Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Grupos de Pontos Racionais Sobre Cônicas

Valdir Barbaresco Filho

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Novembro/2003
João Pessoa - Pb

Grupos de Pontos Racionais Sobre Cônicas

por

Valdir Barbaresco Filho

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva - UFPB (Orientador)

Prof. Dr. João Montenegro de Miranda - UECE

Prof. Dr. Hélio Pires de Almeida - UFPB

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Novembro/2003

Agradecimentos

- Ao Professor Dr. *Antônio de Andrade e Silva*, que compreende o verdadeiro sentido da palavra *orientação*.

- Ao colega Reinaldo Takara Zoppei, por ter me apoiado na decisão de meu afastamento.

- Aos colegas Almir e Tardim pelo apoio inicial.

- Ao competente chefe de Departamento Ubaldo Tolentino de Barros.

- À Pricilla pelo carinho, companheirismo e paciência.

- A todos os funcionários públicos brasileiros, pois sem os quais,eu não teria completado o curso primário, ginásio, segundo grau, graduação, nem tão pouco este que concluo. Guiçá, no futuro, estes abnegados tenham ainda condições de promover outros cidadãos brasileiros desprovidos do mínimo.

- À Sônia, pela competência e presteza no atendimento de secretaria.

- À Ester Rosenbach, mui digníssima e acima de tudo extremamente dedicada secretaria do ICEN.

- Aos colegas do Departamento de Matemática - UFMT - Campus de Rondonópolis.

Dedicatória

À minha esposa Pricilla.

Resumo

Encontrararemos o conjunto dos pontos racionais e a estrutura de grupo sobre o círculo unitário, sobre a hipérbole e sobre as elipses que tenham semi-eixos racionais.

Abstract

We will find the group of the rational points and the group structure on the unitary circle, on the hyperbole and on the ellipses with rational semi-axes.

Notação

$(A, +\cdot)$ - Anel A

$(\mathbb{Z}[i], +, \cdot)$ - Anel dos Inteiros Gaussianos

$\mathbb{Z}[\varepsilon]$ - Anel quociente $\frac{\mathbb{Z}[x]}{(x^2-1)}$

$\overline{a}$ - Classe de equivalência de a

$\mathbb{Z}_m$ - Conjunto das classes residuais módulo m

$U.(\mathbb{Z}_m)$ - Conjunto dos elementos simetrizáveis de $\mathbb{Z}_m$

$\mathbb{Z}$ - Conjunto dos números inteiros

$\mathbb{N}$: Conjunto dos números naturais

$[K : L]$ - Dimensão de K sobre L

x^{-1} - Elemento inverso

$N : \mathbb{C} \to \mathbb{R}^+$ - Função norma dos complexos aos reais não negativos

$C(\mathbb{Q})$ - Grupo dos pontos racionais sobre o círculo unitário

$H(\mathbb{Q})$ - Grupo dos pontos racionais sobre a hipérbole

$E(\mathbb{Q})$ - Grupo dos pontos racionais sobre uma elipse E

$(G, *)$ - Grupo G

$I(\alpha)$ - Ideal gerado por "α"

$N(\alpha)$ - Norma de α

$\mathbb{Z} \times \mathbb{Z}$ - Produto cartesiano de $\mathbb{Z}$ por $\mathbb{Z}$

$\sum\limits_{p \equiv 1 \bmod 4} C_p$ - Soma direta dos subgrupos C_p

C_p - Subgrupo de $C(\mathbb{Q})$ gerado pelo elemento $\left(\frac{m_p^2-n_p^2}{m_p^2+n_p^2}, \frac{2m_pn_p}{m_p^2+n_p^2}\right)$

C_2 - Subgrupo de $C(\mathbb{Q})$ gerado pelo elemento $(0,1)$

$H_1(\mathbb{Q})$ - Subgrupo de $H(\mathbb{Q})$

$H_2(\mathbb{Q})$ - Subgrupo de $H(\mathbb{Q})$ gerado pelo elemento $\left(\frac{5}{4}, \frac{3}{4}\right)$

H_p - Subgrupo de $H(\mathbb{Q})$ gerado pelo elemento $\left(\frac{p^2+1}{2p}, \frac{p^2-1}{2p}\right)$

H' - Subgrupo de $H(\mathbb{Q})$ gerado pelo elemento $(-1, 0)$

Sumário

Introdução

Nosso trabalho tem como objetivo encontrar o conjunto dos pontos racionais sobre determinadas cônicas, a saber, o círculo unitário, a hipérbole dada pela equação $x^2 - y^2 = 1$, e as elipses com semi-eixos racionais, como também obter a estrutura de grupo destas cônicas.

Para se ter uma idéia da importância do estudo dos pontos racionais sobre curvas, podemos citar que o último teorema de Fermat (1601-1665), "sejam m, a, b e c inteiros com $m > 2$. Se $a^m + b^m = c^m$, então $a.b.c = 0$," foi, depois de diversas tentativas, provado por Andrew Wiles em 1993, o qual usou como base a teoria das curvas elípticas, isto é, curvas definidas por equações cúbicas. Uma grande parte desta teoria é devotada ao entendimento dos pontos racionais sobre estas curvas. O conjunto destes pontos tem uma estrutura de grupo, mas a dificuldade maior reside em como encontrar todos os pontos racionais numa curva elíptica.

Nosso estudo inicialmente era sobre o mais fácil e familiar exemplo: "O Grupo dos Pontos Racionais Sobre o Círculo Unitário", o qual é baseado no artigo [10]. Porém neste artigo não há um estudo detalhado a respeito dos pontos racionais sobre elipses, e durante o transcorrer dos trabalhos observamos que uma vez conhecidos os pontos racionais sobre o círculo unitário, os pontos racionais sobre elipses com semi-eixos racionais também são conhecidos. Este detalhe nos levou a ampliar a proposta inicial do trabalho.

No primeiro capítulo faremos uma pequena revisão sobre a teoria de grupos e anéis. No segundo capítulo, abordamos a teoria de números algébricos, corpos quadráticos e descrevemos os elementos irredutíveis de um subconjunto de

$$\frac{\mathbb{Z}[x]}{\langle x^2 - 1 \rangle}.$$

Finalmente, no terceiro capítulo descrevemos os pontos racionais sobre cônicas.

Capítulo 1

Resultados Básicos

Neste capítulo apresentaremos alguns resultados básicos da teoria dos grupos e anéis e números, que serão necessários nos capítulos seguintes.

1.1 Grupos

Nesta seção apresentaremos alguns resultados clássicos da teoria dos grupos que serão necessários para a compreensão desta dissertação. O leitor interessado em mais detalhes pode consultar [1, 2, 3, 5].

Dado um conjunto G, munido de uma operação binária $*$ então:

1. Se a operação "$*$" é associativa, ou seja,

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

   então dizemos que o par $(G, *)$ é um *semigrupo*;

2. Se $(G, *)$ é um semigrupo, que possui um elemento neutro, ou seja,

$$\exists \; e \in G \text{ tal que } a * e = e * a = a, \forall a \in G,$$

   então dizemos $(G, *)$ é um *monóide*.

3. Se $(G, *)$ é um monóide no qual todo elemento tem seu simétrico, ou seja,

$$\forall a \in G, \exists b \in G \text{ tal que } a * b = b * a = e,$$

   então dizemos $(G, *)$ é um *grupo*, e denotamos por $b = a^{-1}$.

4. Se a operação do grupo $(G, *)$ for comutativa, então dizemos que o grupo é *comutativo* ou *abeliano*.

Com o objetivo de simplificar a notação usaremos ab em vez $a * b$ e G em vez $(G, *)$. A *ordem* ou *cardinalidade* de um grupo G é o número de elementos de G e denotamos por $|G|$.

Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um *subgrupo* de G, em símbolos $H \leq G$, se H é um grupo em relação a operação binária herdada de G.

Um critério para se verificar se um subconjunto não vazio H é um subgrupo de G é dado pela seguinte proposição:

Proposição 1.1 *Seja G um grupo. Então um subconjunto não vazio H de G é um subgrupo de G se, somente se, $ab^{-1} \in H$, para todos $a, b \in H$.* ■

Sejam G um grupo e H um subgrupo de G. Dado $a \in G$, o conjunto

$$aH = \{ah : h \in H\}$$

é chamado *classe lateral à esquerda* de H em G determinada por a. De modo semelhante, podemos definir classe lateral à direita Ha de H em G. O conjunto de todas as classes laterais à esquerda (à direita) de H em G forma uma partição de G, o qual denotamos por $\frac{G}{H}$, isto é,

$$\frac{G}{H} = \{aH : a \in G\}.$$

Sejam G um grupo e H um subgrupo de G. Dizemos que H é um *subgrupo normal* de G, em símbolos $H \trianglelefteq G$, se

$$Ha = aH, \forall a \in G,$$

ou, equivalentemente,

$$aHa^{-1} = H, \forall a \in G.$$

Sejam G um grupo e H um subgrupo de G. Então $\frac{G}{H}$ é um grupo com a operação

$$aHbH = abH, \forall a, b \in G,$$

se, e somente se, H é um subgrupo normal de G. Neste caso, $\frac{G}{H}$ é chamado o *grupo quociente* de G por H.

Sejam X um subconjunto não vazio de G e

$$\mathcal{F} = \{H : H \leq G \text{ e } X \subseteq H\}.$$

Então

$$\langle X \rangle = \bigcap_{H \in \mathcal{F}} H$$

é o menor subgrupo de G contendo X e chamado o *subgrupo gerado* por X. Se X é um conjunto finito, digamos

$$X = \{x_1, \ldots, x_n\},$$

denotamos $\langle X \rangle$ por

$$\langle X \rangle = \langle x_1, \ldots, x_n \rangle.$$

Proposição 1.2 *Sejam G um grupo e X um subconjunto não vazio de G. Então*

$$\langle X \rangle = \left\{ \prod_{i=1}^{n} x_i : n \in \mathbb{N} \text{ e } x_i \in X \cup X^{-1}, i = 1, \ldots, n \right\},$$

onde $X^{-1} = \{x^{-1} : x \in X\}$. ■

Seja G um grupo. Se existir $a \in G$ tal que

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\},$$

dizemos que G é um *grupo cíclico*.

A ordem de um elemento $a \in G$, em símbolos $o(a)$, é definida como $o(a) = |\langle a \rangle|$. É fácil verificar que se $o(a)$ é finita, então $o(a)$ é igual ao menor inteiro positivo k tal que $a^k = e$.

Exemplo 1.1 *Dado $n \in \mathbb{N}$, definimos no conjunto*

$$\begin{aligned} \mathbb{Z}_n &= \{\overline{a} : a \in \mathbb{Z}\} \\ &= \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}, \end{aligned}$$

onde

$$\begin{aligned} \overline{a} &= \{m \in \mathbb{Z} : m \equiv a \pmod{n}\} \\ &= \{a + kn : k \in \mathbb{Z}\}, \end{aligned}$$

uma operação binária:

$$\overline{a} \oplus \overline{b} = \overline{a+b}.$$

É fácil verificar que esta operação é bem definida e que $(\mathbb{Z}_n, \oplus)$ *é um grupo cíclico gerado por* $\overline{1}$.

Teorema 1.1 (Lagrange) *Sejam* G *um grupo finito e* H *um subgrupo de* G. *Então* $|H|$ *divide* $|G|$. ■

Corolário 1.1 (Fermat) *Seja* $p \in \mathbb{N}$ *um número primo. Então*

$$a^p \equiv a \pmod{p}, \forall a \in \mathbb{Z}.$$

■

Seja $\{G_i\}_{i \in I}$ uma família de grupos quaisquer. O produto cartesiano

$$G = \prod_{i \in I} G_i$$

é um grupo sob a operação binária componente a componente:

$$ab = (a_i b_i),$$

onde $a = (a_i), b = (b_i) \in G$. É claro que

$$e = (e_i)$$

é o elemento identidade de G e

$$a^{-1} = \left(a_i^{-1}\right)$$

é o elemento inverso de a. O grupo G é chamado de *produto direto* (*externo*). O subconjunto de G tal que os elementos são $a = (a_i)$, onde $a_i = e_i$, exceto para um número finito de índices, é um subgrupo de G chamado *produto direto* (*interno*) ou *soma direta* e é denotado por

$$\sum_{i \in I} G_i.$$

Sejam G e L dois grupos. Uma função φ de G em L é um *homomorfismo de grupos* se

$$\varphi(ab) = \varphi(a)\varphi(b),$$

para todos $a, b \in G$. Neste caso, a *imagem* de φ é o conjunto

$$\begin{aligned} \operatorname{Im}\varphi &= \{h : h = \varphi(a) \text{ para algum } a \in G\} \\ &= \{\varphi(a) : a \in G\}. \end{aligned}$$

O *núcleo* de φ é o conjunto

$$\ker\varphi = \{a \in G : \varphi(a) = e\}.$$

É fácil verificar que $\operatorname{Im}\varphi$ é um subgrupo de L e $\ker\varphi$ é um subgrupo normal de G.

Um homomorfismo de grupos $\varphi : G \longrightarrow L$ é um *isomorfismo* se φ é bijetora. Quando existir um isomorfismo entre G e L dizemos que G e L são *isomorfos* e denotamos por $G \simeq L$. Um *endomorfismo* de um grupo G é um homomorfismo $\varphi : G \longrightarrow G$. Denotamos por

$$\operatorname{End}(G) = \{\varphi : G \longrightarrow G : \varphi \text{ é um homomorfismo}\}.$$

Um *automorfismo* de um grupo G é um isomorfismo $\varphi : G \longrightarrow G$. Denotamos por

$$\operatorname{Aut}(G) = \{\varphi : G \longrightarrow G : \varphi \text{ é um isomorfismo}\}.$$

Teorema 1.2 [5] *Sejam G, L grupos e $\varphi : G \longrightarrow L$ um homomorfismo de grupos. Então*

$$\frac{G}{\ker\varphi} \simeq \operatorname{Im}\varphi.$$

■

Proposição 1.3 *Sejam G e L grupos, com $G = \langle a_1, \ldots, a_n \rangle$, e $\varphi : G \to L$ um homomorfismo de grupos. Então $\varphi(G)$ é um subgrupo de L e $\varphi(G) = \langle \varphi(a_1), \ldots, \varphi(a_n) \rangle$.* ■

1.2 Anéis

Nesta seção apresentaremos alguns resultados clássicos da teoria dos anéis que serão necessários para a compreensão desta dissertação. O leitor interessado em mais detalhes pode consultar [5, 9].

