UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE COMUNICAÇÕES

CÓDIGOS DE BLOCO LINEARES SOBRE ANÉIS DE INTEIROS ALGÉBRICOS COM ALFABETO CASADO A $GF(p)$

Osvaldo Milaré Favareto

Orientador: **Prof. Dr. Trajano Pires da Nóbrega Neto**
Co-orientador: **Prof. Dr. José Carmelo Interlando**
Co-orientador: **Prof. Dr. Reginaldo Palazzo Jr.**

Tese de Doutorado apresentada à Faculdade de Engenharia Elétrica e de Computação - FEEC, da Universidade Estadual de Campinas - UNICAMP, como parte dos requisitos exigidos para obtenção do título de DOUTOR EM ENGENHARIA ELÉTRICA.

Dezembro - 1996

Campinas - SP.

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

F277c

Favareto, Osvaldo Milaré
Códigos de bloco lineares sobre anéis de inteiros algébricos com alfabeto casado a GF(p) / Osvaldo Milaré Favareto.--Campinas, SP: [s.n.], 1996.

Orientadores: Trajano Pires da Nóbrega Neto, José Carmelo Interlando, Reginaldo Palazzo Júnior.
Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Teoria dos números algébricos. 2. Códigos de controle de erros (Teoria da informação). 3. Teoria da codificação. 4. Decodificadores (Eletrônica). I. Nóbrega Neto, Trajano Pires da. II. Interlando, José Carmelo. III. Palazzo Júnior, Reginaldo. IV.Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. V. Título.

À Maria Sylvia,
Paulo e André
razões do
meu viver .

Agradecimentos

- Ao Professor Doutor Trajano Pires da Nóbrega Neto, pela sua orientação eficiente e segura, que, juntamente com seu conhecimento, foram fatores decisivos na realização deste trabalho. Também pela amizade sincera desde há muitos anos.
- Ao Professor Doutor José Carmelo Interlando, pela sua paciência, entusiasmo e discernimento ao me apontar novos e seguros caminhos.
- Ao Professor Doutor Reginaldo Palazzo Júnior pela amizade e constante estímulo. Sua ampla visão científica foi determinante para o desenvolvimento deste trabalho.
- Aos professores da banca examinadora: Prof. Dr. Antonio José Engler (IMECC, UNICAMP, Campinas), Prof. Dr. Norai Romeu Rocco (Dep. Mat., UnB, Brasília), Prof. Dr. Hélio Waldman (FEEC, UNICAMP, Campinas) e Prof. Dr. Max Henrique Machado Costa (FEEC, UNICAMP, Campinas).
- À minha esposa Maria Sylvia e aos meus filhos Paulo e André, pela inesgotável paciência, compreensão e carinho nestes anos todos.
- Aos meus pais, Benedito e Eugênia e aos meus sogros Álvaro e Adahyla pelo amor constante.
- Aos colegas do curso de Doutorado, pelo companheirismo e ajuda mútua.
- À UFPb pela licença concedida.
- Aos amigos e colegas do Departamento de Matemática da UFPb que possibilitaram a realização deste trabalho.
- Ao Departamento de Matemática do IBILCE - S.J. Rio Preto, pela amizade de seus membros e também pelo apoio computacional oferecido, colocando à minha disposição seus equipamentos.

Resumo

Este trabalho trata da construção de códigos de bloco lineares sobre o anel $\mathbb{A}$, dos inteiros algébricos das extensões $\mathbb{Q}\left(\sqrt{d}\right)$, $d = -1$ e $d = -3$, projetados principalmente para a distância de Mannheim. Tal construção é feita sobre um alfabeto $\mathcal{A}$, definido como um conjunto completo de representantes de um ideal primo não nulo $\mathfrak{p}$ de $\mathbb{A}$. Inicialmente, identificamos $\mathbb{A}$ com um subconjunto do espaço $\mathbb{R}^2$ e consideramos o corpo com p elementos $\mathbb{A}/\mathfrak{p}$, que se identifica com o corpo $GF(p)$. Obtemos um rotulamento para os elementos de $\mathcal{A}$ através do grupo aditivo de $GF(p)$ e também determinamos a distância máxima de Mannheim entre os elementos de $\mathcal{A}$. São apresentados códigos lineares constacíclicos, gerados por um polinômio $g(x)$ que divide $x^n - \omega$, onde ω é uma raiz primitiva quarta da unidade se $d = -1$ e ω é uma raiz primitiva sexta da unidade se $d = -3$. Estes códigos também são apresentados em termos de sua matriz verificação de paridade. Determinamos algoritmos eficientes de decodificação para tais códigos, apresentando um procedimento que permite decodificar códigos pertencentes a cada uma das classes construídas.

Abstract

This research is based on the construction of linear block codes over rings of algebraic integers of the extensions $\mathbb{Q}\left(\sqrt{d}\right)$, where $d = -1$ and $d = -3$. These rings are denoted interchangeably by $\mathbb{A}$. The codes being proposed are mainly designed for the Mannheim metric. The codes are constructed over an alphabet $\mathcal{A}$, which is defined as a complete set of representatives of a nonzero prime ideal $\mathfrak{p}$ of $\mathbb{A}$.. Initially, we identify $\mathbb{A}$ with a subset of $\mathbb{R}^2$ and consider the field with p elements, namely, $\mathbb{A}/\mathfrak{p}$ which is isomorphic to $GF(p)$. A labeling of the elements of $\mathcal{A}$ is obtained through the additive group of $GF(p)$ and also we determine the maximum Mannheim distance between any pair of elements of $\mathcal{A}$. We also show that these codes are constacyclic, and are generated by a polynomial $g(x)$ that divides $x^n - \omega$, where ω is a fourth primitive root of unity if $d = -1$, and ω is a sixth primitive root of unity if $d = -3$. Four classes of codes over rings of algebraic integers are presented in terms of parity-check matrices. Finally, efficient decoding algorithms are presented for the classes being proposed.

Lista de Símbolos

A :	anel
$\mathbb{A}$:	anel dos inteiros algébricos de um corpo de números K
$\mathbb{Z}[\omega]$:	anel dos inteiros algébricos de $\mathbb{Q}(\omega)$
$A_n = K[X]/(X^n - 1)$:	anel dos polinômios sobre K, módulo $X^n - 1$
$F[X]$:	anel dos polinômios na variável X sobre o corpo F
$A/\mathfrak{a}$:	anel quociente
$\#(A/\mathfrak{a})$:	cardinalidade do conjunto quociente $A/\mathfrak{a}$
$\overline{a}$:	classe lateral do elemento a
$\mathcal{C}$:	código de bloco linear
$a \equiv b \pmod{\mathfrak{p}}$:	a congruente a b módulo o ideal $\mathfrak{p}$
$\mathbb{C}$:	conjunto dos números complexos
$\mathbb{Z}$:	conjunto dos números inteiros
$\mathbb{Z}[i]$:	conjunto dos números inteiros de Gauss
$\mathbb{Q}$:	conjunto dos números racionais
$\mathbb{R}$:	conjunto dos números reais
$\mathcal{A}$:	conjunto de sinais
$\mathfrak{q} \supset \mathfrak{p}$:	$\mathfrak{q}$ contém $\mathfrak{p}$ ou $\mathfrak{q}$ está acima de $\mathfrak{p}$
F, K :	corpos
$GF(p)$:	corpo de Galois com p elementos
$d^H(\mathbf{x}, \mathbf{y})$:	distância de Hamming entre $\mathbf{x}$ e $\mathbf{y}$
$d^M(\mathbf{x}, \mathbf{y})$:	distância de Mannheim entre $\mathbf{x}$ e $\mathbf{y}$
$d,\ d^H(\mathcal{C})$:	distância mínima de Hamming do código $\mathcal{C}$
$d^M(\mathcal{C})$:	distância mínima de Mannheim do código $\mathcal{C}$
$d^M_{\max}(\mathcal{C})$:	distância máxima de Mannheim do código $\mathcal{C}$
$K(\alpha)$	extensão de K pela adjunção do elemento algébrico α

$F \supset K,\ F/K$:	F extensão de K
ϕ :	função ϕ de Euler
$f, f(\mathfrak{q}/\mathfrak{p})$:	grau de inércia de $\mathfrak{q}$ sobre $\mathfrak{p}$
$\partial(f)$:	grau do polinômio f
$\varphi : A \longrightarrow B$:	homomorfismo de A em B
$\mathfrak{a}, \mathfrak{p}, \mathfrak{q}$:	ideais
(π) :	ideal gerado por π
$m\mathbb{Z}$:	ideal gerado por m em $\mathbb{Z}$
$\mathfrak{p}\mathbb{A}$:	ideal gerado pelo ideal $\mathfrak{p}$ em $\mathbb{A}$
$\mathrm{Im}(\varphi)$:	imagem de φ
$e, e(\mathfrak{q}/\mathfrak{p})$:	índice de ramificação de $\mathfrak{q}$ sobre $\mathfrak{p}$
$A \simeq B$:	A isomorfo a B
G :	matriz geradora do código $\mathcal{C}$
H :	matriz verificação de paridade do código $\mathcal{C}$
$mdc\{a,b\} = (a,b)$:	máximo divisor comum entre a e b
$\lfloor x \rfloor$	menor inteiro maior ou igual a x
$mmc\{a,b\}$:	mínimo múltiplo comum entre a e b
$N_{F/K}(\alpha)$:	norma de α, relativo à extensão $F \supset K$
$N_A(\mathfrak{a})$:	norma do ideal $\mathfrak{a}$ no anel A
$\ker(\varphi)$:	núcleo de φ
w_H :	peso de Hamming
w_M :	peso de Mannheim
$i = \sqrt{-1}$:	raiz primitiva *quarta* da unidade
$\omega = \frac{1+\sqrt{-3}}{2}$:	raiz primitiva *sexta* da unidade
$V_\Lambda(P)$:	região de Voronoi do ponto $P \in \Lambda$
$\left(\frac{d}{p}\right)$:	símbolo de Legendre
$\mathcal{S}$:	subreticulado de $\mathbb{A}$ gerado por $\{\omega, \omega\pi\}$
$T_{F/K}(\alpha)$:	traço de α, relativo à extensão $F \supset K$
$\lvert x \rvert$:	valor absoluto de x

Lista de Figuras

Lista de Tabelas

Conteúdo

Capítulo 1

Introdução

Este trabalho tem como proposta estender o estudo de códigos sobre estruturas algébricas cada vez mais complexas, do ponto de vista matemático. Como sabemos, inicialmente os códigos foram projetados para o corpo $GF(2)$, em seguida este estudo foi estendido para $GF(p)$, p primo e depois para $GF(q)$, onde q é uma potência de primo. O estudo de códigos sobre anéis de inteiros residuais da forma $\mathbb{Z}_M$, onde M é um inteiro maior ou igual a 2, teve início com os trabalhos de Blake [3], [4], Spiegel [29], [30] e Shankar [27]. Em [24], Massey *et al.* propuseram códigos convolucionais sobre $\mathbb{Z}_M$ e mostraram que tais códigos são casados a modulação do tipo $M-PSK$ $(M \geq 2)$, sendo o casamento entendido no sentido estabelecido por Loeliger [20].

O estudo de códigos sobre grupos foi iniciado por Slepian em [28], mas foi somente em [11], que Forney mostrou a sua real importância, isto é, para que um código $\mathcal{C}$ esteja casado a uma dada constelação de sinais S, o alfabeto de $\mathcal{C}$ deve ser um grupo gerador de S. Também neste trabalho, Forney mostrou que códigos sobre grupos são úteis na construção de novos conjuntos de sinais geometricamente uniformes, a partir de sinais geometricamente uniformes já conhecidos. Em [2], Biglieri e Elia propuseram construções de códigos sobre grupos abelianos e mostraram que estes podem ser estudados via códigos lineares sobre anéis de inteiros residuais.

Em 1994, Huber [15] propôs a construção de códigos sobre um subconjunto conveniente

de $\mathbb{Z}[i]$, que vem a ser o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-1}\right)$. Neste trabalho foi definida a distância de Mannheim, que representa o análogo da distância de Manhattan, para o conjunto em questão. Tais códigos foram projetados para a distância de Mannheim, que é a distância apropriada quando se usa modulações do tipo QAM, onde nem a distância de Hamming, nem a distância de Lee são adequadas. Este trabalho de Huber serviu como motivação para o estudo dos códigos sobre o anel dos inteiros algébricos de outros corpos quadráticos. No presente trabalho conseguimos ampliar, nos inteiros de Gauss, vários resultados do trabalho de Huber, mas foi no anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-3}\right)$ que conseguimos os melhores resultados.

Em [12] Giraud *et al.*, usam o anel de inteiros algébricos de uma extensão totalmente real de grau n para projetar conjuntos de sinais baseados em reticulados para canais com desvanecimento do tipo Rayleigh. Também Boutros *et al.*, em [5], apresentam duas famílias de reticulados para atingir bom desempenho sobre canais Gaussianos e canais com desvanecimento de Rayleigh, com alta eficiência espectral. Para canais Gaussianos, a família de reticulados é gerada pelas imersões canônicas de anéis de inteiros algébricos em $\mathbb{R}^n$. As constelações baseadas em reticulados sobre corpos totalmente reais apresentam bom desempenho sobre canais com desvanecimento de Rayleigh com a máxima diversidade de n, mas apresentam ganho negativo sobre canais Gaussianos, devido à fraca densidade de empacotamento dos reticulados associados. Os reticulados sobre corpos totalmente complexos, gerados pelas imersões em corpos ciclotômicos totalmente complexos, apresentam boa relação entre diversidade e densidade de empacotamento. Eles apresentam ganho positivo sobre canais Gaussianos e bom desempenho sobre canais de Rayleigh com a diversidade de $n/2$.

Podemos ver assim que a teoria dos números algébricos começa ser uma ferramenta apropriada, não só para a construção de códigos com distâncias diferentes da convencional distância de Hamming, úteis quando se usam modulações do tipo QAM, como também quando se usam constelações baseadas em reticulados que podem ser aplicadas tanto em canais Gaussianos, quanto em canais com desvanecimento de Rayleigh. Nesta direção e motivados pelos resultados de Huber em [15], nos propomos a apresentar neste trabalho

uma extensão da classe de códigos projetados por Huber para o caso $\mathbb{Z}[i]$ e paralelamente a isto construir códigos sobre o anel dos inteiros algébricos $\mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-3}}{2}$ do corpo de números $\mathbb{Q}\left(\sqrt{-3}\right)$, apresentando também algoritmos de decodificação.

Para a construção desta classe de códigos, consideramos o anel $\mathbb{A}$ dos inteiros algébricos de $\mathbb{Q}(\sqrt{d})$, onde $d = -1$ ou $d = -3$ e um conveniente ideal primo $\mathfrak{p}$ de $\mathbb{A}$ de norma p, $p \equiv 1 \pmod 4$ se $d = -1$ e $p \equiv 1 \pmod 6$ se $d = -3$. Identificamos $\mathbb{A}$ com um subconjunto do espaço $\mathbb{R}^2$, via a representação geométrica de corpos de números, e consideramos o corpo $\mathbb{A}/\mathfrak{p}$ com p elementos, e portanto, isomorfo a $GF(p)$. O alfabeto para a construção destes códigos sobre $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, que denotaremos por $\mathcal{A}$, é um conjunto completo de representantes do ideal primo $\mathfrak{p}$ de $\mathbb{A}$, que herda a estrutura de corpo do quociente $\mathbb{A}/\mathfrak{p}$. Logo, podemos considerar $\mathcal{A}$ isomorfo a $GF(p)$, isto é, $\mathcal{A} \simeq GF(p)$.

O conteúdo deste trabalho está distribuído em quatro capítulos, além deste.

No Capítulo 2, apresentamos os resultados básicos necessários para melhor compreensão dos capítulos seguintes. São revistos, dentre outros, os conceitos de grupos, anéis, corpos, módulos e códigos de bloco lineares. Especial atenção é atribuída à Teoria dos Números Algébricos, sobre os quais serão construídos os códigos propostos no Capítulo 4.

No Capítulo 3, inicialmente construímos um conjunto de sinais $\mathcal{A}$ que é um conjunto completo de classes latrerais de um ideal primo $\mathfrak{p}$ do anel $\mathbb{A}$ dos inteiros algébricos de $K = \mathbb{Q}(\sqrt{d})$, onde $d = -1$, $d = -3$ e $\mathfrak{p} = (\pi)$ é o ideal principal de $\mathbb{A}$ gerado por $\pi \in \mathbb{A}$, tal que $N(\pi) = p$ e o ideal primo $p\mathbb{Z}$ se decompõe completamente em $\mathbb{A}$. Apresentamos em seguida o resultado mais importante desse capítulo que é um procedimento para se determinar o rotulamento do conjunto de sinais $\mathcal{A}$ casado ao grupo aditivo de $GF(p)$. A seguir estendemos o conceito de distância de Mannheim para $\mathcal{A}$, generalizando assim a proposta de Huber em [15]. Obtemos a distância máxima de Mannheim entre os elementos de $\mathcal{A}$, no caso $d = -3$. Um outro resultado central desse capítulo é apresentado no Teorema 3.9, onde mostramos que no caso de $\mathbb{A}$ ser o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{d}\right)$, $d = -1$ ou $d = -3$, este pode ser visto como um reticulado gerado por $\{1, \omega\}$, $\omega = i$ se $d = -1$ e $\omega = \frac{1+\sqrt{-3}}{2}$ se $d = -3$, assim sendo, $\mathbb{A}$ possui um subreticulado $\mathcal{S}$, gerado por $\{\pi, \omega\pi\}$, onde $\pi = a + b\omega$,

$a, b \in \mathbb{Z}$ é tal que sua norma $N(\pi)$ é igual a p. Nesse mesmo teorema determinamos a região de Voronoi da origem de $\mathcal{S}$ e mostramos que o conjunto de sinais $\mathcal{A}$, casado a $GF(p)$, está contido na região de Voronoi da origem de $\mathcal{S}$.

No Capítulo 4, propomos códigos sobre o anel dos inteiros algébricos de $\mathbb{Q}(\sqrt{d})$, onde $d = -1$ ou $d = -3$. Completamos os resultados de Huber e apresentamos novas propostas para construção e decodificação de códigos sobre tais anéis. O alfabeto para tais códigos é o conjunto de sinais $\mathcal{A}$, definido no Capítulo 3, identificado com $GF(p)$ e a distância será a de Mannheim, introduzida por Huber em [15], a qual será estendida e formalizada para o caso de anéis de inteiros algébricos de $\mathbb{Q}\left(\sqrt{d}\right)$, onde $d = -1$ e $d = -3$. Na Seção 4.1 definimos os códigos sobre o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-3}\right)$ em termos de uma matriz verificação de paridade e mostramos que tais códigos são constacíclicos, gerados por um polinômio $g(x)$ que divide $x^n - \omega$, onde ω é uma raiz primitiva sexta da unidade. A partir disto, os principais resultados do Capítulo 4 são: *i*) propriedades da distância de Hamming para códigos sobre anéis de inteiros algébricos, onde mostramos que tais códigos são MDS (Corolário 4.5); *ii*) determinação de classes de códigos. São propostas quatro classes de códigos para cada um dos anéis $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, para a métrica de Mannheim, a saber: uma projetada para corrigir um erro de Mannheim; outra para corrigir todo padrão de erro que apresenta uma posição alterada de qualquer peso de Mannheim; uma outra que é capaz de corrigir todo padrão de erro com até duas posições alteradas, cada uma com peso de Mannheim igual a um e uma quarta classe que corrige todo padrão de erros, com duas posições alteradas, cada uma delas de qualquer peso de Mannheim. Nas demonstrações dos teoremas garantindo as capacidades de correção de erros das classes sendo propostas, derivamos os respectivos algoritmos de decodificação. Na Seção 4.6 fazemos uso do algoritmo de Berlekamp-Massey, adaptado para corrigir múltiplos erros de Hamming. Finalmente, na Seção 4.7 fazemos uma análise comparativa entre os códigos sobre $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$.

No Capítulo 5, as conclusões deste trabalho bem como propostas para estudos futuros são apresentadas.

Capítulo 2

Anéis, Ideais, Corpos e Códigos

2.1 Introdução

Neste Capítulo apresentamos os resultados básicos necessários para o desenvolvimento e o entendimento dos capítulos seguintes. Para tanto, serão definidas as estruturas de grupos, anéis, corpos, módulos, códigos e todos os demais conceitos matemáticos que surgem de modo natural agregados a estas estruturas tais como homomorfismos, isomorfismos, ideais, anéis quociente, etc.

Com o objetivo de tornar o texto auto explicativo, incluiremos as definições usuais das estruturas algébricas tradicionais que constam neste trabalho. Todavia, o leitor poderá encontrar estas considerações nos textos tradicionais de Álgebra Abstrata constante nas referências.

Muito embora as definições a que se refere o parágrafo anterior sejam as mais genéricas possíveis, o interesse central da tese se restringe a uma classe particular de anéis que são os anéis de inteiros algébricos de um corpo de números. Dentre tantas propriedades destes anéis, podemos ressaltar que são comutativos com identidade; com isto, o termo anel, neste contexto, significa anel comutativo com identidade. Outras propriedades, que serão oportunamente listadas, dos anéis de inteiros algébricos serão incorporadas ao termo anéis.

Quanto às demonstrações dos resultados deste Capítulo, serão feitas algumas adaptações

com a finalidade de tornar a leitura mais agradável. Outros resultados terão suas demonstrações omitidas neste texto por considerarmos que as técnicas utilizadas no processo não enriquecem este trabalho.

O conteúdo deste capítulo está distribuído nas próximas quatro seções da seguinte maneira: Na Seção 2.2, apresentamos os principais resultados sobre anéis, ideais e corpos. Na Seção 2.3, fazemos uma revisão de extensões de corpos. Na Seção 2.4, abordamos os conceitos de corpos e anéis de números, bem como os conceitos de traços e normas de um elemento de uma extenção K de $\mathbb{Q}$. Na Seção 2.5 tratamos da decomposição de ideais primos em anéis de números algébricos e em extensões; em particular, mostramos a decomposição de um ideal primo em corpos quadráticos. Dedicamos à Seção 2.6 uma breve revisão de códigos lineares de bloco de um modo geral, em particular, códigos cíclicos e dentre estes, fazemos algumas considerações sobre códigos BCH. Também fazemos uma breve revisão dos princípios de decodificação, os quais serão utilizados no Capítulo 4.

2.2 Anéis, Ideais e Corpos

Dizemos que um conjunto não vazio G é um *grupo* se em G está definida uma operação, que indicaremos por $\cdot$, tal que para todos a, b, c em G temos:

i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

ii) existe um elemento, $e \in G$, tal que $a \cdot e = e \cdot a = a$;

iii) dado $a \in A$, existe um elemento, que denotaremos por $-a$, tal que $a \cdot (a^{-1}) = (a^{-1}) \cdot a = e$.

Um grupo G é dito comutativo se G satisfaz a propriedade

iv) $a \cdot b = b \cdot a$, $\forall a, b \in G$.

Dizemos que um conjunto não vazio A é um *anel* se em A estão definidas duas operações, que indicaremos por $+$ e $\cdot$, tais que para todos a, b, c em A temos:

i) $(a + b) + c = a + (b + c)$;

ii) $a + b = b + a$;

iii) existe um elemento, $0 \in A$, tal que $a + 0 = 0 + a = a$;

iv) dado $a \in A$, existe um elemento, que denotaremos por $-a$ tal que $a+(-a) = (-a)+a = 0$;

v) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

vi) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$.

As quatro primeiras propriedades nos dizem que A é um *grupo abeliano* em relação à operação $+$ (adição). Dizemos que o anel A é *comutativo* se A satisfaz a propriedade:

vii) $a \cdot b = b \cdot a$, para todos $a, b \in A$.

Notação: Denotaremos o produto $a \cdot b$, em um anel A, simplesmente por ab.

Um anel A pode possuir propriedades diversas. Por exemplo,

1. Se existir um elemento 1 em A tal que $a1 = 1a = a$, para todo a em A dizemos que A é um anel com *elemento identidade* 1. Iremos considerar $1 \neq 0$, pois do contrário, A seria o anel *nulo*.

2. Um elemento não nulo a de A diz-se um *divisor de zero* se existe um elemento não nulo b em A tal que $ab = 0$ ou $ba = 0$.

3. Suponhamos que A possua elemento identidade. Dizemos que um elemento a de A é uma *unidade* se existe b em A tal que $ab = ba = 1$. Além disso, b é chamado de inverso de a e denotado por a^{-1}.

Observemos que um divisor de zero nunca pode ser uma unidade.

Definição 2.1 *Um anel comutativo A, com identidade é dito um* domínio de integridade *se não existe divisor de zero em A.*

O conjunto $\mathbb{Z}$ dos números inteiros e o conjunto dos inteiros de Gauss $\mathbb{Z}[i]$, $i = \sqrt{-1}$, são exemplos de domínios de integridade.

Definição 2.2 *Dizemos que um anel comutativo A, com identidade é um* corpo *se todo elemento não nulo de A é uma unidade.*

Como exemplo de um corpo podemos citar o conjunto $\mathbb{Q}$ dos números racionais, com as operações habituais de adição e multiplicação de frações.

Definição 2.3 *Dizemos que um subconjunto B de um anel A é um* subanel *se B é um anel com as operações induzidas por A.*

A noção de módulo sobre um anel A (ou de $A-$ *módulo*) é a generalização da noção de espaço vetorial sobre um corpo.

Definição 2.4 *Um $A-$ módulo M é um grupo abeliano (aditivo) munido de uma aplicação $A \times M \to M$ (geralmente escrita como multiplicação) tal que, para quaisquer $a, b \in A$ e x, $y \in M$ valem as propriedades:*

i) $a(x+y) = ax + ay$, *ii)* $(a+b)x = ax + bx$ *iii)* $(ab)x = a(bx)$ *iv)* $1x = x$.

Logo, todo grupo abeliano, escrito aditivamente, é um $\mathbb{Z}-$módulo, onde a multiplicação $(\pm n)x$ é definida por $\pm(\underbrace{x + \cdots + x}_{|n|-\text{vezes}})$.

Definição 2.5 *Sejam A um anel e $\mathfrak{a}$ um subanel de A. Dizemos que $\mathfrak{a}$ é um* ideal *de A se $ax \in A$, para quaisquer que sejam $a \in A$ e $x \in \mathfrak{a}$.*

Um exemplo importante de ideal é o chamado *ideal principal* gerado por a, isto é, o subconjunto

$$\{ax : x \in A\}$$

de A, que será denotado por aA ou (a) quando não houver ambigüidade sobre o anel.

Por exemplo, se $A = \mathbb{Z}$ e $m \in \mathbb{Z}$, então

$$(m) = m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}.$$

A partir de agora, os *anéis* considerados serão *anéis comutativos com elemento identidade* $1 \neq 0$, a menos que se explicite o contrário

Definição 2.6 *Se todo ideal de um anel A é principal, então dizemos que A é um* anel de ideais principais. *Em particular, quando A é um domínio de integridade, dizemos que A é um* domínio de ideais principais, *ou simplesmente um DIP.*

Como exemplos de DIP, temos o anel dos números inteiros $\mathbb{Z}$ e o conjunto dos polinômios na variável X com coeficientes num corpo F, o qual será denotado por $F[X]$.

Dizemos que um elemento não nulo a de um anel A *divide* $b \in A$, se existe $c \in A$ tal que $b = ac$. Também dizemos neste caso que b é um múltiplo de a. Agora podemos redefinir um ideal principal gerado por $a \in A$ como sendo o conjunto dos múltiplos de a.

Dois elementos a e b de um anel A são ditos *associados* se existir um elemento invertível u de A tal que $a = ub$. Dizemos que um elemento $a \in A$ não nulo e não invertível é *irredutível* se seus únicos divisores são os elementos invertíveis do anel e seus próprios associados. Dizemos que um elemento a não nulo e não invertível de um anel A é *primo* se toda vez que a dividir o produto de dois elementos de A, a dividir também um dos fatores. A relação entre elementos primos e irredutíveis é dada pela proposição a seguir.

Proposição 2.1 *i) Num domínio de integridade, todo elemento primo é irredutível.*
ii) Num domínio principal, todo elemento irredutível é primo.

Exemplo 2.1 *Em $\mathbb{Z}$ o elemento 2 é irredutível, mas no entanto em $\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}$, temos $2 = (1+i)(1-i)$ e $1+i$, $1-i$ são irredutíveis em $\mathbb{Z}[i]$.*

Lema 2.1 *(Lema de Euclides)Sejam a, b, c elementos de um anel principal A; se a divide bc e a é primo com b, então a divide c.*

O conceito de anel quociente, que veremos a seguir, desempenhará um importante papel no trabalho em consideração.

Sejam A um anel e $\mathfrak{a}$ um ideal de A. Dados $a, b \in A$, dizemos que $a \equiv b \pmod{\mathfrak{a}}$ se $a - b \in \mathfrak{a}$. É fato conhecido que esta é uma relação de equivalência, sendo

$$\overline{a} = a + \mathfrak{a} = \{a + x : x \in \mathfrak{a}\}$$

a classe de equivalência do elemento $a \in A$. Um elemento $b \in A$ é dito um representante da classe $\overline{a}$ se $b \in \overline{a}$.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Tabela 2.1: Adição e multiplicação em $\mathbb{Z}/3\mathbb{Z}$

Seja $A/\mathfrak{a}$ o conjunto das classes de equivalência dos elementos de A. Em $A/\mathfrak{a}$ definimos as operações *soma* e *produto* entre as classes laterais:

$$\overline{a} + \overline{b} = \overline{a+b} \text{ (isto é } (a+\mathfrak{a}) + (b+\mathfrak{a}) = (a+b) + \mathfrak{a} \text{)}$$

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} \text{ (isto é } (a+\mathfrak{a}) \cdot (b+\mathfrak{a}) = (a \cdot b) + \mathfrak{a} \text{)}$$

Uma verificação simples mostra que as operações acima estão bem definidas, isto é, o resultado das operações independem da escolha dos representantes das classes. O conjunto $A/\mathfrak{a}$, munido destas duas operações, é um anel, denominado *anel quociente de A pelo ideal* $\mathfrak{a}$.

Um exemplo de anel quociente é o conjunto $\mathbb{Z}/3\mathbb{Z}$, onde as operações $+$ e $\cdot$ são mostradas na Tabela 2.1.

Um ideal $\mathfrak{m}$ de A, $\mathfrak{m} \neq A$, é dito *maximal* se o único ideal que o contém propriamente é o próprio A.

Dizemos que um ideal $\mathfrak{p}$ de A, $\mathfrak{p} \neq A$, é um ideal primo se sempre que $x \cdot y \in \mathfrak{p}$, então $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$.

No anel dos inteiros $\mathbb{Z}$, o ideal $2\mathbb{Z}$ é maximal e o ideal nulo $\{0\}$ é primo. Aliás, A é um domínio de integridade se, e somente se, $\{0\}$ é primo.

Observamos que no conjunto $\mathbb{Z}$, os ideais maximais coincidem com os ideais primos não

nulos, porém isto não é verdade em geral, como mostra a proposição a seguir.

Proposição 2.2 *Sejam A um anel e $\mathfrak{a}$ um ideal de A. Então temos:*

a) $A/\mathfrak{a}$ é um domínio de integridade se, e somente se, $\mathfrak{a}$ é um ideal primo.

b) $A/\mathfrak{a}$ é um corpo se, e somente se, $\mathfrak{a}$ é um ideal maximal.

