduzir o assunto curvas elípticas, iniciando pelas curvas elípticas reais e concluindo com as curvas elípticas sobre corpos finitos. Todos os elementos que compõe a teoria apresentada são extremamente vastos e esse trabalho pode ser aprofundado de diversas maneiras. Para exemplificar, citamos alguns temas, que possuem teorias bem desenvolvidas, com resultados e aplicações específicas ao assunto:

(i) Pontos racionais de curvas elípticas reais
(ii) Curvas elípticas singulares
(iii) Curvas elípticas sobre corpos de característica 2 ou 3
(iv) Aplicações de curvas elípticas (e.g. criptografia)

Deve ficar claro que a lista acima de forma alguma esgota as possibilidades, enfatizamos esses temas somente porque eles foram brevemente mencionados ao longo do texto sem entrarmos em detalhes. Existem diversas direções que podem ser seguidas a partir desse momento, pois a teoria de curvas elípticas vem sendo desenvolvida pelos matemáticos há mais de 200 anos.

8

REFERÊNCIAS BIBLIOGRÁFICAS

ASH, A.; GROSS, R. **Elliptic Tales** : Curves, Counting, and Number Theory. New Jersey : Princeton University Press, 2012.

CRANDALL, R.; POMERANCE, C. **Prime Numbers** : A Computational Perspective. 2 ed. Springer, 2005.

DOOLEY, J.F. **History of Cryptography and Cryptanalysis** : Codes, Ciphers, and Their Algorithms. Springer, 2018.

GIBSON, C.G. **Elementary Geometry of Algebraic Curves** : An Undergraduate Introduction. Cambridge University Press, 1998.

GONÇALVES, A. **Introdução à Álgebra**. 6 ed. Rio de Janeiro : IMPA, 2017.

LANG, S. **Álgebra para Graduação**. 2 ed. Rio de Janeiro : Editora Ciência Moderna, 2008.

SCHOOF, R. **Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p**. Mathematics of Computation, 44(170):483-494, 1985.

SHOUP, V. **A Computational Introduction to Number Theory and Algebra**. 2 ed. Cambridge University Press, 2009.

SILVERMAN, J.J. **The Arithmetic of Elliptic Curves**. 2ed. Springer, 2009.

SILVERMAN, J.H.; TATE, J.T. **Rational Points on Elliptic Curves**. 2 ed. Springer, 2015.

VAINSENCHER, I. **Introdução às Curvas Algébricas Planas**. Rio de Janeiro : IMPA, 2005.

WASHINGTON, L.C. **Elliptic Curves** : Number Theory and Cryptography. Chapman & Hall/CRC, 2003.