Um *anel* R é um conjunto R munido de uma operação binária denotada por $+$ (chamada de *adição*) e de uma operação binária denotada por $\cdot$ (chamada *multiplicação*) que satisfazem as seguintes condições:

1. $(R, +)$ é um grupo comutativo;

2. A multiplicação é associativa, isto é,

$$(x \cdot y) \cdot z = x \cdot (y \cdot z), \forall x, y, z \in R;$$

3. A adição é distributiva relativamente à multiplicação, isto é,

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ e } (x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y, z \in R.$$

Se existir $1 \in R$ tal que $x1 = 1x = x$, para todo $x \in R$, dizemos que R é um *anel com identidade.* Se $xy = yx$, para quaisquer $x, y \in R$, dizemos que R é um *anel comutativo.* Se para todos $x, y \in R$,

$$xy = 0 \Rightarrow x = 0 \text{ ou } y = 0,$$

dizemos que R é um *anel sem divisores de zero.*

Se R é um anel comutativo, com identidade e sem divisores de zero, dizemos que R é um *domínio de integridade* ou simplesmente *domínio.* Um elemento $x \in R$ é dito uma *unidade* de R se existir $y \in R$ tal que

$$xy = yx = 1.$$

Denotamos por $U(R)$, o conjunto de todas as unidades de R. Se

$$U(R) = R^* = R - \{0\},$$

dizemos que R é um *corpo.* Salvo menção explicita em contrário, todos o anéis considerados nesta dissertação são comutativos com identidade.

Sejam K um corpo e D é um subanel de K. Então D é um domínio. Reciprocamente, para todo domínio D existe um menor corpo L que o contém e, é único a menos de isomorfismos, temos que

$$L = \left\{ \frac{a}{b} : a \in D \text{ e } b \in D^* \right\}.$$

O corpo L é chamado o *corpo de frações* de D.

Para $n \in \mathbb{N}$, denotamos o *anel dos inteiros módulo* n por $\mathbb{Z}_n$. Se n é um número composto, então $\mathbb{Z}_n$ tem divisores de zero, mas se n for primo, então $\mathbb{Z}_n$ será um corpo.

Sejam R um anel e S um subconjunto não vazio de R. Dizemos que S é um *subanel* de R se é um anel com as operações binárias herdadas de R.

Proposição 1.4 *Seja R um anel. Então um subconjunto não vazio S de R é um subanel de R se, e somente se, as seguintes condições são satisfeitas:*

1. *$x - y \in S$, para todos $x, y \in S$;*
2. *$xy \in S$, para todos $x, y \in S$.* ■

Sejam K um corpo e F um subconjunto não vazio de K. Dizemos que F é um *subcorpo* de K se é um corpo com as operações binárias herdadas de K.

Um critério para verificar se um subconjunto S é um subcorpo de R é dado pela seguinte proposição

Proposição 1.5 *Seja K um corpo. Então um subconjunto não vazio F de K é um subcorpo de K se, somente se, as seguintes condições são satisfeitas:*

1. *F é um subanel de K;*
2. *$x^{-1} \in F$, para todo $x \in F^*$.* ■

Sejam R um anel e I um subconjunto não vazio de R. Dizemos que I é um *ideal* de R se as seguintes condições são satisfeitas:

1. $x - y \in I$, para todos $x, y \in I$;
2. $ry \in I$, para todos $r \in R$ e $y \in I$.

Sejam R e S dois anéis. Uma função $\varphi : R \longrightarrow S$ é um *homomorfismo de anéis* se as seguintes condições são satisfeitas:

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$, para todos $x, y \in R$;
2. $\varphi(xy) = \varphi(x)\varphi(y)$, para todos $x, y \in R$;
3. $\varphi(1) = 1$.

Um homomorfismo de anéis $\varphi : R \longrightarrow S$ é um *isomorfismo* se φ é bijetora. Quando existir um isomorfismo entre R e S dizemos que R e S são *isomorfos* e denotaremos por $R \simeq S$.

Teorema 1.3 [5] *Sejam R e S dois anéis e $\varphi : R \longrightarrow S$ um homomorfismo de anéis. Então*

$$\frac{G}{\ker \varphi} \simeq \operatorname{Im} \varphi.$$

■

Um ideal I de R é dito *próprio* se $I \neq R$. Um ideal I de R é dito *finitamente gerado* se existir um subconjunto finito $S = \{x_1, x_2, \ldots, x_n\}$ de R tal que

$$\begin{aligned} I &= \langle S \rangle \\ &= Rx_1 + Rx_2 + \cdots + Rx_n \\ &= \{\sum_{i=1}^{n} r_i x_i : r_i \in R\}. \end{aligned}$$

O ideal $I = Rx = \langle x \rangle$ é chamado *ideal principal* gerado por $x \in R$. Um anel R é um *anel de ideais principais* se todo ideal de R for principal.

Sejam R um anel e $x, y \in R$, com $x \neq 0$. Dizemos que x *divide* y, em símbolos $x \mid y$, se existir $z \in R$ tal que $y = xz$. Se $y = xz$, com $x, z \in R - U(R)$, dizemos que x é um *divisor próprio* de y. Sejam $x, y \in R^*$, dizemos que x e y são *associados* se existir $u \in U(R)$ tal que $y = ux$.

Lema 1.1 [5] *Sejam R um domínio e $x, y \in R^*$. Então*:

1. *$x \in U(R)$ se, e somente se, $\langle x \rangle = \langle 1 \rangle = R$;*

2. *x divide y se, e somente se, $\langle y \rangle \subseteq \langle x \rangle$;*

3. *x e y são associados se, e somente se, $\langle y \rangle = \langle x \rangle$;*

4. *x é um divisor próprio de y se, e somente se, $\langle y \rangle \subset \langle x \rangle \subset \langle 1 \rangle$.* ■

Sejam I e J dois ideais de R. Então

$$I + J = \{x + y : x \in I \text{ e } y \in J\}$$

e

$$IJ = \{\sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J \text{ e } n \in \mathbb{N}\}$$

são ideais de R. Note que, a soma e a multiplicação de ideais podem, de forma indutiva, ser generalizadas para qualquer número finito de ideais.

Um ideal P de um anel R é um *ideal primo* de R se $P \neq R$ e para todos $x, y \in R$ tal que $xy \in P$, tem-se $x \in P$ ou $y \in P$.

Teorema 1.4 [5] *Sejam R um anel e P um ideal de R. Então as seguintes condições são equivalentes*:

1. *P é um ideal primo de R;*

2. *Se I e J são ideais de R tais que $IJ \subseteq P$, então $I \subseteq P$ ou $J \subseteq P$;*

3. *$\frac{R}{P}$ é um domínio.* ■

Um ideal não nulo M de um anel R é um *ideal maximal* de R se $M \neq R$ e se, J é um ideal de R tal que $M \subseteq J \subseteq R$, então $M = J$ ou $J = R$.

Proposição 1.6 *Seja I um ideal próprio de R. Então I é maximal se, e somente se, $\langle I, r\rangle = R$, para todo $r \in R - I$.* ■

Observação 1.1 *Todo ideal maximal é primo.*

Teorema 1.5 [5] *Sejam R um anel e M um ideal de R. Então M é maximal se, e somente se, $\frac{R}{M}$ é um corpo.* ■

Seja R um anel. Um elemento $p \in R^*$ é *irredutível* sobre R se as seguintes condições são satisfeitas:

1. $p \notin U(R)$;

2. Se $p = bc$, então $b \in U(R)$ ou $c \in U(R)$, isto é, p não tem divisores próprios.

Seja R um anel. Um elemento $p \in R$ é *primo* sobre R se as seguintes condições são satisfeitas:

1. $p \notin U(R)$;

2. Se p divide ab, então p divide a ou p divide b.

Um anel possui fatoração se todo elemento $a \notin U(R)$ não nulo pode ser escrito como um produto finito de elementos irredutíveis.

Observação 1.2 *Todo elemento primo não nulo é irredutível.*

Um anel R é chamado um *anel de fatoração única* se as seguintes condições são satisfeitas:

1. Para todo $a \in R^*$ e $a \notin U(R)$, existem elementos irredutíveis $p_i \in R$, $1 \leq i \leq n$, tais que
$$a = \prod_{i=1}^{n} p_i;$$
2. Dadas duas fatorações em irredutíveis de a,
$$a = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j,$$
então $m = n$ e existe uma permutação σ de $\{1, \ldots, n\}$ tal que $p_i = uq_{\sigma(i)}$, onde $u \in U(R)$.

Proposição 1.7 [5] *Seja R um anel. Suponhamos que a fatoração exista em R. Então R é um anel de fatoração única se, e somente se, qualquer elemento irredutível é primo.* ■

Proposição 1.8 [5] *Se R é um anel de ideais principais, então R é um anel de fatoração única.* ■

Uma *função Euclidiana* para um domínio R é uma função $\varphi : R^* \longrightarrow \mathbb{Z}$ tal que

1. Se $a, b \in R^*$ e a divide b, então $\varphi(a) \leq \varphi(b)$;

2. Se $a, b \in R$, com $b \neq 0$, então existem $q, r \in R$ tais que
$$a = bq + r, \text{ onde } r = 0 \text{ ou } \varphi(r) < \varphi(b).$$

Exemplo 1.2 *Seja*
$$R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$
o anel dos inteiros de Gauss. Então a função $\varphi : R^* \longrightarrow \mathbb{Z}$ definida por
$$\varphi(\alpha) = a^2 + b^2,$$
onde $\alpha = a + bi$, é Euclidiana. De fato, sejam $\alpha, \beta \in R^*$ e se β divide α, então existe $\gamma \in R^*$ tal que $\alpha = \beta\gamma$. Como $|\gamma|^2 \geq 1$ temos que
$$\varphi(\beta) \leq \varphi(\beta)\,\varphi(\gamma) = \varphi(\beta\gamma) = \varphi(\alpha).$$

Por outro lado, como podemos identificar $\mathbb{C}$ com o plano, temos que cada $\dfrac{\alpha}{\beta} \in \mathbb{C}$ está no interior ou na fronteira de um quadrado de vértices em R com diagonal de comprimento $\sqrt{2}$. Assim, existe um vértice q com distância menor do que ou igual a $\frac{\sqrt{2}}{2}$ de $\dfrac{\alpha}{\beta}$. Logo,

$$\left|\frac{\alpha}{\beta} - q\right| \leq \frac{\sqrt{2}}{2} < 1.$$

Tomando $r = \alpha - q\beta$, obtemos que $\alpha = q\beta + r$, onde

$$|r| = |\alpha - q\beta| = |\beta| \left|\frac{\alpha}{\beta} - q\right| < |\beta|.$$

Assim, $\varphi(r) < \varphi(\beta)$. Portanto, φ é uma função Euclidiana.

Se um domínio R tem uma função Euclidiana, dizemos que R é um *domínio Euclidiano.*

Teorema 1.6 [5] *Se R é um domínio Euclidiano, então R é um domínio de ideais principais.* ■

Seja R um anel. As expressões da forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

onde $n \in \mathbb{Z}_+$ e $a_i \in R, i = 0, 1, \ldots, n$, com as operações binárias de adição e multiplicação

$$f(x) + g(x) = (a_k + b_k)x^k + (a_{k-1} + b_{k-1})x^{k-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

com $g(x) = b_m x^m + m_{m-1} x^{m-1} + \cdots + b_1 x + b_0$, $k \leq \max\{m, n\}$ e

$$f(x)g(x) = c_{m+n} x^{m+n} + c_{m+n-1} x^{m+n-1} + \cdots + c_1 x + c_0$$

onde

$$c_k = \sum_{i+j=k} a_i b_j$$

é um anel comutativo com identidade, $R[x]$, o qual será chamado de *anel dos polinômios* na variável x sobre R.

Se $f(x) \neq 0$, seu *coeficiente líder* é a_n, onde n é o maior inteiro tal que $a_n \neq 0$. Neste caso, n é o *grau* do polinômio $f(x)$. Em particular, se $a_n = 1$ dizemos que $f(x)$ é um *polinômio mônico.* Uma *raiz* de $f(x)$ é um elemento α em alguma extensão (confira a seguir) de R tal que

$$f(\alpha) = 0.$$

Um polinômio $f(x)$ sobre R se *fatora sobre* R se existirem $\alpha_1, \ldots, \alpha_n \in R$ tais que

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n), c \in R^*.$$

Dizemos que E é uma *extensão* de F, se F é um subcorpo do corpo E. Um *corpo de decomposição* de $f(x)$ sobre F é uma extensão E de F tal que as seguintes condições são satisfeitas:

1. $f(x)$ fatora-se sobre E;

2. $f(x)$ não se fatora em qualquer subcorpo próprio de E contendo F.

Por exemplo, o corpo $\mathbb{C}$ é o corpo de decomposição do polinômio $f(x) = x^2 + 1$ sobre $\mathbb{R}$.