Portanto, todo ideal maximal é primo. Em geral, a recíproca não é verdadeira. Entretanto, quando A é um domínio de ideais principais vale a recíproca, ou seja:

Proposição 2.3 *Se A é um domínio de ideais principais, então todo ideal primo não nulo é maximal.*

Demonstração: De fato, seja $\mathfrak{p}$ um ideal primo não nulo de A e suponhamos que $\mathfrak{p} \subset \mathfrak{q} \subset A$, onde $\mathfrak{q}$ é um ideal de A. Como A é um DIP, $\mathfrak{p} = (a)$ e $\mathfrak{q} = (b)$ para alguns $a, b \in A$. Então, $a = bc$ para algum $c \in A$; logo $bc \in \mathfrak{p}$, pois $a \in \mathfrak{p}$, portanto $b \in \mathfrak{p}$ ou $c \in \mathfrak{p}$. Se $b \in \mathfrak{p}$ então $\mathfrak{p} = \mathfrak{q}$. Se $c \in \mathfrak{p}$ então $c = ad$ para algum $d \in A$, e assim $a = bc = bad$, daí temos que $a = 0$, e portanto, $\mathfrak{p} = 0$, o que contradiz a hipótese, ou $bd = 1$, pois A é um domínio de integridade. Portanto, b é uma unidade e, assim, $\mathfrak{q} = A$. Logo, não existe um ideal $\mathfrak{q}$ de A, diferente de $\mathfrak{p}$ e A, tal que $\mathfrak{p} \subset \mathfrak{q} \subset A$, e portanto, $\mathfrak{p}$ é maximal. ■

Portanto, em $\mathbb{Z}$ e em $F[X]$ os ideais maximais coincidem com os ideais primos não nulos, pois estes anéis são DIP.

Definição 2.7 *Definimos a soma de dois ideais $\mathfrak{a}$ e $\mathfrak{b}$ de A por:*

$$\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a}, \quad b \in \mathfrak{b}\},$$

que também é um ideal. Dizemos que os ideais $\mathfrak{a}$ e $\mathfrak{b}$ são relativamente primos *se $\mathfrak{a} + \mathfrak{b} = A$. O* produto *de dois ideais $\mathfrak{a}$ e $\mathfrak{b}$ é definido como sendo o conjunto de todas as somas finitas de produtos $a \cdot b$, com $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, isto é,*

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathfrak{a}, \quad b_i \in \mathfrak{b} \right\}.$$

As definições acima estendem-se de forma análoga para o caso de um número finito de ideais $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ de A.

No estudo de anéis existe uma família de funções entre anéis que desempenha um papel fundamental.

Definição 2.8 *Sejam A e B dois anéis com elementos identidades 1 e $1'$, respectivamente. Um* homomorfismo $\varphi : A \to B$ *é uma aplicação φ de A em B tal que $\varphi(a+b) = \varphi(a)+\varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$ e $\varphi(1) = 1'$, $\forall a, b \in A$.*
Se $\varphi : A \to B$ é um homomorfismo bijetor, então dizemos que φ é um isomorfismo *de A em B. Dizemos que dois anéis A e B são* isomorfos *(e denotamos por $A \simeq B$) se existir um isomorfismo entre eles. Um* automorfismo *do anel A é um isomorfismo de A em A.*

Teorema 2.1 *Sejam A e B anéis e $\varphi : A \to B$ um homomorfismo. Então,*
i) A imagem de φ, $\mathrm{Im}(\varphi) = \{\varphi(a) : a \in A\}$ é um subanel de B;
ii) O núcleo de φ, $\ker(\varphi) = \{a \in A : \varphi(a) = 0\}$ é um ideal de A;
iii) A aplicação φ é injetiva se, e somente se, $\ker(\varphi) = \{0\}$;
iv) Os anéis $A/\ker(\varphi)$ e $\mathrm{Im}(\varphi)$ são isomorfos, isto é, $\frac{A}{Ker(\varphi)} \simeq Im(A)$.

2.3 Extensões de Corpos

Uma extensão de um corpo K é qualquer corpo F contendo K como subcorpo. A notação adotada para este conceito é $F \supset K$ ou F/K.

Quando o corpo F é uma extensão do corpo K, então F pode ser visto como um espaço vetorial sobre K, bastando para isto considerarmos as operações adição e multiplicação por escalar definidos de forma usual, isto é,

$$\begin{array}{rccc} + : & F \times F & \longrightarrow & F \\ & (u, v) & \longmapsto & u + v \end{array}$$

$$\begin{aligned} \cdot : \quad K \times F &\longrightarrow F \\ (\lambda, v) &\longmapsto \lambda v \ . \end{aligned}$$

Usando as propriedades dos corpos K e F, podemos ver que F é um espaço vetorial sobre K. O grau (ou índice) de uma extensão F/K, denotado por $[F : K]$, é a dimensão de F visto como espaço vetorial sobre K. A extensão é dita *finita* se $[F : K]$ é finito; caso contrário a extensão é dita *infinita*.

Definição 2.9 *Sejam F uma extensão de K e α um elemento de F. Dizemos que α é* algébrico *sobre K se existem elementos $a_0, a_1, \cdots, a_n$ $(n \geq 1)$ em K, não todos nulos, tais que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, isto é, se α é raiz de um polinômio não nulo com coeficientes em K. Caso contrário, α é dito* transcendente *sobre K. Dizemos que um número complexo é algébrico, se ele é algébrico sobre o corpo $\mathbb{Q}$ dos números racionais. Uma extensão $F \supset K$ é algébrica, se todo elemento de F é algébrico sobre K. Dizemos que um corpo K é* algebricamente fechado *se todo polinômio em $K[X]$, de grau positivo, possui uma raiz em K.*

Podemos ver que $\alpha = \sqrt{-1} \in \mathbb{C}$ é algébrico sobre $\mathbb{Z}$, pois α é raiz do polinômio $f(X) = X^2 + 1$, por outro lado $\beta = \pi$ é transcendente sobre $\mathbb{Z}$.

O corpo $\mathbb{C}$ dos *números complexos* é um exemplo de corpo algebricamente fechado, enquanto que $\mathbb{Q}(i) = \{a + bi; \quad a, b \in \mathbb{Q}\}$ é uma extensão algébrica, de grau 2, de $\mathbb{Q}$.

Observemos que se K é algebricamente fechado, então todo polinômio $f(X) \in K[X]$ possui todas as suas raízes em K.

Seja $\alpha \in F$ algébrico sobre K e seja

$$\varphi : K[X] \longrightarrow F$$

o homomorfismo definido por $\varphi(f(X)) = f(\alpha)$, $f \in K[X]$. Então a imagem de φ, que

denotamos por $K[\alpha]$, é dada por

$$K[\alpha] = \{f(\alpha) : f \in K[X]\} = \left\{\sum_{i=0}^{n} a_i \alpha^i : a_i \in K,\ n \geq 0\right\}.$$

Pode-se mostrar que $K[\alpha]$ é um domínio de integridade, pois $K[\alpha] \subset F$. Por outro lado, como $\ker(\varphi)$ é um ideal não nulo de $K[X]$ e K sendo um corpo, o ideal $\ker(\varphi)$ é principal, que podemos supor gerado por um polinômio *mônico* $p(X) \in K[X]$, isto é, um polinômio com coeficiente líder igual a 1. Pelo Teorema 2.1, temos um isomorfismo entre $K[X]/(p(X))$ e $K[\alpha]$, isto é:

$$K[X]/(p(X)) \simeq K[\alpha].$$

Pelo isomorfismo acima o quociente $K[X]/(p(X))$ é um domínio de integridade, logo o ideal $(p(X))$ é primo, portanto, $p(X)$ é irredutível. Considerando $p(X)$ mônico e tendo α como raiz, então pode-se ver que $p(X)$ é univocamente determinado por α. Logo, podemos ver que $p(X)$ é o polinômio de menor grau com esta propriedade. Assim, dizemos que $p(X)$ é *o polinômio minimal* de α sobre K.

Como $p(X)$ é irredutível, pois do contrário $p(X)$ não seria o polinômio minimal de α, o ideal $(p(X))$ é primo, logo é maximal, pois $F[X]$ é um domínio de ideais principais. Portanto, o quociente $F[X]/(p(X))$ é um corpo, assim o domínio $K[\alpha]$ também é um corpo. Observemos que $K[\alpha]$ é uma extensão de K de grau n, onde n é o grau do polinômio minimal de α sobre K, isto porque $K[\alpha]$ é o conjunto das expressões polinomiais $\sum_{i=0}^{n} a_i \alpha^i$, $a_i \in K$ e α sendo algébrico, temos que $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base de $K[\alpha]$ sobre K. As raízes de $p(X)$ em $\mathbb{C}$ são chamadas os *conjugados* de α sobre K e o número destas raízes é n.

O processo usado acima para obtermos $K[\alpha]$ é denominado *adjunção de raízes*. É fácil ver que $K[\alpha]$ é o menor corpo que contém K e α. Também podemos ver que $K[\alpha]$ coincide com o corpo $K(\alpha)$ formado pelas razões polinomiais $f(\alpha)/g(\alpha)$; $f, g \in K[X]$, $g(\alpha) \neq 0$, isto é,

$$K(\alpha) = \{f(\alpha)/g(\alpha) : f, g \in K[X],\quad g(\alpha) \neq 0\}.$$

De agora em diante, usaremos a notação $K(\alpha)$ ao invés de $K[\alpha]$.

Proposição 2.4 *Se $F \supset K$ é uma extensão finita , então a extensão F de K é algébrica.*

Proposição 2.5 *Se $\alpha \in F \supset K$, então as seguintes afirmações são equivalentes:*
i) α é algébrico sobre K;
ii) A extensão $K(\alpha) \supset K$ é finita;
iii) $K(\alpha)$ é uma extensão algébrica de K.

Proposição 2.6 *Sejam $E \supset F \supset K$ corpos tais que $[E:F]$ e $[F:K]$ são finitos. Então $[E:K]$ é finito e vale:*

$$[E:K] = [E:F][F:K].$$

Uma extensão $L \supset K$ é dita *simples*, se existe $\alpha \in L$, tal que $L = K(\alpha)$.

Teorema 2.2 *Sejam L, K subcorpos de $\mathbb{C}$. Se a extensão $L \supset K$ é finita, então $L = K(\alpha)$ para algum $\alpha \in L$, isto é, L é uma* extensão simples *de K.*

2.4 Corpos e Anéis de Números

Um *corpo de números* K é uma extensão finita de $\mathbb{Q}$. Pelo Teorema 2.2 , K é da forma $\mathbb{Q}(\alpha)$ para algum elemento $\alpha \in K$, mais ainda, se o polinômio minimal de α sobre $\mathbb{Q}$ é de grau n então

$$\mathbb{Q}(\alpha) = \left\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q},\ i = 0, 1, 2, \cdots, n-1\right\}$$

e esta representação é única, ou seja, $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base para o espaço vetorial $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

Como exemplos de tais extensões podemos citar os *corpos ciclotômicos* $\mathbb{Q}(\zeta_m)$, onde $\zeta_m = e^{\frac{2\pi i}{m}}$, $m \in \mathbb{Z}$, é uma raiz primitiva $m-ésima$ da unidade. O grau do corpo ciclotômico

$\mathbb{Q}(\zeta_m)$ é dado pela função ϕ de Euler, que é o número de inteiros positivos menores que m e primos com m, isto é,

$$\phi(m) = \#\{n : 1 \leq n < m,\ (m,n) = 1\}$$

Por exemplo, se $m = 8$, então $\phi(8) = 4$, enquanto $\phi(7) = 6$.

Uma outra classe importante de corpos de números é a classe dos *corpos quadráticos,* isto é, extensões $K \supset \mathbb{Q}$, de grau 2 que, pelo Teorema 2.2, é da forma $\mathbb{Q}(\alpha)$. No entanto, mostraremos que existe $d \in \mathbb{Z}$, livre de quadrados, tal que $K = \mathbb{Q}\left(\sqrt{d}\right)$. De fato, seja $f(x) = X^2 + bX + c \in \mathbb{Q}[x]$, o polinômio minimal de α sobre $\mathbb{Q}$, então $2\alpha = -b \pm \sqrt{b^2 - 4c}$. Assim, $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{b^2 - 4c}\right)$, mas $b^2 - 4c$ é um número racional, assim $b^2 - 4c = r/s = rs/s^2 \in \mathbb{Q}$, daí $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{rs/s^2}\right) = \mathbb{Q}(\sqrt{rs})$. Suponhamos que $rs = k^2 d$; $k, d \in \mathbb{Z}$, d livre de quadrados, logo $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{rs}) = \mathbb{Q}\left(\sqrt{k^2 d}\right) = \mathbb{Q}\left(\sqrt{d}\right)$. Assim, $K = \mathbb{Q}\left(\sqrt{d}\right)$, $d \in \mathbb{Z}$ livre de quadrados. Portanto, $\left\{1, \sqrt{d}\right\}$ é uma base do espaço vetorial $\mathbb{Q}\left(\sqrt{d}\right)$ sobre $\mathbb{Q}$.

Quando $d > 0$, dizemos que $\mathbb{Q}\left(\sqrt{d}\right)$ é um *corpo quadrático real,* e quando $d < 0$, dizemos que $\mathbb{Q}\left(\sqrt{d}\right)$ é um *corpo quadrático imaginário.* Por exemplo, $\mathbb{Q}(i)$, $(i = \sqrt{-1})$, é um corpo quadrático imaginário, e também um corpo ciclotômico, pois i é uma raiz primitiva *quarta* da unidade, enquanto que $\mathbb{Q}\left(\sqrt{2}\right)$ é um corpo quadrático real.

Definição 2.10 *a) Um número complexo α diz-se um* inteiro algébrico *se α é raiz de um polinômio f, mônico com coeficientes em $\mathbb{Z}$. A equação $f(\alpha) = 0$, diz-se, uma equação de* dependência integral *de α sobre $\mathbb{Z}$.*
b) Dizemos que um anel A é integralmente fechado, *se todo elemento de seu corpo de frações K, que é* inteiro *sobre A, pertence a A.*

O anel $\mathbb{Z}$, dos números inteiros, é um exemplo de anel integralmente fechado. Este exemplo não é um fato isolado, pois, em geral, temos o seguinte:

Proposição 2.7 *Todo domínio D de ideais principais é integralmente fechado.*

Demonstração: Seja F o corpo de frações do domínio D e $\alpha \in F$ inteiro sobre D. Então α satisfaz uma equação de dependência integral

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0, \quad a_i \in F.$$

Como α está em F, podemos escrever $\alpha = a/b, \quad a, b \in A$, primos entre si. Logo,

$$a^n + b(a_{n-1}a^{n-1} + \cdots + a_1ab^{n-2} + a_0b^{n-1}) = 0,$$

ou seja b divide a^n, como $(a, b) = 1$, com a aplicação repetida do Lema 2.1, temos que b divide a, assim $\alpha = a/b \in A$, portanto, A é integralmente fechado. ■

Embora, na definição, não exigimos que f seja irredutível sobre $\mathbb{Q}$, ele na verdade o é, como mostra o Teorema 2.3 a seguir.

Teorema 2.3 *Sejam $\alpha \in \mathbb{C}$ um inteiro algébrico e f o polinômio minimal de α sobre $\mathbb{Q}$. Então f é irredutível sobre $\mathbb{Q}$.*

Na demonstração deste Teorema, faz-se uso do Lema a seguir.

Lema 2.2 *(Lema de Gauss) Seja f um polinômio mônico com coeficientes em $\mathbb{Z}$, e suponhamos que $f = gh$, com $g, h \in \mathbb{Q}[X]$. Então g e h possuem coeficientes em $\mathbb{Z}$, isto é, $g, h \in \mathbb{Z}[X]$.*

Demonstração: (do Teorema 2.3). Suponhamos que f não seja irredutível sobre $\mathbb{Q}$, então $f = gh$, com $g, h \in \mathbb{Q}[X]$, g e h não constantes. Sem perda de generalidade, podemos supor f e g mônicos, Então, pelo Lema 2.2, $g, h \in \mathbb{Z}[X]$. De $f(\alpha) = 0$, temos $g(\alpha)\, h(\alpha) = 0$, como $\mathbb{Z}[\alpha]$ é um domínio, temos $g(\alpha) = 0$ ou $h(\alpha) = 0$. Como ambos possuem grau menor que f, temos uma contradição. ■

Corolário 2.1 *Os únicos inteiros algébricos em* $\mathbb{Q}$ *são os números* inteiros ordinários, *isto é, os elementos de* $\mathbb{Z}$.

Vamos agora determinar os inteiros algébricos de uma extensão quadrática.

Denotaremos por $\mathbb{A}$ o conjunto dos inteiros algébricos de um corpo de números K.

Proposição 2.8 *Seja* $K = \mathbb{Q}\left(\sqrt{d}\right)$ *um corpo quadrático, com* d *inteiro livre de quadrados. Então* $\mathbb{A} = \mathbb{Z}[\omega]$, *onde* $\omega = \begin{cases} \sqrt{d}, & \text{se } d \equiv 2 \text{ ou } 3 (\text{mod } 4) \\ \frac{1+\sqrt{d}}{2}, & \text{se } d \equiv 1 (\text{mod } 4). \end{cases}$

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathbb{A}$, $a, b \in \mathbb{Q}$. Se $b = 0$, então $X - a$ é o polinômio minimal de α sobre $\mathbb{Q}$, logo $a \in \mathbb{Z}$. Se $b \neq 0$ o polinômio minimal de α sobre $\mathbb{Q}$ é de grau 2 e, podemos ver que, este polinômio é dado por $m(X) = X^2 - 2aX + a^2 - db^2$, então $2a$, $a^2 - db^2 \in \mathbb{Z}$. Como d é livre de quadrados, $2b \in \mathbb{Z}$, pois se $2b$ possuísse um denominador c, então este conteria um fator primo p, cujo quadrado não se cancelaria com algum fator de d, pois este não possui fatores quadrados, e assim, $d(2b)^2$ não seria inteiro. Logo, $2b \in \mathbb{Z}$. Portanto; $2a$, $a^2 - db^2 \in \mathbb{Z}$, $\forall \alpha = a + b\sqrt{d} \in \mathbb{A}$. Assim, podemos escrever:

$$a = u/2, \quad b = v/2 \quad u, v \in \mathbb{Z}.$$

Logo $(2a)^2 - d(2b)^2 \in 4\mathbb{Z}$. Substituindo a por $u/2$ e b por $v/2$, temos $u^2 - dv^2 \in 4\mathbb{Z}$

(I) Se $b \in \mathbb{Z}$, então v é par, logo u é par, e portanto, $a \in \mathbb{Z}$.

(II) Se $b \notin \mathbb{Z}$, então v é ímpar, logo, $d \equiv 1 (\text{mod } 4)$ e u é ímpar. Portanto, $a \notin \mathbb{Z}$.

Se $d \equiv 2$ ou $3 (\text{mod } 4)$ então ocorre a condição (I), isto é, $a, b \in \mathbb{Z}$. Portanto, $\alpha = a + b\sqrt{d} \in \mathbb{Z}$ e, mais ainda, $a + b\sqrt{d}$ é raiz do polinômio $X^2 - 2aX + a^2 - db^2 \in \mathbb{Z}[X]$, portanto, $\mathbb{A} = \mathbb{Z}\left[\sqrt{d}\right]$.

Se $d \equiv 1 (\text{mod } 4)$, então u e v possuem mesma paridade, isto é, ambos são pares ou ímpares.

Se u e v são pares, então $a, b \in \mathbb{Z}$. Logo, $\alpha = a + b\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right]$. Se u e v são ímpares, então $\alpha = a + b\sqrt{d} = u/2 + v/2\sqrt{d} = (u - v)/2 + v\left(\left(1 + \sqrt{d}/2\right)\right) \in \mathbb{Z}\left[\left(1 + \sqrt{d}\right)/2\right]$. Portanto, $\alpha \in \mathbb{Z}\left[\left(1 + \sqrt{d}\right)/2\right] \quad \forall \alpha \in \mathbb{A}$. Logo, $\mathbb{A} \subset \mathbb{Z}\left[\left(1 + \sqrt{d}\right)/2\right]$.

Seja $\alpha = a + b\left(\left(1 + \sqrt{d}\right)/2\right) \in \mathbb{Z}\left[\left(1 + \sqrt{d}\right)/2\right]$; $a, b \in \mathbb{Z}$. Logo, $2a + b \in \mathbb{Z}$ e $(a + b/2)^2 -$

$d(b/2)^2 = a^2 + ab + (1-d)b^2/4 \in \mathbb{Z}$, pois $d \equiv 1 \pmod 4$. Logo, $\mathbb{Z}\left[\left(1+\sqrt{d}\right)/2\right] \subset \mathbb{A}$, pois $m(X) = X^2 - (2a+b)X + (a^2+ab+(1-d)b^2/4) \in \mathbb{Z}[X]$ é o polinômio minimal de α. Logo, $\mathbb{Z}\left[\left(1+\sqrt{d}\right)/2\right] \subset \mathbb{A}$. Portanto, $\mathbb{Z}\left[\left(1+\sqrt{d}\right)/2\right] = \mathbb{A}$. ■

Pela Proposição 2.8, o conjunto $\mathbb{A}$, dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{d}\right)$, é um *anel*. Na verdade, isto vale para qualquer corpo de números; para verificarmos este fato basta mostrarmos que a soma e o produto de dois inteiros algébricos são também inteiros algébricos, ver [26]. Assim, para vermos que $\alpha = \sqrt{2} + \sqrt{3}$ é um inteiro algébrico, basta fazermos

$$\left(\alpha - \sqrt{2}\right)^2 = \left(\sqrt{3}\right)^2$$

e depois

$$\left(\alpha^2 - 1\right)^2 = \left(2\sqrt{2}\alpha\right)^2,$$

para obtermos

$$\alpha^4 - 8\alpha^2 - 2\alpha + 1 = 0,$$

e este é, de fato, o polinômio minimal de α sobre $\mathbb{Q}$.

2.4.1 Traços e Normas

Sejam $\alpha \in \mathbb{C}$ um inteiro algébrico e $f \in \mathbb{Z}[X]$ o polinômio minimal de α sobre $\mathbb{Q}$, de grau n. Então f possui n raizes em $\mathbb{C}$, ou seja, α possui n conjugados em $\mathbb{C}$.

Definição 2.11 *Uma função σ de K em $\mathbb{C}$ é dita uma* imersão *se σ é um homomorfismo injetivo.*

Portanto, existem n *imersões* de K em $\mathbb{C}$ e, estas são determinadas pelos n conjugados de α.

Por exemplo, o corpo quadrático $\mathbb{Q}\left(\sqrt{d}\right)$, d um inteiro livre de quadrados, possui *duas* imersões em $\mathbb{C}$; a aplicação identidade que leva α em si mesmo, e a que leva $\alpha = a + b\sqrt{d}$ no seu conjugado $\overline{\alpha} = a - b\sqrt{d}$. Por outro lado, os corpos ciclotômicos possuem $\phi(m)$ imersões.

Sejam K um corpo de números de grau n, $\beta \in K$ e $\sigma_1, \sigma_2, \cdots, \sigma_n$, as n imersões de K em $\mathbb{C}$. Chamaremos de *traço* de β, relativo a extensão $K/\mathbb{Q}$, o elemento

$$T_{K/\mathbb{Q}}(\beta) = \sigma_1(\beta) + \sigma_2(\beta) + \cdots + \sigma_n(\beta)$$

e a *norma* de β, relativo a extensão $K/\mathbb{Q}$, o elemento

$$N_{K/\mathbb{Q}}(\beta) = \sigma_1(\beta)\,\sigma_2(\beta)\cdots\sigma_n(\beta).$$

Podemos ver que as funções traço e norma gozam das seguintes propriedades, para todos $\alpha, \beta \in K$, e $r \in \mathbb{Q}$, (lembre que $n = [K : \mathbb{Q}]$)

$i) T_{K/\mathbb{Q}}(\alpha + \beta) = T_{K/\mathbb{Q}}(\alpha) + T_{K/\mathbb{Q}}(\beta)$;

$ii) T_{K/\mathbb{Q}}(r) = nr$;

$iii) T_{K/\mathbb{Q}}(r\alpha) = rT_{K/\mathbb{Q}}(\alpha)$;

$iv) N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)\,N_{K/\mathbb{Q}}(\beta)$;

$v) N_{K/\mathbb{Q}}(r) = r^n$;

$vi) N_{K/\mathbb{Q}}(r\alpha) = r^n N_{K/\mathbb{Q}}(\alpha)$.

Suponhamos, agora, que α seja de grau s sobre $\mathbb{Q}$, isto é, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = s$, como o grau de K sobre $\mathbb{Q}$ é n, temos, pela Proposição 2.6, que n/s é um inteiro, pois

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] = n.$$

Portanto, $n/s = [K : \mathbb{Q}[\alpha]]$.

Sejam $t(\alpha)$ e $n(\alpha)$ a soma e o produto, respectivamente, dos conjugados de α sobre $\mathbb{Q}$, isto é, $t(\beta) = T_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)$ e $n(\beta) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)$.

Teorema 2.4 *De acordo com a notação acima temos:*

$$T_{K/\mathbb{Q}}(\beta) = \frac{n}{s} \cdot t(\beta),$$

$$N_{K/\mathbb{Q}}(\beta) = n(\beta)^{\frac{n}{s}}.$$

Obs. 2.1 *Vamos denotar* $T_{K/\mathbb{Q}}(\alpha)$ *e* $N_{K/\mathbb{Q}}(\alpha)$ *por* $T(\alpha)$ *e* $N(\alpha)$ *respectivamente, quando não houver ambigüidade de notação.*

Corolário 2.2 *Os elementos* $T(\alpha)$ *e* $N(\alpha)$ *são números racionais, para todo* $\alpha \in \mathbb{C}$ *algébrico.*

Demonstração: Como $t(\alpha)$ é a soma e $n(\alpha)$ é o produto dos conjugados de α sobre $\mathbb{Q}$ e o polinômio minimal f de α sobre $\mathbb{Q}$ se escreve como $f(\alpha) = \alpha^n - t(\alpha) + \cdots + (-1)^n n(\alpha)$, logo, $t(\alpha)$ e $n(\alpha)$ são números racionais. ■

Corolário 2.3 *Se* α *é um inteiro algébrico, então* $T(\alpha)$ *e* $N(\alpha)$ *são números inteiros.*

Demonstração: De fato, pois α sendo um inteiro algébrico, o seu polinômio minimal sobre $\mathbb{Q}$ possui coeficientes em $\mathbb{Z}$. ■

Proposição 2.9 *Nos corpos quadráticos* $\mathbb{Q}\left(\sqrt{d}\right)$ *temos:*

$$T\left(a + b\sqrt{d}\right) = 2a,$$

$$N\left(a + b\sqrt{d}\right) = a^2 - db^2.$$

Neste caso α é um inteiro algébrico se, e somente se, seu traço e sua norma forem inteiros.

Uma das aplicações importantes das funções traço e norma é a determinação das unidades do anel de inteiros algébricos $\mathbb{A}$ do corpo K.

Definição 2.12 *Chamamos de* unidades *de um corpo de números* K *os elementos invertíveis do anel dos inteiros algébricos de* K.

É fácil ver que as unidades formam um grupo multiplicativo. A seguir veremos uma proposição que relaciona normas e unidades, caracterizando estas.

Proposição 2.10 *Seja K um corpo de números e $u \in K$. Então u é uma unidade de K se, e somente se, u é um inteiro algébrico e $N(u) = \pm 1$.*

Demonstração: De fato, se u é uma unidade de K, então, como $N(u)$ e $N(u^{-1})$ são elementos de $\mathbb{Z}$, cujo produto é 1, $(N(1) = N(u/u) = N(u)\,N(u^{-1}) = 1)$. Assim, $N(u) = \pm 1$. Reciprocamente, seja u um inteiro algébrico de K, de norma ± 1, então sabemos que a equação de dependência integral de u é dada por:

$$u^n + a_{n-1}u^{n-1} + \cdots + a_1 u \pm 1 = 0,\ a_i \in \mathbb{Z},$$

então,

$$u\left(u^{n-1} + a_{n-1}u^{n-2} + \cdots + a_1\right) = \mp 1.$$

Logo, $\pm\left(u^{n-1} + a_{n-1}u^{n-2} + \cdots + a_1\right)$ é um inteiro algébrico e é o inverso de u, portanto, u é uma unidade de K. ■

Em um corpo quadrático real $K = \mathbb{Q}\left(\sqrt{d}\right)$ temos infinitas unidades. Pode-se mostrar que as unidades, neste caso, formam um grupo multiplicativo abeliano infinito. Por outro lado, as unidades de um corpo quadrático imaginário são: 1 e -1, exceto nos casos $d = -1$ e $d = -3$, nestes casos temos:
i) Se $d = -1$, então as unidades de $K = \mathbb{Q}\left(\sqrt{-1}\right)$ são as raízes *quartas* da unidade: $\{1, -1, i, -i\}$.
ii) Se $d = -3$, então as unidades de $K = \mathbb{Q}\left(\sqrt{-3}\right)$ são as raízes *sextas* da unidade: $\left\{\left(\frac{1+\sqrt{-3}}{2}\right)^j,\ \ j = 0, 1, \cdots, 5\right\}$.

2.5 Decomposição de Ideais Primos em Anéis de Números

Vamos iniciar esta seção mostrando que todo anel de números $\mathbb{A}$ possui três propriedades especiais e que em todo domínio com estas propriedades vale a fatorização única para ideais, embora os elementos do anel $\mathbb{A}$ não possuam tal fatoração única, como um produto de

elementos irredutíveis. Em $\mathbb{Z}\left[\sqrt{-5}\right]$, por exemplo, temos

$$14 = 2 \cdot 7 = \left(3 + \sqrt{-5}\right)\left(3 - \sqrt{-5}\right),$$

isto é, 14 se decompõe no produto dos elementos irredutíveis 2, 7, $3 + \sqrt{-5}$ e $3 - \sqrt{-5}$ de $\mathbb{Z}\left[\sqrt{-5}\right]$.

Definição 2.13 *Dizemos que um domínio D é um* domínio de Dedekind *se:*

i) Todo ideal de D é finitamente gerado;

ii) Todo ideal primo não nulo de D é maximal;

iii) D é integralmente fechado em seu corpo de frações,

$$F = \{a/b : \quad a, b \in D, \quad b \neq 0\}.$$

Teorema 2.5 *Todo anel de números é um domínio de Dedekind.*

Teorema 2.6 *Todo ideal, em um domínio de Dedekind D, é univocamente representado por um produto finito de ideais primos.*

Como consequência dos Teoremas 2.5 e 2.6 , temos,

Corolário 2.4 *Os ideais, em um anel de números, se fatoram univocamente em um produto finito de ideais primos, isto é, se $\mathfrak{a}$ é um ideal de $\mathbb{A}$, então $\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$, $\mathfrak{p}_i$ ideal primo de $\mathbb{A}$, $e_i \in \mathbb{N}$, $i = 1, 2, \cdots, s$.*

Definição 2.14 *Dizemos que M é um $\mathbb{Z}-$módulo livre de posto n se M é uma soma direta de n submódulos cada um deles isomorfo a $\mathbb{Z}$.*

Teorema 2.7 *Se K é um corpo de números algébricos de grau n, então o anel $\mathbb{A}$ dos inteiros algébricos de K é um $\mathbb{Z}-$módulo livre de posto n.*

Portanto, o anel $\mathbb{A}$ possui uma $\mathbb{Z}$ $-base$, isto é, $\mathbb{A} = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\boldsymbol{\alpha}_2 \oplus \cdots \oplus \mathbb{Z}\boldsymbol{\alpha}_n$, $\alpha_i \in \mathbb{A}$, $i = 1, 2, \cdots, n$, ou seja qualquer elemento α de $\mathbb{A}$ se escreve de modo único como

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n, \quad a_i \in \mathbb{Z}, \quad i = 1, 2, \cdots, n.$$

O conjunto $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ é dito uma *base integral* para $\mathbb{A}$, ou uma *base* de $\mathbb{A}$ *sobre* $\mathbb{Z}$. Podemos ver ainda que $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ é também uma base de K sobre $\mathbb{Q}$.