Seja $f(x) \in F[x]$ um polinômio de grau n tendo corpo de decomposição E. Se

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n),$$

onde $c \in F^*$ e $\alpha_1, \ldots, \alpha_n \in E$, definimos

$$\Delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

O *discriminante* de $f(x)$ é definido por $D = \Delta^2$. Se $a \in F^*$, então é fácil verificar que $f(x)$ e $af(x)$ têm o mesmo discriminante. Assim, não há perda de generalidade, em considerarmos apenas polinônios mônicos, isto é, polinômios da forma

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

De modo inteiramente análogo à construção de $R[x]$, obtemos o anel dos polinômios nas variáveis x e y, $R[x, y]$, pois

$$R[x, y] = R[x][y].$$

Proposição 1.9 (Princípio da Substituição) [5] *Seja $\varphi : R \longrightarrow S$ um homomorfismo de anéis. Então para cada $\alpha \in S$, existe um único homomorfismo $\widehat{\varphi} : R[x] \longrightarrow S$ tal que $\widehat{\varphi}(a) = \varphi(a)$, para todo $a \in R$ e $\widehat{\varphi}(x) = \alpha$.* ■

Proposição 1.10 [5] *Sejam R um anel e $f \in R[x]$ irredutível sobre R. Seja $R[\alpha]$ o anel obtido pela adjunção de uma raiz α de f. Então*

$$R[\alpha] \simeq R^n,$$

onde n é o grau de f. ■

Esta proposição afirma que as potências

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

formam uma base para $R[\alpha]$ sobre R. A soma é definida de maneira óbvia e para multiplicar duas destas combinações lineares em $R[\alpha]$, usamos a multiplicação polinomial de $R[x]$ e então dividimos o produto por f. O resto é a combinação linear de

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

que representa o produto.

1.3 Triângulos Pitagorianos

Nesta seção consideraremos o problema de encontrar todas as soluções inteiras positivas x, y e z para a equação Diofantina

$$x^2 + y^2 = z^2. \tag{1.1}$$

Suponhamos que $x, y, z \in \mathbb{N}$ seja uma solução da equação 1.1 e $d = \text{mdc}(x, y)$. Então $d^2 \mid x^2$ e $d^2 \mid y^2$ e, assim, $d^2 \mid x^2 + y^2$, isto é, $d^2 \mid z^2$. Temos, pela unicidade do Teorema Fundamental da Aritmética, que $d \mid z$. Portanto,

$$\text{mdc}(x, y) = \text{mdc}(x, z) = \text{mdc}(y, z) = \text{mdc}(x, y, z).$$

Assim, se $x, y, z \in \mathbb{N}$ é uma solução da equação 1.1 e $d = \text{mdc}(x, y)$, então

$$a = \frac{x}{d}, \ b = \frac{y}{d} \ \text{ e } \ c = \frac{z}{d}$$

é uma solução da equação 1.1 com $\text{mdc}(a, b) = 1$, chamamos (a, b, c) uma solução *primitiva*, por exemplo, 3, 4 e 5 e 5, 12 e 13 são soluções primitivas da equação 1.1. Assim, todo triângulo Pitagoriano é similar a um triângulo Pitagoriano primitivo. Portanto, basta considerar o problema de encontrar todas as soluções primitivas da equação 1.1.

Seja x, y e z uma solução primitiva da equação 1.1. Então x e y não podem ser simltaneamente pares, nem tão pouco podem ser simultaneamente ímpares, pois

$$x^2 \equiv 1 \pmod 4 \ \text{ e } \ y^2 \equiv 1 \pmod 4 \Rightarrow z^2 \equiv 2 \pmod 4,$$

o que é impossível. Como x e y aparecem simetricamente na equação 1.1, podemos supor, sem perda de generalidade, que y é par e x e z são ímpares. E, para continuar nossa análise necessitamos do seguinte Lema:

Lema 1.2 *Se u e v são inteiros relativamente primos cujo produto uv é um quadrado perfeito, então u e v são simultaneamente quadrados perfeitos.*

Prova. Seja p um primo que divide u, e α o maior expoente inteiro tal que p^α divide u. Entao, pelo fato de u e v serem relativamente primos, temos que p não divide v. Portanto, α é o maior expoente tal que p^α divide uv um quadrado perfeito. Logo, α é par. Como isto é válido para todos os primos que dividem u, segue que u é um quadrado perfeito. Similarmente, v também é um quadrado perfeito. ■

Note que

$$x^2 + y^2 = z^2 \Leftrightarrow y^2 = (z+x)(z-x) \Leftrightarrow (\frac{y}{2})^2 = (\frac{z+x}{2})(\frac{z-x}{2})$$

e a última equação tem sentido, pois y, $z+x$ e $z-x$ são pares. Afirmação:

$$\text{mdc}(\frac{z+x}{2}, \frac{z-x}{2}) = 1.$$

De fato, seja $d = \text{mdc}(\frac{z+x}{2}, \frac{z-x}{2})$. Então $d \mid x$ e $d \mid z$. Logo, por hipótese, $d = 1$. Assim, pelo Lema 1.2, existem $r, s \in \mathbb{N}$ tais que

$$\frac{z+x}{2} = r^2, \frac{z-x}{2} = s^2 \text{ e } \frac{y}{2} = rs.$$

É fácil verificar que r e s têm paridades distintas com $\text{mdc}(r,s) = 1$ e $r > s > 0$. Finalmente, das equações acima, temos que

$$y = r^2 - s^2, \;\; x = 2rs \text{ e } z = r^2 + s^2, \forall r, s \in \mathbb{N},$$

onde r e s têm paridades distintas com $\text{mdc}(r,s) = 1$ e $r > s > 0$, são todas as soluções primitivas da equação 1.1 (Confira [8]).

Capítulo 2

Inteiros Algébricos.

Neste capítulo apresentaremos algumas definições e resultados básicos da teoria algébrica dos números que serão necessários para a compreensão deste trabalho. O leitor interessado em mais detalhes pode consultar [9].

Sejam K um subcorpo de $\mathbb{C}$ e $\theta \in \mathbb{C}$. Denotamos por

$$K[\theta] = \{f(\theta) : f \in K[x]\}$$

o menor subdomínio de $\mathbb{C}$ contendo K e θ, e

$$K(\theta) = \left\{\frac{f(\theta)}{g(\theta)} : f, g \in K[x], g(\theta) \neq 0\right\}$$

o corpo quociente de $K[\theta]$.

Um elemento $\theta \in \mathbb{C}$ é um *número algébrico* se existir $m \in \mathbb{N}$ tal que o conjunto

$$\{1, \theta, \ldots, \theta^m\}$$

é linearmente dependente sobre $\mathbb{Q}$.

Seja L um subcorpo de K. Podemos ver K como um espaço vetorial sobre L, e K é chamado uma extensão de L. Dizemos que K é uma extensão finita se K é um espaço vetorial de dimensão finita sobre L. Se K é uma extensão finita de L, indicamos por

$$[K : L]$$

a dimensão de K visto como um espaço vetorial sobre L e $[K : L]$ é chamado o *grau* de K sobre L.

Teorema 2.1 *Seja $\theta \in \mathbb{C}$. Então θ é algébrico sobre $\mathbb{Q}$ se, e somente se, $\mathbb{Q}[\theta]$ é uma extensão finita de $\mathbb{Q}$.*

Prova. Suponhamos que $[\mathbb{Q}[\theta]:\mathbb{Q}]=n$. Então os elementos $1,\theta,\ldots,\theta^n$ são linearmente dependentes sobre $\mathbb{Q}$. Portanto, θ é algébrico sobre $\mathbb{Q}$.

Reciprocamente, seja $f=\operatorname{irr}(\theta,\mathbb{Q})$, com $\partial f=n$.

Afirmação: $\mathbb{Q}[\theta]$ é um espaço vetorial sobre $\mathbb{Q}$ gerado por $1,\theta,\ldots,\theta^{n-1}$.

De fato, basta mostrar que $\mathbb{Q}[\theta]$ é um corpo. Para isto, é suficiente mostrar que $\theta^n\in\mathbb{Q}[\theta]$ e $\frac{1}{\beta}\in\mathbb{Q}[\theta]$, para todo $\beta\in\mathbb{Q}[\theta]^*$. Como $f(\theta)=0$, temos que

$$a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}+\theta^n=0,$$

isto é,

$$\theta^n=-(a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1})\in\mathbb{Q}[\theta].$$

Seja $\beta\in\mathbb{Q}[\theta]^*$ e $\beta=h(\theta)$, onde $h\in\mathbb{Q}[x]$ e $\partial h<n$. Então $\operatorname{mdc}(f,h)=1$. Logo, existem $g_1,g_2\in\mathbb{Q}[x]$ tais que

$$fg_1+hg_2=1.$$

Assim,

$$1=f(\theta)g_1(\theta)+h(\theta)g_2(\theta)=h(\theta)g_2(\theta).$$

Portanto, $\frac{1}{\beta}=g_2(\theta)\in\mathbb{Q}[\theta]$. Neste caso, $\mathbb{Q}[\theta]=\mathbb{Q}(\theta)$. ■

Um elemento $\theta\in\mathbb{C}$ é um *inteiro algébrico* se existir um polinômio mônico $f(x)\in\mathbb{Z}[x]$ tal que $f(\theta)=0$. Seja

$$\overline{\mathbb{Z}}=\{\theta\in\mathbb{C}:\theta \text{ é um inteiro algébrico}\}.$$

Então $\overline{\mathbb{Z}}$ é um subanel de $\mathbb{C}$.

Um subcorpo K de $\mathbb{C}$ é um *corpo de números* se ele é uma extensão finita de $\mathbb{Q}$, isto é, K é um espaço vetorial sobre $\mathbb{Q}$ de dimensão finita.

Teorema 2.2 *Se K é uma extensão finita de $\mathbb{Q}$, então existe um número (inteiro) algébrico $\theta\in K$ tal que $K=\mathbb{Q}(\theta)$. Neste caso, qualquer $\theta\in K$ tal que $K=\mathbb{Q}(\theta)$ é chamado um elemento primitivo de K.*

Prova. Vamos usar indução sobre $[K:\mathbb{Q}]=n$. Se $n=1$, nada há para provar. Suponhamos que $n>1$ e que o resultado seja válido para todas as extensões de $\mathbb{Q}$ com dimensão menor do que n.

Seja $\alpha_1 \in K$, com $\alpha_1 \notin \mathbb{Q}$. Se $K_1 = \mathbb{Q}(\alpha_1)$ e $K = K_1$, nada mais a demonstrar; caso contrário, existe $\alpha_2 \in K$ tal que $\alpha_2 \notin K_1$. Seja $K_2 = K_1(\alpha_2) = \mathbb{Q}(\alpha_1, \alpha_2)$. Prosseguindo assim, temos que existem $\alpha_1, \alpha_2, \ldots, \alpha_m \in K$, $m > 1$, tais que

$$K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_m) \text{ e } \alpha_i \notin K_{i-1} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}).$$

Como $[K_{m-1} : \mathbb{Q}] < n$ temos, pela hipótese de indução, que existe $\alpha \in K_{m-1}$ tal que $K_{m-1} = \mathbb{Q}(\alpha)$. Mas

$$K = K_m = K_{m-1}(\alpha_m) = \mathbb{Q}(\alpha, \alpha_m).$$

Assim, fazendo $\alpha_m = \beta$, obtemos que $K = \mathbb{Q}(\alpha, \beta)$. Agora, vamos provar que existe $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$.

Sejam $p = \operatorname{irr}(\alpha, \mathbb{Q})$ e $q = \operatorname{irr}(\beta, \mathbb{Q})$, com $\partial(p) = r$ e $\partial(q) = s$. Como a característica de $\mathbb{Q}$ é zero temos que todas as raízes de p e q em $\mathbb{C}$ são distintas. Sejam $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ e $\beta = \beta_1, \beta_2, \ldots, \beta_s$ as raízes de p e q, respectivamente. Assim, cada equação

$$\alpha_i + \beta_j x = \alpha + \beta x, i = 1, \ldots, r, j = 2, \ldots, s,$$

tem um número finito de soluções em $\mathbb{C}$ e no máximo uma em $\mathbb{Q}$. Como $\mathbb{Q}$ é infinito temos que existe $c \in \mathbb{Q}$ tal que

$$\alpha_i + \beta_j c \neq \alpha + \beta c, i = 1, \ldots, r, j = 2, \ldots, s.$$

Seja $\theta = \alpha + c\beta \in K$. Então é claro que $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$ e $\theta - c\beta_j \neq \alpha_i$, para todo $i = 1, \ldots, r, j = 2, \ldots, s$. Defina

$$f = p(\theta - cx) \in \mathbb{Q}(\theta)[x].$$

Logo, $f(\beta) = p(\alpha) = 0$ e $f(\beta_j) \neq 0$, para todo $j = 2, \ldots, s$, isto é, β é uma raiz de f e nenhum β_j é raiz de f, $j = 2, \ldots, s$. Seja $g = \operatorname{irr}(\beta, \mathbb{Q}(\theta))$. Então g divide f e q. Logo, $g = x - \beta$, isto é, $\beta \in \mathbb{Q}(\theta)$ e $\alpha = \theta - c\beta \in \mathbb{Q}(\theta)$. Portanto, $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\theta)$. ■

Teorema 2.3 *Seja $K = \mathbb{Q}(\theta)$, tal que $[K : \mathbb{Q}] = n$. Então existem exatamente n homomorfismos injetores $\sigma_i : K \to \mathbb{C}$. Além disso, $\theta_i = \sigma_i(\theta)$ são as raízes de $f = \operatorname{irr}(\theta, \mathbb{Q})$.*

Prova. Sejam $\theta_1, \ldots, \theta_n$ as raízes distintas de f. Então cada θ_i tem como polinômio irredutível o f, pois se $f_i = \operatorname{irr}(\theta_i, \mathbb{Q})$, então f_i divide f e $f_i = f$. Assim, existe um único isomorfismo de corpos

$$\sigma_i : \mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta_i)$$

tal que $\sigma_i(\theta) = \theta_i$. De fato, se $\alpha \in \mathbb{Q}(\theta)$, então existe $g \in \mathbb{Q}[x]$ tal que $\alpha = g(\theta)$. Assim, pelo Algoritmo da Divisão, existem únicos $q, r \in \mathbb{Q}[x]$ tais que

$$g = fq + r, \text{ onde } 0 \leq \partial r < n.$$

Logo, $\alpha = r(\theta)$ com $\partial r < n$. Como $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ temos que $\sigma_i(\alpha) = r(\theta_i)$.

Reciprocamente, se $\sigma : K \longrightarrow \mathbb{C}$ é um homomorfismo injetor, então

$$0 = \sigma(0) = \sigma(f(\theta)) = f(\sigma(\theta)).$$

Assim, $\sigma(\theta)$ é um dos θ_i. Portanto, $\sigma = \sigma_i$, para algum $i = 1, \ldots, n$. ■

Os elementos $\theta_i = \sigma_i(\theta)$ são chamados os *conjugados* de θ. Neste caso,

$$B = \{1, \theta, \ldots, \theta^{n-1}\}$$

é uma base de K como espaço vetorial sobre $\mathbb{Q}$.

2.1 Corpos Quadráticos

Um *corpo quadrático* é um corpo de números K de dimensão 2 sobre $\mathbb{Q}$. Portanto, $K = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico e raiz do polinômio

$$f = \mathrm{irr}(\theta, \mathbb{Q}) = x^2 + ax + b, \text{ com } a, b \in \mathbb{Z}.$$

Assim,

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2} \text{ ou } 2\theta = -a \pm \sqrt{a^2 - 4b}.$$

Seja $a^2 - 4b = c^2 d$, onde $c, d \in \mathbb{Z}$ e d livre de quadrado. Então

$$\begin{aligned} K &= \mathbb{Q}(\theta) \\ &= \mathbb{Q}(2\theta) \\ &= \mathbb{Q}(-a \pm c\sqrt{d}) \\ &= \mathbb{Q}(\sqrt{d}). \end{aligned}$$

Se d é negativo, K é chamado um *corpo quadrático imaginário* e se d é positivo, K é chamado um *corpo quadrático real*.

Seja $\omega \in K$. Então $\omega = a + b\sqrt{d}$, onde $a, b \in \mathbb{Q}$. Se $\overline{\omega} = a - b\sqrt{d}$, então

$$\begin{aligned} f &= (x-\omega)(x-\overline{\omega}) \\ &= x^2 - 2ax + (a^2 - b^2 d). \end{aligned}$$

Portanto, $\omega \in \mathbb{Z}_K$ se, e somente se, $2a \in \mathbb{Z}$ e $a^2 - b^2 d \in \mathbb{Z}$.

Teorema 2.4 *Seja $d \in \mathbb{Z}$ livre de quadrado. Então*

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & se\ \ d \equiv 2\ \ ou\ \ 3 (\operatorname{mod} 4), \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & se\ \ d \equiv 1 (\operatorname{mod} 4). \end{cases}$$

Prova. Se $\omega \in \mathbb{Z}_K$, então $2a \in \mathbb{Z}$ e $a^2 - b^2 d \in \mathbb{Z}$. Como

$$4a^2 - 4b^2 d = (2a)^2 - d(2b)^2 \in 4\mathbb{Z} \subset \mathbb{Z}$$

temos que $(2b)^2 \in \mathbb{Z}$. Seja $2b = \frac{r}{s}$, onde $r, s \in \mathbb{Z}$, $s \neq 0$ e $\operatorname{mdc}(r, s) = 1$. Então

$$d(2b)^2 = \frac{dr^2}{s^2} \in \mathbb{Z}.$$

Se $s \neq \pm 1$, então existe um fator primo p de s. Assim, p^2 divide dr^2. Sendo $\operatorname{mdc}(p^2, r^2) = 1$ temos que p^2 divide d, o que é uma contradição. Logo, $2b \in \mathbb{Z}$. Portanto, podemos assumir $a = \frac{m}{2}$ e $b = \frac{n}{2}$. Assim, há dois casos a serem considerados:

1º **Caso**. Se n é par, então m é par, pois $m^2 - dn^2 \in 4\mathbb{Z}$. Portanto, $a, b \in \mathbb{Z}$.

2º **Caso**. Se n é ímpar, então m é ímpar, pois $m^2 - dn^2 \in 4\mathbb{Z}$. Portanto, $a, b \in \mathbb{Z} + \frac{1}{2}$, isto é,

$$\omega = \frac{m}{2} + \frac{n}{2}\sqrt{d},$$

com m, n ímpares. Como $m^2 \equiv dn^2 (\operatorname{mod} 4)$ e d livre de quadrado temos que

$$d \equiv 1, 2\ \text{ ou }\ 3 (\operatorname{mod} 4).$$

Se $d \equiv 1 (\operatorname{mod} 4)$, então $m^2 - n^2 \equiv 0 (\operatorname{mod} 4)$. Logo, m e n têm a mesma paridade. Portanto,

$$\mathbb{Z}_K \subseteq \mathbb{Z}[\frac{1+\sqrt{d}}{2}].$$

Reciprocamente, se m e n têm a mesma paridade, então

$$\frac{m+n\sqrt{d}}{2} + \frac{m-n\sqrt{d}}{2} = m \in \mathbb{Z}$$

e

$$\left(\frac{m+n\sqrt{d}}{2}\right)\left(\frac{m-n\sqrt{d}}{2}\right)=\frac{m-dn^2}{4}\in\mathbb{Z}.$$

Portanto,

$$\frac{m}{2}+\frac{n}{2}\sqrt{d}\in\mathbb{Z}_K.$$

Neste caso,

$$\mathbb{Z}_K=\mathbb{Z}[\frac{1+\sqrt{d}}{2}].$$

Se $d\equiv 2$ ou $3(\bmod 4)$, então prova-se, de modo análogo, que $\mathbb{Z}_K=\mathbb{Z}[\sqrt{d}]$. ■

Teorema 2.5 *Se $d\equiv 2$ ou $3(\bmod 4)$, então $B=\{1,\sqrt{d}\}$ é uma base minimal de $\mathbb{Z}_K=\mathbb{Z}[\sqrt{d}]$.*

Prova. Se $d\equiv 2$ ou $3(\bmod 4)$, então $\mathbb{Z}_K=\mathbb{Z}[\sqrt{d}]$ e $\alpha\in\mathbb{Z}_K$ é da forma $\alpha=a+b\sqrt{d}$, com $a,b\in\mathbb{Z}$, e $\operatorname{irr}(\sqrt{d},\mathbb{Q})=x^2-d$ temos que

$$\begin{aligned}\phi_\alpha(1)&=\alpha\\ \phi_\alpha(\sqrt{d})&=bd+a\sqrt{d}.\end{aligned}$$

Logo, $\mathbb{Z}_K$ é isomorfo ao conjunto das matrizes da forma

$$\begin{pmatrix} a & bd\\ b & a\end{pmatrix},\ \text{onde } a,b\in\mathbb{Z}.$$

Neste caso,

$$Tr(\alpha)=2a \text{ e } N(\alpha)=a^2-db^2.$$

Assim, o discriminante associado à base B é dado por

$$\begin{aligned}D(B)&=\det\begin{pmatrix} Tr(1) & Tr(\sqrt{d})\\ Tr(\sqrt{d}) & Tr(d)\end{pmatrix}\\ &=\det\begin{pmatrix} 2 & 0\\ 0 & 2d\end{pmatrix}\\ &=4d.\end{aligned}$$

Como $Tr(\alpha)$ é um número inteiro par, temos que o discriminante de qualquer base inteira B' de $\mathbb{Z}_K$ é um múltiplo de 4, por exemplo $D(B')=4m$. Assim, se r é o determinante da matriz mudança de base, então $D(B) = r^2 D(B')$ ou $d = r^2 m$. Suponhamos que $|m| < |d|$. Então

$$|m| < \left|r^2 m\right| \Rightarrow |r| > 1.$$

Logo, d possui um fator quadrático, o que é uma contradição. Portanto, a base $B = \{1, \sqrt{d}\}$ é minimal. ■

Complementamos esta seção, expondo em detalhes o corpo quadrático $\mathbb{Q}[\sqrt{d}]$, para o caso particular $d = -1$. O anel dos inteiros $\mathbb{Z}[i]$ de $\mathbb{Q}[\sqrt{d}]$ é chamado "Anel dos Inteiros Gaussianos" e é uma ferramenta importante para descrever o grupo dos pontos racionais sobre o círculo unitário via homomorfismo de monóides.

Proposição 2.1 *Seja $\alpha \in \mathbb{Z}[i]$. Então as seguintes afirmações são equivalentes:*

1. α é invertível em $\mathbb{Z}[i]$;

2. $N(\alpha) = 1$;

3. $\alpha \in \{-1, 1, -i, i\}$.

Prova. (1. $\Rightarrow$ 2.) Sendo α invertível, existe $\beta \in \mathbb{Z}[i]$ tal que $\alpha\beta = 1$. Consequentemente,

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1.$$

Como $N(\alpha) \in \mathbb{Z}^+$, segue dessas igualdades que $N(\alpha) = 1$.

(2. $\Rightarrow$ 3) Suponhamos que $N(\alpha) = 1$. Fazendo $\alpha = x + yi$, obtemos $x^2 + y^2 = 1$, cujas soluções em $\mathbb{Z} \times \mathbb{Z}$ são $(0, \pm 1)$ e $(\pm 1, 0)$. Portanto, $\alpha \in \{-1, 1, -i, i\}$.

(2. $\Rightarrow$ 3.) Se $\alpha \in \{-1, 1, -i, i\}$, então α é invertível em $\mathbb{Z}[i]$. ■

Lema 2.1 [4] *Todo elemento primo de $\mathbb{Z}[i]$ divide um número primo de $\mathbb{Z}$.* ■

Lema 2.2 [4] *Seja $\alpha \in \mathbb{Z}[i]$ tal que $N(\alpha)$ é um número primo em $\mathbb{Z}$. Então α é primo em $\mathbb{Z}[i]$.* ■

Lema 2.3 [4] *Seja p é um número primo em $\mathbb{Z}$. Então as seguintes afirmações são equivalentes:*

1. *p é redutível em $\mathbb{Z}[i]$;*

2. *$p = \alpha\overline{\alpha}$, onde α primo em $\mathbb{Z}[i]$;*

3. p é a soma de dois quadrados.

Prova.(1. $\Rightarrow$ 2.) Suponhamos que p seja redutível em $\mathbb{Z}[i]$. Então $p = \alpha\beta$, para alguns $\alpha, \beta \notin U(\mathbb{Z}[i])$. Como $p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$ temos que $N(\alpha) = N(\beta) = p$, pois $\alpha, \beta \notin U(\mathbb{Z}[i])$. Logo, pelo Lema 2.2, obtemos que α é primo em $\mathbb{Z}[i]$. Por outro lado,

$$\beta = \frac{p}{\alpha} = \frac{p\overline{\alpha}}{N(\alpha)} = \overline{\alpha}.$$

Logo, $p = \alpha\beta = \alpha\overline{\alpha}$.

(2. $\Rightarrow$ 3.) Suponhamos que $p = \alpha\overline{\alpha}$ e $\alpha = a + bi$ seja primo em $\mathbb{Z}[i]$. Então

$$p = \alpha\overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2,$$

e, portanto p é a soma de dois quadrados.

(3. $\Rightarrow$ 1.) Se $p = a^2 + b^2$, então $p = (a + bi)(a - bi)$. ■

Um elemento $x \in \mathbb{Z}$ é um *resíduo quadrático* módulo m se existir $y \in \mathbb{Z}$ tal que

$$y^2 \equiv x \pmod{m}$$

Lema 2.4 [4]*Para todo primo ímpar p existe $x \in \mathbb{Z}$ tal que*

$$y^2 \not\equiv x \pmod{p}, \forall y \in \mathbb{Z}.$$

■

Lema 2.5 [4]*Sejam p um número primo com $p > 2$ e a um inteiro não resíduo quadrático módulo p. Então*

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

■

Teorema 2.6 (Fermat) [4]*Seja p um número primo em $\mathbb{Z}$. Então as seguintes afirmações são equivalentes*:

1. p é a soma de dois quadrados;

2. $p = 2$ ou $p \equiv 1 \pmod{4}$;

3. -1 é resíduo quadrático módulo p.

Prova. (1. $\Rightarrow$ 2.) Suponhamos que $p = a^2 + b^2$. Supondo $p > 2$, vamos provar que $p \equiv 1 \pmod 4$. Como p é um primo não par, temos que a e b são de paridades diferentes, portanto

$$p = a^2 + b^2 = (2n+1)^2 + (2m)^2 \,,$$

e consequentemente, $p \equiv 1 \pmod 4$.

(2. $\Rightarrow$ 3.): Se $p = 2$, então $-1 \equiv 1 \pmod 2$ e portanto -1 é resíduo quadrático módulo 2. Suponhamos agora que $p \equiv 1 \pmod 4$. Seja a um inteiro que não é resíduo quadrático módulo p (tal inteiro existe em virtude do Lema 2.4). Como $p \equiv 1 \pmod 4$, temos que $b = a^{\frac{p-1}{4}}$ é um inteiro e pelo Lema 2.5,

$$b^2 = a^{\frac{p-1}{2}} \equiv -1 \,(\mathrm{mod}\, p) \,,$$

e consequentemente -1 é um resíduo quadrático módulo p.

(3. $\Rightarrow$ 1.): Suponhamos que existe $b \in \mathbb{Z}$ tal que

$$b^2 \equiv -1 \,(\mathrm{mod}\, p) \,.$$

Logo p divide $b^2 + 1$ e portanto

$$p \mid (b+i)\,(b-i) \,.$$

Observe que $p \nmid (b \pm i)$ pois caso contrário, teríamos para algum $t + si \in \mathbb{Z}\,[i]$ que $p\,(t+si) = b \pm i$, o que implicaria que $ps = \pm 1$, absurdo.

Temos então que p não é primo em $\mathbb{Z}\,[i]$ e portanto redutível. Pelo Lema 2.3, temos que p é a soma de dois quadrados. ∎

Corolário 2.1 *[4] Os elementos primos de $\mathbb{Z}\,[i]$ são:*

1. Os associados dos primos p de $\mathbb{Z}\,[i]$ tais que $p \equiv 3 \,(\mathrm{mod}\, 4)\,;$

2. Os elementos da forma $a + bi$ tais que $a^2 + b^2$ é primo em $\mathbb{Z}\,[i]$

Prova. Pelo Lema 2.1, temos que todo primo α de $\mathbb{Z}\,[i]$ é divisor primo de um número primo p de $\mathbb{Z}$. Se p não é soma de dois quadrados, pelo Lema 2.3, temos que p é irredutível em $\mathbb{Z}\,[i]$, logo primo e isto ocorre se e somente se $p \equiv 3 \pmod 4$. Neste caso α é associado de p.