Proposição 2.11 *Seja* $\mathfrak{a}$ *um ideal não nulo em um anel de números* $\mathbb{A}$; *então o quociente* $\mathbb{A}/\mathfrak{a}$ *é finito.*

Demonstração: Sejam $\alpha \in \mathbb{A}$, $\alpha \neq 0$ e $m = N(\alpha)$, logo $m \in \mathbb{Z}$ e m é não nulo. Vamos mostrar que $m \in \mathbb{A}$. Sabemos que $N(\alpha) = \alpha\beta$, onde β é o produto dos conjugados de α, assim $m = \alpha\beta$, e o elemento β pertence a $\mathbb{A}$, pois $\beta = \alpha/m$. Como $\alpha, m \in K$ temos $\beta = \alpha/m \in K$. Como β é um inteiro algébrico, então $\beta \in \mathbb{A}$, e portanto, como $\alpha \in \mathfrak{a}$, o produto $\alpha\beta = m$ pertence a $\mathfrak{a}$, logo o ideal $(m) \subseteq \mathfrak{a}$ e, assim, $\mathbb{A}/\mathfrak{a} \subseteq \mathbb{A}/(m)$, mas $\mathbb{A}/(m) = \mathbb{Z}\boldsymbol{\alpha}_1/(m) \oplus \mathbb{Z}\boldsymbol{\alpha}_2/(m) \oplus \cdots \oplus \mathbb{Z}\boldsymbol{\alpha}_n/(m)$, logo $\#\left(\frac{\mathbb{A}}{(m)}\right) = m^n$. Como $\mathbb{A}/\mathfrak{a} \subseteq \mathbb{A}/(m)$ temos $\#(\mathbb{A}/\mathfrak{a}) \leq m^n$, ou seja o quociente $\mathbb{A}/\mathfrak{a}$ é finito. ■

2.5.1 Decomposição de ideais primos em extensões

Quando passamos do anel $\mathbb{Z}$ para um outro anel que o contém, como por exemplo, $\mathbb{Z}\left[\sqrt{-5}\right]$, podemos perder algumas propriedades que vale naquele, mas não neste.

Por exemplo, na extensão $\mathbb{Z}\left[\sqrt{-5}\right] \supset \mathbb{Z}$ o número 41 é irredutível, em $\mathbb{Z}$, mas em $\mathbb{Z}\left[\sqrt{-5}\right]$ temos,

$$41 = \left(6 + \sqrt{-5}\right)\left(6 - \sqrt{-5}\right),$$

os elementos $6 + \sqrt{-5}$ e $6 - \sqrt{-5}$ não são unidades em $\mathbb{Z}\left[\sqrt{-5}\right]$, pois pela Proposição 2.10, uma unidade possui norma ± 1 e no entanto $N(6 + \sqrt{-5}) = N(6 - \sqrt{-5}) = 41$.

Fato semelhante pode ocorrer com ideais de $\mathbb{A}$ que estendidos (Definição 2.15 a seguir) a $\mathbb{B} \supset \mathbb{A}$ mudam suas características. Por exemplo, o ideal $2\mathbb{Z}$ é primo em $\mathbb{Z}$ mas sua extensão em $\mathbb{Z}\left[\sqrt{-5}\right]$ é o quadrado do ideal gerado por 2 e $1+\sqrt{-5}$, ou seja, não é um ideal primo. Podemos ver também que o ideal $3\mathbb{Z}$ é primo em $\mathbb{Z}$ mas sua extensão $3\mathbb{Z}\left[\sqrt{-5}\right]$ em $\mathbb{Z}\left[\sqrt{-5}\right]$ é o produto do ideal gerado por 3 e $1+\sqrt{-5}$ pelo ideal gerado por 3 e $1-\sqrt{-5}$, ou seja, $3\mathbb{Z}\left[\sqrt{-5}\right]$ não é um ideal primo em $\mathbb{Z}\left[\sqrt{-5}\right]$. De maneira simbólica podemos escrever

$$(2) = \left(2, 1+\sqrt{-5}\right)^2$$

e

$$(3) = \left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right).$$

Obs. 2.2 *Às vezes, diremos apenas que, p se decompõe em um produto de primos no anel de inteiros $\mathbb{A}$, ao invés de, o ideal (p) se decompõe em um produto de ideais primos no anel de inteiros $\mathbb{A}$*

Nosso objetivo, agora, é determinar a decomposição de ideais primos em um anel de números $\mathbb{A}$.

Definição 2.15 *Sejam $B \supset A$, anéis, e $\mathfrak{a} \subset A$ um ideal; o conjunto*

$$\left\{\sum_{i=1}^{n} a_i b_i \ ; \ a_i \in \mathfrak{a}, \ b_i \in B\right\}$$

é um ideal de B que será denotado por $\mathfrak{a}B$ e dito a extensão de $\mathfrak{a}$ em B.

Sejam $L \supset K$ uma extensão de corpos de números, $\mathbb{B} \supset \mathbb{A}$ seus respectivos anéis de inteiros e seja $\mathfrak{p}$ um ideal primo de $\mathbb{A}$. Vamos determinar a decomposição da extensão de $\mathfrak{p}$ em $\mathbb{B}$.

Teorema 2.8 *Sejam $\mathfrak{p}$ um ideal primo de $\mathbb{A}$ e $\mathfrak{q}$ um ideal primo de $\mathbb{B}$. Então as condições seguintes são equivalentes:*

i) $\mathfrak{q} \supset \mathfrak{p}$

ii) $\mathfrak{q} \cap \mathbb{A} = \mathfrak{p}$

iii) $\mathfrak{q} \cap K = \mathfrak{p}$

iv) $\mathfrak{q} \supset \mathfrak{p}\mathbb{B}$

No decorrer deste trabalho usaremos, de modo mais constante, as condições *i)* e *ii)* do Teorema 2.8. Vamos então, demonstrar a equivalência entre elas.

Demonstração: Vamos mostrar que *i)* $\Rightarrow$ *ii)*. É claro que $\mathfrak{p} \subset \mathfrak{q} \cap \mathbb{A}$. Também é fácil de ver que $\mathfrak{q} \cap \mathbb{A}$ é um ideal de $\mathbb{A}$. Como $\mathfrak{p}$ é maximal, então $\mathfrak{q} \cap \mathbb{A} = \mathfrak{p}$ ou $\mathbb{A}$. Se $\mathfrak{q} \cap \mathbb{A} = \mathbb{A}$, então $1 \in \mathfrak{q}$ e daí $\mathfrak{q} = \mathbb{B}$, absurdo. Portanto, $\mathfrak{q} \cap \mathbb{A} = \mathfrak{p}$. A implicação *ii)* $\Rightarrow$ *i)* é trivial. ■

Definição 2.16 *Quando vale uma das, e portanto todas, condições do Teorema 2.8, dizemos que o primo* $\mathfrak{q}$ *está* acima (ou sobre) *de* $\mathfrak{p}$, *ou que* $\mathfrak{p}$ *está* abaixo (*ou* sob) $\mathfrak{q}$.

Teorema 2.9 *Todo ideal primo* $\mathfrak{q}$ *de* $\mathbb{B}$ *está acima de um único ideal primo* $\mathfrak{p}$ *de* $\mathbb{A}$. *Todo ideal primo* $\mathfrak{p}$ *de* $\mathbb{A}$ *está abaixo de pelo menos um ideal primo* $\mathfrak{q}$ *de* $\mathbb{B}$.

Os ideais primos $\mathfrak{q}_i$, que estão sobre $\mathfrak{p}$, são aqueles que ocorrem na decomposição prima de $\mathfrak{p}\mathbb{B}$. Portanto,

$$\mathfrak{p}\mathbb{B} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}.$$

Os expoentes e_i são chamados de *índices de ramificação* de $\mathfrak{q}_i$ sobre $\mathfrak{p}$, denotado por $e_i\left(\mathfrak{q}_i \mid \mathfrak{p}\right)$.

Definição 2.17 *Dizemos que* $\mathfrak{p}$ *se ramifica em* $\mathbb{B}$, *se pelo menos um dos* $e_i \geq 2$. *Se* $\mathfrak{p}\mathbb{B} = \mathfrak{q}$, *dizemos que* $\mathfrak{p}$ *é inerte em* $\mathbb{B}$.

Sabemos que os anéis quocientes $\mathbb{A}/\mathfrak{p}$ e $\mathbb{B}/\mathfrak{q}$ são corpos, pois $\mathfrak{p}$ e $\mathfrak{q}$ são maximais. Como $\mathbb{A} \subset \mathbb{B}$, podemos ver que $\mathbb{B}/\mathfrak{q}$ é uma extensão de $\mathbb{A}/\mathfrak{p}$. Estes corpos são chamados de *corpos residuais* associados a $\mathfrak{p}$ e $\mathfrak{q}$. Sabemos, pela Proposição 2.11, que estes quocientes são finitos, portanto $\mathbb{B}/\mathfrak{q}$ é um espaço vetorial de dimensão finita sobre $\mathbb{A}/\mathfrak{p}$. Seja f esta dimensão, logo $f = [\mathbb{B}/\mathfrak{q} : \mathbb{A}/\mathfrak{p}]$. Dizemos que f é o *grau de inércia* de $\mathfrak{q}$ sobre $\mathfrak{p}$, denotado por $f = f\left(\mathfrak{q}/\mathfrak{p}\right)$.

Teorema 2.10 *(Igualdade Fundamental) Seja n o grau de $\mathbb{B}$ sobre $\mathbb{A}$. Dado um primo $\mathfrak{p}$ de $\mathbb{A}$, sejam $\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_g$ os ideais primos distintos de $\mathbb{B}$ que estão sobre $\mathfrak{p}$. Sejam $e_1, e_2, \cdots, e_g$ e $f_1, f_2, \cdots, f_g$ os índices de ramificação e os graus de inércia correspondentes. Então:*

$$\sum_{i=1}^{g} e_i f_i = n.$$

Iremos demonstrar o Teorema 2.10 para o caso de $K = \mathbb{Q}$. Para tanto, necessitamos do conceito de *norma de um ideal.* O ideal nulo terá norma *zero.* Se $\mathfrak{a}$ é um ideal não nulo de $\mathbb{A}$, então a norma de $\mathfrak{a}$, que será denotada por $N_A(\mathfrak{a})$, é o número finito $\#(A/\mathfrak{a})$.

Obs. 2.3 *Quando não houver dúvida quanto ao anel A, que contém o ideal $\mathfrak{a}$, usaremos $N(\mathfrak{a})$ ao invés de $N_A(\mathfrak{a})$.*

Proposição 2.12 *Sejam $L \supset K$ corpos de números, $\mathbb{B} \supset \mathbb{A}$ seus anéis de números, respectivamente e $n = [L : K]$.*
i) Sejam $\mathfrak{a}$ e $\mathfrak{b}$ ideais de $\mathbb{A}$, então

$$N(\mathfrak{ab}) = N(\mathfrak{a})\, N(\mathfrak{b}),$$

ii) Seja $\mathfrak{a}$ um ideal de $\mathbb{A}$, para o ideal $\mathfrak{a}\mathbb{B}$ temos:

$$N_{\mathbb{B}}(\mathfrak{a}\mathbb{B}) = N_{\mathbb{A}}(\mathfrak{a})^n,$$

iii) Seja $\alpha \in \mathbb{A}$, $\alpha \neq 0$, para o ideal principal (α) temos:

$$N_{\mathbb{A}}((\alpha)) = \left| N_{\mathbb{Q}}^{K}(\alpha) \right|,$$

isto é, o valor absoluto da norma de α, na extensão $K \supset \mathbb{Q}$.

Demonstração: (Do Teorema 2.10, no caso de $K = \mathbb{Q}$.) Como $K = \mathbb{Q}$ temos $\mathbb{A} = \mathbb{Z}$. Seja $\mathfrak{p}$ um ideal primo de $\mathbb{Z}$, logo $\mathfrak{p} = p\mathbb{Z}$, para algum primo $p \in \mathbb{Z}$. Então temos:

$$\mathfrak{p}\mathbb{B} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i},$$

logo,

$$N_{\mathbb{B}}(\mathfrak{p}) = \prod_{i=1}^{g} (N(\mathfrak{q}_i)^{e_i} = \prod_{i=1}^{g} \left|p^{f_i}\right|^{e_i} = p^{\sum_{i=1}^{g} e_i f_i}.$$

Por outro lado, sabemos que

$$N_{\mathbb{B}}(\mathfrak{p}) = (N_{\mathbb{A}}(\mathfrak{p}))^n = p^n,$$

portanto,

$$\sum_{i=1}^{g} e_i f_i = n.$$

■

2.5.2 Decomposição de um ideal primo em corpos quadráticos

Sejam d um inteiro livre de quadrados, $K = \mathbb{Q}\left(\sqrt{d}\right)$ e $\mathbb{A}$ o anel de inteiros de K. Seja p um número primo. Vamos determinar a decomposição do ideal gerado por p em $\mathbb{A}$, que denotaremos por $p\mathbb{A}$.

Do Teorema 2.10 temos que $\mathfrak{p}\mathbb{B} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$, com $\sum_{i=1}^{g} e_i f_i = 2$, logo $g \leq 2$. Desse modo, temos três possíveis casos a considerar. São eles:

i) $g = 2, \quad e_1 = e_2 = 1, \quad f_1 = f_2 = 1$; dizemos, neste caso, que p se *decompõe* em K, isto é, $p\mathbb{A} = \mathfrak{p}_1\mathfrak{p}_2$, onde $\mathfrak{p}_1$ e $\mathfrak{p}_2$ são ideais primos de $\mathbb{A}$ acima de $p\mathbb{Z}$ e $\#(\mathbb{A}/\mathfrak{p}_i) = p_i$, $i = 1, 2$;

ii) $g = 1, \quad e_1 = 1, \quad f_1 = 2$; dizemos, neste caso, que p é *inerte* em K, isto é $p\mathbb{A} = \mathfrak{p}$, onde $\mathfrak{p}$ é um ideal primo de $\mathbb{A}$ acima de $p\mathbb{Z}$. Aqui $\mathbb{A}/\mathfrak{p}$ tem p^2 elementos;

iii) $g = 1, \quad e_1 = 1, \quad f_1 = 1$; dizemos, neste caso, que p se ramifica em K, isto é $p\mathbb{A} = \mathfrak{p}^2$, onde $\mathfrak{p}$ é um ideal primo de $\mathbb{A}$ acima de $p\mathbb{Z}$, e além disso $N(\mathfrak{p}) = p$.

Definição 2.18 *Dados um número primo ímpar p e um inteiro d, primo com p, dizemos que d é um* resíduo quadrático $\bmod p$ *se a classe de d módulo p for um quadrado em $\mathbb{Z}/p\mathbb{Z}$, ou seja, a equação $x^2 = d$ tem solução módulo p.*

Exemplo 2.2 *Quando $p = 5$ então -1 é um resíduo quadrático* $\bmod 5$, *enquanto que -1 não é resíduo quadrático* $\bmod 7$.

Teorema 2.11 *Seja $K = \mathbb{Q}\left(\sqrt{d}\right)$, onde d um inteiro livre de quadrados. Temos:*
i) São decompostos *em K os números primos ímpares p tais que d é um resíduo quadrático* $\bmod p$, *e $p = 2$ se $d \equiv 1 (\bmod 8)$,*
ii) São inertes *em K os primos ímpares p tais que d não é um resíduo quadrático* $\bmod p$,
iii) Se ramificam *em K os divisores primos ímpares de d, e o primo 2 se $d \equiv 2$ ou $3 (\bmod 4)$.*

Para aplicarmos o Teorema 2.11 é necessário saber quando um dado número é um quadrado $\bmod p$. Isto pode ser feito, de um modo relativamente simples, usando-se a *Lei da Reciprocidade Quadrática de Gauss.* Para tanto, vamos introduzir o símbolo de Legendre $\left(\frac{d}{p}\right)$.

Definição 2.19 *Sejam p um inteiro primo e d um inteiro primo com p. Definimos o símbolo de Legendre $\left(\frac{d}{p}\right)$ por,*

$$\begin{cases} \left(\frac{d}{p}\right) = 1, \text{se } d \text{ é um resíduo quadrático } (\bmod p) \\ \\ \left(\frac{d}{p}\right) = -1, \text{se } d \text{ não é um resíduo quadrático } (\bmod p) \end{cases}.$$

Proposição 2.13 *Sejam $a, b \in \mathbb{Z}$, primos com p. Então vale:*
i)

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right);$$

ii) (Critério de Euler) Se p é um primo ímpar, então

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\bmod p),$$

em particular,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}};$$

iii) Se p é um primo ímpar, então

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Teorema 2.12 *(Lei da Reciprocidade Quadrática de Gauss). Se p e q são números primos ímpares distintos, então:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Vamos agora reescrever o Teorema 2.11 fazendo uso do símbolo de Legendre $\left(\frac{m}{p}\right)$.

Teorema 2.13 *Seja $K = \mathbb{Q}\left(\sqrt{d}\right)$, onde d um inteiro livre de quadrados.*

a) Seja p um primo ímpar.

i) Se $p \mid d$, então $p\mathbb{A} = \left(p, \sqrt{d}\right)^2$, isto é, p se ramifica em K;

ii) Se $\left(\frac{d}{p}\right) = -1$, então $p\mathbb{A}$ é um ideal primo em K, isto é, p é inerte em K;

iii) Se $\left(\frac{d}{p}\right) = 1$, então $p\mathbb{A} = \left(p, \sqrt{d} - a\right)\left(p, \sqrt{d} + a\right)$, $a \in \mathbb{Z}$, $a^2 \equiv d (\mathrm{mod}\, p)$, isto é, p se decompõe em K.

b) Seja agora $p = 2$.

i) Se $d \equiv 2 \,(\mathrm{mod}\, 4)$, então $2\mathbb{A} = \left(2, \sqrt{d}\right)^2$, e se $d \equiv 3 \,(\mathrm{mod}\, 4)$, então $2\mathbb{A} = \left(2, \sqrt{d} - 1\right)^2$; em ambos os casos, 2 se ramifica;

ii) Se $d \equiv 1 \,(\mathrm{mod}\, 8)$, então $2\mathbb{A} = \left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right)$, isto é, 2 se decompõe em K;

iii) Se $d \equiv 5 \,(\mathrm{mod}\, 8)$, então $2\mathbb{A}$ é um ideal primo em K, isto é, 2 é inerte em K.

Exemplo 2.3 $K = \mathbb{Q}\left(\sqrt{-1}\right)$.

i) p se ramifica se, e somente se, $p = 2$,

ii) p é inerte se, e somente se, $p \equiv -1 \,(\mathrm{mod}\, 4)$,

iii) p se decompõe se, e somente se, $p \equiv 1 \,(\mathrm{mod}\, 4)$. Portanto os primos $p = 5, 13, 17, 29, 37, \cdots$ se decompõem em $K = \mathbb{Q}\left(\sqrt{-1}\right)$.

Exemplo 2.4 $K = \mathbb{Q}\left(\sqrt{-3}\right)$.

i) p *se ramifica se, e somente se* $p = 3$;

ii) p *é inerte se, e somente se* $p \equiv -1 \pmod 3$;

iii) p *se decompõe se, e somente se* $p \equiv 1 \pmod 3$. *Portanto, os primos* $p = 7, 13, 19, 31, 37, \cdots$ *se decompõem em* $K = \mathbb{Q}\left(\sqrt{-3}\right)$.

A seguir, veremos um Teorema que relaciona a decomposição de ideais primos às soluções da forma quadrática $N(\alpha)$, $\alpha \in \mathbb{A}$. Como vimos na Proposição 2.9, se $K = \mathbb{Q}\left[\sqrt{d}\right]$, então $N\left(a + b\sqrt{d}\right) = a^2 - db^2$.

Teorema 2.14 *Sejam* K *um corpo quadrático,* $\mathbb{A}$ *seu anel de inteiros algébricos e* N *a norma relativa de* K *em* $\mathbb{Q}$. *Seja* $n = \prod_{i=1}^{s} p_i^{a_i}$, $a_i \in \mathbb{N}$, p_i *primos,* $i = 1, 2, \cdots, s$.

i) Se existe $\alpha \in \mathbb{A}$, *tal que* $N(\alpha) = p_i^n$, *então* a_i *é par quando* p_i *é inerte;*

ii) Se $\mathbb{A}$ *é um domínio de ideais principais, e* a_i *é par quando* p_i *é inerte, então existe* $\alpha \in \mathbb{A}$ *tal que* $N(\alpha) = n$.

Demonstração: Seja $\alpha \in \mathbb{A}$, então $(\alpha) = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_s^{a_s}$, onde $\mathfrak{p}_i$ são os ideais primos de $\mathbb{A}$, acima dos primos p_i de $\mathbb{Z}$.

Seja σ a conjugação de K. De $N(\alpha) = \alpha\sigma(\alpha)$, temos

$$\begin{aligned}(N(\alpha)) &= (\alpha)\cdot(\sigma(\alpha)) = (\mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_s^{a_s})\cdot(\sigma(\mathfrak{p}_1)^{a_1}\sigma(\mathfrak{p}_2)^{a_2}\cdots\sigma(\mathfrak{p}_s)^{as}) = \\ &= (\mathfrak{p}_1\cdot\sigma(\mathfrak{p}_1))^{a_1}\cdot(\mathfrak{p}_2\cdot\sigma(\mathfrak{p}_2))^{a_2}\cdots(\mathfrak{p}_s\cdot\sigma(\mathfrak{p}_s))^{a_s}.\end{aligned}$$

Se p_i é inerte, então $\mathfrak{p}_i = \sigma(\mathfrak{p}_i)$ e $p_i\mathbb{A} = \mathfrak{p}_i$, onde $p_i = \mathfrak{p}_i \cap \mathbb{Z}$.

Se p_i se decompõe, então $p_i\mathbb{A} = \mathfrak{p}_i\cdot\sigma(\mathfrak{p}_i)$, $\sigma(\mathfrak{p}_i) = \overline{\mathfrak{p}}_i$.

Se p_i se ramifica, então $p_i\mathbb{A} = \mathfrak{p}_i^2$

Visto que numa extensão quadrática todo primo se ramifica, é inerte ou se decompõe, temos

$$(N(\alpha)) = \prod_{p_i \text{ é inerte}} (\mathfrak{p}_i\cdot\sigma(\mathfrak{p}_i))^{a_i} \prod_{p_i \text{ se decompõe}} (\mathfrak{p}_i\cdot\sigma(\mathfrak{p}_i))^{a_i} \prod_{p_i \text{ se ramifica}} (\mathfrak{p}_i\cdot\sigma(\mathfrak{p}_i))^{a_i} =$$

$$= \prod_{p_i \text{ é inerte}} p_i^{2a_i} \prod_{p_i \text{ se decompõe}} p_i^{a_i} \prod_{p_i \text{ se ramifica}} p_i^{a_i}.$$

Portanto, o expoente do ideal primo que é inerte é sempre par.

Reciprocamente, seja n um número inteiro, cuja fatoração em números primos seja:

$$\begin{aligned} n &= \prod_{\mathfrak{p}_i \text{ é inerte}} p_i^{2a_i} \prod_{\mathfrak{p}_i \text{ se decompõe}} p_i^{a_i} \prod_{\mathfrak{p}_i \text{ se ramifica}} p_i^{a_i} = \\ &= \prod_{\mathfrak{p}_i \text{ é inerte}} N(\mathfrak{p}_i)^{a_i} \prod_{\mathfrak{p}_i \text{ se decompõe}} N(\mathfrak{p}_i)^{a_i} \prod_{\mathfrak{p}_i \text{ se ramifica}} N(\mathfrak{p}_i)^{a_i} = \\ &= N\left(\prod_{i=1}^{s} \mathfrak{p}_i^{a_i}\right), \quad a_i \in \mathbb{N}. \end{aligned}$$

Portanto, n é a norma de um ideal. Como $\mathbb{A}$ é um DIP o ideal $\prod_{i=1}^{s} \mathfrak{p}_i^{a_i}$ é principal, que suponhamos gerado por $\alpha \in \mathbb{A}$, logo

$$n = N\left(\prod_{i=1}^{s} \mathfrak{p}_i^{a_i}\right) = N((\alpha)) = N(\alpha).$$

■

Conforme vimos na Seção 2.2, a norma de um elemento $\alpha = x + \omega y$ do anel dos inteiros algébricos de $K = \mathbb{Q}\left(\sqrt{d}\right)$ é dada por $N(\alpha) = x^2 - dy^2$. Portanto:

1. Se $d = -1$, então $N(\alpha) = x^2 + y^2$, pois $\alpha = x + \sqrt{-1}\, y$.
2. Se $d = -3$, então $N(\alpha) = x^2 + xy + y^2$, pois $\alpha = x + (\frac{1+\sqrt{-3}}{2})\, y = (x + \frac{y}{2}) + \frac{\sqrt{-3}}{2} y$.

No Capítulo 3, as soluções destas formas quadráticas serão fundamentais para se determinar o rótulo de um elemento pertencente a um conjunto de sinais, através do corpo $GF(p)$. Veremos, a seguir, um exemplo que será usado de maneira intensa naquele capítulo.

Exemplo 2.5 *Seja* $\mathbb{A} = \mathbb{Z}[\omega]$, $\omega = \sqrt{-1}$ *ou* $\omega = \frac{1+\sqrt{-3}}{2}$, *o anel dos inteiros algébricos de* $K = \mathbb{Q}\left(\sqrt{d}\right)$, $d = -1$ *ou* $d = -3$, *respectivamente. Pelo Teorema* 2.57, *combinado com os*

Exemplos 2.55 *e* 2.56, *os valores assumidos pela função norma são:*

i) Se $d = -1$, *então* $N(\alpha) = 2^{a_2}3^{2a_3}5^{a_5}7^{2a_7}11^{2a_{11}}13^{a_{13}}\cdots$, *além do valor nulo.*

Portanto, neste caso, $N(\alpha)$ *assume os valores* $0, 1, 2, 4, 5, 8, 9, 10, \cdots$.

ii) Se $d = -3$, *então* $N(\alpha) = 2^{2a_2}3^{a_3}5^{2a_5}7^{a_7}11^{2a_{11}}\cdots$, *além do valor nulo.*

Portanto, neste caso, $N(\alpha)$ *assume os valores* $0, 1, 3, 4, 7, 9, \cdots$.

2.6 Códigos Lineares

Nesta seção faremos uma breve revisão a respeito de conceitos básicos da teoria de códigos de bloco lineares. Tais conceitos incluem: descrição de um código de bloco $\mathcal{C}$ em termos das matrizes geradora e verificação de paridade; distância mínima de Hamming entre palavras código e algoritmos de decodificação. Serão revistas também as duas principais classes de códigos lineares, isto é, códigos cíclicos e códigos BCH. Essas classes serão descritas algebricamente em termos de polinômios e das relações que possuem com a teoria de anéis, apresentada na Seção 2.2.

Nesta seção denotaremos por K o corpo de Galois com q elementos $GF(q)$.

Definição 2.20 *Um* código linear $\mathcal{C}$ *de comprimento* n *e dimensão* k *sobre um corpo finito* K *com* q *elementos é um subespaço vetorial de dimensão* k *do espaço vetorial* K^n.

Aos vetores de $\mathcal{C}$ dá-se o nome de *palavras código*, ou simplesmente *palavras*. Portanto, $\mathcal{C}$ possui q^k palavras. Dizemos, nestas condições, que $\mathcal{C}$ é um (n, k) código linear sobre K.

Como $\mathcal{C}$ é um subespaço vetorial de K^n de dimensão k, então existem k vetores em $\mathcal{C}$, $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$, linearmente independentes, e que geram $\mathcal{C}$. Seja, agora, G a matriz $k \times n$, cujas linhas são os vetores $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$. Tal matriz G é denominada a *matriz geradora* do código linear $\mathcal{C}$. Note que $\mathcal{C}$ é na verdade o espaço linha de G.

Consideremos em K^n o *produto interno* definido por:

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1v_1 + u_2v_2 + \cdots + u_nv_n,$$

onde $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ e $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ são elementos de K^n.

Seja $\mathcal{C} \subset K^n$ um código linear de dimensão k. Consideremos o conjunto

$$\mathcal{C}^{\perp} = \{\mathbf{v} \in K^n : \langle \mathbf{u}, \mathbf{v} \rangle = 0, \ \forall \ \mathbf{u} \in K^n\}.$$

Sabemos da álgebra linear que $\mathcal{C}^{\perp}$ é um subespaço de K^n de dimensão $n - k$, chamado de *espaço ortogonal de* $\mathcal{C}$. Portanto, $\mathcal{C}^{\perp}$ é também um código linear, que é chamado *código dual de* $\mathcal{C}$.

Definição 2.21 *Dado um código linear* $\mathcal{C}$, *a matriz* H *geradora de* $\mathcal{C}^{\perp}$ *é chamada de* matriz verificação de paridade de $\mathcal{C}$.

Além do comprimento n e da dimensão k de um código linear $\mathcal{C}$, temos um outro parâmetro importante, que é a *distância mínima de Hamming* entre as palavras de $\mathcal{C}$, cuja definição veremos a seguir.

Definição 2.22 *A* distância de Hamming $d_H(\mathbf{x}, \mathbf{y})$ *entre dois vetores* $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ *e* $\mathbf{y} = (y_1, y_2, \cdots, y_n)$ *de* K^n *é o número de posições onde eles diferem.*

Definição 2.23 *A* distância mínima de Hamming, d, *de um código* $\mathcal{C}$ *é dada por*

$$d = \min\{d_H(\mathbf{x}, \mathbf{y}), \quad \mathbf{x}, \mathbf{y} \in \mathcal{C}, \quad \mathbf{x} \neq \mathbf{y}\}.$$

Um código linear de comprimento n, dimensão k e distância mínima d será chamado um (n, k, d) código linear.

Definição 2.24 *O* peso de Hamming $w_H(\mathbf{x})$ *de um vetor* $\mathbf{x} = (x_1, x_2, \cdots, x_n) \in K^n$ *é dado por*

$$w_H(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0}),$$

onde $\mathbf{0}$ *é o vetor todo nulo.*

Como consequência, temos que

$$d_H(\mathbf{x}, \mathbf{y}) = d_H(\mathbf{x} - \mathbf{y}, \mathbf{0}) = w_H(\mathbf{x} - \mathbf{y}).$$

Agora, sejam $\mathcal{C}$ um código linear, e $\mathbf{x}, \mathbf{y} \in \mathcal{C}$. Então $\mathbf{x} - \mathbf{y} \in \mathcal{C}$, e portanto, o teorema a seguir é válido.

Teorema 2.15 *Em um código linear $\mathcal{C}$ a distância mínima de Hamming é igual ao peso mínimo de Hamming de suas palavras código, isto é,*

$$d = \min_{\mathbf{x} \neq \mathbf{0}} \{w_H(\mathbf{x}),\ \mathbf{x} \in \mathcal{C}\}.$$

Suponhamos que seja transmitida uma palavra código $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ através de um canal ruidoso. Devido ao ruído introduzido pelo canal, o vetor recebido $\mathbf{r} = (r_1, r_2, \cdots, r_n)$ pode ser diferente de $\mathbf{v}$. Define-se então o *vetor erro* por

$$\mathbf{e} = \mathbf{r} - \mathbf{v} = (e_1, e_2, \cdots, e_n).$$

Dizemos que um código $\mathcal{C}$ detecta erros quando ele é capaz de decidir se o vetor recebido é ou não uma palavra código. Se, além de detectar erros, ele ainda é capaz de determinar a palavra transmitida, então dizemos que $\mathcal{C}$ corrige erros.