Se $p = 2$ ou $p \equiv 1 \pmod 4$, então pelo Teorema 2.6 temos que p é a soma de dois quadrados e, portanto, pelo Lema 2.3, temos que $\alpha = a + bi$ com $a^2 + b^2 = p$.

2.2 O Anel $\mathbb{Z}[\varepsilon]$.

Seja $\mathbb{Z}[\varepsilon]$ o anel quociente

$$\mathbb{Z}[\varepsilon] = \frac{\mathbb{Z}[x]}{\langle x^2 - 1 \rangle}.$$

Então, denotando $\varepsilon = \bar{x}$ temos que $\varepsilon^2 = 1$ e

$$\mathbb{Z}[\varepsilon] = \{m + n\varepsilon : m, n \in \mathbb{Z}\}.$$

Note que $\mathbb{Z}[\varepsilon]$ não é um domínio de integridade, pois

$$(\varepsilon - 1)(\varepsilon + 1) = \varepsilon^2 - 1 = 0.$$

Para contornar esta situação, consideremos

$$R[\varepsilon\} = \{m + n\varepsilon : m > n \text{ com } m \neq -n\} \subseteq \mathbb{Z}[\varepsilon].$$

Note que, se identificarmos cada elemento $(m + n\varepsilon)$ de $R[\varepsilon]$ com o $(m, n) \in \mathbb{Z} \times \mathbb{Z}$, obtemos

$$(m_1, n_1)(m_2, n_2) = (m_1 m_2 + n_1 n_2, m_1 n_2 + m_2 n_1),$$

e pelo fato de que $m_1 > n_1$ e $m_2 > n_2$ implica que existem $a_1, a_2 \in \mathbb{N}$ tais que $m_1 = n_1 + a_1$ e $m_2 = n_2 + a_2$. Logo,

$$m_1 m_2 + n_1 n_2 - (m_1 n_2 + m_2 n_1) = a_1 a_2 > 0.$$

Portanto, $R[\varepsilon]$ é um monóide sob a multiplicação. Além disso, $R[\varepsilon]$ possui a propriedade de fatoração única com a norma $N : R[\varepsilon] \to \mathbb{Z}^*$ definida por

$$N(m + n\varepsilon) = m^2 - n^2,$$

exceto, para aqueles elementos redutíveis com norma uma potência de 2, pelo fato de que

$$2^n = 2^2 2^{n-2} = 2^3 2^{n-3} = \cdots,$$

por exemplo,

$$N(12 + 4\varepsilon) = 128 = 2^7 = 2^2 2^2 2^3 = 2^4 2^3$$

Neste caso, as formas de se agrupar as potências de dois, nos permite fatorar

$$12 + 4\varepsilon = (2, 0)(2, 0)(3, 1),$$

ou

$$12 + 4\varepsilon = (3, -1)(5, 3)$$

onde

$$N(2,0) = 2^2, N(3,\pm 1) = 2^3 \text{ e } N(5,3) = 2^4.$$

Proposição 2.2 *Se $N(m + n\varepsilon) = m^2 - n^2$ é um número primo em $\mathbb{Z}$, então $m + n\varepsilon$ é irredutível em $R[\varepsilon]$.*

Prova. Suponhamos, por absurdo, que $m+n\varepsilon$ não seja irredutível em $R[\varepsilon]$. Então existem $\alpha, \beta \in R[\varepsilon]$ tais que

$$N(m + n\varepsilon) = N(\alpha)\, N(\beta),$$

onde $N(\alpha) \neq 1$ e $N(\beta) \neq 1$, o que é uma contradição, pois $N(m + n\varepsilon)$ é um número primo. ■

Proposição 2.3 *Sejam $p_1, p_2, \ldots p_n$ primos ímpares, não necessariamente distintos, com $n \in \mathbb{N}$. Então*

$$\prod_{i=1}^{n} \left(\frac{p_i + 1}{2}, \frac{p_i - 1}{2} \right) = \left(\frac{1}{2} \left(\prod_{i=1}^{n} p_i + 1 \right), \frac{1}{2} \left(\prod_{i=1}^{n} p_i - 1 \right) \right).$$

para todo $\left(\frac{p_i+1}{2}, \frac{p_i-1}{2}\right) \in R[\varepsilon] \subset \mathbb{Z}[\varepsilon]$.

Prova. Vamos usar indução sobre n. Se $n = 2$, então é claro que

$$\left(\frac{p_1 + 1}{2}, \frac{p_1 - 1}{2} \right) \left(\frac{p_2 + 1}{2}, \frac{p_2 - 1}{2} \right) = \left(\frac{p_1 p_2 + 1}{2}, \frac{p_1 p_2 - 1}{2} \right).$$

Suponhamos que o resultado seja válido para $n > 2$. Então

$$\begin{aligned}
\prod_{i=1}^{n+1} \left(\frac{p_i + 1}{2}, \frac{p_i - 1}{2} \right) &= \prod_{i=1}^{n} \left(\frac{p_i + 1}{2}, \frac{p_i - 1}{2} \right) \left(\frac{p_{n+1} + 1}{2}, \frac{p_{n+1} - 1}{2} \right) \\
&= \left(\frac{1}{2} \left(\prod_{i=1}^{n} p_i + 1 \right), \frac{1}{2} \left(\prod_{i=1}^{n} p_i - 1 \right) \right) \left(\frac{p_{n+1} + 1}{2}, \frac{p_{n+1} - 1}{2} \right) \\
&= \left(\frac{1}{2} \left(\prod_{i=1}^{n+1} p_i + 1 \right), \frac{1}{2} \left(\prod_{i=1}^{n+1} p_i - 1 \right) \right).
\end{aligned}$$

■

Proposição 2.4 *Sejam $p_1, p_2, \ldots, p_n$ primos ímpares. Então*

$$\alpha = \prod_{i=1}^{n} \left(\frac{p_i + 1}{2}, \frac{p_i - 1}{2} \right)$$

tem norma $N(\alpha) = p_1 p_2 \cdots p_n$.

Prova. Pela Proposição 2.3

$$\begin{aligned}
N(\alpha) &= N\left(\frac{1}{2}\left(\prod_{i=1}^{n} p_i + 1\right), \frac{1}{2}\left(\prod_{i=1}^{n} p_i - 1\right)\right) \\
&= \frac{1}{4}\left(\prod_{i=1}^{n} p_i + 1\right)^2 - \frac{1}{4}\left(\prod_{i=1}^{n} p_i - 1\right)^2 \\
&= \prod_{i=1}^{n} p_i \\
&= p_1 p_2 \cdots p_n.
\end{aligned}$$

■

Proposição 2.5 *Todos os elementos irredutíveis em $R[\varepsilon]$ são da forma:*

1. $\left(\frac{p+1}{2}, \frac{p-1}{2}\right)$, *onde p é um primo ímpar;*

2. $(3,1)$;

3. $(m, m-2)$, *com $N(m,(m-2)) = 2^k$, $k = 2$ e $k \neq 3$.*

Prova. Como

$$N\left(\left(\frac{p+1}{2}, \frac{p-1}{2}\right)\right) = p$$

para todo número primo ímpar temos, pela Proposição 2.2, que o elemento

$$\left(\frac{p+1}{2}, \frac{p-1}{2}\right)$$

é irredutível sobre $R[\varepsilon]$. Finalmente, como a única fatoração possível dos elementos da forma

$$(m, m-2) \text{ com } N(m,(m-2)) = 2^k, k = 2 \text{ e } k > 3,$$

é

$$(m, m-2) = (2,0)\left(\frac{3}{2}, \frac{1}{2}\right)^{k-2}$$

em $\mathbb{Q}[\varepsilon]$, temos que eles são irredutíveis, pois

$$\frac{3}{2}, \frac{1}{2} \notin \mathbb{Z}.$$

■

Observação 2.1 1. *Todos os elementos irredutíveis da forma*

$$\left(\frac{p+1}{2}, \frac{p-1}{2}\right)$$

em $R[\varepsilon]$, com p um número primo ímpar e estão sobre a reta

$$y = x - 1.$$

Além disso, estes são os únicos elementos irredutíveis sobre esta reta.

2. *Todos os elementos*

$$\alpha = (m, m-2) \text{ com } N(\alpha) = 2^k \text{ e } k > 1,$$

em $R[\varepsilon]$, são irredutíveis e estão sobre a reta $y = x - 2$. Além disso, estes são os únicos elementos irredutíveis sobre esta reta, isto é, todo elemento $(m, m-2) \in R[\varepsilon]$, com

$$N(m, (m-2)) \neq 2^k.$$

é redutível.

3. *Todos os elementos de forma $(m, m-a) \in R[\varepsilon]$, com $2 < a < m$, têm norma*

$$N(m, m-a) = 2am - a^2.$$

Logo,

$$a \mid N(m, m-a).$$

Assim, há dois casos a considerar:

   (a) *Se $N(m, m-a)$ é ímpar, então*

$$\frac{N(m, m-a)}{a} = p_1 \cdots p_k,$$

   onde p_j é um número primo ímpar em $\mathbb{Z}$, e

$$(m, m-a) = (\frac{a+1}{2}, -\frac{a-1}{2}) \oplus \left(\frac{1}{2} \left(\prod_{i=1}^{k} p_i + 1 \right), \frac{1}{2} \left(\prod_{i=1}^{k} p_i - 1 \right) \right).$$

   (b) *Se $N(m, m-a)$ é par, então há dois casos a considerar:*

      i. *$N(m, m-a) = 2^t$ para $a \geq 4$.*
      Neste caso $a = 2^k$, ou seja, os elementos de $R[\varepsilon]$ estão nas retas $y = x - 2^k$, e a fatoração destes elementos ocorre da seguinte forma: Se $a = 4$ então $(m, m-4)$ é o produto de dois ou mais elementos do tipo $(m, m-2)$. Se $a = 8$ então $(m, m-8)$ é escrito como produto de dois ou mais elementos do tipo $(m, m-2)$ e $(m, m-4)$ e assim sucessivamente.

ii. $N(m, m-a) = 2^t P$, *onde* P *é um inteiro ímpar.*

Considere as retas

$$\begin{aligned} rs_a &= \{(x, x-a) : a \in \mathbb{N}^*\} \\ rs_b &= \{(x, b-x) : b \in \mathbb{N}^*\} \end{aligned}$$

então dado $\alpha \in R[\varepsilon]$, *basta considerar o caso em que*

$$\alpha \in A = \{m + n\varepsilon : -n > m > n\},$$

visto que $\alpha \in A$ *ou* $(0, -1) \oplus \alpha \in A$. *Seja* $\alpha \in A$, *tal que* $N(m, m-a) = 2^t P$, *onde* P *é um inteiro ímpar. Então existem* $a, b \in \mathbb{N}^*$ *tal que*

$$\alpha = rs_a \cap rd_b$$

e seguindo os passos do seguinte algoritmo fatoraremos α.

Algoritmo

1. Fatore

$$N(\alpha) = 2^r P,$$

onde P é um inteiro ímpar

2. Faça:

$$mrs_a = \min\{N(\beta) : \beta \in (x, x-a)\},$$

$$mrs_b = \min\{N(\beta) : \beta \in (x, b-x)\},$$

e

$$I = 1; \quad m_a := mrs_a; \quad m_b := mrs_b.$$

3. Faça $P = \frac{N(\alpha)}{m_a}$;

Se P é ímpar, então considere $\beta \in A$ correspondente ao m_a e

$$\alpha = \left(\frac{P+1}{2}, \frac{P-1}{2}\right) \cdot \beta.$$

Caso contrário, vá para o item seguinte.

4. Faça $P = \frac{N(\alpha)}{m_b}$;

   Se P é ímpar então considere $\beta \in A$ correspondente ao m_b e

$$\alpha = \left(\frac{P+1}{2}, -\frac{P-1}{2} \right) \cdot \beta.$$

   Caso contrário, vá para o item seguinte

5. Faça

$$\begin{aligned} I &= I+1; \\ m_a &= I \cdot m_a; \\ m_b &= I \cdot m_b; \end{aligned}$$

6. Vá para o item 3.

Capítulo 3

Pontos Racionais sobre Cônicas

3.1 Introdução

Sejam $\mathbb{R}[x, y]$ o anel dos polinômios em duas variáveis e $f(x, y) \in \mathbb{R}[x, y]$. O conjunto de pontos $(x, y) \in \mathbb{R}^2$ tais que

$$f(x, y) = 0$$

é chamado uma *curva algébrica*, o qual denotamos por C_f ou, mais precisamente, por $C_f(\mathbb{R})$.

Um ponto $(x, y) \in \mathbb{R}^2$ é chamado um *ponto racional* se $x, y \in \mathbb{Q}$. O principal objetivo desta seção é apresentar uma generalização do problema de encontrar pontos racionais sobre uma curva, isto é, os pontos de $C_f(\mathbb{Q})$. Note que $C_f(\mathbb{Q}) \subset C_f(\mathbb{R})$. A curva $C_f(\mathbb{R})$ pode ser vazia, por exemplo

$$f(x, y) = x^2 + y^2 + 1.$$

Mesmo que a curva $C_f(\mathbb{R})$ não seja vazia, esta pode não conter pontos racionais. Por exemplo, se

$$f(x, y) = x^2 + y^2 - 3,$$

então $C_f(\mathbb{R})$ é a circunferência de raio $\sqrt{3}$ centrada na origem. A existência de um ponto racional nesta curva é equivalente a existência de inteiros u, v e w, não todos nulos e $\mathrm{mdc}(u, v, w) = 1$, tais que

$$u^2 + v^2 = 3w^2. \tag{3.1}$$

A hipótese de que a equação (3.1) tenha solução em $\mathbb{Z}$ pode ser considerada para qualquer anel quociente. Em particular, para o anel $\mathbb{Z}_n$, para todo inteiro n. A escolha de

$n = 4$ é particularmente eficaz, pela seguinte razão: os resíduos quadráticos $(\bmod 4)$ são simplesmente 0 e 1. Assim, substituindo estes valores para u^2, v^2 e w^2 na equação (3.1), veremos que só o terno $(0,0,0)$ satisfaz a equação acima. Isto significa que u, v e w são inteiros pares pois os quadrados de inteiros ímpares são congruentes a $1(\bmod 4)$. O que é uma contradição. Portanto $C_f(\mathbb{Q})$ é vazia.