Teorema 2.16 *Seja $\mathcal{C}$ um código com distância mínima d. Se $\mathcal{C}$ for usado somente para detecção, então $\mathcal{C}$ é capaz de detectar a presença de erros se ocorrerem até $d-1$ erros. Se $\mathcal{C}$ for usado somente para correção, ele é capaz de corrigir até $\left\lfloor \frac{d-1}{2} \right\rfloor$ erros, onde $\lfloor m \rfloor$ denota o maior inteiro menor ou igual ao número m.*

Teorema 2.17 *Um código $\mathcal{C}$, com distância mínima d, é capaz de detectar até λ erros e corrigir até t erros, simultaneamente, se $\lambda + t + 1 \leq d$ e $t \leq \lambda$.*

Dados um código $\mathcal{C}$, com matriz verificação de paridade H, e um vetor $\mathbf{v} \in K^n$, chamamos o vetor $\mathbf{s} = H\mathbf{v}^t$ de *síndrome* de $\mathbf{v}$.

Quando $\mathbf{v}$ é uma palavra de $\mathcal{C}$, temos $H\mathbf{v}^t = \mathbf{0}$. Logo,

$$HG^t = \mathbf{0}.$$

Portanto, a síndrome $\mathbf{s} = H\mathbf{r}^t = \mathbf{0}$ se, e somente se, $\mathbf{r}$ é uma palavra código.

Seja $\mathbf{v} \in \mathcal{C}$ a palavra transmitida, $\mathbf{e}$ o padrão de erro introduzido pelo canal, e $\mathbf{r}$ a palavra recebida. Logo, a síndrome de $\mathbf{r}$ é:

$$\mathbf{s} = H\mathbf{r}^t = H\left(\mathbf{v} + \mathbf{e}\right)^t = H\mathbf{v}^t + H\mathbf{e}^t = H\mathbf{e}^t,$$

isto é, a síndrome de $\mathbf{r}$ é igual à síndrome de $\mathbf{e}$.

Assim, a síndrome do vetor recebido pode ser útil na detecção de erros, no seguinte sentido. Se $\mathbf{s} \neq \mathbf{0}$, então certamente o canal introduziu um padrão de erro. Agora, se o canal não introduziu erros, isto é, $\mathbf{e} = \mathbf{0}$, ou se o padrão de erro é uma palavra código, então $\mathbf{s} = \mathbf{0}$.

Entretanto, sempre que a síndrome do vetor recebido $\mathbf{r}$ for nula, assumiremos que não ocorreram erros.

Veremos, agora, um teorema bastante útil na determinação da distância mínima de Hamming de um código $\mathcal{C}$.

Teorema 2.18 *Seja H a matriz verificação de paridade de um código $\mathcal{C}$. Tem-se que o peso de $\mathcal{C}$ é d se, e somente se, quaisquer $d-1$ colunas de H são linearmente independentes, $(l.i.)$, e existem d colunas de H que são linearmente dependentes, $(l.d.)$.*

Corolário 2.5 *(Cota de Singleton) Os parâmetros (n, k, d) de um código linear $\mathcal{C}$ satisfazem a desigualdade*

$$d \leq n - k + 1.$$

Definição 2.25 *Códigos com $d = n-k+1$ são chamados de códigos com* máxima distância de separação, *ou códigos MDS (maximum distance separable).*

Isto significa que a distância mínima de Hamming de um código MDS é a maior possível.

Teorema 2.19 *Um código $\mathcal{C}$, com matriz verificação de paridade H, é MDS se, e somente se, quaisquer $n-k$ colunas de H são linearmente independentes.*

2.6.1 Princípios de decodificação

Seja o sistema de comunicações digitais como mostrado na Figura 2-1.

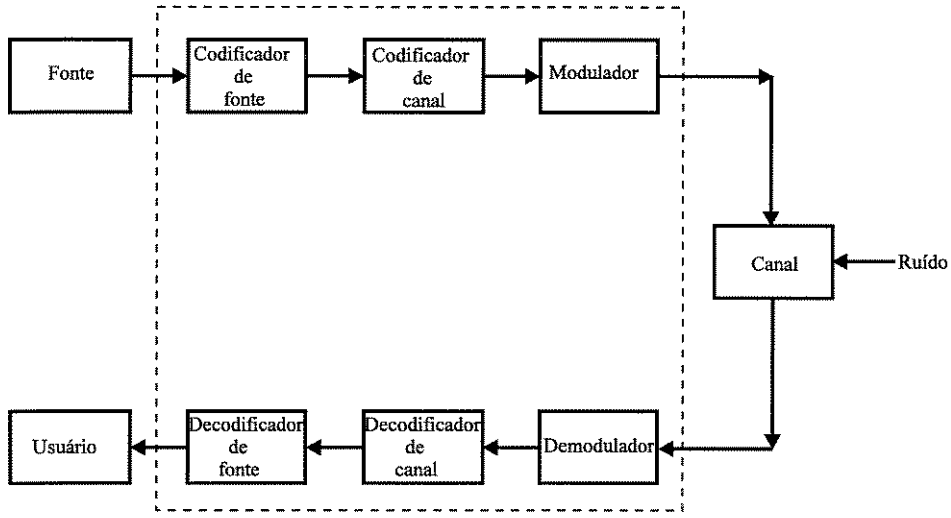

Figura 2-1: Sistema de Comunicações Digitais

Vamos supor que a palavra código a ser enviada através do canal seja $\mathbf{v}$. Suponhamos também que o canal introduza um padrão de erro $\mathbf{e}$. Assim, a palavra recebida será

$$\mathbf{r} = \mathbf{v} + \mathbf{e}.$$

O decodificador deve decidir a partir de $\mathbf{r}$ qual foi a palavra transmitida. Devido à natureza aleatória do ruído, o decodificador não é capaz de determinar com certeza absoluta qual foi o erro que realmente ocorreu. Diante disto, ele escolherá o vetor erro que tenha ocorrido com maior probabilidade, dado que $\mathbf{r}$ foi recebido. Supondo que todas as palavras sejam igualmente prováveis, esta estratégia é ótima no sentido de que ela minimiza a probabilidade de erro de palavra, e é conhecida como *decodificação de máxima verossimilhança.*

Diz-se que não ocorreram erros durante a transmissão, em uma determinada palavra código, quando o vetor erro for todo nulo.

Seja, agora, X uma variável aleatória que representa o número de erros ocorridos em uma transmissão, isto é, X é o número de componentes não nulas de $\mathbf{e}$. Em geral, se os erros forem independentes, tem-se que:

$$P(X=0) > P(X=1) > \cdots > P(X=n).$$

Portanto, a estratégia de decodificação de máxima verossimilhança é tomar o vetor erro de menor peso de Hamming, isto é, a palavra recebida será decodificada como a palavra código mais próxima, no espaço de Hamming. Em particular, este tipo de decodificação é conhecida por *decodificação pelo vizinho mais próximo.* Uma maneira de implementá-la é a seguinte: recebida uma palavra, compare-a com todas as palavras código e tome a mais próxima. Entretanto, em geral, o número de palavras código é muito grande e este método torna-se altamente complexo e impraticável. Ao estudarmos códigos sobre anéis de inteiros algébricos, no Capítulo 4, optaremos por métodos alternativos de decodificação.

2.6.2 Códigos cíclicos

Dentre os códigos lineares, a classe dos *códigos cíclicos* constitui a mais importante, não somente do ponto de vista prático (redução da complexidade de codificadores e decodificadores), como também do ponto de vista teórico, pelas suas estreitas relações com a teoria de anéis e ideais.

Definição 2.26 *Um código linear $\mathcal{C}$ é* cíclico *se todo deslocamento cíclico de uma palavra de $\mathcal{C}$ é ainda uma palavra de $\mathcal{C}$, isto é, se $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$, então $\mathbf{c}' = (c_{n-1}, c_0, \cdots, c_{n-2})$ também pertence a* C.

Para descrevermos os códigos cíclicos numa linguagem algébrica, associamos ao vetor código $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1}) \in K^n$ o polinômio $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, o qual é denominado o polinômio código associado a $\mathbf{c}$.

Dados um corpo finito K e n um inteiro positivo, (n representa o comprimento de $\mathcal{C}$), definimos A_n como sendo o anel quociente $K[x]/(x^n-1)$. Em outras palavras, A_n é o anel formado pelas classes residuais de $K[x]$ módulo x^n-1. Cada polinômio de grau menor ou igual a $n-1$ pertence a uma classe residual distinta, e consequentemente, podemos tomar este polinômio como representante de sua classe residual. Portanto, podemos dizer que $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ pertence a A_n.

Agora, multiplicando $c(x)$ por x em A_n, obtemos

$$\begin{aligned} xc(x) &= c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n \\ &= c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}, \end{aligned}$$

pois $x^n = 1$ em A_n. Mas este é o polinômio associado a $\mathbf{c}' = (c_{n-1}, c_0, \cdots, c_{n-2})$. Assim multiplicar $c(x)$ por x em A_n corresponde a fazer um deslocamento cíclico em $\mathbf{c}$.

Portanto, podemos reescrever a Definição 2.26.

Definição 2.27 *Um código cíclico de comprimento n é um ideal do anel A_n.*

Como K é um corpo, $K[x]$ e $K[x]/(x^n-1)$ são anéis de ideais principais. Portanto, cada ideal $\mathfrak{a}$ de $K[x]$ é gerado por uma expressão polinomial em x. Se escolhermos um gerador $g(x)$ mônico de grau mínimo, então $g(x)$ é único.

Podemos resumir estes fatos no seguinte teorema:

Teorema 2.20 *Seja $\mathcal{C}$ um código cíclico de comprimento n, isto é, um ideal não nulo de A_n. Então:*

a) Existe um único polinômio mônico $g(x)$ de grau mínimo em $\mathcal{C}$;

b) $\mathcal{C} = (g(x))$, isto é, $g(x)$ é um polinômio gerador *de $\mathcal{C}$;*

c) $g(x)$ é um divisor de x^n-1;

d) Qualquer $c(x) \in \mathcal{C}$ pode ser escrito de modo único como $c(x) = f(x)g(x)$ em $K[x]$, onde $f(x) \in K[x]$, $\partial(f) \leq n-r$, $r = \partial(g)$. A dimensão de $\mathcal{C}$ é $n-r$;

e) Se $g(x) = g_0 + g_1x + \cdots + g_rx^r$, então $\mathcal{C}$ é gerado (como um subespaço de K^n) pelas linhas

da matriz

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{r-1} & g_r & \cdots & 0 \\ & & & & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_r \end{pmatrix}.$$

Definição 2.28 *A matriz G, acima, é dita a matriz geradora do código cíclico $\mathcal{C}$.*

Seja $\mathcal{C}$ um código cíclico com polinômio gerador $g(x)$. Pelo item c) do Teorema 2.20, temos que $g(x)$ divide $x^n - 1$, isto é, existe $h(x) \in K[x]$ tal que $h(x)g(x) = x^n - 1$. Suponhamos $h(x) = \sum_{i=0}^{k} h_i x^i$.

Seja $c(x) \in \mathcal{C}$, onde $c(x) = \sum_{i=0}^{k} c_i x^i = f(x)g(x)$. Então,

$$c(x)h(x) = \sum_{i=0}^{k} c_i x^i \sum_{j=0}^{k} h_j x^j = f(x)g(x)h(x) = f(x)(x^n - 1) = 0 \text{ em } A_n. \tag{2.1}$$

O coeficiente de x^j no produto $c(x)h(x)$ é dado por $\sum_{i=1}^{n-1} c_i h_{j-i}$, $j = 0, 1, \cdots, n-1$. Logo, os coeficientes do produto $c(x)h(x)$ são todos nulos. Portanto, as equações em (2.1) são equações de verificação de paridade. Isto justifica a seguinte definição:

Definição 2.29 *O polinômio $h(x)$ diz-se o* polinômio verificação de paridade *de $\mathcal{C}$.*

Seja

$$H = \begin{pmatrix} 0 & \cdots & \cdots & h_k & \cdots & h_2 & h_1 & h_0 \\ 0 & \cdots & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 \\ & & & & & & & \\ h_k & \cdots & \cdots & h_1 & h_0 & 0 & \cdots & 0 \end{pmatrix}.$$

Portanto, as equações (2.1) mostram que $H\mathbf{c}^t = 0$.

Definição 2.30 *A matriz H diz-se a matriz de verificação de paridade do código $\mathcal{C}$.*

2.6.3 Códigos BCH

Dentre os códigos cíclicos, existe uma classe de códigos de muito interesse prático, devido a facilidade de implementação de algoritmos de decodificação. Estes códigos são chamados códigos *BCH,* em homenagem a seus descobridores R.C. Bose e D.K. Ray-Chaudhuri (1960) e, independentemente, por A. Hocquenghem (1959).

Definição 2.31 *Um código cíclico C de comprimento n sobre $K = GF(q)$ é dito um código BCH com* distância projetada δ, *se seu polinômio gerador $g(x)$ é o mínimo múltiplo comum dos polinômios minimais de β^l, β^{l+1}, $\cdots$,$\beta^{l+\delta-2}$, para algum $l \in \mathbb{N}$, onde β é uma raiz primitiva $n-$ésima da unidade,isto é,*

$$g(x) = mmc\{m^l(x),\ m^{l+1}(x),\ \cdots,m^{l+\delta-2}(x)\},$$

onde $m^{l+j}(x)$ é o polinômio minimal de β^{l+j} sobre K, $j = 0, 1, \cdots, \delta-2$, ou seja ,$g(x)$ é o polinômio mônico de menor grau sobre K que possui β^l, β^{l+1}, $\cdots$,$\beta^{l+\delta-2}$ como raízes.

Obs. 2.4 *a) Normalmente usa-se $l = 1$, e neste caso temos os chamados códigos BCH no sentido estrito,* (narrow-sense)*.*
b) Se $n = q^m - 1$, isto é, β é um elemento primitivo de $GF(q^m)$, então C é dito um código BCH primitivo.

Como consequência da Definição 2.31, $c(x)$ é um polinômio código de C se, e somente se,

$$c\left(\beta^l\right) = c\left(\beta^{l+1}\right) = \cdots = c\left(\beta^{l+\delta-2}\right) = 0. \tag{2.2}$$

Logo, o código C possui uma seqüência de $\delta - 1$ potências consecutivas de β como raízes.

A Equação 2.2 mostra que a matriz verificação de paridade de $\mathcal{C}$ é dada por

$$H = \begin{pmatrix} 1 & \beta^{l} & \beta^{2l} & \cdots & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \cdots & \beta^{(n-1)(l+1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^{l+\delta-2} & \beta^{2(l+\delta-2)} & \cdots & \beta^{(n-1)(l+\delta-2)} \end{pmatrix}.$$

Um exemplo de códigos BCH são os códigos Reed-Solomon.

Definição 2.32 *Um código Reed-Solomon, (ou um código RS), é um código BCH primitivo de comprimento $n = q - 1$ sobre $GF(q)$. O polinômio gerador deste código é da forma,*

$$g(x) = (x - \alpha)\left(x - \alpha^{2}\right) \cdots \left(x - \alpha^{d-1}\right),$$

onde α é um elemento primitivo de $GF(q)$.

2.7 Conclusão

Neste Capítulo revimos, principalmente, os conceitos básicos da teoria de anéis, ideais, corpos, extensões de corpos, corpos e anéis de números algébricos, decomposição de ideais primos em anéis de números. Também fizemos uma breve revisão dos conceitos básicos envolvendo códigos lineares, cíclicos e BCH.

Capítulo 3

Conjunto de Sinais Casado a $GF(p)$

3.1 Introdução

Em [15], Huber propôs a construção de códigos sobre o anel dos inteiros algébricos $\mathbb{Z}[i]$, da extensão $\mathbb{Q}\left(\sqrt{-1}\right)$ de $\mathbb{Q}$, usando como alfabeto um subconjunto $\mathcal{A}$ de $\mathbb{Z}[i]$ com p elementos, onde p é um número primo congruente a 1 módulo 4. Uma proposta importante, naquele trabalho foi projetar códigos sobre $\mathcal{A}$, com a distância de Mannheim. Estes códigos juntamente com a distância de Mannheim são apropriados para o caso em que a modulação é do tipo QAM, onde as distâncias de Hamming e de Lee não são apropriadas, isto deve-se ao fato que, dentre estas três distâncias, a de Mannheim é a que mais se aproxima da distância euclidiana, no sentido que vetores que estão próximos segundo a métrica euclidiana também estão próximos segundo a métrica de Mannheim. Disto deduzimos que esta distância também se aplica em processos de decodificação com decisão suave.

O objetivo, neste capítulo, será o de estender os resultados de Huber, bem como outros, considerando o anel dos inteiros algébricos $\mathbb{Z}[\omega]$ da extensão $\mathbb{Q}\left(\sqrt{d}\right)$ de $\mathbb{Q}$, $d=-1$ e $d=-3$, onde $\omega=\sqrt{-1}$ ou $\omega=\frac{1+\sqrt{-3}}{2}$, respectivamente. Na Seção 3.2, inicialmente, construímos um conjunto de sinais $\mathcal{A}$, rotulado pelo grupo aditivo de $GF(p)$, sendo $\mathcal{A}$ visto como o quociente $\mathbb{A}/\mathfrak{p}$, do anel dos inteiros algébricos $\mathbb{A}$, da extensão quadrática $K=\mathbb{Q}\left(\sqrt{d}\right)$, onde d é um inteiro livre de quadrados, por um ideal primo $\mathfrak{p}$ de $\mathbb{A}$, gerado por um elemento

π de $\mathbb{A}$, com norma p, onde p é um primo que se decompõe completamente em $\mathbb{A}$. Em seguida, apresentamos um procedimento para determinar o rotulamento do conjunto de sinais $\mathcal{A}$ casado, sob a distância de Mannheim, com o corpo $GF(p)$, que é o resultado mais importante deste capítulo. A Seção 3.3, é dedicada à obtenção da distância máxima de Mannheim entre os elementos de $\mathcal{A}$, no caso $d = -3$. Mostramos também que o anel $\mathbb{A}$, quando visto como um reticulado gerado por $\{1, \omega\}$, $\omega = \sqrt{-1}$ se $d = -1$ e $\omega = \frac{1+\sqrt{-3}}{2}$ se $d = -3$, possui um subreticulado $\mathcal{S}$ gerado por $\{\pi, \omega\pi\}$, onde $\pi = a + b\omega$, $a, b \in \mathbb{Z}$ é tal que a *norma* de π, $N(\pi)$ é igual a p, isto é, $N(\pi) = p$. Para este subreticulado $\mathcal{S}$, determinamos a região de Voronoi, $V_{\mathcal{S}}(0)$, da origem de $\mathcal{S}$ e mostramos que o conjunto de sinais $\mathcal{A}$ casado a $GF(p)$ está contido nesta região $V_{\mathcal{S}}(0)$. Apresentamos também a região de Voronoi para um subreticulado $\mathcal{S} \subset \mathbb{Z}\left(\sqrt{-5}\right)$.

Nosso objetivo, na próxima seção, é determinar um rotulamento para um particular conjunto de sinais $\mathcal{A}$ casado com um corpo $GF(p)$.

3.2 Constelações de Sinais Casadas a $GF(p)$

Uma *constelação de sinais* é um subconjunto discreto S de $\mathbb{R}^n$ e seus elementos são chamados *pontos de sinais.*

Uma constelação de sinais S é *casada com um grupo* G, segundo uma distância d de S, se existe uma aplicação μ de G *sobre* S tal que

$$d(\mu(g), \mu(h)) = d\left(\mu(e), \mu\left(g^{-1}h\right)\right),$$

para todo $g, h \in G$, onde e é o elemento neutro de G e $d(.\,,.)$ é uma distância em S. A aplicação μ é chamada de *aplicação casada.* Além disso, se μ é *injetivo* dizemos que μ^{-1} é um *rotulamento casado.*

Nossa intenção é determinar um rotulamento casado entre o grupo aditivo $GF(p)$ e um conveniente subconjunto $\mathcal{A}$ de $\mathbb{R}^2$. Para tanto, consideraremos $\mathcal{A} \subset \mathbb{C}$, identificando $\mathbb{C}$ com $\mathbb{R}^2$. De fato, $\mathcal{A}$ será um subconjunto do anel dos inteiros algébricos $\mathbb{A}$ de uma extensão

quadrática $K = \mathbb{Q}\left(\sqrt{d}\right)$, $d = -1$ e $d = -3$. Nestes casos, o anel $\mathbb{A}$, dos intiros algébricos de K é $\mathbb{Z}[\omega]$, onde $\omega = \sqrt{-1}$ ou $\omega = \frac{1+\sqrt{-3}}{2}$ se $d = -1$ ou $d = -3$, respectivamente.

O anel $\mathbb{A}$, dos inteiros algébricos de K, é um domínio de ideais principais; em particular os ideais primos $\mathfrak{p}$ de $\mathbb{A}$ são da forma:

$$\mathfrak{p} = (\pi), \quad \pi = a + b\omega, \quad a, b \in \mathbb{Z}. \tag{3.1}$$

Além disso, os ideais primos $\mathfrak{p}$ não nulos de $\mathbb{A}$ são maximais. Assim, o quociente $\mathbb{A}/\mathfrak{p}$ é um corpo.

Doravante os ideais primos $p\mathbb{Z}$ de $\mathbb{Z}$, aqui considerados, se decompõem completamente em $\mathbb{A}$, a menos que se explicite o contrário. Logo, os quocientes $\mathbb{A}/\mathfrak{p}$ são corpos com p elementos e consequentemente $\{0, 1, \cdots, p-1\}$ sempre será um conjunto completo de classes laterais de $\mathfrak{p}$ em $\mathbb{A}$, onde $\mathfrak{p}$ é um ideal primo de $\mathbb{A}$ acima de $p\mathbb{Z}$.

Pela observação acima, ω pertence a alguma classe lateral $\overline{s} \in \mathbb{A}/\mathfrak{p}$, onde $0 \leq s \leq p-1$. Assim, $\forall x, y \in \mathbb{Z}$, $\overline{x + y\omega} = \overline{x} + \overline{y}\ \overline{\omega} = \overline{x} + \overline{y}\ \overline{s} = \overline{x + ys} = \overline{l}$, $l \in \{0, 1, \cdots, p-1\}$. Agora, $\overline{x + ys} = \overline{l} \Leftrightarrow x + ys - l \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Em resumo:

$$x + y\omega \equiv l \,(\mathrm{mod}\,\mathfrak{p}) \Leftrightarrow x + ys \equiv l \,(\mathrm{mod}\, p), \tag{3.2}$$

onde s é um representante da classe lateral contendo ω.

Para determinar s, de uma maneira simples, basta observarmos que 0 é o rótulo do elemento $\pi = a + b\omega$. A relação (3.2) será fundamental para determinarmos os rótulos dos pontos de $\mathcal{A}$ pelos elementos de $GF(p)$.

Voltando ao conjunto $\mathcal{A}$, sejam K uma extensão quadrática de $\mathbb{Q}$, $\mathbb{A}$ seu anel de inteiros algébricos e p um número primo de $\mathbb{Z}$. Tomemos $\mathcal{A}$ como o conjunto $\{\alpha_0, \alpha_1, \cdots, \alpha_{p-1}\}$ de modo que $\mathcal{A}$ seja um conjunto completo de representantes de $\mathfrak{p}$ em $\mathbb{A}$, satisfazendo $\alpha_i \equiv i \,(\mathrm{mod}\,\mathfrak{p})$ e $N(\alpha_i)$ mínimo, onde $\mathfrak{p}$ é um ideal primo de $\mathbb{A}$ acima de $p\mathbb{Z}$ e $N(\alpha_i)$ é a norma relativa a K para $\mathbb{Q}$ de α_i. O conjunto $\mathcal{A}$ estará munido das seguintes operações, de adição

e multiplicação, definidas por

$$\alpha_i + \alpha_j = \alpha_k, \quad \text{onde } k \equiv i + j \,(\mathrm{mod}\, p)\,, \quad \forall\, i, j = 0, 1, \cdots, p-1,$$

$$\alpha_i \cdot \alpha_j = \alpha_k, \quad \text{onde } k \equiv i \cdot j \,(\mathrm{mod}\, p)\,, \quad \forall\, i, j = 0, 1, \cdots, p-1.$$

Pode-se ver que $\mathcal{A}$, com estas operações, é um corpo com p elementos, e portanto, isomorfo a $GF(p)$.

3.2.1 Distância de Mannheim

Dado um conjunto não vazio S, uma *distância* em S é uma função $d : S \times S \to \mathbb{R}$ que satisfaz:

1. $d(x,y) \geq 0 \quad \forall x, y \in S, \qquad d(x,y) = 0 \Leftrightarrow x = y.$
2. $d(x,y) = d(y,x) \quad \forall x, y \in S.$
3. $d(x,y) \leq d(x,z) + d(z,y) \quad \forall x, y, z \in S.$

Definição 3.1 *i) Dado $\gamma = a + b\omega \in \mathcal{A}$, definimos o* peso de Mannheim *de γ, por:*

$$w^M(\gamma) = |a| + |b|\,,$$

ii) Se $\alpha, \beta \in \mathcal{A}$ e $\alpha - \beta \equiv \gamma \,(\mathrm{mod}\, \mathfrak{p})$, $\gamma \in \mathcal{A}$, definimos a distância de Mannheim, *entre α e β, por:*

$$d^M(\alpha, \beta) = w^M(\gamma)\,.$$

É fácil ver que $d^M(.\,,.)$ é uma distância em $\mathcal{A}$.

Obs. 3.1 *Esta definição de distância de Mannheim generaliza aquela com mesmo nome definida em [15] por Huber.*

Portanto, pelo exposto, temos um *rotulamento casado,* definido de modo natural, do conjunto de sinais $\mathcal{A} = \{\alpha_0, \alpha_1, \cdots, \alpha_{p-1}\} \subset \mathbb{A}$ com o grupo aditivo de $GF(p)$. A aplicação casada μ de $GF(p)$ sobre $\mathcal{A}$ é definida por $\mu(\overline{r}) = \alpha_r, \quad r = 0, 1, \cdots, p-1$.

A seguir, veremos um procedimento que reproduz o processo acima e determina o rótulo de um elemento do conjunto de sinais $\mathcal{A}$, através do corpo $GF(p)$.

Procedimento para Rotular um Conjunto de Sinais Casado a $GF(p)$

1. Dado um número primo p, que se decompõe completamente em $\mathbb{A}$, seja $\pi = a + b\omega$ uma solução de $N(\alpha) = p, \quad \alpha \in \mathbb{A}$.

2. Seja $s \in \mathbb{Z}$ a única solução em r da equação $a + br \equiv 0 \pmod{p}$, $0 \leq r \leq p-1$.

3. O elemento $l \in GF(p)$ será o rótulo do ponto $x + y\omega \in \mathbb{A}$ se $x + ys \equiv l \pmod{p}$ e $N(x + y\omega)$ mínimo. O elemento $x + y\omega$ será denotado por α_l.

A unicidade do ponto α_l é consequência do Lema A, (veja Apêndice A).

Obs. 3.2 *i) No Exemplo* 2.5 *apresentamos um método para resolver as equações* $N(\alpha) = p$. *ii) Podemos otimizar o processo se ordenarmos inicialmente os valores de* $N(\alpha)$ *em ordem crescente e a seguir, para cada ponto* $\alpha = x + y\omega$ *de* $\mathcal{A}$, *atribuirmos o rótulo* l, *onde* $l \equiv x + ys \pmod{p}$.

Tendo em vista o passo 3, $\{\alpha_0, \alpha_1, \cdots, \alpha_{p-1}\}$ é um conjunto completo de resíduos mod $\mathfrak{p}$. Portanto, $\mathbb{A}/\mathfrak{p} = \{\overline{\alpha}_0, \overline{\alpha}_1, \cdots, \overline{\alpha}_{p-1}\}$.

Veremos, agora, alguns exemplos de rotulamento, que serão utilizados no decorrer deste trabalho.

3.2.2 Exemplos

Em todos os exemplos a seguir $\alpha = x + \omega y$ denota um elemento genérico de $\mathcal{A}$.

Exemplos em $\mathbb{Z}\left[\sqrt{-1}\right]$.

Neste caso temos a forma quadrática $N(x+iy) = x^2+y^2$. Como vimos no Exemplo 2.5, $N(x+iy)$ assume os valores $0, 1, 2, 4, 5, 8, 9, 10, \cdots$. Também observemos que, conforme vimos no Exemplo 2.3, os primos p que se decompõem completamente em $\mathbb{Z}[i]$ são aqueles congruentes a 1 módulo 4, isto é, $p \equiv 1 \pmod 4$. Veremos em seguida exemplos para $p = 13$ e $p = 37$.

a) $p = 13 \equiv 1 \pmod 4$.

1. Uma solução para a equação $N(\alpha) = x^2+y^2 = 13$ é o par $(a,b) = (3,2)$. Assim, podemos considerar $\pi = 3+2i$.

2. Como $\pi = 3+2i$ o número inteiro $s = 5$ satisfaz $s \equiv i \pmod{\mathfrak{p}}$.

3. Assim, $l \in GF(13)$ será o rótulo do ponto $\alpha = x+\omega y$ de $\mathcal{A}$ que satisfaz $x+5y \equiv l \pmod{13}$ e $N(\alpha)$ mínimo. Portanto, $N(\alpha) \in \{0,1,2,4\}$ e $\mathcal{A} = \{\alpha_l,\ l = 0,1,\cdots,36\}$, vide Tabela 3.1. Os pontos do conjunto de sinais $\mathcal{A}$ estão representados na Figura 3-1.

b) $p = 37 \equiv 1 \pmod 4$.

1. Agora, $N(\alpha) = x^2+y^2 = 37$. Logo, $\pi = 6+i$.

2. O número inteiro $s = 31$ é tal que $s \equiv i \pmod{\mathfrak{p}}$.

3. Assim, $l \in GF(37)$ será o rótulo do ponto $\alpha = x+\omega y$ de $\mathcal{A}$ que satisfaz $x+31y \equiv l \pmod{37}$ e $N(\alpha)$ mínimo. Portanto, $N(\alpha) \in \{0,1,2,4,5,8,9,10,13\}$ e $\mathcal{A} = \{\alpha_l,\ l = 0,1,\cdots,36\}$, vide Tabela 3.2. Os pontos de $\mathcal{A}$ estão representados na Figura ??.

Exemplos em $\mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-3}}{2}$

Neste caso temos a forma quadrática inteira $N(x+\omega y) = x^2+xy+y^2$, onde $\omega = \frac{1+\sqrt{-3}}{2}$. Conforme vimos no Exemplo 2.5, $N(x+\omega y)$ assume os valores $0, 1, 3, 4, 7, 9, \cdots$. Observemos

$(\ x,\ y)$	$N(\alpha)$	$l \equiv x + 5y \pmod{13}$
$(\ 0,\ 0)$	0	0
$(\ 1,\ 0)$	1	1
$(-1,\ 0)$	1	12
$(\ 0,\ 1)$	1	5
$(\ 0, -1)$	1	8
$(\ 1,\ 1)$	2	6
$(-1, -1)$	2	7
$(\ 1, -1)$	2	9
$(-1,\ 1)$	2	4
$(\ 2,\ 0)$	4	2
$(-2,\ 0)$	4	11
$(\ 0,\ 2)$	4	10
$(\ 0, -2)$	4	3

Tabela 3.1: $\mathcal{A}$ rotulado por $GF(13), d = -1$.