Todas as curvas consideradas nesta dissertação, salvo menção explicita ao contrário, estão em $\mathbb{R}^2$ e, por isto, são chamadas de *curvas planas*. O *grau* da curva C_f é simplesmente o grau do polinômio f. Se o grau de f é igual a 1, C_f é uma reta, se o grau f é igual 2, C_f é uma cônica. Uma cônica pode ser uma elipse, uma parábola, uma hipérbole ou cônicas degeneradas.

As interseções de uma reta com uma curva C_f, podem gerar novos pontos racionais em C_f, além daqueles já conhecidos. (Confira [6])

Exemplo 3.1 *Encontrar todos os pontos racionais na elipse* $x^2 + 5y^2 = 1$.

Solução. Note que o ponto $(1,0)$ é um ponto racional desta curva. Se (x_1, y_1) é um segundo ponto racional nesta curva, então a inclinação m da reta unindo estes dois pontos é um número racional. A reta que passa no ponto $(1,0)$ com inclinação m tem como equação

$$y = m(x-1). \tag{3.2}$$

Para determinar a outra interseção desta reta com a elipse, substituímos y por $m(x-1)$ na equação $x^2 + 5y^2 = 1$, obtendo

$$(5m^2+1)x^2 - 10m^2x + (5m^2-1) = 0.$$

e esta equação do 2^0 grau na variável x, tem como solução, $x_0 = 1$ já conhecida e

$$x_1 = \frac{5m^2-1}{5m^2+1}.$$

Substituindo x_1 na equação (3.2), obtemos

$$y_1 = \frac{-2m}{5m^2+1}.$$

Como, por hipótese, m é racional temos que x_1 e y_1 são racionais. Portanto, as equações

$$\begin{cases} m = \frac{y_1}{x_1-1} \\ x_1 = \frac{5m^2-1}{5m^2+1} \\ y_1 = \frac{-2m}{5m^2+1} \end{cases}$$

determinam uma correspondência biunívoca entre números racionais m e pontos racionais (x_1, y_1) na elipse $x^2 + 5y^2 = 1$, menos o ponto inicial $(1, 0)$.

Como todo número racional m pode ser escrito sob a forma

$$m = \frac{r}{s}; r, s \in \mathbb{Z} \text{ e } s \neq 0$$

temos que

$$\begin{cases} x_1 = \frac{5r^2 - s^2}{5r^2 + s^2}, \\ y_1 = \frac{-2rs}{5r^2 + s^2}. \end{cases}$$

Conseqüentemente, se $(u, v, w) \in \mathbb{Z}^3$ é tal que

$$u^2 + 5v^2 = w^2,$$

então o ponto $\left(\frac{u}{w}, \frac{v}{w}\right)$ pertence a

$$x^2 + 5y^2 = 1$$

e, portanto, existem $r, s \in \mathbb{Z}$ tais que

$$(5r^2 - s^2, -2rs, 5r^2 + s^2) = k(u, v, w).$$

Note que não obtemos todas as triplas primitivas desta forma, pois é fácil verificar que não existem r, $s \in \mathbb{Z}$ que gerem $(2, 3, 7) \in \mathbb{Z}^3$.

3.2 O Grupo dos Pontos Racionais sobre o Círculo Unitário

Seja C o círculo de centro na origem e raio unitário em $\mathbb{R}^2$, isto é,

$$x^2 + y^2 = 1.$$

Note que

$$\left(\frac{3}{5}, \frac{4}{5}\right), \left(-\frac{5}{13}, \frac{12}{13}\right) \text{ e } (0, 1)$$

são pontos racionais, enquanto que

$$\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$$

não o é. Denotamos o conjunto dos pontos racionais sobre C por $C(\mathbb{Q})$. Um ponto racional $\left(\frac{a}{c}, \frac{b}{c}\right)$ em C corresponde a uma solução *inteira* da equação

$$u^2 + v^2 = w^2,$$

com $u = a$, $v = b$ e $w = c$. Mais geralmente, um ponto racional sobre a curva

$$x^m + y^m = 1$$

corresponde a uma solução inteira da equação

$$u^m + v^m = w^m, \forall m \in \mathbb{N}.$$

O círculo unitário C é um grupo abeliano sob a "adição de ângulos $\oplus$" definida por

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1), \tag{3.3}$$

para todos $(x_1, y_1), (x_2, y_2) \in C$. O elemento identidade é $(1, 0)$ e $(x, -y)$ é o elemento inverso de (x, y).

Note que a correspondência

$$\theta \to (x, y) = (\cos\theta, \operatorname{sen}\theta)$$

transforma a operação (3.3), na "fórmula de adição" da trigonometria ou na fórmula usual para a multiplicação no corpo dos números complexos.

$C(\mathbb{Q})$ é um subgrupo de C, e antes de encontrarmos a sua estrutura de grupo, vamos fazer alguns comentários:

Qualquer solução inteira da equação diofantina

$$x^2 + y^2 = z^2$$

é chamada um *terno pitagórico*. Seja (a, b, c) um terno pitagórico. Então $\left(\frac{a}{c}, \frac{b}{c}\right)$ é um ponto racional em $C(\mathbb{Q})$. Dois termos pitagóricos (a, b, c) e (a', b', c') correspondem ao mesmo ponto em $C(\mathbb{Q})$ se, e somente se,

$$(a, b, c) = r(a', b', c'),$$

para algum $r \in \mathbb{Q}^*$. Portanto, se (a, b, c) é *primitivo* (isto é, se $c > 0$ e $\operatorname{mdc}(a, b, c) = 1$), então qualquer terno pitagórico correspondente ao ponto racional $\left(\frac{a}{c}, \frac{b}{c}\right)$ será da forma (ka, kb, kc), para algum $k \in \mathbb{Z}^*$.

Vimos no primeiro capítulo, que

$$(m^2 - n^2, 2mn, m^2 + n^2),$$

com $m, n \in \mathbb{Z}$ e $m^2 + n^2 \neq 0$, são todos os ternos pitagóricos (a, b, c) com $c > 0$. Aqueles m e n que satisfazem

$$\mathrm{mdc}(m, n) = 1 \text{ e } m - n \equiv 1 (\mathrm{mod}\, 2)$$

produzem ternos pitagóricos primitivos. Vamos agora dar uma interpretação geométrica desta parametrização. As expressões

$$m^2 - n^2 \text{ e } 2mn,$$

lembram-nos as fórmulas do dobro de ângulos para o cosseno e seno, respectivamente. Assim, considerando a 3.1 e a parametrização de C dada por

$$r(\theta) = (\cos\theta, \operatorname{sen}\theta), \forall \theta \in \mathbb{R}.$$

e fazendo

$$\cos\theta = \tfrac{1-\tan^2\beta}{1+\tan^2\beta}$$
$$\operatorname{sen}\theta = \tfrac{2\tan\beta}{1+\tan^2\beta}$$
$$t = \tan\beta, \text{ e } \beta = \tfrac{\theta}{2}$$

obtemos *parametrização racional* $\rho : \mathbb{R} \to \mathbb{C}$ de C, onde

$$\rho(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

e

$$\rho(\mathbb{R}) = C.$$

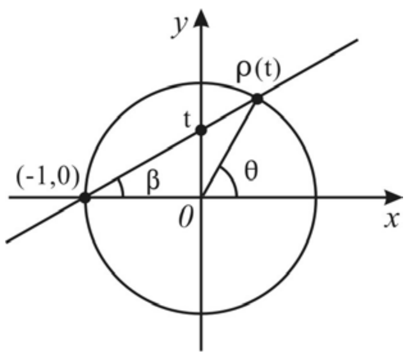

Figura 3.1: Representação geométrica da parametrização racional ρ.

Em particular, se $t = \frac{n}{m}$, com $n, m \in \mathbb{Z}$ e $m \neq 0$, então

$$\rho(\frac{n}{m}) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2} \right).$$

É fácil verificar que toda reta que passa em $(-1, 0)$ e tem inclinação racional intercepta $C - \{(-1, 0)\}$ em um ponto racional, ou seja, um ponto de $C(\mathbb{Q})$.

Seja $\hat{\rho} = \rho|_{\mathbb{Q}}$, isto é, $\hat{\rho}\,(r) = \rho\,(r)$, para todo $r \in \mathbb{Q}$. É fácil verificar que

$$\hat{\rho}(\mathbb{Q}) = C(\mathbb{Q}) - \{(-1, 0)\}.$$

Para cada $m + ni \in \mathbb{Z}\,[i]$, com $m \neq 0$, a reta que passa em $m + ni = (m, n)$ e $0 = (0, 0)$ intercepta a reta $x = 1$ em $\left(1, \frac{n}{m}\right)$, conforme a Figura 3.2.

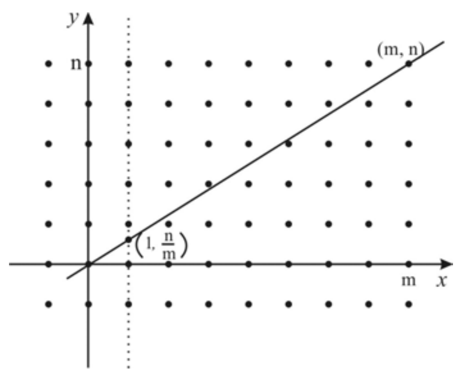

Figura 3.2: Representação geométrica de $\mathbb{Z}\,[i]$.

Pelas observações acima, a translação de eixo $u = x - 1$ e $v = y$ na Figura 3.1 e depois juntando num só gráfico com a Figura 3.2, obtemos a função sobrejetora $f : \mathbb{Z}\,[i]^* \to C(\mathbb{Q})$ definida por

$$f(m + ni) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2} \right) \tag{3.4}$$

onde $f(ni) = (-1, 0)$.

Observação 3.1 *Seja s a reta, cuja equação é*

$$y = \frac{n}{m}x,$$

conforme Figura 3.2. *Então para cada $a + bi = (a, b) \in s \cap \mathbb{Z}\,[i]$, obtemos*

$$f(a + bi) = f(m + ni).$$

Proposição 3.1 *Seja* $f : \mathbb{Z}[i]^* \to C(\mathbb{Q})$ *definida por* 3.4*. Então*:

1. f *é um homomorfismo de monóides*;

2. $f(m - ni) \oplus f(m + ni) = (1, 0)$;

3. $f(m + ni) = (1, 0)$ *se, e somente se,* $n = 0$;

4. $f(m + ni) = (-1, 0)$ *se, e somente se,* $m = 0$. ■

3.3 A Estrutura do Grupo $C(\mathbb{Q})$

Dado um grupo qualquer, sabemos o quanto é importante obter informações sobre seu conjunto de geradores e relações. Nesta seção mostraremos que para elementos irredutíveis α em $\mathbb{Z}[i]$, suas imagens $f(\alpha) \in C(\mathbb{Q})$ são suficientes para gerar $C(\mathbb{Q})$.

Proposição 3.2 *Sejam* $f : \mathbb{Z}[i]^* \to C(\mathbb{Q})$ *definida por* 3.4 *e*

$$(c_k, s_k) = f\left(m_k + n_k i\right), k = 1, 2, 3.$$

Então

$$(c_1, s_1) = (c_2, s_2) \oplus (c_3, s_3)$$

se, e somente se, existem $a, b \in \mathbb{Z}^*$ *tais que*

$$(m_1 + n_1 i)b = (m_2 + n_2 i)(m_3 + n_3 i)a.$$

Prova. Suponhamos que

$$(c_1, s_1) = (c_2, s_2) \oplus (c_3, s_3).$$

Então

$$\begin{aligned} f\left(m_1 + n_1 i\right) &= f\left(m_2 + n_2 i\right) \oplus f\left(m_3 + n_3 i\right) \\ &= f((m_2 + n_2 i)(m_3 + n_3 i)) \\ &= f((m_2 m_3 - n_2 n_3) + (m_2 n_3 + m_3 n_2) i). \end{aligned}$$

Logo, pela observação 3.1,

$$m_1 + n_1 i \text{ e } (m_2 m_3 - n_2 n_3) + (m_2 n_3 + m_3 n_2) i$$

estão sobre a reta que passa em $(0,0)$ e tem inclinação racional. Portanto, existe

$$r = \frac{a}{b} \in \mathbb{Q}^*$$

tal que

$$m_1 + n_1 i = \frac{a}{b}\left[(m_2m_3 - n_2n_3) + (m_2n_3 + m_3n_2)i\right],$$

isto é,

$$(m_1 + n_1 i)b = (m_2 + n_2 i)(m_3 + n_3 i)a.$$

A recíproca é clara. ■

Pelo Corolário 2.1, temos que os elementos irredutíveis em $\mathbb{Z}[i]$ são da forma $\pm p$, $\pm pi$, onde p é um número primo em $\mathbb{Z}$ tal que

$$p \equiv 3 \pmod 4$$

ou $\alpha = x + yi$ tais que $N(\alpha) = x^2 + y^2$ seja um número primo em $\mathbb{Z}$. Logo, pela Proposição 3.1,

$$f(\pm p) = (1,0) \text{ e } f(\pm ip) = (-1,0).$$

Note que $f(\pm p)$ é o elemento identidade de $C(\mathbb{Q})$ e

$$\begin{aligned} 2f(\pm ip) &= f(\pm ip) \oplus f(\pm ip) \\ &= (-1,0) \oplus (-1,0) \\ &= (1,0), \end{aligned}$$

implica que $f(\pm ip)$ é um elemento de ordem 2 em $C(\mathbb{Q})$. Para os elementos irredutíveis $\alpha = x + yi$ tal que $N(\alpha) = x^2 + y^2 = p$ seja um número primo em $\mathbb{Z}$ temos, pelo Teorema 2.6, que $p = 2$ ou

$$p \equiv 1 \pmod 4.$$

Se $p = 2$, então $\alpha = 1 + i$ ou $\alpha = 1 - i$. Logo,

$$f(\alpha) = (0, \pm 1).$$

É fácil verificar que

$$4f(\alpha) = (1,0).$$

Assim, α é um elemento de ordem 4 em $C(\mathbb{Q})$. Se

$$p \equiv 1 \pmod 4,$$

então existem $m_p, n_p \in \mathbb{N}$, com $m_p > n_p$, tais que $p = m_p^2 + n_p^2$. Logo,

$$f(m_p + n_p i) = \left(\frac{m_p^2 - n_p^2}{m_p^2 + n_p^2}, \frac{2m_p n_p}{m_p^2 + n_p^2} \right).$$

Para todo $\beta \in \mathbb{Z}[i]$, existem $\alpha_1, \ldots, \alpha_r$ tais que

$$\beta = \alpha_1 \cdots \alpha_r, \forall \beta \in \mathbb{Z}[i],$$

onde α_j são elementos irredutíveis em $\mathbb{Z}[i]$, temos que

$$\left\{ \left(\frac{m_p^2 - n_p^2}{m_p^2 + n_p^2}, \frac{2m_p n_p}{m_p^2 + n_p^2} \right) \right\}_{p \equiv 1 \pmod 4} \bigcup \{(0,1)\}$$

é o conjunto de todos os geradores de $C(\mathbb{Q})$.