$(x,\ y)$	$N(\alpha)$	$l \equiv x + 31y \pmod{37}$
$(0,\ 0)$	0	0
$(1,\ 0)$	1	1
$(-1,\ 0)$	1	36
$(0,\ 1)$	1	31
$(0, -1)$	1	6
$(1,\ 1)$	2	32
$(-1, -1)$	2	5
$(1, -1)$	2	7
$(-1,\ 1)$	2	30
$(2,\ 0)$	4	2
$(-2,\ 0)$	4	35
$(0,\ 2)$	4	25
$(0, -2)$	4	12
$(1,\ 2)$	5	26
$(-1, -2)$	5	11
$(1, -2)$	5	13
$(-1,\ 2)$	5	24
$(2,\ 1)$	5	33
$(-2, -1)$	5	4

$(x,\ y)$	$N(\alpha)$	$l \equiv x + 31y \pmod{37}$
$(2, -1)$	5	8
$(-2,\ 1)$	5	29
$(2,\ 2)$	8	27
$(-2, -2)$	8	10
$(2, -2)$	8	14
$(-2,\ 2)$	8	23
$(3,\ 0)$	9	3
$(-3,\ 0)$	9	34
$(0,\ 3)$	9	19
$(0, -3)$	9	18
$(1,\ 3)$	10	20
$(-1, -3)$	10	17
$(3, -1)$	10	9
$(-3,\ 1)$	10	28
$(2,\ 3)$	13	21
$(-2, -3)$	13	16
$(3, -2)$	13	15
$(-3,\ 2)$	13	22

Tabela 3.2: $\mathcal{A}$ rotulado por $GF(37), d = -1$.

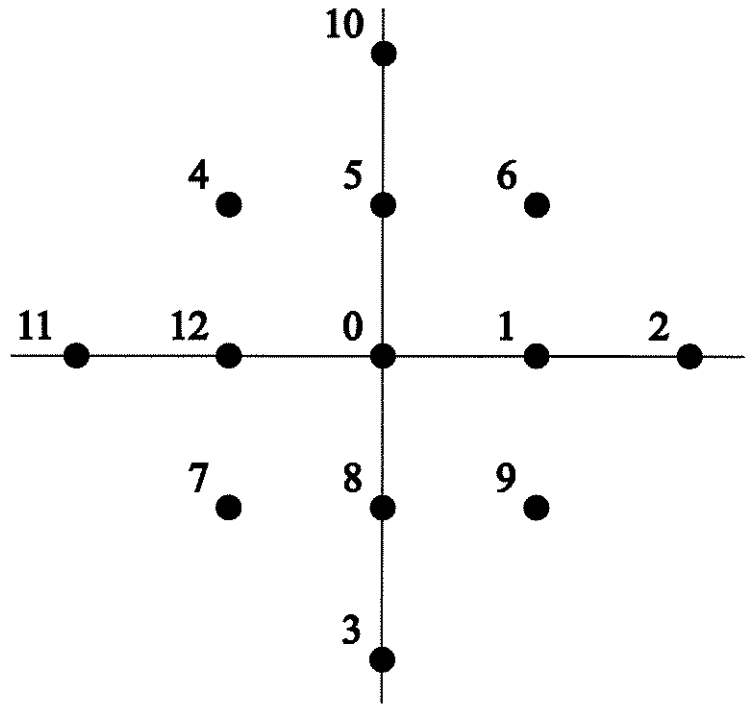

Figura 3-1: Constelação com 13 sinais rotulada por $GF(13)$, $d = -1$.

também que, os primos p que se decompõe completamente em $\mathbb{Z}[\omega]$, (conforme Exemplo 2.4), são aqueles congruentes a 1 módulo 3, isto é, $p \equiv 1 \pmod 3$, logo $p \neq 2$, e podemos considerar $p \equiv 1 \pmod 6$. Veremos em seguida exemplos para $p = 13,\ 19,\ 37,\ 61$.

c) $p = 13 \equiv 1 \pmod 6$.

1. Visto que o par $(-1, 4)$, é uma solução de $N(x + \omega y) = x^2 + xy + y^2 = 13$, podemos considerar $\pi = -1 + 4\omega$.

2. Vamos, agora, determinar $s \in \{0, 1, \cdots 12\}$ tal que $s \equiv \omega \pmod{\mathfrak{p}}$. Como $\pi = -1 + 4\omega$, podemos ver que $s = 10$.

3. Assim, $l \in GF(13)$ será o rótulo do ponto $\alpha = x + \omega y$ de $\mathcal{A}$ que satisfaz $x + 10y \equiv l \pmod{13}$ e $N(\alpha)$ mínimo. Portanto, $N(\alpha) \in \{0, 1, 3\}$ e $\mathcal{A} = \{\alpha_0,\ \alpha_1, \cdots, \alpha_{12}\}$, vide Tabela 3.3. A Figura 3-3 mostra os elementos do conjunto de sinais $\mathcal{A}$.

$(x,\ y)$	$N(\alpha)$	$l \equiv x + 10y \pmod{13}$
$(0,\ 0)$	0	0
$(1,\ 0)$	1	1
$(-1,\ 0)$	1	12
$(0,\ 1)$	1	10
$(0, -1)$	1	3
$(1, -1)$	1	4
$(-1,\ 1)$	1	9
$(1,\ 1)$	3	11
$(-1, -1)$	3	2
$(1, -2)$	3	7
$(-1,\ 2)$	3	6
$(2, -1)$	3	5
$(-2,\ 1)$	3	8

Tabela 3.3: $\mathcal{A}$ rotulado por $GF(13), d = -3$.

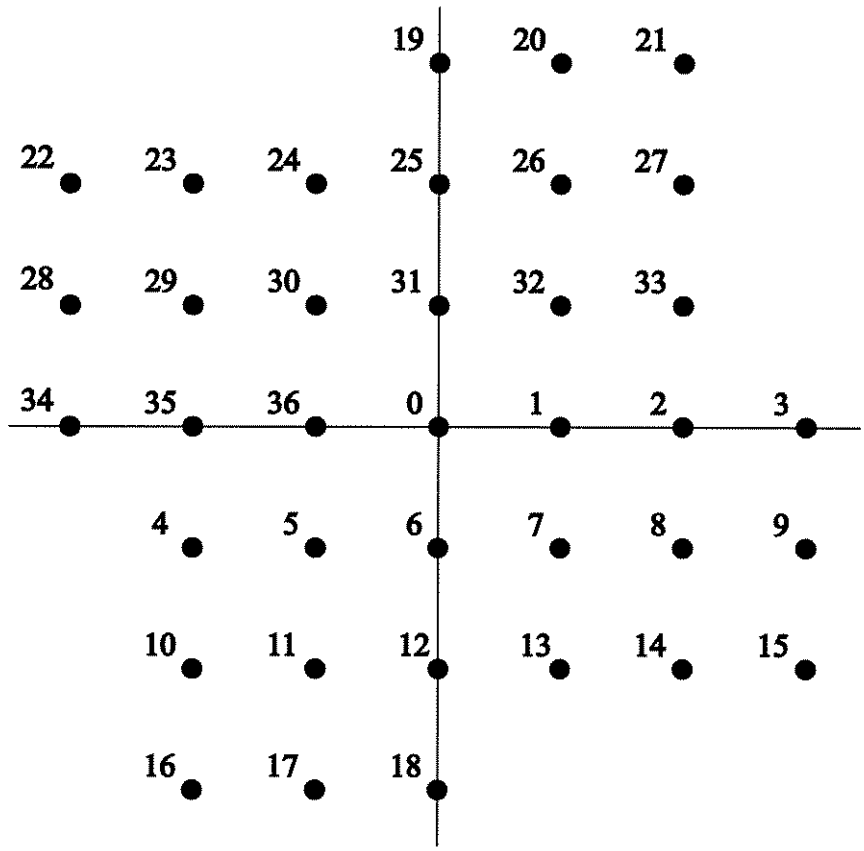

Figura 3-2: Constelação com 37 sinais rotulada por $GF(37)$, $d = -1$.

d) $p = 19 \equiv 1 \pmod 6$.

1. Como o par $(2,3)$, é uma solução de $N(x+\omega y) = x^2 + xy + y^2 = 19$, podemos considerar $\pi = 2 + 3\omega$.

2. Vamos, agora, determinar $s \in \{0, 1, \cdots 18\}$ tal que $s \equiv \omega \pmod{(\pi)}$. Como $\pi = 2+3\omega$, podemos ver que $s = 12$.

3. Assim, $l \in GF(19)$ será o rótulo do ponto $\alpha = x + \omega y$ de $\mathcal{A}$ que satisfaz $x + 12y \equiv l \pmod{19}$ e $N(\alpha)$ mínimo. Portanto, $N(\alpha) \in \{0, 1, 3\}$ e $\mathcal{A} = \{\alpha_0,\ \alpha_1, \cdots, \alpha_{18}\}$, vide Tabela 3.4. os pontos de $\mathcal{A}$ estão representados na Figura 3-4.

$(x,\ y)$	$N(\alpha)$	$l \equiv x + 12y \pmod{19}$
$(0,\ 0)$	0	0
$(1,\ 0)$	1	1
$(-1,\ 0)$	1	18
$(0,\ 1)$	1	12
$(0, -1)$	1	7
$(-1,\ 1)$	1	8
$(1, -1)$	1	11
$(2, -1)$	3	9
$(-2,\ 1)$	3	10
$(-1,\ 2)$	3	15
$(1, -2)$	3	4
$(1,\ 1)$	3	13
$(-1, -1)$	3	6
$(2,\ 0)$	4	2
$(-2,\ 0)$	4	17
$(0,\ 2)$	4	5
$(0, -2)$	4	14
$(2, -2)$	4	16
$(-2,\ 2)$	4	3

Tabela 3.4: $\mathcal{A}$ rotulado por $GF(19), d = -3$

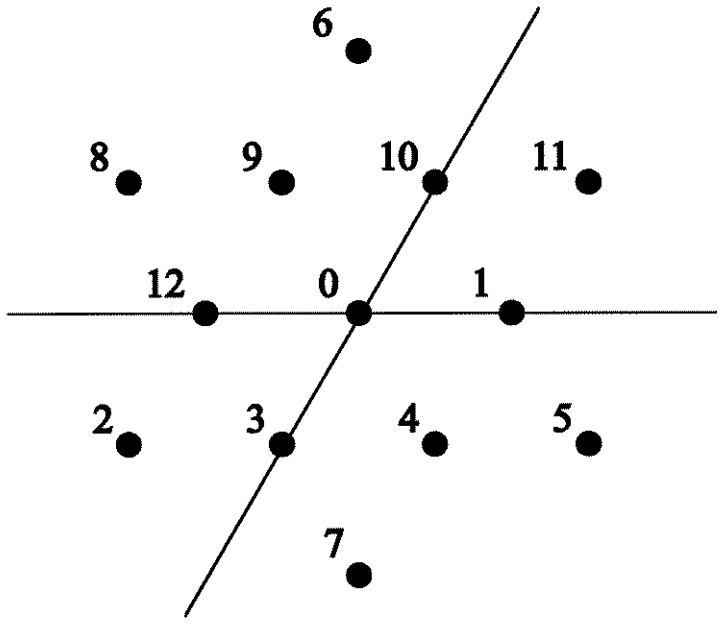

Figura 3-3: Constelação com 13 sinais rotulada por $GF(13)$, $d = -3$.

e) $p = 37 \equiv 1 \pmod 6$.

1. Neste caso $N(\alpha) = x^2 + xy + y^2 = 37$. Logo $\pi = 3 + 4\omega$.

2. Como $\pi = 3 + 4\omega$, temos que $s = 27$, satisfaz $s \equiv \omega \pmod{\mathfrak{p}}$.

3. Assim, $l \in GF(37)$ será o rótulo do ponto $\alpha = x + \omega y$ de $\mathcal{A}$ que satisfaz $x + 27y \equiv l \pmod{37}$ e $N(\alpha)$ mínimo. Logo, $N(\alpha) \in \{0, 1, 3, 4, 7, 9\}$ e $\mathcal{A} = \{\alpha_l,\ l = 0, 1, \cdots, 36\}$, vide Tabela 3.5. A Figura 3-5 mostra os elementos da constelação $\mathcal{A}$.

$(x,\ y)$	$N(\alpha)$	$l \equiv x + 27y \pmod{37}$
$(0,\ 0)$	0	0
$(1,\ 0)$	1	1
$(-1,\ 0)$	1	36
$(0,\ 1)$	1	27
$(0, -1)$	1	10
$(-1,\ 1)$	1	26
$(1, -1)$	1	11
$(2, -1)$	3	12
$(-2,\ 1)$	3	25
$(-1,\ 2)$	3	16
$(1, -2)$	3	21
$(1,\ 1)$	3	28
$(-1, -1)$	3	9
$(2,\ 0)$	4	2
$(-2,\ 0)$	4	35
$(0,\ 2)$	4	17
$(0, -2)$	4	20
$(2, -2)$	4	22
$(-2,\ 2)$	4	15

$(x,\ y)$	$N(\alpha)$	$l \equiv x + 27y \pmod{37}$
$(3, -1)$	7	13
$(-3,\ 1)$	7	24
$(-3,\ 2)$	7	14
$(3, -2)$	7	23
$(-2, -1)$	7	8
$(2,\ 1)$	7	29
$(-2,\ 3)$	7	5
$(2, -3)$	7	32
$(1,\ 2)$	7	18
$(-1, -2)$	7	19
$(-1,\ 3)$	7	6
$(1, -3)$	7	31
$(3,\ 0)$	9	3
$(-3,\ 0)$	9	34
$(0,\ 3)$	9	7
$(0, -3)$	9	30
$(3, -3)$	9	33
$(-3,\ 3)$	9	4

Tabela 3.5: $\mathcal{A}$ rotulado por $GF(37), d = -3$

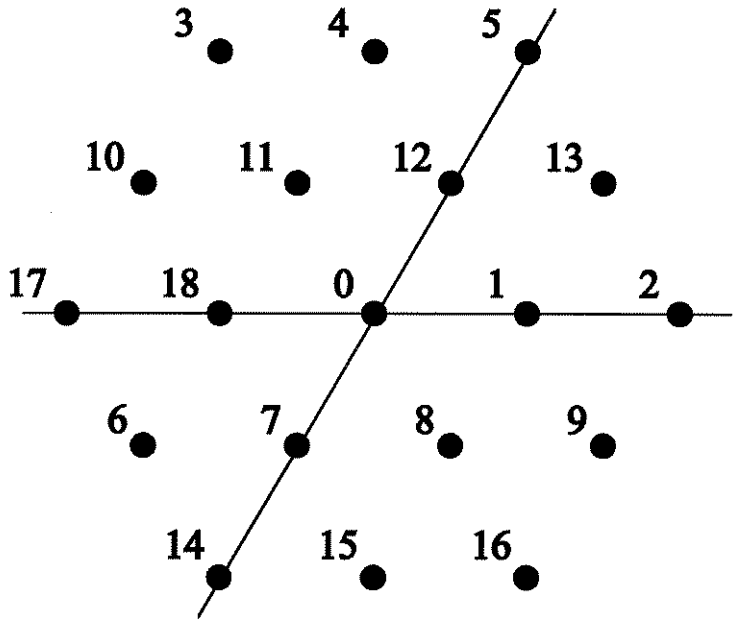

Figura 3-4: Constelação com 19 sinais rotulada por $GF(19)$, $d = -3$.

$f)$ $p = 61 \equiv 1 \pmod 6$.

1. Agora, $N(\alpha) = x^2 + xy + y^2 = 61$, logo $\pi = 5 + 4\omega$.

2. O número inteiro $s = 14$ é tal que $s \equiv \omega \pmod{\mathfrak{p}}$.

3. Assim, $l \in GF(61)$ será o rótulo do ponto $\alpha = x + \omega y$ de $\mathcal{A}$ que satisfaz $x + 14y \equiv l \pmod{61}$ e $N(\alpha)$ mínimo. Logo, $N(\alpha) \in \{0, 1, 3, 4, 7, 9, 12, 13, 16\}$ e $\mathcal{A} = \{\alpha_l,\ l = 0, 1, \cdots, 60\}$, vide Tabela 3.6.

$(x,\ y)$	$N(\alpha)$	$l \equiv x + 14y \pmod{61}$
$(0,\ 0)$	0	0
$(1,\ 0)$	1	1
$(-1,\ 0)$	1	60
$(0,\ 1)$	1	14
$(0, -1)$	1	47
$(1, -1)$	1	48
$(-1,\ 1)$	1	13
$(1,\ 1)$	3	15
$(-1, -1)$	3	46
$(2, -1)$	3	49
$(-2,\ 1)$	3	12
$(1, -2)$	3	34
$(-1,\ 2)$	3	27
$(2,\ 0)$	4	2
$(-2,\ 0)$	4	59
$(0,\ 2)$	4	28
$(0, -2)$	4	33
$(2, -2)$	4	35
$(-2,\ 2)$	4	26

$(x,\ y)$	$N(\alpha)$	$l \equiv x + 14y \pmod{61}$
$(1,\ 2)$	7	29
$(-1, -2)$	7	32
$(2,\ 1)$	7	16
$(-2, -1)$	7	45
$(1, -3)$	7	20
$(-1,\ 3)$	7	41
$(2, -3)$	7	21
$(-2,\ 3)$	7	40
$(3, -1)$	7	50
$(-3,\ 1)$	7	11
$(3, -2)$	7	36
$(-3,\ 2)$	7	25
$(3,\ 0)$	9	3
$(-3,\ 0)$	9	58
$(0,\ 3)$	9	42
$(0, -3)$	9	19
$(3, -3)$	9	22
$(-3,\ 3)$	9	39

Tabela 3.6: $\mathcal{A}$ rotulado por $GF(61), d = -3$.

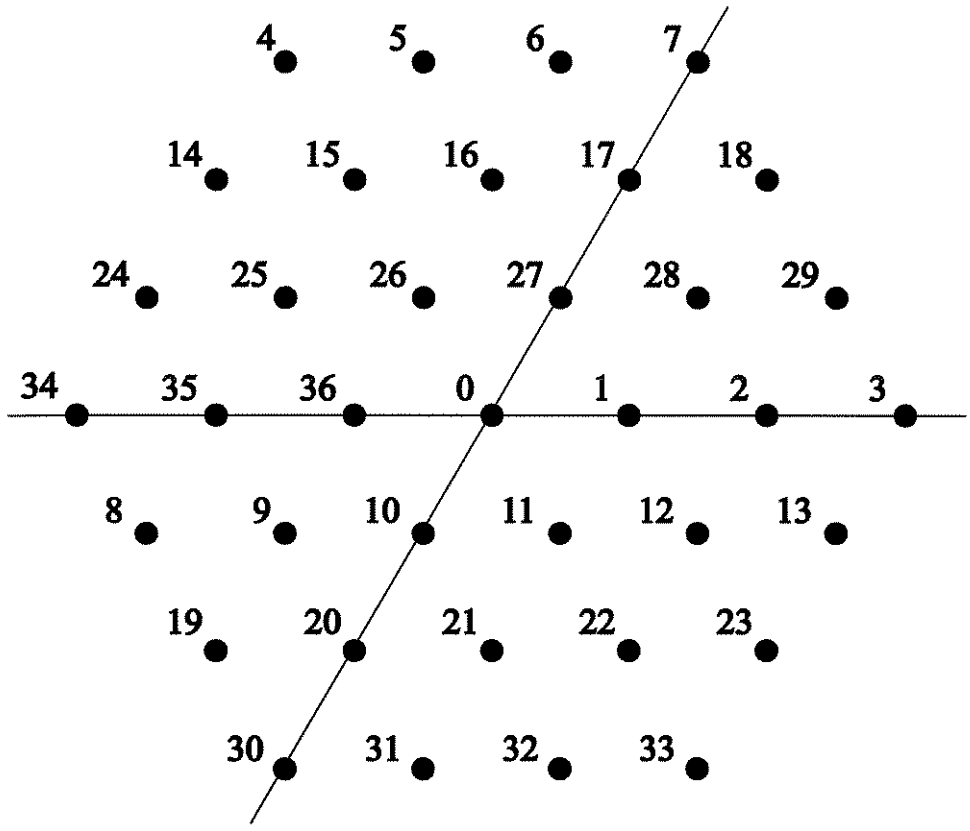

Figura 3-5: Constelação com 37 sinais rotulada por $GF(37)$, $d = -3$.

$(x,\ y)$	$N(\alpha)$	$l \equiv x + 14y \pmod{61}$
$(2,\ 2)$	12	30
$(-2,-2)$	12	31
$(2,-4)$	12	7
$(-2,\ 4)$	12	54
$(4,-2)$	12	37
$(-4,\ 2)$	12	24
$(1,\ 3)$	13	43
$(-1,-3)$	13	18
$(1,-4)$	13	6
$(-1,\ 4)$	13	55
$(3,\ 1)$	13	17
$(-3,-1)$	13	44
$(3,-4)$	13	8
$(-3,\ 4)$	13	53
$(4,-3)$	13	23
$(-4,\ 3)$	13	38
$(4,-1)$	13	51
$(-4,\ 1)$	13	10
$(4,\ 0)$	16	4
$(-4,\ 0)$	16	57
$(0,\ 4)$	16	56
$(0,-4)$	16	5
$(4,-4)$	16	9
$(-4,\ 4)$	16	52

continuação da Tabela 3.6.

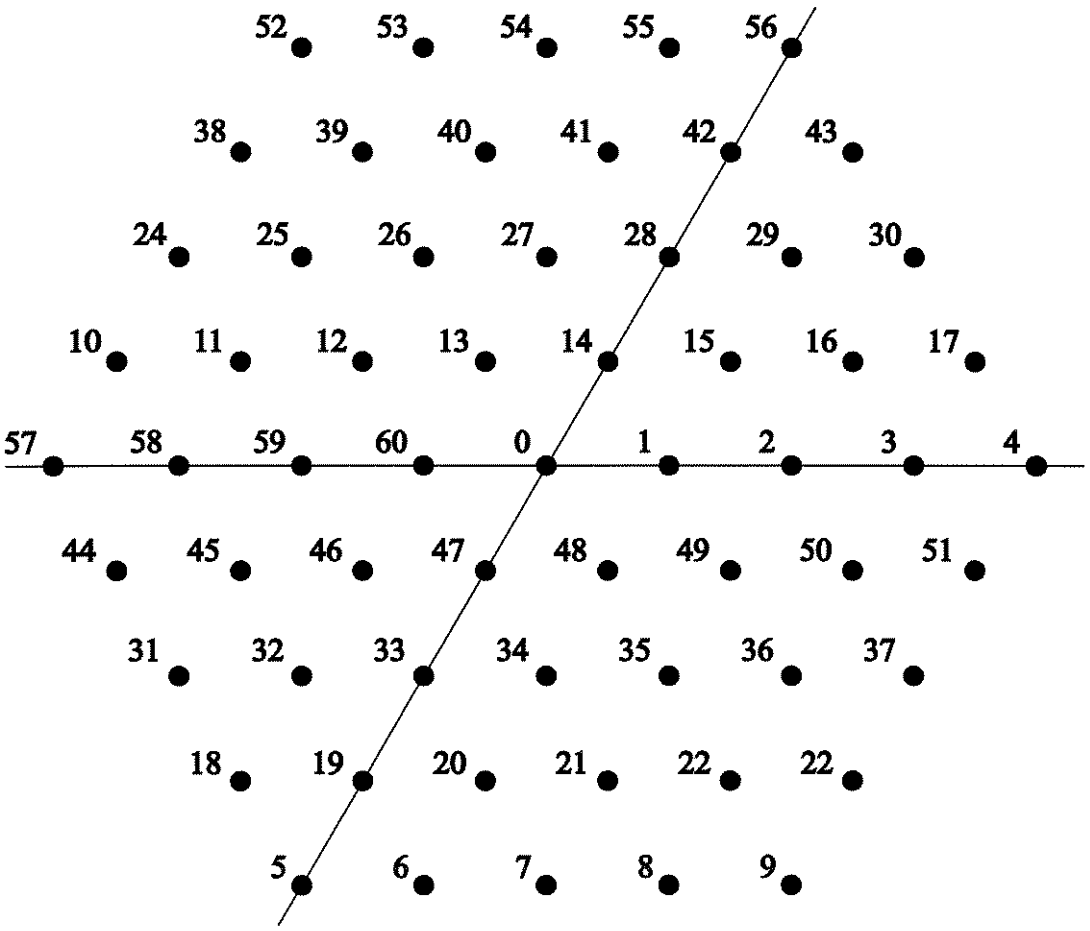

Figura 3-6: Constelação com 61 sinais rotulada por $GF(61)$, $d = -3$.

Obs. 3.3 *Quando p é um primo, $p \equiv 1 \pmod{12}$, então o corpo $GF(p)$ é representado por dois tipos de constelações de sinais, uma contida em $\mathbb{Z}\left[\sqrt{-1}\right]$ e a outra em $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, ao primeiro temos associado o reticulado $\mathbb{Z}^2$ e ao segundo o reticulado A_2.*

3.3 Distância Máxima

Sejam $\mathbb{A} = \mathbb{Z}[\omega]$ o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-3}\right)$, onde $\omega = \frac{1+\sqrt{-3}}{2}$ e $\pi = a + b\omega \in \mathbb{A}$, tal que $N(\pi) = a^2 + ab + b^2$ seja um número primo $p \equiv 1 \pmod{6}$. Assim, o ideal $p\mathbb{Z}$ se decompõe completamente em $\mathbb{A}$. Podemos escolher $\pi = a + b\omega$ com $a, b > 0$,

pois sabemos que $(\pi) = (\mu\pi)$ onde μ é uma unidade de $\mathbb{A}$, isto é, $\mu = \omega^i$, para algum $i = 0, 1, \cdots, 5$. De fato: Se $a, b < 0$, então multiplicando π por $\omega^3 = -1$, temos $-a - b\omega$, com $-a, -b > 0$. Se $a > 0$ e $b < 0$, então multiplicando π por ω, temos $a\omega + b\omega^2 = (a + b)\omega - b$. Aqui, temos duas possibilidades: *a)* $a + b > 0$ ou *b)* $a + b < 0$. Se ocorrer *a)* então $-b > 0$ e $a + b > 0$. Se ocorrer *b)* então multiplicando π por ω^2, temos $a\omega - a - b = -(a + b) + a\omega$, onde $-(a + b) > 0$ e $a > 0$. Se $a < 0$ e $b > 0$, então basta trocarmos a por b. Portanto, qualquer outra relação envolvendo a e b pode ser reduzida à esta através de uma multiplicação conveniente de π por uma unidade de $\mathbb{A}$.

Nosso objetivo, a partir de agora, será determinar a distância máxima de Mannheim entre os elementos de $\mathcal{A}$, e determinar a região de Voronoi da origem do subreticulado $\mathcal{S}$ de $\mathbb{A}$ gerado por $\{\pi,\ \omega\pi\}$.

Obs. 3.4 *Em [15] Huber determinou a distância máxima de Mannheim entre os elementos de $\mathcal{A}$ onde π é um elemento do anel $\mathbb{A} = \mathbb{Z}[i]$ dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-1}\right)$, (Teorema 3.2)*

Definição 3.2 *Sejam $\mathcal{P}$ um subconjunto discreto de $\mathbb{R}^n$ e $X \in \mathcal{P}$. A* região de Voronoi *de X em $\mathcal{P}$ consiste dos pontos de $\mathbb{R}^n$ que estão mais próximos de X do que de qualquer outro ponto de $\mathcal{P}$, ou seja,*

$$V(X) = \{x \in \mathbb{R}^n : d(x, X) \leq d(x, Y), \quad \forall\, Y \in \mathcal{P}, \quad Y \neq X\}$$

O ponto Y de $\mathcal{P}$, $Y \neq X$, é um vizinho do ponto X de $\mathcal{P}$ se $d(X, Y) \leq d(X, Z)$, $\quad \forall Z \in \mathcal{P}$.

Estaremos interessados nos casos em que o subconjunto discreto $\mathcal{P}$ de $\mathbb{R}^n$ tem estrutura de $\mathbb{Z}-$módulo, o qual será chamado de reticulado.

Quando X é um ponto do reticulado $\mathcal{P}$, $V(X) = X + V(0)$ e Y é vizinho de X se, e somente se, $Y - X$ é vizinho de 0.

Em $\mathbb{A} = \mathbb{Z}[\omega]$, os vizinhos da origem são as raízes sextas da unidade ω^j, $j = 0, 1, \cdots, 5$. Logo, os vizinhos da origem do subreticulado $\mathcal{S}$ de $\mathbb{A}$ gerado por $\{\pi,\ \omega\pi\}$ são: $\omega^i\pi$, $i =$

$0, 1, \cdots, 5$. De fato, seja $\alpha \in (\pi)$, digamos que $\alpha = \gamma\pi$, $\gamma \in \mathbb{A}$. Logo, $d^2(\alpha, 0) = N(\alpha) = N(\gamma\pi) = N(\gamma)\, N(\pi)$, onde d é a distância euclidiana. Para que α seja um vizinho da origem, sua distância a esta deve ser mínima, logo devemos ter $N(\gamma) = 1$. Portanto, γ é uma unidade em $\mathbb{A}$. Assim, $\gamma = \omega^j$, $j = 0, 1, \cdots, 5$, e consequentemente, $\alpha = \omega^j\pi$, $j = 0, 1, \cdots, 5$.

A próxima etapa consiste na determinação da distância máxima de Mannheim entre os pontos de $\mathcal{A}$.

Identifiquemos $\mathbb{A}$ com um subconjunto de $\mathbb{R}^2$ e seja $\pi \in \mathbb{A}$, π não nulo. Consideremos os segmentos de reta com extremidades na origem e nos pontos $\omega^j\pi$, $j = 0, 1, \cdots, 5$, Para cada um destes segmentos, tomemos a reta perpendicular a este passando pelo seu ponto médio. Fazendo $\pi = a + b\omega$, não nulo em $\mathbb{A}$, as interseções das retas acima citadas constituem os vértices de um hexágono regular $\mathcal{H}$, cujas coordenadas são dadas por: $C_1 = \left(\frac{a-b}{3}, \frac{a+2b}{3}\right)$; $C_2 = \left(\frac{-(a+2b)}{3}, \frac{2a+b}{3}\right)$; $C_3 = \left(\frac{-(2a+b)}{3}, \frac{a-b}{3}\right)$; $C_4 = \left(\frac{-(a-b)}{3}, \frac{-(a+2b)}{3}\right)$; $C_5 = \left(\frac{a+2b}{3}, \frac{-(2a+b)}{3}\right)$ e $C_6 = \left(\frac{2a+b}{3}, \frac{-(a-b)}{3}\right)$, expressos na base $\{1, \omega\}$.

De fato: Seja $\pi = a + b\omega = a + \frac{b}{2} + \frac{b\sqrt{-3}}{2} = \left(a + \frac{b}{2}\right) + \frac{b\sqrt{3}i}{2}$. Assim, π possui coordenadas (a, b) na base $\{1,\ \omega\}$ e $\left(\frac{2a+b}{2}, \frac{b\sqrt{3}}{2}\right)$ na base canônica $\{1, i\}$. Seja $\pi^\perp = \left(\frac{-b\sqrt{3}}{2}, \frac{2a+b}{2}\right)$ um vetor ortogonal a π, em coordenadas retangulares. Vamos determinar as coordenadas do ponto C_1, que é um dos vértices do hexágono $\mathcal{H}$ acima.

$$\overrightarrow{OC_1} = \frac{\pi}{2} + \frac{1}{2}\frac{|\pi|}{|\pi^\perp|}\frac{\sqrt{3}}{3}\pi^\perp = \frac{\pi}{2} + \frac{\sqrt{3}}{6}\pi^\perp \Rightarrow$$

$$2\overrightarrow{OC_1} = \left(\frac{2a+b}{2}, \frac{b\sqrt{3}}{2}\right) + \frac{\sqrt{3}}{3}\left(\frac{-b\sqrt{3}}{2}, \frac{2a+b}{2}\right) \Rightarrow$$

$$4\overrightarrow{OC_1} = \left(2a+b,\ b\sqrt{3}\right) + \left(-b,\ \frac{(2a+b)\sqrt{3}}{3}\right) = (2a,\ \frac{2(a+2b)\sqrt{3}}{3}) \Rightarrow$$

$$\overrightarrow{OC_1} = \left(\frac{a}{2},\ \frac{(a+2b)\sqrt{3}}{6}\right).$$

Logo, podemos escrever

$$\overrightarrow{OC_1} = \frac{a}{2} + \frac{(a+2b)\sqrt{3}i}{6} = \frac{a}{2} + \frac{a+2b}{3}\left(\frac{\sqrt{-3}}{2}\right) + \frac{a+2b}{6} - \frac{a+2b}{6} =$$

$$\left(\frac{a+2b}{3}\right)\left(\frac{1}{2}+\frac{\sqrt{-3}}{2}\right)+\frac{3a-a-2b}{6}=\frac{a-b}{3}+\frac{a+2b}{3}\omega.$$

Portanto, as coordenadas do ponto C_1, na base, $\{1,\omega\}$ são: $\left(\frac{a-b}{3},\frac{a+2b}{3}\right)$.