Lema 3.1 *O conjunto*

$$\left\{ \left(\frac{m_p^2 - n_p^2}{m_p^2 + n_p^2}, \frac{2m_p n_p}{m_p^2 + n_p^2} \right) \right\}_{p \equiv 1 \pmod 4}$$

não tem relação não trivial.

Prova. Sejam $p_1, \ldots, p_k$ números primos distintos em $\mathbb{Z}$ tais que

$$p_j \equiv 1 \pmod 4, j = 1, \ldots, k.$$

Suponhamos que

$$a_1 f(m_1 + n_1 i) \oplus a_2 f(m_2 + n_2 i) \oplus \cdots \oplus a_k f(m_k + n_k i) = (1,0), \tag{3.5}$$

onde $p_j = m_j^2 + n_j^2$, $m_j > n_j > 0$ e $a_j \in \mathbb{Z}$. Então, pela Proposição 3.2, existem $a, b \in \mathbb{Z}^*$ tais que

$$(m_1 + n_1 i)^{a_1} (m_2 + n_2 i)^{a_2} \cdots (m_k + n_k i)^{a_k} a = b.$$

Sejam

$$a = q_1 q_2 \cdots \text{ e } b = r_1 r_2 \cdots$$

as decomposições de a e b em fatores primos. Pela unicidade da fatoração podemos assumir que $a = 1$. Portanto,

$$(m_1 + n_1 i)^{a_1} (m_2 + n_2 i)^{a_2} \cdots (m_k + n_k i)^{a_k} = r_1 r_2 \cdots.$$

Novamente, pela unicidade da fatoração, cada r_l é associado a $(m_j + n_j i)(m_j - n_j i) = p_j$. Assim, pela Proposição 3.1,

$$f(m_j - n_j i) \oplus f(m_j + n_j i) = (1, 0).$$

Logo, $f(m_j - n_j i)$ é o inverso de $f(m_j + n_j i)$ em $C(\mathbb{Q})$. Portanto, $a_j = 0$, $j = 1, \ldots, k$, pois $m_j > n_j > 0$. ■

Observação 3.2 *Como*

$$f\,(1 + i) = (0, 1),$$

então

$$f\,(1 + i) \oplus f\,(1 + i) \oplus f\,(1 + i) \oplus f\,(1 + i) = (1, 0)\,.$$

Portanto, pela prova do Lema 3.1*, esta relação é não trivial, isto é,*

$$4(0, 1) = (1, 0).$$

Lema 3.2 (Dirichlet) *O conjunto dos números primos da forma* $4n + 1$*, com* $n \in \mathbb{N}$*, é infinito.* ■

Teorema 3.1

$$C(\mathbb{Q}) \simeq C_2 \oplus \left(\underset{p \equiv 1 \bmod 4}{\oplus C_p} \right),$$

onde

$$C_2 = \langle (0, 1) \rangle \;\; e \;\; C_p = \left\langle \left(\frac{m_p^2 - n_p^2}{m_p^2 + n_p^2}, \frac{2 m_p n_p}{m_p^2 + n_p^2} \right) \right\rangle,$$

com m_p, n_p *as únicas soluções de* $m_p^2 + n_p^2 = p$ *e* $m_p > n_p > 0$.

Exemplo 3.2 *Seja* $\alpha = 5 + 4i \in \mathbb{Z}[i]$*. Então* $N(\alpha) = 41$ *é um número primo em* $\mathbb{Z}$ *e*

$$f(\alpha) = \left(\frac{9}{41}, \frac{40}{41} \right).$$

Logo,

$$\begin{aligned} C_{41} &= \left\langle \left(\frac{9}{41}, \frac{40}{41} \right) \right\rangle \\ &= \left\{ k \left(\frac{9}{41}, \frac{40}{41} \right) \in \mathbb{Q}^2 : k \in \mathbb{Z} \right\}. \end{aligned}$$

Usando o Teorema 3.1 e o Lema 3.1, podemos fazer um algoritmo para fatorar

$$f(\alpha) = \left(\frac{a}{c}, \frac{b}{c}\right) \in C(\mathbb{Q}).$$

nas suas C_p-componentes.

Algoritmo

1. Calcule a fatoração de $c = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ da seguinte forma: escreva c como

   $$c = 2^r d,$$

   onde d é um número ímpar e $r \in \mathbb{N} \cup \{0\}$. Se d é um número primo, então nada há para fazer. Se d é um número composto, então faça iterativamente os seguintes passos:

   i. Faça $l = \lfloor \sqrt{d} \rfloor$;

   ii. Se $l^2 - d = k^2$, então $d = (l-k)(l+k)$;

   iii. Se $l^2 - d \neq k^2$, faça $l := l + 1$ volte para *ii.*;

2. Calcule os $m_j + n_j i \in \mathbb{Z}[i]$ tais que

   $$m_j^2 + n_j^2 = p_j, j = 1, \ldots, k.$$

3. Considere

   $$\left(\frac{a}{c}, \frac{b}{c}\right) = k\,(0, -1) \oplus (\pm\alpha_1) f(m_1 + n_1 i) \oplus \cdots \oplus (\pm\alpha_k) f(m_k + n_k i).$$

4. Para $j = 1, \ldots, k$ determine α_j da seguinte forma: se o denominador da operação

   $$\left(\frac{a}{c}, \frac{b}{c}\right) \oplus (-\alpha_j) f(m_j + n_j)$$

   for igual a

   $$\frac{c}{p_j},$$

   o coeficiente de $f(m_j + n_j)$ será α_j. Caso contrário, $-\alpha_j$.

5. Finalmente, o coeficiente $k \in \{0,1,2,3\}$ de $(0,-1)$ é determinado de tal forma que a ordem e os sinais da expressão

$$(\pm\alpha_1)f(m_1+n_1i) \oplus \cdots \oplus (\pm\alpha_k)f(m_k+n_ki)$$

coincidam com

$$\left(\frac{a}{c}, \frac{b}{c}\right).$$

Exemplo 3.3 *Seja $\alpha \in \mathbb{Z}[i]^*$ tal que*

$$f(\alpha) = \left(\frac{-76}{1445}, \frac{1443}{1445}\right).$$

Para determinar α, usaremos o Algoritmo acima: como $c = 1445 = 5 \cdot 17^2$ e

$$5 = 2^2 + 1^2 = N(2+i) \ \text{ e } \ 17 = 4^2 + 1^2 = N(4+i).$$

temos que

$$\left(\frac{-76}{1445}, \frac{1443}{1445}\right) = n\,(0,1) \oplus (\pm 1)\left(\frac{3}{5}, \frac{4}{5}\right) \oplus (\pm 2)\left(\frac{15}{17}, \frac{8}{17}\right).$$

Como o denominador da operação

$$\left(\frac{-76}{1445}, \frac{1443}{1445}\right) \oplus (-1)\left(\frac{3}{5}, \frac{4}{5}\right)$$

é igual a

$$5^2 17^2 \neq \frac{c}{5}$$

temos que o coeficiente de

$$\left(\frac{3}{5}, \frac{4}{5}\right)$$

é igual a -1. Prosseguindo assim, obtemos

$$\left(\frac{-76}{1445}, \frac{1443}{1445}\right) = (0,1) \oplus (-1)\left(\frac{3}{5}, \frac{4}{5}\right) \oplus (2)\left(\frac{15}{17}, \frac{8}{17}\right).$$

Portanto,

$$\alpha = 1 \cdot (1+i)(2+i)^{-1}(4+i)^2 = 37 + 39i.$$

Corolário 3.1 *Sejam $\alpha, \beta \in \mathbb{R}$ e $P_\alpha = (\cos\alpha, \operatorname{sen}\alpha)\,, P_\beta = (\cos\beta, \operatorname{sen}\beta) \in C(\mathbb{Q})$ tal que $\frac{\alpha}{\beta} \in \mathbb{Q}$. Então existem $r, s \in \mathbb{Z}$, $P_\gamma = (\cos\gamma, \operatorname{sen}\gamma) \in C(\mathbb{Q})$ e $c_\alpha, c_\beta \in C_2$ tais que*

$$P_\alpha = rP_\gamma \oplus c_\alpha \ \text{ e } \ P_\beta = sP\gamma \oplus c_\beta.$$

Em particular, se $P_\alpha \in C(\mathbb{Q})$ e α é um múltiplo racional de π, então $P_\alpha \in C_2$.

Prova. Seja $\frac{\alpha}{\beta} = \frac{r}{s} \in \mathbb{Q}$, com $\text{mdc}(r, s) = 1$. Então $s\alpha = r\beta$. Logo,

$$\begin{aligned} sP_\alpha &= s(\cos\alpha, \operatorname{sen}\alpha) \\ &= (\cos(s\alpha), \operatorname{sen}(s\alpha)) \\ &= (\cos(r\beta), \operatorname{sen}(r\beta) \\ &= r(\cos\beta, \operatorname{sen}\beta) = rP_\beta. \end{aligned}$$

Sejam C_α e C_β as C_p-componentes de P_α e P_β, respectivamente. Como r divide P_α e s divide P_β, podemos construir P_γ, definindo suas C_p-componentes por

$$C_\gamma = \frac{1}{r}\{C_\alpha\} = \frac{1}{s}\{C_\beta\}.$$

Além disso, sendo C_2 finito, não podemos comparar as C_2-componentes e devemos incluí-las como termos c_α e c_β. Portanto, pelo Teorema 3.1 e comparando as C_p-componentes de P_α e P_β, obtemos

$$P_\alpha = rP_\gamma \oplus c_\alpha \text{ e } P_\beta = sP\gamma \oplus c_\beta.$$

Finalmente, tomando $\beta = \pi$, obtemos

$$P_\alpha = -s(r(-1, 0)) \in C_2.$$

Portanto,

$$P_\alpha = rP_\gamma \oplus c_\alpha \in C_2.$$

■

Corolário 3.2 *Sejam* $P_\alpha = (\cos\alpha, \operatorname{sen}\alpha)$, $P_\beta = (\cos\beta, \operatorname{sen}\beta) \in C(\mathbb{Q})$ *e* $\alpha - \beta$ *um múltiplo racional de* π. *Então* $\alpha = \beta + \frac{k\pi}{2}$.

Prova. Pelo Corolário 3.1, obtemos $P_{\alpha-\beta} \in C_2$. Portanto,

$$\alpha - \beta = \frac{k\pi}{2}.$$

■

Corolário 3.3 [7] *Os únicos ângulos com medida racional no reticulado* $\mathbb{Z} \times \mathbb{Z}$ *que podem ser formados por três pontos, são múltiplos inteiros de* 45^o .

Prova. Como $\mathbb{Z} \times \mathbb{Z}$ é invariante por translações podemos, sem perda de generalidade, escolher $B = (0,0)$, $A = (a,b)$, $C = (c,d)$ e $\theta \in \mathbb{Q}$ tal que $\theta = \angle ABC$. Então

$$\theta = \frac{1}{2}\beta,$$

onde $\beta = \angle f(A)Of(C)$, O o centro de C e f o homomorfismo de monóides. Logo, medido em radianos,

$$\beta = \frac{2\theta\pi}{180}, \theta \in \mathbb{Q}.$$

Assim, pelo Corolário 3.1, $P_\beta \in C_2$. Portanto, pelo Corolário 3.2,

$$\beta = \frac{k\pi}{2} \text{ e } \theta = k\frac{\pi}{4}, k \in \mathbb{Z}.$$

■

Seja a elipse

$$E = \left\{ (x,y) \in \mathbb{R}^2 : \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \text{ e } a, b \in \mathbb{R} \right\}.$$

e $T : \mathbb{R}^2 \to \mathbb{R}^2$ a aplicação definida por

$$T(x,y) = (ax, by), \forall a, b \in \mathbb{R}.$$

Então é claro que T é linear e bijetora, isto é, T é um isomorfismo. Note que a imagem de C, onde C é o círculo unitário, é E, isto é

$$T(C) = E.$$

Portanto, quando $a, b \in \mathbb{Q}$ todos os resultados obtidos para o grupo dos pontos racionais sobre o círculo unitário $C(\mathbb{Q})$ são válidos para $E(\mathbb{Q})$, o grupo dos pontos racionais sobre a elipse E com semi-eixos racionais.