As coordenadas dos demais vértices do hexágono são obtidas tomando-se os vetores $\omega\pi$, $\omega^2\pi$, $\omega^3\pi$, $\omega^4\pi$, e $\omega^5\pi$. De $\pi=a+b\omega$, temos: $\omega\pi=-b+(a+b)\,\omega$, $\omega^2\pi=-(a+b)+a\omega$, $\omega^3\pi=-a-b\omega$, $\omega^4\pi=b-(a+b)\,\omega$ e $\omega^5\pi=(a+b)-a\omega$.

Vamos agora considerar as regiões semi-abertas $\mathcal{R}_1$, $\mathcal{R}_2$ e $\mathcal{R}_3$ limitadas, respectivamente, pelos pares de retas determinadas por: C_1C_6 e C_3C_4, C_1C_2 e C_4C_5, C_2C_3 e C_5C_6. Logo:

$$\mathcal{R}_1=\left\{(x,y)\in\mathbb{R}^2:-N(\pi)<(a+2b)\,y+(2a+b)\,x\leq N(\pi)\right\},$$

$$\mathcal{R}_2=\left\{(x,y)\in\mathbb{R}^2:-N(\pi)<(2a+b)\,y+(a-b)\,x\leq N(\pi)\right\},$$

$$\mathcal{R}_3=\left\{(x,y)\in\mathbb{R}^2:-N(\pi)<(a-b)\,y-(a+2b)\,x\leq N(\pi)\right\}.$$

O conjunto $\mathcal{R}=\mathcal{R}_1\cap\mathcal{R}_2\cap\mathcal{R}_3$ tem como fronteira o hexágono $\mathcal{H}$.

Vamos determinar as coordenadas inteiras, na base $\{1,\ \omega\}$, dos pontos de $\mathcal{R}$ mais próximos dos vértices de $\mathcal{H}$, e consequentemente, mais distantes da origem.

Obs: Se $a\equiv b\,(\mathrm{mod}\,3)$, então $p=a^2+ab+b^2\equiv a^2+a^2+a^2=3a^2$. Logo, p não será um primo congruente a $1\,(\mathrm{mod}\,6)$.

Portanto, vamos considerar apenas os casos: $a-b\equiv 1\,(\mathrm{mod}\,3)$ e $a-b\equiv 2\,(\mathrm{mod}\,3)$.

Temos dois casos a considerar: $1^{\underline{o}}: a>b>0$ e $2^{\underline{o}}: b>a>0$

$1^{\underline{o}}$ Caso: $a>b>0$

1. *a)* $a-b\equiv 1\,(\mathrm{mod}\,3)$.

Para $j=1,2,\ldots,6$; seja C_j^1 o ponto de coordenadas inteiras na base $\{1,\omega\}$, mais próximo de C_j. Então, $C_1^1=\left(\frac{a-b-1}{3},\frac{a+2b-1}{3}\right)$; $C_2^1=\left(\frac{-a-2b+1}{3},\frac{2a+b-2}{3}\right)$; $C_3^1=\left(\frac{-2a-b+2}{3},\frac{a-b-1}{3}\right)$; $C_4^1=\left(\frac{-a+b+1}{3},\frac{-a-2b+1}{3}\right)$; $C_5^1=\left(\frac{a+2b-1}{3},\frac{-2a-b+2}{3}\right)$ e $C_6^1=\left(\frac{2a+b-2}{3},\frac{-a+b+1}{3}\right)$.

1. *b)* $a-b\equiv 2\,(\mathrm{mod}\,3)$.

Para $j=1,2,\ldots,6$; seja C_j^2 o ponto de coordenadas inteiras na base $\{1,\omega\}$, mais

	$a-b \equiv 1 \,(\mathrm{mod}\, 3)$	$a-b \equiv 2 \,(\mathrm{mod}\, 3)$
$j=1$	$\frac{2a+b-2}{3}$	$\frac{2a+b-4}{3}$
$j=2$	$a+b-1$	$a+b-1$
$j=3$	$a-1$	$a-1$
$j=4$	$\frac{2a+b-2}{3}$	$\frac{2a+b-4}{3}$
$j=5$	$a+b-1$	$a+b-1$
$j=6$	$a-1$	$a-1$

Tabela 3.7: Distância dos pontos C_j^k à origem, $j=1,2,\cdots,6$, $k=1,2$.

próximo de C_j. Então, $C_1^2=\left(\frac{a-b-2}{3},\frac{a+2b-2}{3}\right)$; $C_2^2=\left(\frac{-a-2b+2}{3},\frac{2a+b-1}{3}\right)$; $C_3^2=\left(\frac{-2a-b+1}{3},\frac{a-b-2}{3}\right)$; $C_4^2=\left(\frac{-a+b+2}{3},\frac{-a-2b+2}{3}\right)$; $C_5^2=\left(\frac{a+2b-2}{3},\frac{-2a-b+1}{3}\right)$ e $C_6^2=\left(\frac{2a+b-1}{3},\frac{-a+b+2}{3}\right)$.

Consideremos a Tabela 3.7 definida por $A=(a_{jk})$, onde $a_{jk}=w^M\left(C_j^k\right)$, $j=1,2,\cdots,6$; $k=1,2$.

A Tabela 3.7 mostra as distâncias de Mannheim da origem aos pontos C_j^k com coordenadas inteiras na base $\{1,\omega\}$, no 1º Caso. Esta mesma tabela mostra que a distância máxima de Mannheim entre os pontos de $\mathcal{A}$ é $a+b-1$.

	$a-b\equiv 1\,(\mathrm{mod}\,3)$	$a-b\equiv 2\,(\mathrm{mod}\,3)$
$j=1$	$\frac{2a+b-2}{3}$	$\frac{2a+b-4}{3}$
$j=2$	$a+b-1$	$a+b-1$
$j=3$	$a-1$	$a-1$
$j=4$	$\frac{2a+b-2}{3}$	$\frac{2a+b-4}{3}$
$j=5$	$a+b-1$	$a+b-1$
$j=6$	$a-1$	$a-1$

Tabela 3.8: Distância dos pontos C_j^k à origem, $j=1,2,\cdots,6$, $k=3,4$.

2º Caso: $b>a>0$

2. *a*) $a-b\equiv 1\,(\mathrm{mod}\,3)$.

Para $j=1,2,\ldots,6$; seja C_j^3 o ponto de coordenadas inteiras na base $\{1,\omega\}$, mais próximo de C_j. Então, $C_1^3=\left(\frac{a-b+2}{3},\frac{a+2b-1}{3}\right)$; $C_2^3=\left(\frac{-a-2b+1}{3},\frac{2a+b-2}{3}\right)$; $C_3^3=\left(\frac{-2a-b+2}{3},\frac{a-b+2}{3}\right)$; $C_4^3=\left(\frac{-a+b-2}{3},\frac{-a-2b+1}{3}\right)$; $C_5^3=\left(\frac{a+2b-1}{3},\frac{-2a-b+2}{3}\right)$ e $C_6^3=\left(\frac{2a+b-2}{3},\frac{-a+b-2}{3}\right)$.

2. *b*) $a-b\equiv 2\,(\mathrm{mod}\,3)$.

Para $j=1,2,\ldots,6$; seja C_j^4 o ponto de coordenadas inteiras na base $\{1,\omega\}$, mais próximo de C_j. Então, $C_1^4=\left(\frac{a-b+1}{3},\frac{a+2b-2}{3}\right)$; $C_2^4=\left(\frac{-a-2b+2}{3},\frac{2a+b-1}{3}\right)$; $C_3^4=\left(\frac{-2a-b+1}{3},\frac{a-b+1}{3}\right)$; $C_4^4=\left(\frac{-a+b-1}{3},\frac{-a-2b+2}{3}\right)$; $C_5^4=\left(\frac{a+2b-2}{3},\frac{-2a-b+1}{3}\right)$ e $C_6^4=\left(\frac{2a+b-1}{3},\frac{-a+b-1}{3}\right)$.

Consideremos a Tabela 3.8 definida por $B=(b_{jk})$, onde $b_{jk}=w^M\left(C_j^k\right)$, $j=1,2,\cdots,6$, $k=3,4$.

A Tabela 3.8 mostra as distâncias de Mannheim da origem aos pontos C_j^k com coordenadas inteiras na base $\{1,\ \omega\}$, no 2º Caso. Esta tabela também mostra que a distância máxima de Mannheim entre os pontos de $\mathcal{A}$ é $a+b-1$.

Com estes argumentos acabamos de provar o seguinte teorema.

Teorema 3.1 *Sejam* $\mathbb{A}=\mathbb{Z}[\omega]$ *o anel dos inteiros algébricos de* $\mathbb{Q}\left(\sqrt{-3}\right)$ *e* $\pi=a+b\omega\in\mathbb{A}$,

tal que $N(\pi) = a^2 + ab + b^2$ *seja um primo* $p \equiv 1 \pmod 6$. *Então a distância máxima de Mannheim entre os elementos de* $\mathcal{A}$ *é dada por*

$$d_{\max}^{M}(\mathcal{A}) = \max\{|a|,\ |b|,\ |a+b|\} - 1.$$

Para o caso $\mathbb{A} = \mathbb{Z}[i]$, Huber em [15], demonstrou o seguinte teorema.

Teorema 3.2 *[15] Sejam* $\mathbb{A} = \mathbb{Z}[i]$ *o anel dos inteiros algébricos de* $\mathbb{Q}\left(\sqrt{-1}\right)$ *e* $\pi = a+bi \in \mathbb{A}$, *tal que* $N(\pi) = a^2 + b^2$ *seja um primo* $p \equiv 1 \pmod 4$. *Então a distância máxima de Mannheim entre os elementos de* $\mathcal{A}$ *é dada por* $d_{\max}^{M}(\mathcal{A}) = \max\{|a|,\ |b|\} - 1$.

Este resultado também pode ser obtido, fazendo-se uso das mesmas técnicas acima utilizadas.

O Teorema a seguir, estabelece as relações entre os conjuntos $\mathbb{A}$, $\mathcal{R}$, $\mathcal{S}$ e $\mathcal{H}$.

Teorema 3.3 *a) Os pontos de coordenadas inteiras na base* $\{1, \omega\}$ *localizados no interior de* $\mathcal{R}$ *constituem um conjunto completo de resíduos módulo* π.
b) O conjunto $\mathcal{R}$ *pode ser visto como a região de Voronoi da origem do subreticulado* $\mathcal{S}$.
c) Além disso pode-se ver $\mathcal{R}$ *como sendo uma rotação seguida de uma expansão da região de Voronoi da origem como ponto do reticulado* $\mathbb{A}$.

A demonstração deste Teorema será consequência das observações que faremos a seguir e dos Lemas 3.1, 3.2 e 3.3.

Por conveniência, os conjuntos $\mathbb{A}$, $\mathcal{R}$, $\mathcal{S}$ e $\mathcal{H}$ serão considerados tanto como subconjuntos de $\mathbb{R}^2$ como subconjuntos de $\mathbb{C}$.

Inicialmente, determinamos as coordenadas cartesianas dos vértices de $\mathcal{H}$. Como vimos, estes vértices têm coordenadas na base $\{1, \omega\}$ dadas por $C_1 = \left(\frac{a-b}{3}, \frac{a+2b}{3}\right)$; $C_2 = \left(\frac{-(a+2b)}{3}, \frac{2a+b}{3}\right)$; $C_3 = \left(\frac{-(2a+b)}{3}, \frac{a-b}{3}\right)$; $C_4 = \left(\frac{-(a-b)}{3}, \frac{-(a+2b)}{3}\right)$; $C_5 = \left(\frac{a+2b}{3}, \frac{-(2a+b)}{3}\right)$ e $C_6 = \left(\frac{2a+b}{3}, \frac{-(a-b)}{3}\right)$. Consideremos o vértice $C_1 = (\frac{a-b}{3}, \frac{a+2b}{3})$, que como elemento de $\mathbb{C}$ pode ser escrito como $C_1 = \frac{a-b}{3} + \frac{a+2b}{3}\omega = \frac{a-b}{3} + \frac{a+2b}{3}\left(\frac{1+\sqrt{-3}}{2}\right) = \frac{2a-2b+a+2b}{6} + \frac{(a+2b)\sqrt{3}i}{6} = \frac{a}{2} + \frac{(a+2b)\sqrt{3}i}{6}$,

ou seja, $C_1 = \left(\frac{a}{2}, \frac{(a+2b)\sqrt{3}}{6}\right)$ na base $\{1, i\}$. De maneira análoga, determinamos as coordenadas dos demais vértices na base $\{1, i\}$: $C_2 = \left(\frac{-b}{2}, \frac{(2a+b)\sqrt{3}}{6}\right)$; $C_3 = \left(\frac{-a-b}{2}, \frac{(a-b)\sqrt{3}}{6}\right)$; $C_4 = \left(\frac{-a}{2}, \frac{-(a+2b)\sqrt{3}}{6}\right)$; $C_5 = \left(\frac{b}{2}, \frac{-(2a+b)\sqrt{3}}{6}\right)$ e $C_6 = \left(\frac{a+b}{2}, \frac{(-a+b)\sqrt{3}}{6}\right)$.

Vamos agora determinar a distância de cada vértice C_j, $j = 0, 1, \cdots, 5$ à origem. Seja $\pi = a + b\omega \in \mathbb{A}$, não nulo, então $d^2(C_i, 0) = \left(\frac{a}{2}\right)^2 + \frac{3(a+2b)^2}{36} = \frac{a^2}{4} + \frac{a^2+4ab+4b^2}{12} = \frac{4a^2+4ab+4b^2}{12} = \frac{N(\pi)}{3}$. Como $\mathcal{H}$ é um hexágono regular centrado na origem, a distância de qualquer um de seus vértices à origem é a mesma, logo $d(C_j, 0) = \sqrt{N(\pi)/3}, \quad j = 1, 2, \cdots, 6$.

Faremos agora algumas observações que serão utilizadas nas demonstrações a seguir.

1. Em coordenadas cartesianas as retas r_j, $j = 1, 2, \cdots, 6$ são dadas por

$$r_1 : 3by + (2a + b)\sqrt{3}x + \sqrt{3}N(\pi) = 0,$$

$$r_2 : 3by + (2a + b)\sqrt{3}x - \sqrt{3}N(\pi) = 0,$$

$$r_3 : 3(a + b)y + (a - b)\sqrt{3}x - \sqrt{3}N(\pi) = 0,$$

$$r_4 : 3(a + b)y + (a - b)\sqrt{3}x + \sqrt{3}N(\pi) = 0,$$

$$r_5 : 3ay - (a + 2b)\sqrt{3}x - \sqrt{3}N(\pi) = 0,$$

$$r_6 : 3ay - (a + 2b)\sqrt{3}x + \sqrt{3}N(\pi) = 0.$$

2. $\mathcal{R}_j$, $j = 1, 2, 3$ é a região limitada pelas retas r_j e r_{j+1}.

3. A distância $d(r_1, r_2) = d(r_3, r_4) = d(r_5, r_6) = \sqrt{N(\pi)} = d(\omega^j\pi, 0)$. Portanto, a largura da cada faixa $\mathcal{R}_j$, $j = 1, 2, 3$; é dada por $l = \sqrt{N(\pi)}$.

4. Fazendo uma mudança de base em $\mathbb{R}^2$, da base $\{1,\ i\}$ para a base $\left\{\pi,\ \pi^{\perp}\right\}$ a primeira coordenada x de qualquer ponto $\alpha = (x, y) \in \mathcal{R}$, nesta nova base, é tal que $-1/2 \leq x < 1/2$. Portanto, o ponto $\alpha + \pi = (x, y) + (1, 0) = (1 + x, y)$ e $1/2 \leq 1 + x < 3/2$, logo $\alpha + \pi \notin \mathcal{R}_1$, também $\alpha - \pi = (x, y) + (-1, 0) = (-1 + x, y)$ e $-3/2 \leq -1 + x < -1/2$, logo $\alpha - \pi \notin \mathcal{R}_1$. De maneira análoga, se considerarmos as novas bases $\left\{\omega\pi,\ (\omega\pi)^{\perp}\right\}$

e $\left\{\omega^2\pi,\ (\omega^2\pi)^{\perp}\right\}$ de $\mathbb{R}^2$ os pontos $\alpha \pm \omega\pi \notin \mathcal{R}_2$ e $\alpha \pm \omega^2\pi \notin \mathcal{R}_3$, respectivamente. Portanto, se $\alpha \in \mathcal{R}$, então $\alpha + \omega^j\pi \notin \mathcal{R}$, $\forall j = 0, 1, \cdots, 5$.

5. Observemos que o único elemento de $\mathcal{S}$ contido em $\mathcal{H}$ é a origem, pois $\forall \alpha \in \mathcal{S}$, $\alpha = a\pi + b\omega\pi \neq 0$; $a, b \in \mathbb{Z}$ é tal que

$$N(\alpha) = N(\pi)\, N(a + b\omega) = \left(a^2 + ab + b^2\right) N(\pi) \geq N(\pi).$$

Lema 3.1 *Seja $V = V_{\mathcal{S}}(0)$ a região de Voronoi da origem de $\mathcal{S}$, isto é,*

$$V = \left\{x \in \mathbb{R}^2 : d(x,0) \leq d(x,y), \quad \forall y \in \mathcal{S}, \quad y \neq 0\right\}.$$

Então $V = \mathcal{R}$.

Demonstração:

a) $V \subseteq \mathcal{R}$.

Seja $\alpha \in V$ e suponhamos que $\alpha \notin \mathcal{R} = \bigcap_{i=1}^{3} \mathcal{R}_i$, então $\alpha \notin \mathcal{R}_j$, para algum $j \in \{1,2,3\}$. Sem perda de generalidade, podemos supor que $\alpha \notin \mathcal{R}_1$, logo $d(\alpha,\pi) \leq d(\alpha,0)$ ou $d(\alpha,-\pi) \leq d(\alpha,0)$, logo $\alpha \notin V$. Absurdo, portanto $V \subseteq \mathcal{R}$.

b) $V \supseteq \mathcal{R}$

Sejam $\alpha \in \mathcal{R}$ e $x \in \mathcal{S}$, $x \neq 0$. Suponhamos, por absurdo, que $d(\alpha,x) < d(\alpha,0)$, isto é, que $\alpha \notin V$. Assim, $d(\alpha,x) < d(\alpha,0) \leq \sqrt{N(\pi)/3}$. Logo, $d(x,0) \leq d(x,\alpha) + d(\alpha,0) \leq 2\sqrt{N(\pi)/3}$. Como $x \in \mathcal{S}$, $x = \pi\gamma$, $\gamma \in \mathbb{A}$, temos $N(x) = N(\pi)\, N(\gamma)$, aqui temos duas possibilidades: *a)* $N(\gamma) = 1$ ou *b)* $N(\gamma) > 1$.

a) Se $N(\gamma) = 1$, então $\gamma = \omega^j$, $j = 0, 1, \cdots, 5$. Suponhamos que $\gamma = \pm 1$, como $\alpha \in \bigcap_{j=1}^{3} \mathcal{R}_j \Rightarrow \alpha \in \mathcal{R}_1 \Leftrightarrow d(\alpha,0) < d(\alpha,\pi)$ e $d(\alpha,0) < d(\alpha,-\pi)$. Absurdo, pois estamos supondo $d(\alpha,x) < d(\alpha,0)$, $\forall x \in \mathcal{S}$, portanto $j \neq 0, 3$. Analogamente, mostramos que $j \neq 1, 2, 4$ e 5.

b) Se $N(\gamma) > 1$, então $d(x,0) \geq \sqrt{2N(\pi)}$, logo $\sqrt{2N(\pi)} \leq d(x,0) \leq 2\sqrt{N(\pi)/3}$, o que é um absurdo. Portanto, a hipótese $d(\alpha,x) < d(\alpha,0)$ é falsa, e assim $\alpha \in V$. ■

Lema 3.2 *Os pontos de coordenadas inteiras de $\mathcal{R}$ formam um conjunto completo de resíduos* mod $((\pi))$, $\pi \in \mathbb{A}$.

Demonstração:

Vimos, no Lema 3.1 que $\mathcal{R} = V_{\mathcal{S}}(0)$. Também é fato conhecido que $V_{\mathcal{S}}(0)$ é um mosaico de $\mathbb{R}^2$, isto é, $\mathbb{R}^2 = \bigcup_{X \in \mathcal{S}} (X + V(0))$, esta união é disjunta exceto possivelmente pelas arestas que podem se auto-interceptarem. Logo, dado $Y \in \mathbb{A}$, qualquer, existe um único $X \in \mathcal{S}$ tal que $Y \in X + V(0)$, logo $Y - X = \tilde{Y} \in V(0) = \mathcal{R}$. Portanto, $\forall\, Y \in \mathbb{A}$, $Y \equiv \tilde{Y}\,(\mathrm{mod}\,(\pi))$, isto é, em $\mathcal{R}$ sempre existe um representante do conjunto de resíduos mod (π). Mostremos agora que este elemento é único. De fato, suponhamos que $\exists \alpha, \beta \in \mathcal{R}$, tais que $\alpha \equiv \beta\,(\mathrm{mod}\,(\pi))$, logo $\alpha - \beta = \gamma\pi$, para algum $\gamma \in \mathbb{A}$.

$$d(\alpha, \beta) = d(\alpha - \beta, 0) = d(\gamma\pi, 0) = \sqrt{N(\gamma\pi)} = \sqrt{N(\pi)\,N(\gamma)}.$$

a) Se $N(\gamma) \geq 2$, então $\sqrt{2N(\pi)} \leq d(\alpha, \beta) \leq d(\alpha, 0) + d(\beta, 0) \leq 2\sqrt{N(\pi)/3}$, portanto $2N(\pi) \leq 4N(\pi)/3$. Absurdo. *b*) Se $N(\gamma) = 1$, então $\alpha - \beta = \omega^j \pi$, $j = 0, 1, \cdots, 5$. Suponhamos que $\alpha - \beta = \pi$, então $\alpha = \beta + \pi$, mas como $\beta \in \mathcal{R} = \bigcap_{j=1}^{3} \mathcal{R}_j$, então $\beta + \pi \notin \mathcal{R}_1$, portanto $\alpha \notin \mathcal{R}_1$, logo $\alpha \notin \mathcal{R}$. Absurdo. Analogamente se $j = 0, 2, 3, 4$ e 5. ■

Lema 3.3 *O conjunto $\mathcal{S}$ pode ser obtido a partir de $\mathbb{A}$ através de uma rotação seguida de uma expansão. Além disso, a região de Voronoi da origem de $\mathcal{S}$ é obtida da região de Voronoi da origem de $\mathbb{A}$ pela mesma ação. A rotação é determinada por $\theta = \arg(\pi)$ e a expansão sendo a multiplicação por $\sqrt{N(\pi)}$, onde $\pi = a + b\omega$; $a, b \in \mathbb{Z}$; é um elemento de $\mathbb{A}$.*

Demonstração:

Seja $\pi \in \mathbb{A}$, $\pi = \sqrt{N(\pi)}e^{i\theta}$. Visto que o ideal gerado por π é o mesmo ideal gerado por $\omega^j\pi$, $j = 0, 1, \cdots, 5$, podemos considerar $0 \leq \theta \leq 60°$, pois sendo $\omega = \frac{1+\sqrt{-3}}{2}$ uma raiz sexta

da unidade, existe $j \in \{0,1,\cdots,5\}$ tal que $0 \leq \arg(\omega^j \pi) \leq 60°$. Assim sendo, podemos considerar, sem perda de generalidade, que $0 \leq \theta < 60°$. Consideremos a rotação ρ,

$$\begin{array}{rccc} \rho: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \longmapsto & (xcos\theta - ysen\theta, xsen\theta + ycos\theta) \end{array}$$

e a expansão ϕ,

$$\begin{array}{rccc} \phi: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \longmapsto & \sqrt{N(\pi)}(x,y) \end{array}.$$

Seja ψ a transformação linear $\phi \circ \rho$. Identificando $\mathcal{S}$ como um subconjunto de $\mathbb{R}^2$, 1 e $\omega = \frac{1+\sqrt{-3}}{2}$ podem ser vistos como os pares $(1,0)$ e $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ e portanto,

$$\psi(1) = \psi(1,0) = \phi(\rho(1,0)) = \phi(cos\theta, sen\theta) = \sqrt{N(\pi)}(cos\theta, sen\theta) = \pi.$$

e

$$\psi(\omega) = \psi\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = \phi\left(\rho\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right) =$$

$$= \phi\left(\frac{1}{2}cos\theta - \frac{\sqrt{3}}{2}sen\theta, \frac{1}{2}sen\theta + \frac{\sqrt{3}}{2}cos\theta\right) =$$

$$= \sqrt{N(\pi)}\left(\frac{1}{2}cos\theta - \frac{\sqrt{3}}{2}sen\theta, \frac{1}{2}sen\theta + \frac{\sqrt{3}}{2}cos\theta\right) =$$

$$= \sqrt{N(\pi)}(cos\theta + isen\theta)\left(\frac{1}{2} + \frac{\sqrt{3}}{2}\right) = \omega\pi;$$

logo, ψ leva 1 em π e ω em $\omega\pi$, e assim, por linearidade, ψ leva $\mathbb{A} = \mathbb{Z} + \mathbb{Z}\omega$ em $\mathcal{S} = \mathbb{Z}\pi + \mathbb{Z}\omega\pi$. É fácil ver que ψ leva a região de Voronoi da origem de $\mathbb{A}$ na região de Voronoi da origem de $\mathcal{S}$. ■

Considerando outros corpos quadráticos $\mathbb{Q}\left(\sqrt{d}\right)$, d um número inteiro livre de quadrados, $d \equiv 2$ ou $3 (\mathrm{mod}\, 4)$, pode-se observar que as respectivas regiões $\mathcal{R}$ são retângulos.

Exemplos 3.1 *1) Sejam* $d = -1 \equiv 3 (\mathrm{mod}\, 4)$, $p = 37$ *e* $\pi = 6 + i$, *como no Exemplo*

d) da Seção 3.2.2, aqui $\omega = i$. Consideremos os segmentos de reta com extremidades na origem e nos pontos $\pm\pi$, $\pm\pi i$. Para cada um destes segmentos, tomemos a reta perpendicular a este passando pelo seu ponto médio. Assim, temos as retas perpendiculares aos segmentos de extremidades $(-6,-1)$ e $(6,1)$ passando pelos pontos $\pm\left(3,\frac{1}{2}\right)$ e as retas perpendiculares ao segmento de extremidades $(-1,6)$ e $(1,-6)$ passando pelos pontos $\pm\left(\frac{-1}{2},3\right)$ (as coordenadas dos pontos estão expressas na base $\{1,\ i\}$). Seja $\mathcal{R}$ o interior da região limitada pelas retas acima. Vemos, assim, que $\mathcal{R}$ é um quadrado de vértices $\pm\left(\frac{5}{2},\frac{7}{2}\right)$ e $\pm\left(\frac{7}{2},\frac{-5}{2}\right)$. Vale observar que os vetores π e πi possuem o mesmo comprimento e $\theta = \arg(i) = 90°$. A Figura 3-7 mostra o conjunto de sinais $\mathcal{A}$ representado na região $\mathcal{R}$.

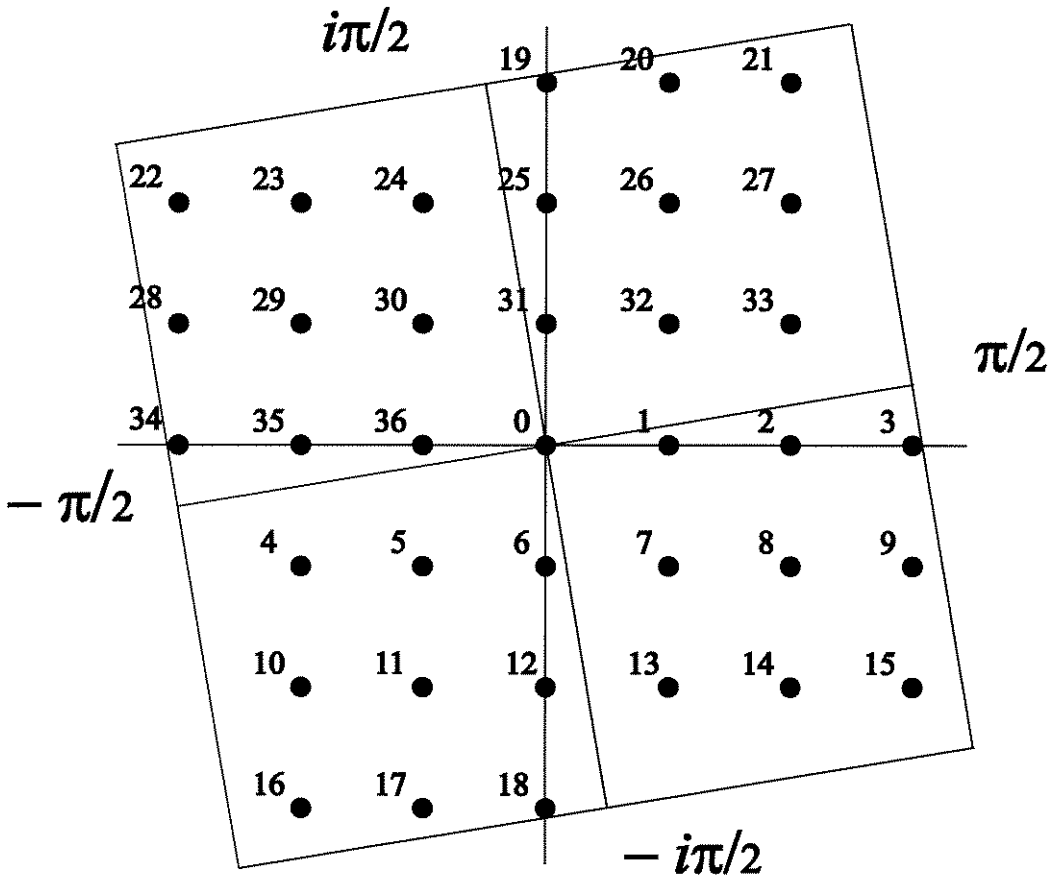

Figura 3-7: Região de Voronoi de $GF(37)$, $d = -3$.