Teorema 3.2

$$E(\mathbb{Q}) \simeq T(C_2) \oplus \left(\bigoplus_{p \equiv 1 \bmod 4} T(C_p) \right),$$

onde

$$C_2 = \langle (0,1) \rangle \text{ e } C_p = \left\langle \left(\frac{m_p^2 - n_p^2}{m_p^2 + n_p^2}, \frac{2m_p n_p}{m_p^2 + n_p^2} \right) \right\rangle,$$

com m_p, n_p as únicas soluções de $m_p^2 + n_p^2 = p$ e $m_p > n_p > 0$. ■

3.4 Pontos Racionais na Hipérbole

Nesta seção vamos estudar o grupo dos pontos racionais sobre a hipérbole H, cuja equação é

$$x^2 - y^2 = 1.$$

A hipérbole H é um grupo abeliano sob a operação $\oplus$ definida por

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1x_2 + y_1y_2, x_1y_2 + x_2y_1), \tag{3.6}$$

para todos $(x_1, y_1), (x_2, y_2) \in H$. O elemento identidade é $(1, 0)$ e $(x, -y)$ é o elemento inverso de (x, y). Denotando por $H(\mathbb{Q})$ o conjunto de seus pontos racionais, verifica-se facilmente que $H(\mathbb{Q})$ é um subgrupo de H.

Fazendo-se a interseção de H com as retas que passam pelo ponto $(-1, 0)$ e têm inclinação t, obtemos uma parametrização racional $\rho : \mathbb{R} - \{\pm 1\} \to \mathbb{R}^2$ de H, onde

$$\rho(t) = \left(\frac{1+t^2}{1-t^2}, \frac{2t}{1-t^2} \right)$$

e

$$\rho(\mathbb{R} - \{\pm 1\}) = H,$$

conforme Figura 3.3.

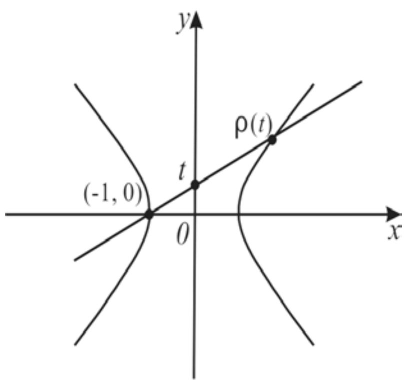

Figura 3.3: Representação geométrica da parametrização racional ρ.

Em particular, se $t = \frac{n}{m}$, com $n, m \in \mathbb{Z}$ e $m \neq 0$, então

$$\rho(\frac{n}{m}) = \left(\frac{m^2+n^2}{m^2-n^2}, \frac{2mn}{m^2-n^2} \right).$$

É fácil verificar que toda reta que passa em $(-1, 0)$ e tem inclinação racional intercepta $H - \{(-1, 0)\}$ em um ponto racional, ou seja, um ponto de $H(\mathbb{Q})$.

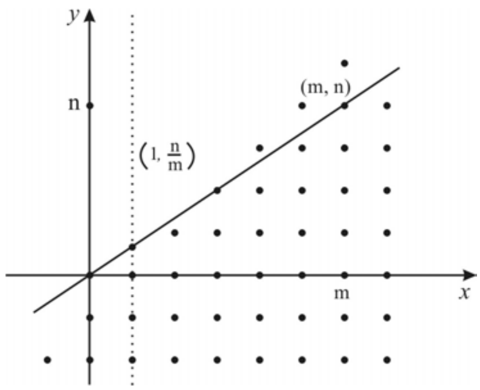

Figura 3.4: Representação geométrica de $R\,[\varepsilon]$.

Seja $\hat{\rho} = \rho|_{\mathbb{Q}-\{\pm 1\}}$, isto é, $\hat{\rho}\,(r) = \rho\,(r)$, para todo $r \in \mathbb{Q} - \{\pm 1\}$. É fácil verificar que

$$\hat{\rho}(\mathbb{Q} - \{\pm 1\}) = H(\mathbb{Q}) - \{(-1, 0)\}\,.$$

Para cada $m + n\varepsilon \in R[\varepsilon]$, a reta que passa em $m + n\varepsilon = (m, n)$ e $0 = (0, 0)$ intercepta a reta $x = 1$ em $\left(1, \frac{n}{m}\right)$, conforme a Figura 3.4.

Como H consiste de dois ramos

$$H_1 = \{(x, y) \in H : x > 0\}$$

e

$$H_2 = \{(x, y) \in H : x < 0\}\,,$$

temos que o subgrupo $H(\mathbb{Q})$ tem uma decomposição

$$H(\mathbb{Q}) = H_1(\mathbb{Q}) \cup H_2(\mathbb{Q}). \tag{3.7}$$

É fácil verificar que $H_1(\mathbb{Q})$ é um subgrupo de H. Portanto, pela equação 3.7, obtemos

$$H(\mathbb{Q}) = H_1(\mathbb{Q}) \cup H_2(\mathbb{Q}),$$

onde

$$H_2(\mathbb{Q}) = (-1, 0) \oplus H_1(\mathbb{Q}).$$

Portanto,

$$H(\mathbb{Q}) = H' \oplus H_1(\mathbb{Q})$$

onde $H' = \{(1, 0)\,, (-1, 0)\}$.

Pelas observações acima, a translação de eixos $u = x - 1$ e $v = y$ na Figura 3.3 e depois juntando num só gráfico com a Figura 3.4, obtemos a função sobrejetora $f : R[\varepsilon] \to H(\mathbb{Q})$ definida por

$$f(m + n\varepsilon) = \left(\frac{m^2 + n^2}{m^2 - n^2}, \frac{2mn}{m^2 - n^2}\right) \tag{3.8}$$

onde $f(n\varepsilon) = (-1, 0)$.

Observação 3.3 *Seja s a reta, cuja equação é*

$$y = \frac{n}{m}x.$$

Então para cada $a + b\varepsilon = (a, b) \in s \cap R[\varepsilon]$, obtemos

$$f(a + b\varepsilon) = f(m + n\varepsilon).$$

Proposição 3.3 *Seja $f : R[\varepsilon] \to H_1(\mathbb{Q})$ definida por* 3.8*. Então f é um homomorfismo de monóides.* ■

3.5 A Estrutura de Grupo de $H(\mathbb{Q})$

Nesta seção obteremos a estrutura de grupo de $H(\mathbb{Q})$.

Proposição 3.4 *Sejam $f : R[\varepsilon] \longrightarrow H(\mathbb{Q})$ e $(c_k, s_k) = f(m_k + n_k\varepsilon) \in H(\mathbb{Q})$. Então*

$$(c_1, s_1) = (c_2, s_2) \oplus (c_3, s_3)$$

se, e somente se, existem $a, b \in \mathbb{N}$ tais que

$$(m_1 + n_1\varepsilon)a = (m_2 + n_2\varepsilon)\,(m_3 + n_3\varepsilon)b.$$

■

Pela Proposição 2.5, temos que os elementos irredutíveis em $R[\varepsilon]$ são da forma

$$\beta = \frac{p+1}{2} + \frac{p-1}{2}\varepsilon,$$

onde p é um número primo ímpar em $\mathbb{Z}$, ou $3 + \varepsilon$ ou $\alpha = n + (n-2)\,\varepsilon$ tal que $N(\alpha) = 2^k$, $k = 2$ ou $k > 3$. Logo,

$$f(\beta) = (\frac{p^2+1}{2p}, \frac{p^2-1}{2p}), f(3+\varepsilon) = \left(\frac{5}{4}, \frac{3}{4}\right) \text{ e } f(\alpha) = (k-2)f(3+\varepsilon).$$

Note que $f(m) = (1,0)$ é o elemento identidade de $H(\mathbb{Q})$ e se $n < 0$ então

$$\begin{aligned} 2f(n\varepsilon) &= f(n\varepsilon) \oplus f(n\varepsilon) \\ &= (-1,0) \oplus (-1,0) \\ &= (1,0), \end{aligned}$$

o que implica que $f(n\varepsilon)$ é um elemento de ordem 2 em $H(\mathbb{Q})$.

Lema 3.3 *O conjunto*

$$\left\{ \left(\frac{5}{4}, \frac{3}{4} \right), \left(\frac{p_j^2+1}{p_j}, \frac{p_j^2-1}{p_j} \right)_{p_j \ \mathit{primo}} \right\}$$

não tem relação não trivial.

Prova. Sejam $p_1, \ldots, p_k$ números primos distintos em $\mathbb{Z}$. Suponhamos que

$$af(3+\varepsilon) \oplus a_1 f(\alpha_1) \oplus \cdots \oplus f(\alpha_k) = (1,0),$$

onde

$$\alpha_j = \frac{p_j+1}{2} + \frac{p_j-1}{2}\varepsilon \ \text{ e } \ a, a_j \in \mathbb{Z}, j = 1, \ldots k.$$

Pela Proposição 2.3,

$$a\left(\frac{5}{4}, \frac{3}{4}\right) \oplus f\left(\frac{1}{2}\left(\prod_{j=1}^{k} p_j^{a_j} + 1\right), \frac{1}{2}\left(\prod_{j=1}^{k} p_j^{a_j} - 1\right)\right) = (1,0),$$

isto é,

$$a\left(\frac{5}{4}, \frac{3}{4}\right) \oplus \left(\frac{\prod_{j=1}^{k} p_j^{2a_j} + 1}{2\prod_{j=1}^{k} p_j^{a_j}}, \frac{\prod_{j=1}^{k} p_j^{2a_j} - 1}{2\prod_{j=1}^{k} p_j^{a_j}} \right) = (1,0),$$

mas isto é impossível, a menos que $a = a_j = 0$. ■

Teorema 3.3

$$H(\mathbb{Q}) \simeq H' \oplus H_2 \oplus \left(\sum_{p \ \mathit{primo\ ímpar}} H_p \right),$$

onde

$$H' = \langle(-1,0)\rangle, H_2 = \left\langle \left(\frac{5}{4}, \frac{3}{4} \right) \right\rangle \ \ e \ \ H_p = \left\langle \left(\frac{p^2+1}{2p}, \frac{p^2-1}{2p} \right) \right\rangle.$$

Exemplo 3.4 *Seja $\alpha \in R[\varepsilon]$ tal que*

$$f(\alpha) = \left(\frac{-409}{120}, \frac{391}{120}\right).$$

Para determinar α, procedemos de forma quase similar ao Exemplo 3.3, fazendo as devidas adaptações para o caso aqui da hipérbole: Primeiramente fatoramos

$$c = 120 = 2^3 \cdot 3 \cdot 5$$

Ao fator 2^3 associamos o elemento

$$f(3,1)^{3-1} = 2.\left(\frac{5}{4}, \frac{3}{4}\right) \in H_2.$$

Ao fator 3 associamos

$$f\left(\frac{3+1}{2}, \frac{3-1}{2}\right) = \left(\frac{3^2+1}{2\cdot 3}, \frac{3^2-1}{2\cdot 3}\right) \in H_3,$$

e ao fator 5,

$$f\left(\frac{5+1}{2}, \frac{5-1}{2}\right) = \left(\frac{5^2+1}{2\cdot 5}, \frac{5^2-1}{2.5}\right) \in H_5.$$

Portanto,

$$\left(-\frac{409}{120}, -\frac{391}{120}\right) = (\pm 1, 0) \oplus (\pm 2)\left(\frac{5}{4}, \frac{3}{4}\right) \oplus (\pm 1)\left(\frac{5}{3}, \frac{4}{3}\right) \oplus (\pm 1)\left(\frac{5}{4}, \frac{3}{4}\right)\left(\frac{13}{5}, \frac{12}{5}\right).$$

Como o denominador da operação

$$\left(-\frac{409}{120}, -\frac{391}{120}\right) \oplus (2)\left(\frac{5}{4}, \frac{3}{4}\right)$$

é

$$2^5 35 \neq \frac{120}{2^3}$$

temos que o coeficiente de

$$\left(\frac{5}{4}, \frac{3}{4}\right)$$

é igual a 2. Como o denominador de

$$\left(-\frac{409}{120}, -\frac{391}{120}\right) \oplus \left(\frac{5}{3}, \frac{4}{3}\right)$$

é

$$2^3 5 = \frac{120}{3}$$

temos que o coeficiente de

$$\left(\frac{5}{3}, \frac{4}{3}\right)$$

é -1. Prosseguindo assim, obtemos

$$\left(-\frac{409}{120}, -\frac{391}{120}\right) = (-1, 0) \oplus 2.\left(\frac{5}{4}, \frac{3}{4}\right) \oplus (-1)\,.\left(\frac{5}{3}, \frac{4}{3}\right) \oplus \left(\frac{13}{5}, \frac{12}{5}\right)$$

Portanto,

$$\alpha = 1 \cdot (0, -1)(3, 1)^2(2, 1)^{-1}(3, 2) = (-34, -46).$$

Referências Bibliográficas

[1] Bhattacharya, P. B. Jain, S. K. and Nagpaul, S. R., *Basic Abstract Algebra*, Cambridge, New York, 1995.

[2] Dummit, D. S. and Foote, R., *Abstract Algebra*, Prentice-Hall, 1991.

[3] Garcia, A. L. e Lequain, Y., *Álgebra*: *Um Curso de Introdução*, IMPA, Rio de Janeiro, 1988.

[4] Hefez, A., *Curso de Álgebra, vol.* 1, IMPA, Rio de Janeiro, 1993.

[5] Michael, A., *Algebra*, New Jersey, 1991.

[6] Niven, I. Zuckerman, H. S. and Montgomery, H. L., *An Introduction to The Theory of Numbers*, 5 ed., John Wiley & Sons, New York, 1991.

[7] Olmsted, J. M. H., "Rational Values of Trigonometric Functions," *Amer. Math. Monthly* 52(1945), 507-508.

[8] Silva, A. de A e, *Notas de Aulas*, Depto de Matemática, UFPB.

[9] Stewart, I. N. and Tall, D. O., *Algebraic Number Theory*, Chapman and Hall, 1986.

[10] Tan, L., "The Group of Rational Points on the Unit Circle," *Mathematics Magazine*, 69(1996), June 1996.