$(x,\ y)$	$N(\alpha)$	$l \equiv x+13y \pmod{29}$
$(0,\ 0)$	0	0
$(1,\ 0)$	1	1
$(-1,\ 0)$	1	28
$(2,\ 0)$	4	2
$(-2,\ 0)$	4	27
$(0,\ 1)$	5	13
$(0,-1)$	5	16
$(1,\ 1)$	6	14
$(-1,-1)$	6	15
$(1,-1)$	6	17
$(-1,\ 1)$	6	12
$(3,\ 0)$	9	3
$(-3,\ 0)$	9	26
$(2,-1)$	9	18
$(-2,\ 1)$	9	11

$(x,\ y)$	$N(\alpha)$	$l \equiv x+13y \pmod{29}$
$(3,-1)$	14	19
$(-3,\ 1)$	14	10
$(4,\ 0)$	16	4
$(-4,\ 0)$	16	25
$(4,-1)$	21	20
$(-4,\ 1)$	21	9
$(2,-2)$	24	5
$(-2,\ 2)$	24	24
$(3,-2)$	29	6
$(-3,\ 2)$	29	23
$(5,-1)$	30	21
$(-5,\ 1)$	30	8
$(4,-2)$	36	7
$(-4,\ 2)$	36	22

Tabela 3.9: $\mathcal{A}$ rotulado por $GF(37), d=-5$.

2) Sejam $d=-5\equiv 3\pmod 4$ e $p=29$. Neste caso $\mathbb{A}=\mathbb{Z}[\omega]$, $\omega=\sqrt{-5}$. Se $\alpha=x+y\omega\in\mathbb{A}$, então $N(\alpha)=x^2+5y^2$.

Seguindo o procedimento dos exemplos da Seção 3.2.2, determinamos $\pi=3+2\omega\in\mathbb{A}$ e o elemento $l\in GF(29)$ será o rótulo do ponto $\alpha=x+\omega y$ de $\mathcal{A}$. Note que este rótulo satisfaz $x+13y\equiv l\pmod{29}$ e que torna $N(\alpha)=x^2+5y^2$ mínimo. Assim, de modo análogo aos exemplos da Seção 3.2.2, temos a Tabela 3.9

Conforme o modelo de 1) dos exemplos da Seção 3.2.2, temos as retas perpendiculares aos segmentos de reta determinados pelos vetores $\pm\pi$ e $\pm\omega\pi$, passando pelos seus pontos médios, que neste caso são $\pm\left(\frac{3}{2},1\right)$ e $\pm\left(5,\frac{-3}{2}\right)$, respectivamente, (as coordenadas

são expressas na base $\{1,\ \omega\}$*). Seja* $\mathcal{R}$ *o interior da região limitada pelas retas acima. Vemos, assim, que* $\mathcal{R}$ *é um retângulo de vértices* $\pm\left(\frac{7}{2}, \frac{-5}{2}\right)$ *e* $\pm\left(\frac{13}{2}, \frac{-1}{2}\right)$*. Vale observar que* $N(\omega\pi) = N(\omega)\,N(\pi) = \sqrt{5}N(\pi) \neq N(\pi)$*. Portanto,* $\mathcal{R}$ *não é um quadrado. Na Figura 3-8 vemos a distribuição dos pontos da constelação* $\mathcal{A}$ *em* $\mathcal{R}$*.*

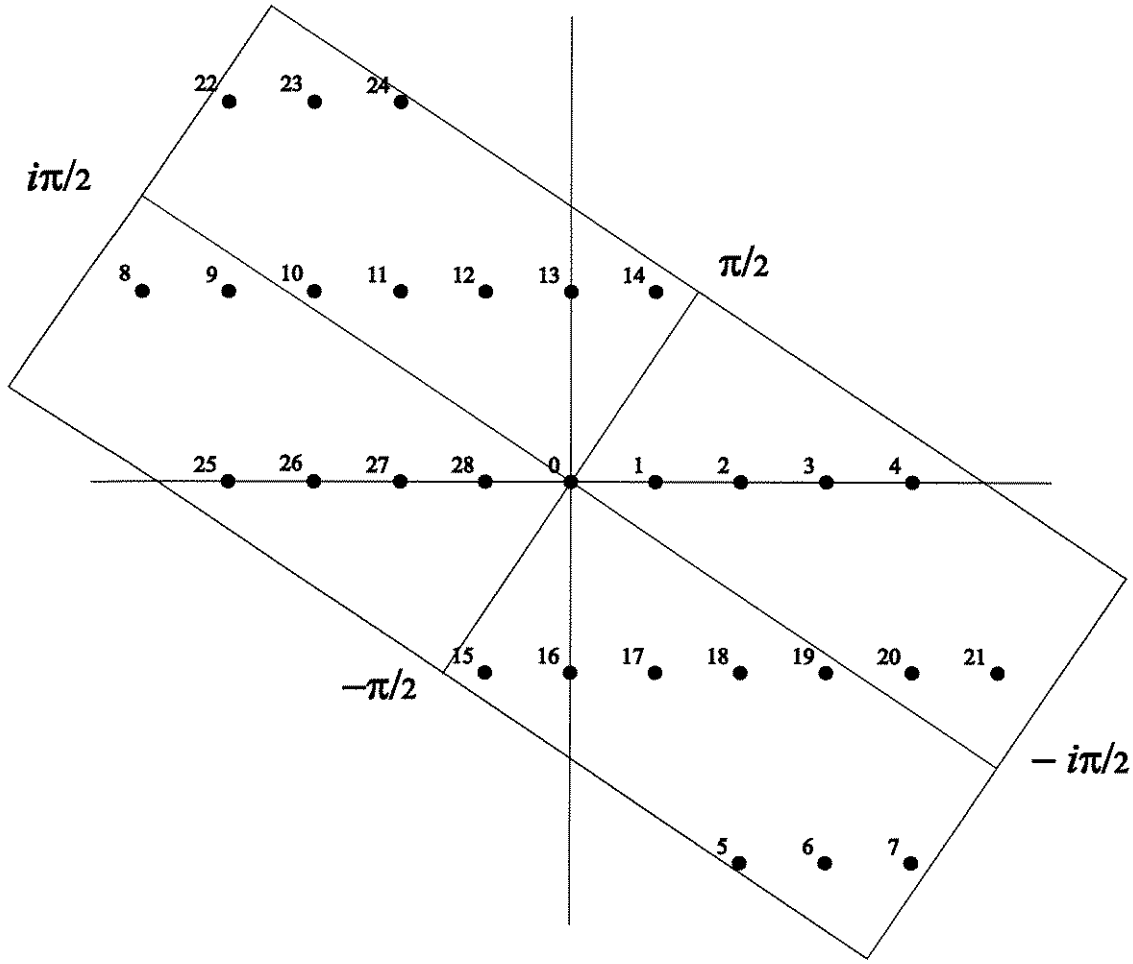

Figura 3-8: Região de Voronoi de $GF(29)$, $d = -5$.

Exemplos 3.2 *3) Sejam* $d = -3 \equiv 1 \pmod 4$, $p = 37$ *e* $\pi = 3 + 4\omega$, *como no Exemplo e) da Seção* 3.2.2, *aqui* $\omega = \frac{1+\sqrt{-3}}{2}$.

Consideremos os segmentos de reta com extremidades na origem e nos pontos $\pm\pi$, $\pm\omega\pi$ *e* $\pm\omega^2\pi = \pm(\omega\pi - \pi)$. *Para cada um destes segmentos, tomemos a reta perpendicular a este passando pelo seu ponto médio. Assim, temos as retas perpendiculares aos segmentos de extremidades* $(0,0)$ *e* $\pm(3,4)$; $(0,0)$ *e* $\pm(-4,7)$; $(0,0)$ *e* $\pm(-7,3)$ *passando pelos seus pontos médios* $\pm\left(\frac{3}{2},2\right)$, $\pm\left(-2,\frac{7}{2}\right)$ *e* $\pm\left(\frac{-7}{2},\frac{3}{2}\right)$, *respectivamente.*

(as coordenadas dos pontos são expressas na base $\{1,\ \omega\}$*). Seja* $\mathcal{R}$ *o interior da região limitada pelas retas acima. Vemos, assim, que* $\mathcal{R}$ *é um hexágono regular de vértices* $\pm\left(\frac{-1}{3}, \frac{11}{3}\right)$, $\pm\left(\frac{10}{3}, \frac{1}{3}\right)$ *e* $\pm(\frac{-11}{3}, \frac{10}{3})$. *Vale observar que os vetores* π, $\omega\pi$ *e* $\omega^2\pi$ *possuem o mesmo comprimento, pois* $N(\omega) = 1$, *e* $\theta = \arg(\omega) = 60°$. *A Figura 3-9 mostra o conjunto de sinais* $\mathcal{A}$ *representado na região* $\mathcal{R}$.

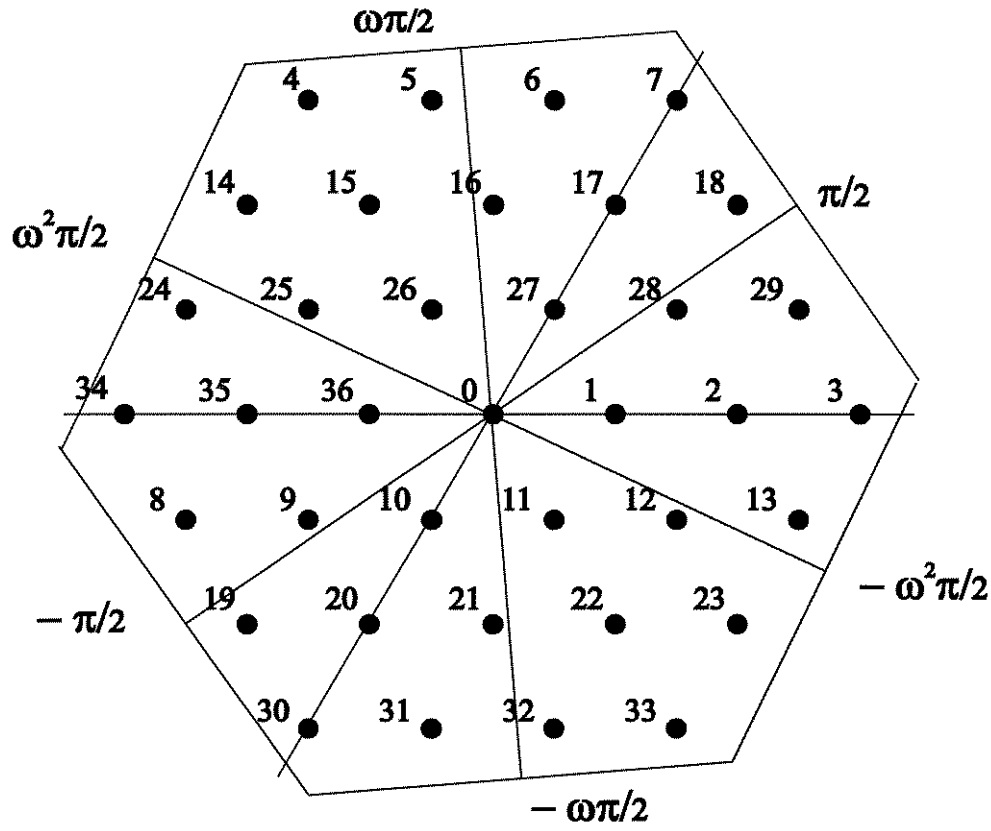

Figura 3-9: Região de Voronoi de $GF(37)$, $d = -3$.

3.4 Conclusões

Neste Capítulo, obtivemos um procedimento para o rotulamento dos elementos de um conjunto de sinais $\mathcal{A}$, pelo grupo aditivo do corpo $GF(p)$. Mostramos que este rotulamento é casado, segundo a distância de Mannheim, ao corpo $GF(p)$. Determinamos a distância máxima de Mannheim entre os elementos de $\mathcal{A}$, e também a região de Voronoi de um subreticulado $\mathcal{S}$ do anel dos inteiros algébricos $\mathbb{Z}[\omega]$.

Capítulo 4

Códigos sobre Anéis de Inteiros Algébricos

4.1 Introdução

Em [15], Huber apresenta algumas construções de códigos sobre os inteiros gaussianos, $\mathbb{Z}[i]$, isto é, o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-1}\right)$. Duas classes foram consideradas, a saber, os códigos corretores de um erro de Mannheim (códigos OMEC), e os códigos com distância de Mannheim maior do que três. Os códigos destas classes são códigos $i-$cíclicos [1]. Naquele trabalho, o principal objetivo era projetar códigos para a métrica de Mannheim, a qual é apropriada para uso com modulações do tipo QAM. Para os códigos OMEC, um algoritmo eficiente de decodificação foi apresentado. Também foi apresentado um exemplo de decodificação de um código com distância de Mannheim maior ou igual a quatro. Entretanto, não se pode desse exemplo, deduzir um método geral de decodificação.

Neste capítulo são propostos códigos sobre o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{d}\right)$, para $d = -1$ e $d = -3$. Nosso objetivo consiste em completar os resultados de [15] e apresentar novas propostas de construção de códigos sobre tais anéis. Por exemplo, todos os códigos tratados em [15] são sobre o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-1}\right)$. Os códigos aqui propostos são sobre os inteiros algébricos de $\mathbb{Q}\left(\sqrt{d}\right)$, para $d = -1$ e $d = -3$. Tais

inteiros algébricos são $\mathbb{Z}[i]$ (inteiros de Gauss) e $\mathbb{Z}[\omega]$, onde $\omega = \frac{1+\sqrt{-3}}{2}$, respectivamente, e serão denotados por $\mathbb{A}$.

Os alfabetos dos códigos sendo propostos são, na verdade, subconjuntos finitos dos anéis $\mathbb{A}$, tendo p elementos, onde p é um primo congruente a 1 módulo 4 se $d = -1$, e congruente a 1 módulo 6 se $d = -3$. Este alfabeto, denotado por $\mathcal{A}$, é um conjunto completo de representantes em $\mathbb{A}$ de um conveniente ideal primo $\mathfrak{p}$, e portanto, herda uma estrutura natural de corpo, isto é, podemos considerar o conjunto $\mathcal{A}$ como sendo isomorfo ao corpo $GF(p)$. Mediante esta identificação, foi introduzido por Huber, uma distância em $GF(p)$, denominada *distância de Mannheim*. Neste trabalho estendemos o conceito de distância de Mannheim para o caso de um anel $\mathbb{A}$ de inteiros algébricos de $\mathbb{Q}\left(\sqrt{d}\right)$, $d = -1$ e $d = -3$. (Capítulo 3, Seção 3.2). Na Seção 4.2, projetamos códigos sobre $\mathbb{Z}[\omega]$, para a métrica de Mannheim.

Essencialmente, quatro classes de códigos são propostas. Uma classe é projetada para corrigir um erro de Mannheim; outra para corrigir um erro de Hamming de *qualquer* peso de Mannheim; outra para corrigir dois erros de Hamming, cada um de peso de Mannheim igual a um; e finalmente, uma outra para corrigir dois erros de Hamming, cada um de *qualquer* peso de Mannheim. Todos os códigos sendo propostos são constacíclicos [1]. Nas Seções 4.3 e 4.4, apresentamos algoritmos eficientes de decodificação, para as classes de códigos sobre $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente. Embora as demonstrações nos dois casos sejam semelhantes, elas diferem quanto à sua complexidade, o que exige um tratamento diferenciado para cada caso, um exemplo dessa situação são as demonstrações dos Teoremas 4.5 e 4.9, onde tratamos com polinômios de graus 4 e 8, no primeiro caso e com polinômios de graus 6 e 12 no segundo. Na Seção 4.5 fazemos uma análise comparativa entre os códigos sobre $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, com respeito à taxa, capacidade de correção e energia média entre as respectivas constelações.

Na Seção 4.6 apresentamos alguns resultados a respeito dos códigos projetados sobre $\mathbb{Z}[\omega]$, quando considerados sob a distância de Hamming. Finalmente, na Seção 4.7 fazemos uso do algoritmo de Berlekamp-Massey [23] para correção de múltiplos erros de Hamming.

O interesse prático nesses códigos sobre anéis de inteiros algébricos com distância de

Mannheim é para uso em canais gaussianos e em esquemas de modulação codificada usando constelações do tipo QAM, onde nem a distância de Hamming nem a distância de Lee são apropriadas. Especificamente, códigos sobre $\mathbb{Z}[i]$ são usados quando a constelação de sinais for um subconjunto do reticulado $\mathbb{Z}^2$ e os códigos sobre $\mathbb{Z}[\omega]$, quando a constelação de sinais for um subconjunto do reticulado A_2.

4.2 Códigos sobre $\mathbb{Z}[\omega]$: Preliminares

Nosso objetivo, nesta seção, será caracterizar códigos sobre o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-3}\right)$, em termos de polinômios geradores. Para tanto, sejam p um número primo, $p \equiv 1 \pmod 6$, $\mathfrak{p}$ um ideal primo de $\mathbb{A}$ acima de $p\mathbb{Z}$, $\pi \in \mathbb{A}$ um gerador de $\mathfrak{p}$ e $\mathcal{A}$ um conjunto completo de representantes de $\mathfrak{p}$ em $\mathbb{A}$, como na Seção 3.2, ou seja, $\mathcal{A} \simeq GF(p)$. Seja $\beta \in \mathcal{A}$, um elemento de ordem $6n = p-1$, isto é, $o(\beta) = 6n$ e tal que $\beta^n = \omega$. Logo, β é um elemento primitivo, e portanto, podemos considerar $\mathcal{A} = (\beta) \cup \{0\}$.

Seja $\mathcal{C}$ o código definido pela matriz verificação de paridade H,

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^7 & (\beta^7)^2 & \cdots & (\beta^7)^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^{6t+1} & (\beta^{6t+1})^2 & \cdots & (\beta^{6t+1})^{n-1} \end{pmatrix}_{(t+1)\times n},$$

onde $0 \leq t \leq n-1$.

Um vetor $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1})$ de $\mathcal{A}^n$ é uma palavra código de $\mathcal{C}$ se, e somente se, $H\mathbf{c}^t = 0$, isto é,

$$\begin{cases} c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1} = 0 \\ c_0 + c_1\beta^7 + \cdots + c_{n-1}(\beta^7)^{n-1} = 0 \\ \\ c_0 + c_1\beta^{6t+1} + \cdots + c_{n-1}(\beta^{6t+1})^{n-1} = 0 \end{cases}.$$

Identificando $\mathbf{c}$ com o polinômio $c(x) = \sum_{i=0}^{n-1} c_i x^i$, temos $c\left(\beta^{6k+1}\right) = 0$ para $k = 0, 1, \cdots, t$.

Seja $g(x) = (x-\beta)(x-\beta^7)\cdots(x-\beta^{6t+1})$. Então $\partial(g) = t+1$ e os elementos β, β^7, $\cdots, \beta^{6t+1}$ de $\mathcal{A}$ são distintos. Como podemos ver, eles são raízes de $c(x)$ e são todas as $t+1$ raízes de $g(x)$. Agora, como $\left(\beta^{6k+1}\right)^n - \omega = \beta^{6nk}\beta^n - \omega = \beta^n - \omega = 0$, temos que $g(x)$ divide $x^n - \omega$.

Teorema 4.1 *O polinômio $g(x)$ é um gerador do código $\mathcal{C}$, isto é, todo polinômio código $c(x) \in \mathcal{C}$ é um múltiplo de $g(x)$.*

Demonstração: De fato, para que $\mathbf{c}$ pertença a $\mathcal{C}$ é necessário e suficiente que $c(x)$ tenha $\beta, \beta^7, \cdots, \beta^{6t+1}$ como raízes; mas isto é verdade se, e somente se, $c(x)$ é múltiplo de $g(x)$, que é o polinômio de menor grau que tem $\beta, \beta^7, \ldots, \beta^{6t+1}$ como raízes. Portanto, $c(x)$ é um múltiplo do polinômio $g(x)$ que divide $x^n - \omega$. ■

Agora, se

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathcal{C},$$

então,

$$xc(x) - c_{n-1}(x^n - \omega) = \omega c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-1} \in \mathcal{C}.$$

Assim, multiplicando-se $c(x)$ por $x \bmod (x^n - \omega)$, obtemos o seguinte:

1. Um deslocamento para a direita de uma posição da palavra código.
2. O coeficiente c_{n-1} é rotacionado de 60° e torna-se o primeiro símbolo da palavra obtida.

Portanto, o código C pertence à família dos códigos constacíclicos, ou códigos $\omega-$cíclicos [1].

Os resultados já discutidos nesta seção podem ser facilmente adaptados se considerarmos $\beta^n = -\omega$.

Definição 4.1 *Códigos ω-cíclicos (respectivamente $-\omega$-cíclicos) são códigos sobre $\mathcal{A}$, cujas palavras são múltiplos de um polinômio gerador $g(x) = \prod_{k=0}^{t}(x - \beta^{6t+1})$, que divide $f(x) = x^n - \omega$, (resp. $x^n + \omega$).*

Portanto, códigos $\omega-$cíclicos (ou $-\omega-$cíclicos) são invariantes por rotação de 60^o, assim como os códigos $i-$cíclicos (ou $-i-$cíclicos) são invariantes por rotação de 90^o.

Obs. 4.1 *Da mesma forma que associamos um polinômio* $c(x)$ *à palavra código* $\mathbf{c} = (c_0,\ c_1,\ \cdots, c_{n-1}$ *também associamos ao padrão de erro* $\mathbf{e} = (e_0, e_1, \cdots, e_{n-1})$ *o seguinte polinômio* $e(x) = e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + \cdots + e_{i_s}x^{i_s}$, *onde* $0 \leq i_1 < i_2 < \cdots < i_j \leq n-1$ *e* $e_{i_j} \neq 0$, *para* $0 \leq j \leq s$.

4.3 Códigos sobre $\mathbb{Z}[i]$.

Nosso objetivo nesta seção será projetar novos códigos sobre $\mathbb{Z}[i]$ e desenvolver algoritmos eficientes de decodificação para os mesmos, com a finalidade de estender os resultados de Huber em [15].

Em toda esta seção, p denotará um número primo congruente a 1 módulo 4 e β designará um elemento de $\mathcal{A} \simeq GF(p)$, de ordem $4n = p-1$, tal que $\beta^n = i$ (ou $\beta^n = -i$). Portanto, β é primitivo e podemos considerar $\mathcal{A} = (\beta) \cup \{0\}$. Logo, nestas condições, $\mathbb{A} = \mathbb{Z}[i]$ é o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-1}\right)$.

Em [15], Huber construiu os códigos OMEC, isto é, códigos que corrigem um erro de Mannheim e demonstrou o seguinte teorema.

Teorema 4.2 *[15] Seja* $\mathcal{C}$ *o código definido pela matriz verificação de paridade* H,

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^{n-1} \end{pmatrix}.$$

Então $\mathcal{C}$ *é capaz de corrigir todo padrão de um erro de Mannheim. Portanto* $d^M(\mathcal{C}) \geq 3$.

O teorema a seguir, generaliza o anterior, e fornece um algoritmo para a correção de um erro de de qualquer peso de Mannheim.

Teorema 4.3 *Seja* $\mathcal{C}$ *o código definido pela matriz verificação de paridade* H,

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^5 & \cdots & \beta^{5(n-1)} \end{pmatrix}.$$

Então $\mathcal{C}$ é capaz de corrigir todo padrão de erro da forma $e(x) = e_i x^i$, onde $1 \leq w^M(e_i) \leq d^M_{\max}(\mathcal{A})$, $0 \leq i \leq n-1$. Portanto, $d^M(\mathcal{C}) \geq 2d^M_{\max}(\mathcal{A}) + 1$.

Demonstração: Suponhamos que tenha ocorrido um erro de magnitude β^k, $0 \leq k \leq 4n-1$, na posição j, $0 \leq j \leq n-1$. Seja $\mathbf{r} = \left(0, 0, \cdots, \beta^k, \cdots, 0, 0\right)$ a palavra recebida.
Assim, a síndrome S é dada por

$$S = H\mathbf{r}^t = \begin{pmatrix} \beta^{j+k} \\ \beta^{5j+k} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_5 \end{pmatrix}.$$

Mas,

$$\beta^{j+k} = S_1 \Rightarrow j + k \equiv L_1 (\mathrm{mod}(p-1)),$$

$$\beta^{5j+k} = S_5 \Rightarrow 5j + k \equiv L_2 (\mathrm{mod}(p-1)).$$

O sistema

$$\begin{cases} j + k \equiv L_1 (\mathrm{mod}(p-1)) \\ 5j + k \equiv L_2 (\mathrm{mod}(p-1)) \end{cases},$$

possui uma única solução,

$$\begin{cases} j \equiv \dfrac{L_2 - L_1}{4} \, (\mathrm{mod}\, n), \\ k \equiv L_1 - j (\mathrm{mod}(p-1)). \end{cases}$$

Deste modo, temos que o erro ocorreu na posição $\dfrac{L_2 - L_1}{4} \, (\mathrm{mod}\, n)$ e que sua magnitude é β^k, onde $k \equiv L_1 - j(\mathrm{mod}(p-1))$. ■

Exemplo 4.1 *Consideremos $p = 37 = 4 \cdot 9 + 1$, logo $n = 9$. Sejam $\mathcal{A}$ como no Exemplo b) da Seção 3.2.2 e $\beta = -1 - i$. Assim, os rótulos $l \in GF(37)$ dos elementos $x + \omega y$ de $\mathcal{A}$ são dados por $l \equiv x + 31y \, (\mathrm{mod}\, 37)$. Seja $\mathbf{r} = (0,0,0,0,0,0,\beta^{35},0,0)$ a palavra recebida, onde*

$\beta^{35} = 3 - 2i$, $w^M(\mathbf{r}) = 5$. *Assim, a matriz* H *é dada por*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 \\ 1 & \beta^5 & \beta^{10} & \beta^{15} & \beta^{20} & \beta^{25} & \beta^{30} & \beta^{35} & \beta^4 \end{pmatrix}.$$

Logo,

$$H\mathbf{r}^t = \begin{pmatrix} \beta^{41} \\ \beta^{65} \end{pmatrix} \equiv \begin{pmatrix} \beta^5 \\ \beta^{29} \end{pmatrix} (\mathrm{mod}\,(\pi)),$$

então,

$$\begin{cases} j + k \equiv 5\,(\mathrm{mod}\,36) \\ 5j + k \equiv 29\,(\mathrm{mod}\,36). \end{cases}$$

Disto temos que

$$\begin{cases} j \equiv \frac{29-5}{4} \equiv 6\,(\mathrm{mod}\,9) \\ k \equiv 5 - 6 \equiv -1 \equiv 35\,(\mathrm{mod}\,36). \end{cases}$$

Portanto, o erro ocorreu na $7^{\underline{a}}$ *posição e sua magnitude é* β^{35}, *isto é,* $\mathbf{e} = (0,0,0,0,0,0,\beta^{35},0,0)$ *foi o erro cometido. Logo,* $\mathbf{v} = \mathbf{r} - \mathbf{e} = (0,0,0,0,0,0,0,0,0)$ *foi a palavra transmitida.*

Huber propôs, em [15], códigos que corrigem dois erros de Mannheim de peso um, e demonstrou o seguinte teorema:

Teorema 4.4 *[15] Seja* $\mathcal{C}$ *o código definido pela matriz verificação de paridade* H,

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^5 & \beta^{10} & \cdots & \beta^{5(n-1)} \end{pmatrix}.$$

Se $p \equiv 5\,(\mathrm{mod}\,12)$, *então* $d^M(\mathcal{C}) \geq 4$.

O resultado a seguir, generaliza o teorema anterior.

Teorema 4.5 *Seja $\mathcal{C}$ o código definido pela matriz verificação de paridade H,*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^5 & \beta^{10} & \cdots & \beta^{5(n-1)} \\ 1 & \beta^9 & \beta^{18} & \cdots & \beta^{9(n-1)} \end{pmatrix}.$$

Então $\mathcal{C}$ é capaz de corrigir todo padrão de erro da forma $e(x) = e_i x^i + e_j x^j$, onde $w^M(e_i) = w^M(e_j) = 1$, $0 \leq i \neq j \leq n-1$. Portanto, $d^M(\mathcal{C}) \geq 5$.

Demonstração: Sejam $\mathbf{v} \in \mathcal{C}$ a palavra transmitida, $\mathbf{e}$ o erro cometido e $\mathbf{r}$ a palavra recebida. Suponhamos que os erros, de peso de Mannheim igual a um, ocorreram nas posições j e k, $0 \leq j, k \leq n-1$ e que seus valores sejam, respectivamente, β^{un} e β^{vn}, onde, $0 \leq u, v \leq 3$. Sejam

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^j & \cdots & \beta^k & \cdots & \beta^{n-1} \\ 1 & \beta^5 & \cdots & \beta^{5j} & \cdots & \beta^{5k} & \cdots & \beta^{5(n-1)} \\ 1 & \beta^9 & \cdots & \beta^{9j} & \cdots & \beta^{9k} & \cdots & \beta^{9(n-1)} \end{pmatrix}$$

a matriz verificação de paridade, e $\mathbf{r} = \begin{pmatrix} 0 & 0 & \cdots & \beta^{un} & \cdots & \beta^{vn} & \cdots & 0 \end{pmatrix}$ a palavra recebida.

Então,

$$H\mathbf{r}^t = \begin{pmatrix} \beta^{j+un} + \beta^{k+vn} \\ \beta^{5j+un} + \beta^{5k+vn} \\ \beta^{9j+un} + \beta^{9k+vn} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_5 \\ S_9 \end{pmatrix}$$

é a síndrome.

Como $\beta^{4n} = 1$, segue que $\beta^{un} = \beta^{4un}\beta^{un} = \beta^{5un} = \beta^{8un}\beta^{un} = \beta^{9un}$ (analogamente $\beta^{vn} =$

$\beta^{5vn} = \beta^{9vn}$). Logo, temos o seguinte sistema de equações:

$$\begin{cases} \beta^{j+un} + \beta^{k+vn} = S_1 \\ \beta^{5(j+un)} + \beta^{5(k+vn)} = S_5 \\ \beta^{9(j+un)} + \beta^{9(k+vn)} = S_9 \end{cases}.$$

Fazendo $\beta^{j+un} = x$, $\beta^{k+vn} = y$, $S_1 = a$, $S_5 = b$ e $S_9 = c$ temos

$$\begin{cases} x + y = a \\ x^5 + y^5 = b \\ x^9 + y^9 = c \end{cases}. \tag{1}$$

O código $\mathcal{C}$ será capaz de corrigir todo padrão contendo dois erros de Mannheim de peso um se, e somente, se o sistema (1) admitir somente duas soluções.

Como estamos admitindo que ocorreram dois erros, temos as seguintes possibilidades: *a*) $a \neq 0$ e *b*) O sistema (1) admite pelo menos duas soluções.

A seguir, mostramos a veracidade destas possibilidades.

a) Mostremos que $a \neq 0$. Suponhamos, por absurdo, que $a = 0$. Logo, $\beta^{j+un} = -\beta^{k+vn}$. Assim, $b = \beta^{5(j+un)} + \beta^{5(k+vn)} = (\beta^{j+un})^5 + (\beta^{k+vn})^5 = -(\beta^{k+un})^5 + (\beta^{k+vn})^5 = 0$. Analogamente, $c = 0$. Logo, $a = b = c = 0$. Portanto, não ocorreram erros. Absurdo.

b) Seja (x_0, y_0) uma solução de (1), mostraremos que $x_0 \neq y_0$.
De fato, se $x_0 = \beta^{j+un} = \beta^{k+vn} = y_0$, então $\beta^{k-j+n(v-u)} = 1$. Mas $k - j + n(v - u) \leq n - 1 + n \cdot 3 = 4n - 1 < 4n = o(\beta)$, o que é uma contradição. Assim, $x_0 \neq y_0$. Como o sistema (1) é simétrico em relação a x e y, temos então que (y_0, x_0) também é uma solução. Observamos, assim, que as soluções de (1) ocorrem sempre aos pares.
No sistema (1) temos $y = a - x$, portanto podemos considerar os polinômios :

$$f(x) = x^9 + (a - x)^9 - c$$

e

$$g(x) = x^5 + (a-x)^5 - b$$

$f, g \in GF(p)[x]$. Seja x_0 uma raiz de $f(x)$, isto é, $f(x_0) = 0$.

Agora, $f(a-x_0) = (a-x_0)^9 + (a-a+x_0)^9 - c = x_0^9 + (a-x_0)^9 - c = f(x_0) = 0$.

Portanto, $f(x_0) = 0 \Leftrightarrow f(a-x_0) = f(y_0) = 0$. Analogamente, para $g(x)$.

Considerando, então os polinômios $f(x)$ e $g(x)$ e usando o Algoritmo de Euclides temos:

$\exists\ q,\ h \in GF(p)[x]$ tais que: $f(x) = q(x)\,g(x) + h(x)$ onde $\partial(h) \leq 3$.

De fato, neste caso, $h(x) = \frac{1}{25a}(4a^{10} + 12a^5b + 9b^2 - 25ac) - \frac{3a^3}{5}(a^5 + 4b)\,x + \frac{3a^2}{5}(a^5 + 4b)\,x^2$.

Assim, $\partial(h) = 2$ ou $\partial(h) = 0$

1) Se $\partial(h) = 2$, então as raízes comuns a $f(x)$ e $g(x)$ são as raízes de $h(x)$.

2) Se $\partial(h) = 0$, visto que as raízes de $f(x)$ e $g(x)$ ocorrem aos pares, $h(x)$ é o polinômio identicamente nulo, ou seja:

$$\begin{cases} a^5 + 4b = 0 \\ \frac{1}{25a}(4a^{10} + 12a^5 + 9b^2 - 25ac) = 0 \end{cases},$$

ou de modo equivalente,

$$\begin{cases} b = -a^5/4 \\ c = a^9/16 \end{cases}.$$

Portanto,

i) Se $b \neq -a^5/4$ ou $c \neq a^9/16$, então $f(x)$ e $g(x)$ possuem apenas duas raízes em comum, que são as raízes de $h(x)$.

ii) Se $b = -a^5/4$ e $c = a^9/16$, então $g(x) = 5a\left(x^2 - ax + \frac{a^2}{2}\right)^2 = 5a\left(x - \frac{(1+i)a}{2}\right)^2\left(x - \frac{(1+i)a}{2}\right)^2$.

Neste caso $f(x) = q(x)\,g(x)$, então $f(x)$ e $g(x)$ possuem apenas duas raízes distintas em comum.

Assim, em ambas as situações, o sistema (1) possui somente duas soluções, e portanto C é capaz de corrigir dois erros de Mannheim de peso um. ■

Obs. 4.2 *Mostraremos que este procedimento também se aplica no caso de ocorrer apenas um erro de peso um de Mannheim.*
De fato, suponhamos que ocorreu apenas um erro de peso um de Mannheim, logo $S_1 \neq 0$. *Então do sistema* (1) *temos,*

$$x = a, \quad x^5 = b \quad e\ x^9 = c,$$

logo, $b = a^5$ *e* $c = a^9$. *Portanto,*

$$\begin{aligned} f(x) &= x^9 + (a-x)^9 - a^9, \\ g(x) &= x^5 + (a-x)^5 - a^5. \end{aligned}$$

Dividindo $f(x)$ *por* $g(x)$, *obtemos,*

$$f(x) = q(x)\, g(x) + 3a^7 x\,(x-a), \quad q(x) \in GF(p).$$

Portanto, as raízes $x = 0$ *e* $x = a$, *são também raízes de* $f(x)$ *e* $g(x)$.
a) Se $x = 0$ *então, não ocorreram erros pois* $x = S_1$, *mas por hipótese* $S_1 \neq 0$.
b) Se $x = a$ *então, do sistema* (1), *temos que* $y = 0$, *mas* $y = \beta^{k+vn}$, *o que é uma contradição, a menos que ocorreu apenas um erro.*
Concluímos, assim, que o procedimento se aplica no caso de ocorrer um único erro de Mannheim de peso um.

A seguir fornecemos um procedimento de correção de erros para os códigos do Teorema 4.5.

Algoritmo de decodificação para os códigos definidos no Teorema 4.5

1. Se $S_1 = 0$, então não ocorreram erros, logo $\mathbf{r} = \mathbf{v}$.

2. Se $b = a^5$ e $c = a^9$, isto é, se $S_5 = S_1^5$ e $S_9 = S_1^9$, então ocorreu apenas um erro e procedemos como no Teorema 4.3.

3. Se $b \neq a^5$ ou $c \neq a^9$, isto é, se $S_5 \neq S_1^5$ ou $S_9 \neq S_1^9$, então ocorreram dois erros e procedemos como segue.

   Resolvendo $h(x) = 0$, (ou $g(x) = 0$, se h for identicamente nulo), temos as raízes:

$$\begin{cases} x_1 = \beta^{j+un} = \beta^{L_1}, \\ x_2 = \beta^{k+vn} = \beta^{L_2}, \end{cases}$$

   então,

$$\begin{cases} j \equiv L_1 \pmod{n}, \\ k \equiv L_2 \pmod{n}, \end{cases}$$

   e isto nos dá a localização dos erros.

4. As magnitudes dos erros serão dadas por: $\begin{cases} Y_1 = \beta^{L_1 - j}, \\ Y_2 = \beta^{L_2 - k} \end{cases}$.

5. Obtemos a palavra $\mathbf{v} \in \mathcal{C}$ transmitida calculando a diferença $\mathbf{v} = \mathbf{r} - \mathbf{e}$.

Exemplo 4.2 *Seja* $p = 37 = 4 \cdot 9 + 1$, *logo* $n = 9$. *Sejam* $\mathcal{A}$ *como no Exemplo b) da Seção* 3.2.2 *e* $\beta = -1 - i$. *Portanto, os elementos* $x + \omega y$ *de* $\mathcal{A}$ *são rotulados por* $l \in GF(37)$, *onde* $l \equiv x + 31y \pmod{37}$. *Sejam* $\mathcal{C}$ *o código definido pela matriz verificação de paridade:*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 \\ 1 & \beta^5 & \beta^{10} & \beta^{15} & \beta^{20} & \beta^{25} & \beta^{30} & \beta^{35} & \beta^4 \\ 1 & \beta^9 & \beta^{18} & \beta^{27} & 1 & \beta^9 & \beta^{18} & \beta^{27} & 1 \end{pmatrix}$$

e $\mathbf{r} = (0, 0, 0, \beta^{18}, 0, 0, \beta^9, 0, 0)$ *a palavra recebida, onde* $\beta^{18} = -1$, $\beta^9 = -i$, $w^M(\beta^9) =$

$w^M(\beta^{18}) = 1$. *Então a síndrome é obtida como*

$$H\mathbf{r}^t = \begin{pmatrix} \beta^{21}+\beta^{15} \\ \beta^{33}+\beta^{3} \\ \beta^{9}+\beta^{27} \end{pmatrix} \equiv \begin{pmatrix} 23+29 \\ 8+14 \\ 6+31 \end{pmatrix} (\mathrm{mod}\,(\pi)) = \begin{pmatrix} 15 \\ 22 \\ 0 \end{pmatrix} (\mathrm{mod}\,(\pi)) = \begin{pmatrix} \beta^{35} \\ \beta^{17} \\ 0 \end{pmatrix} (\mathrm{mod}\,(\pi)).$$

Portanto,

$$\begin{cases} x+y = 15 = a \\ x^5+y^5 = 22 = b \\ x^9+y^9 = 0 = c \end{cases} \tag{2}$$

Assim, temos $-a^5/4 = 9a^5 = 9\cdot(15)^5 = 31 \neq 22 = b$. *Portanto,* $b \neq -a^5/4$. *Logo, as soluções de* (2) *são as soluções de* $h(x) = 24(x-23)(x-29) = 0$, *isto é,*

$$x_1 = 23 \equiv \beta^{21}\,(\mathrm{mod}\,(\pi)),$$

$$x_2 = 29 \equiv \beta^{15}\,(\mathrm{mod}\,(\pi)).$$

Logo,

$$j \equiv 21 \equiv 3\,(\mathrm{mod}\,9),$$

$$k \equiv 15 \equiv 6(\mathrm{mod}\,9),$$

com isso $L_1 = 21-3 = 18$ *e* $L_2 = 15-6 = 9$. *Portanto, os dois erros ocorreram nas posições* $j = 3$ $(4^{\underline{a}})$ *e* $k = 6$ $(7^{\underline{a}})$ *e seus valores são* β^{18} *e* β^9, *respectivamente. Logo,* $\mathbf{v} = (0,0,0,0,0,0,0,0,0)$ *foi a palavra transmitida.*

Nossa proposta, agora será apresentar um código, com o respectivo algoritmo de decodificação, que permite corrigir até dois erros de Hamming.

Teorema 4.6 *Seja $\mathcal{C}$ o código definido pela matriz verificação de paridade H,*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^5 & (\beta^5)^2 & \cdots & (\beta^5)^{n-1} \\ 1 & \beta^9 & (\beta^9)^2 & \cdots & (\beta^9)^{n-1} \\ 1 & \beta^{13} & (\beta^{13})^2 & \cdots & (\beta^{13})^{n-1} \end{pmatrix}.$$

Então $\mathcal{C}$ é capaz de corrigir todo padrão de erro da forma $e(x) = e_i x^i + e_j x^j$, onde $1 \leq w^M(e_i), w^M(e_j) \leq d^M_{\max}(\mathcal{A})$, $0 \leq i \neq j \leq n-1$. Portanto, $d^M(\mathcal{C}) \geq 4d^M_{\max}(\mathcal{A}) + 1$.

Demonstração: Sejam $\mathbf{v} \in \mathcal{C}$ a palavra transmitida, $\mathbf{e}$ o erro cometido e $\mathbf{r}$ a palavra recebida. Suponhamos que os erros ocorreram nas posições i e j, $0 \leq i, j \leq n-1$ e que seus valores sejam, respectivamente, β^k e β^l, $0 \leq k, l \leq p-1 = 4n$. Sejam

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^i & \cdots & \beta^j & \cdots & \beta^{n-1} \\ 1 & \beta^5 & \cdots & (\beta^5)^i & \cdots & (\beta^5)^j & \cdots & (\beta^5)^{n-1} \\ 1 & \beta^9 & \cdots & (\beta^9)^i & \cdots & (\beta^9)^j & \cdots & (\beta^9)^{n-1} \\ 1 & \beta^{13} & \cdots & (\beta^{13})^i & \cdots & (\beta^{13})^j & \cdots & (\beta^{13})^{n-1} \end{pmatrix}$$

a matriz verificação de paridade e $\mathbf{r} = \begin{pmatrix} 0 & 0 & \cdots & \beta^k & \cdots & \beta^l & \cdots & 0 \end{pmatrix}$ a palavra recebida. Então,

$$S = H\mathbf{r}^t = \begin{pmatrix} \beta^{i+k} + \beta^{j+l} \\ \beta^{5i+k} + \beta^{5j+l} \\ \beta^{9i+k} + \beta^{9j+l} \\ \beta^{13i+k} + \beta^{13j+l} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_5 \\ S_9 \\ S_{13} \end{pmatrix}$$

é a síndrome.

Fazendo $x = \beta^{i+k}$ e $y = \beta^{j+l}$, temos o seguinte sistema de equações:

$$\begin{cases} x + y = S_1 \\ \beta^{4i}x + \beta^{4j}y = S_5 \\ \beta^{8i}x + \beta^{8j}y = S_9 \\ \beta^{12i}x + \beta^{12j}y = S_{13} \end{cases} \tag{3}$$

O código $\mathcal{C}$ será capaz de corrigir dois erros se, e somente se, o sistema acima admitir somente duas soluções. Como estamos supondo que ocorreram pelo menos dois erros, então o sistema admite pelo menos duas soluções. Vamos mostrar que existem somente duas.
De fato, de $x + y = S_1$, temos $y = S_1 - x$ e, assim, o sistema (3) transforma-se em:

$$\begin{cases} y = S_1 - x \\ \beta^{4i}x + \beta^{4j}S_1 - \beta^{4j}x = S_5 \\ \beta^{8i}x + \beta^{8j}S_1 - \beta^{8j}x = S_9 \\ \beta^{12i}x + \beta^{12j}S_1 - \beta^{12j}x = S_{13} \end{cases},$$

ou seja

$$\begin{cases} (\beta^{4i} - \beta^{4j})x = S_5 - \beta^{4j}S_1 \\ (\beta^{8i} - \beta^{8j})x = S_9 - \beta^{8j}S_1 \\ (\beta^{12i} - \beta^{12j})x = S_{13} - \beta^{12j}S_1 \end{cases},$$

o que implica em

$$(\beta^{4i} - \beta^{4j})x = S_5 - \beta^{4j}S_1, \tag{I}$$

$$(\beta^{4i} - \beta^{4j})(\beta^{4i} + \beta^{4j})x = S_9 - \beta^{8j}S_1, \tag{II}$$

$$(\beta^{4i} - \beta^{4j})\left(\beta^{8i} + \beta^{4i}\beta^{4j} + \beta^{8j}\right)x = S_{13} - \beta^{12j}S_1. \tag{III}$$

Agora, substituindo (I) em (II) e em (III) obtemos

$$(\beta^{4i} + \beta^{4j})\left(S_5 - \beta^{4j}S_1\right) = S_9 - \beta^{8j}S_1, \tag{IV}$$

$$\left(\beta^{8i} + \beta^{4i}\beta^{4j} + \beta^{8j}\right)\left(S_5 - \beta^{4j}S_1\right) = S_{13} - \beta^{12j}S_1. \tag{V}$$

Sejam $\beta^{4i} + \beta^{4j} = S$ e $\beta^{4i}\beta^{4j} = P$. Então temos

$$S\left(S_5 - \beta^{4j}S_1\right) = S_9 - \beta^{8j}S,$$
$$\left(S^2 - P\right)\left(S_5 - \beta^{4j}S_1\ \right) = S_{13} - \beta^{12j}S_1,$$

isto é,

$$SS_5 - \beta^{4j}\beta^{4i}S_1 - \beta^{8j}S_1 = S_9 - \beta^{8j}S_1, \tag{VI}$$

$$\left(S^2 - P\right)\left(S_5 - \beta^{4j}S_1\ \right) = S_{13} - \beta^{12j}S_1. \tag{VII}$$

De (VI) concluímos que:

$$SS_5 - PS_1 = S_9.$$

Logo,

$$P = \frac{SS_5 - S_9}{S_1}. \tag{VIII}$$

($S_1 \neq 0$, pois estamos assumindo que ocorreram pelo menos dois erros).

De (VII) temos:

$$S_5\left(S^2 - P\right) - \beta^{4j}S_1\left(\beta^{8i} + \beta^{4i+4j} + \beta^{8j}\right) = S_{13} - \beta^{12j}S_1,$$

o que implica que,

$$S_5\left(S^2 - P\right) - \beta^{4j+8i}S_1 - \beta^{8j+4i}S_1 - \beta^{12j}S_1 = S_{13} - \beta^{12j}S_1.$$

Assim,

$$S_5\left(S^2 - P\right) - \beta^{4j+4i}S_1\left(\beta^{4i} + \beta^{4j}\right) = S_{13}.$$

Portanto,

$$S_5\left(S^2 - P\right) - PSS_1 = S_{13}. \tag{IX}$$

Substituindo (VIII) em (IX), temos

$$S_5\left(S^2 - \frac{SS_5 - S_9}{S_1}\right) - S_1 S \frac{SS_5 - S_9}{S_1} = S_{13},$$

o que implica que

$$S_1 S_5 S^2 - S_5^2 S + S_5 S_9 - S_1 S_5 S^2 + S_1 S_9 S = S_1 S_{13}.$$

Assim,

$$S\left(S_1 S_9 - S_5^2\right) = S_1 S_{13} - S_5 S_9.$$

Portanto,

$$S = \frac{S_1 S_{13} - S_5 S_9}{S_1 S_9 - S_5^2}. \quad (*) \tag{X}$$

(*)No Lema 4.1 mostraremos que $S_1 S_9 - S_5^2 \neq 0$, a menos que tenha ocorrido um único erro de Hamming.

Substituindo (X) em (VIII), obtemos:

$$P = \frac{S_5 S_{13} - S_9^2}{S_1 S_9 - S_5^2}.$$

Resolvendo a equação: $X^2 - SX + P = 0$, determinamos suas raízes:

$$X_1 = \beta^{4i}, \quad X_2 = \beta^{4j},$$

e, consequentemente, determinamos i e j.

Por outro lado, usando as duas primeiras equações de (3) temos:

$$x + y = S_1,$$

$$\beta^{4i} x + \beta^{4j} y = S_5,$$

o que implica em

$$x = \frac{S_5 - \beta^{4j} S_1}{\beta^{4i} - \beta^{4j}},$$

$$y = \frac{S_5 - \beta^{4i} S_1}{\beta^{4j} - \beta^{4i}},$$

assim, determinamos k e l, pois $x = \beta^{i+k}$ e $y = \beta^{j+l}$. ■

Lema 4.1 *Com a notação acima adotada, temos:*

a) $S_1 S_9 - S_5^2 \neq 0$, *a não ser que ocorreu apenas um erro.*

b) $\beta^{4j} - \beta^{4i} \neq 0$, *onde* $i, j \in \mathbb{Z}$, $0 \leq i, j \leq 4n$.

Demonstração: *a)* Suponhamos que $S_1 S_9 - S_5^2 = 0$.

Mas

$$S_1 S_9 - S_5^2 = 0, \text{ isto é, } S_1 S_9 = S_5^2,$$

se e somente se,

$$\beta^{8i} S_1 x + \beta^{8j} S_1^2 - \beta^{8j} S_1 x = (\beta^{4i} - \beta^{4j})^2 x^2 + \beta^{8j} S_1^2 + 2\beta^{4j} \left(\beta^{4i} - \beta^{4j}\right) S_1 x.$$

Logo,

$$(\beta^{4i} - \beta^{4j})^2 x^2 + 2\beta^{4j+4i} S_1 x - 2\beta^{8j} S_1 x - \beta^{8i} S_1 x = 0,$$

ou seja,

$$(\beta^{4i} - \beta^{4j})^2 x^2 + 2\beta^{4j+4i} S_1 x - \beta^{8j} S_1 x - \beta^{8i} S_1 x = 0.$$

Portanto,

$$x = 0,$$

ou

$$(\beta^{4i} - \beta^{4j})^2 x + 2\beta^{4j+4i} S_1 - \beta^{8j} S_1 - \beta^{8i} S_1 = 0.$$

Agora,

$$x = 0 \text{ é impossível pois } \beta^{i+k} \neq 0.$$

Se

$$(\beta^{4i} - \beta^{4j})^2 x + 2\beta^{4j+4i} S_1 - \beta^{8j} S_1 - \beta^{8i} S_1 = 0,$$

então,

$$x = \frac{(\beta^{8j} + \beta^{8i} - 2\beta^{4i+4j}) S_1}{(\beta^{4i} - \beta^{4j})^2} = \frac{(\beta^{4i} - \beta^{4j})^2 S_1}{(\beta^{4i} - \beta^{4j})^2} = S_1,$$

se e somente se,

$$y = 0, \text{ isto é, } \beta^{j+l} = 0,$$

o que é um absurdo, a não ser que tenha ocorrido um único erro. Portanto, $S_1 S_9 - S_5^2 \neq 0$, sempre que ocorrerem dois erros.

b) Suponhamos, por absurdo, que $\beta^{4i} - \beta^{4j} = 0$. Mas, $\beta^{4i} = \beta^{4j}$ se, e somente se, $\beta^{4(i-j)} = 1$, portanto, $4n \mid 4(i-j)$. Mas como $4(i-j) \leq 4(n-1) < 4n$, temos uma contradição. ■

Apresentaremos a seguir um procedimento de correção de erros para os códigos do Teorema 4.6.

Algoritmo de decodificação para os códigos definidos no Teorema 4.6

1. Se $S_1 = 0$, então não ocorreram erros, logo $\mathbf{r} = \mathbf{v}$.

2. Se $S_1 S_9 - S_5^2 = 0$, então ocorreu apenas um erro de magnitude β^k, na posição i. Determinamos i e k como no Teorema 4.3.

3. Se $S_1 S_9 - S_5^2 \neq 0$, logo ocorreram dois erros, então procedemos como segue:
   a) Resolvemos a equação $X^2 - SX + P = 0$, onde $S = \beta^{4i} + \beta^{4j}$ e $P = \beta^{4i}\beta^{4j}$, cujas raízes são $X_1 = \beta^{4i}$ e $X_2 = \beta^{4j}$, logo, determinamos i *e* j.
   b) Usando as duas primeiras equações de (3), temos

$$\begin{cases} x + y = S_1 \\ \beta^{4i} x + \beta^{4j} = S_5 \end{cases},$$

o que implica em

$$\begin{cases} x = \frac{S_5 - \beta^{4j} S_1}{\beta^{4i} - \beta^{4j}} \\ \\ y = \frac{S_5 - \beta^{4i} S_1}{\beta^{4j} - \beta^{4i}} \end{cases},$$

daqui determinamos k e l, pois, $x = \beta^{i+k}$ e $y = \beta^{j+l}$.

Exemplo 4.3 *Consideremos* $p = 37 = 4 \cdot 9 + 1$, *logo* $n = 9$. *Sejam* $\mathcal{A}$ *como no Exemplo b) da Seção* 3.2.2 *e* $\beta = -1 - i$. *Portanto, os rótulos* $l \in GF(37)$ *dos elemento* $x + \omega y$ *de* $\mathcal{A}$ *são dados por* $l \equiv x + 31y \pmod{37}$. *Sejam* $\mathcal{C}$ *o código definido pela matriz verificação de paridade* H,

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 \\ 1 & \beta^5 & \beta^{10} & \beta^{15} & \beta^{20} & \beta^{25} & \beta^{30} & \beta^{35} & \beta^4 \\ 1 & \beta^9 & \beta^{18} & \beta^{27} & 1 & \beta^9 & \beta^{18} & \beta^{27} & 1 \\ 1 & \beta^{13} & \beta^{26} & \beta^3 & \beta^{16} & \beta^{29} & \beta^6 & \beta^{19} & \beta^{32} \end{pmatrix}$$

e $\mathbf{r} = (0, 0, \beta^8, 0, 0, \beta^{22}, 0, 0, 0)$, *a palavra recebida, onde* $\beta^8 = -2 - 3i$ *e* $\beta^{22} = -2 - i$, $w^M(\beta^8) = 5$, $w^M(\beta^{22}) = 3$.

A síndrome é dada por

$$S = H\mathbf{r}^t = \begin{pmatrix} \beta^{10} + \beta^{27} \\ \beta^{18} + \beta^{11} \\ \beta^{26} + \beta^{31} \\ \beta^{34} + \beta^{15} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_5 \\ S_9 \\ S_{13} \end{pmatrix}.$$

Portanto,

$$S_1 = \beta^{10} + \beta^{27} \equiv 30 + 31 \equiv 24 \pmod{(\pi)}$$

$$S_5 = \beta^{18} + \beta^{11} \equiv 36 + 2 \equiv 1 \pmod{(\pi)}$$

$$S_9 = \beta^{26} + \beta^{31} \equiv 21 + 24 \equiv 8 \pmod{(\pi)}$$

$$S_{13} = \beta^{34} + \beta^{15} \equiv 3 + 29 \equiv 32 \pmod{(\pi)}.$$

Logo,

$$P = \frac{S_5 S_{13} - S_9^2}{S_1 S_9 - S_5^2} \equiv \frac{1 \cdot 32 - 8^2}{24 \cdot 8 - 1^2} \equiv \frac{5}{6} \equiv 7 \bmod (\pi),$$

$$S = \frac{S_1 S_{13} - S_5 S_9}{S_1 S_9 - S_5^2} \equiv \frac{24 \cdot 32 - 1 \cdot 8}{1} \equiv \frac{20}{6} \equiv 28 \,(\mathrm{mod}\,(\pi)).$$

Assim,

$$X^2 - SX + P = 0, \ \textit{logo,}\ X^2 - 28X + 7 = 0$$

então,

$$X_1 = 16 \equiv \beta^8 \,(\mathrm{mod}\,(\pi)), \ \textit{então,}\ \beta^{4i} = \beta^8, \ \textit{assim}\ i = 2 \ \ (3^{\underline{a}}\ \textit{posição})$$

$$X_2 = 12 \equiv \beta^{20} \,(\mathrm{mod}\,(\pi)), \ \textit{logo,}\ \beta^{4j} = \beta^{20}, \ \textit{portanto,}\ j = 5 \ \ (6^{\underline{a}}\ \textit{posição}).$$

Determinação das magnitudes dos erros:

$$x = \frac{S_5 - \beta^{4j} S_1}{\beta^{4i} - \beta^{4j}} \equiv \frac{1 - 12 \cdot 24}{16 - 12} \equiv \frac{9}{4} \equiv 30 \equiv \beta^{10} \,(\mathrm{mod}\,(\pi)),$$

$$y = \frac{S_5 - \beta^{4i} S_1}{\beta^{4j} - \beta^{4i}} \equiv \frac{1 - 16 \cdot 24}{-4} \equiv \frac{24}{-4} \equiv 31 \equiv \beta^{27} \,(\mathrm{mod}\,(\pi)),$$

ou seja,

$$x = \beta^{i+k} = \beta^{2+k} \equiv \beta^{10} \,(\mathrm{mod}\,(\pi)),$$

$$y = \beta^{j+l} = \beta^{5+l} \equiv \beta^{27} \,(\mathrm{mod}\,(\pi)),$$

logo,

$$k = 8 \quad e \quad l = 22$$

Portanto, ocorreu um erro de magnitude β^8 *na* $3^{\underline{a}}$ *posição e um erro de magnitude* β^{22} *na* $6^{\underline{a}}$ *posição. Então,* $\mathbf{v} = (0,0,0,0,0,0,0,0,0,0)$ *foi a palavra transmitida.*

4.4 Códigos sobre $\mathbb{Z}[\omega]$

Nosso objetivo nesta seção será determinar a capacidade de correção e obter algoritmos de decodificação para códigos construídos sobre o anel $\mathbb{A}$ dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-3}\right)$, o qual é dado por $\mathbb{A} = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-3}}{2}$, conforme vimos na Proposição 2.23.

Sejam p um número primo, $p \equiv 1 \pmod 6$, $\mathfrak{p}$ um ideal primo de $\mathbb{A}$ acima de $p\mathbb{Z}$, $\pi \in \mathbb{A}$ um gerador de $\mathfrak{p}$ e $\mathcal{A}$ um conjunto completo de representantes de $\mathfrak{p}$ em $\mathbb{A}$. Como já vimos na Seção 3.2, podemos considerar $\mathcal{A} \simeq GF(p)$. Seja $\beta \in \mathcal{A}$ um elemento de ordem $6n = p-1$, isto é, $o(\beta) = 6n$. Logo, β é um elemento primitivo e portanto, podemos considerar $\mathcal{A} = (\beta) \cup \{0\}$.

Vamos iniciar esta seção mostrando o análogo do Teorema 4.2, para o caso $\mathbb{Z}[\omega]$, observando que, neste caso, a capacidade de correção de $\mathcal{C}$ é maior do que em [15].

Teorema 4.7 *Seja $\mathcal{C}$ o código definido pela matriz verificação de paridade H,*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \end{pmatrix}.$$

Então $\mathcal{C}$ é capaz de corrigir todo padrão de erro da forma $e(x) = e_i x^i$, onde $w^M(e_i) = 1$ e os padrões de erro $e(x) = \pm\omega^2 x^i$, onde $w^M(\pm\omega^2) = 2$. Portanto, $d^M(\mathcal{C}) \geq 3$.

Demonstração: Recordemos que os elementos de peso 1 do alfabeto $\mathcal{A}$ são ± 1 e $\pm\omega$, onde $\omega = \frac{1+\sqrt{-3}}{2}$ é uma raiz $6^{\underline{a}}$ da unidade. As outras raízes da unidade, a saber, $\pm\omega^2 = \pm(\omega - 1)$, são elementos de peso 2. Notemos que o conjunto $\{\pm 1, \pm\omega, \pm\omega^2\}$ pode ser representado por $\{\beta^{nu},\ u = 1, 2, \cdots, 6\}$. Sem perda de generalidade, podemos supor que a palavra toda nula tenha sido transmitida e que $\mathbf{r} = (0, \cdots, \beta^{nu}, \cdots, 0)$ seja a palavra recebida. Então a síndrome $S = H\mathbf{r}^t$ será dada por:

$$S = \beta^{j+nu} = \beta^L, \text{ onde, } L, j \in \mathbb{Z}, \quad 0 \leq L, j \leq n-1.$$

Reduzindo L módulo n, determinamos j e posteriormente u será determinado por $u = \frac{L-j}{n}$

e assim temos a localização e a magnitude do erro. ■

Exemplo 4.4 *Seja* $p = 37 = 6 \cdot 6 + 1$, *logo* $n = 6$. *Sejam* $\mathcal{A}$ *e* $\beta = 2$ *como no Exemplo e) da Seção* 3.2.2. *Assim, os elementos* $x + \omega y \in \mathcal{A}$ *são rotulados por* $l \in GF(37)$, *onde* $l \equiv x + 27y \pmod{37}$.

a) Seja $\mathbf{r} = (0,0,0,0,\beta^{24},0)$ *a palavra recebida, onde* $\beta^{24} = -\omega$, *logo* β^{24} *é de peso* 1, *a síndrome de* $\mathbf{r}$ *é dada por* S,

$$S = H\mathbf{r}^t = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \end{pmatrix} (0,0,0,0,\beta^{24},0)^t = \beta^{28}.$$

Portanto, $\beta^L = \beta^{28}$, *logo* $L = 28 = j + 6u \equiv j \pmod{6} \equiv 4 \pmod{6}$. *Daí* $j = 4$ *e* $u = 4$. *Assim, o erro ocorreu na* $5^{\underline{a}}$ *posição e seu valor é* β^{24}. *Logo,* $\mathbf{c} = (0,0,0,0,0,0)$ *foi a palavra transmitida.*

b)Seja agora $\mathbf{r} = (0,0,\beta^{30},0,0,0)$ *a palavra recebida, onde* $\beta^{30} = 1 - \omega$. *Logo,* β^{30} *é de peso* 2, *mas é uma raiz* $6^{\underline{a}}$ *da unidade. Assim sendo, a síndrome* S *é dada por*

$$S = H\mathbf{r}^t = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \end{pmatrix} (0,0,\beta^{30},0,0,0)^t = \beta^{32}.$$

Portanto, $\beta^L = \beta^{32}$, *logo,* $L = 32 = j + 6u \equiv j \pmod{6} \equiv 2 \pmod{6}$. *Daí* $j = 2$ *e* $u = 5$. *Assim, o erro ocorreu na* $3^{\underline{a}}$ *posição e seu valor é* β^{30}. *Portanto,* $\mathbf{c} = (0,0,0,0,0,0)$ *foi a palavra transmitida.*

Veremos agora códigos que corrigem um erro de Mannheim de qualquer peso.

Teorema 4.8 *Seja* $\mathcal{C}$ *o código definido pela matriz verificação de paridade* H,

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \cdots & \beta^{7(n-1)} \end{pmatrix}.$$

Então $\mathcal{C}$ *é capaz de corrigir todo padrão de erro do forma* $e(x) = e_i x^i$, *onde* $1 \leq w^M(e_i) \leq d^M_{\max}(\mathcal{A})$, $0 \leq i \leq n-1$. *Portanto,* $d^M(\mathcal{C}) \geq 2d^M_{\max}(\mathcal{A}) + 1$.

Demonstração: Suponhamos que tenha ocorrido um erro de magnitude β^k, $0 \leq k \leq 6n-1$, na posição j, $0 \leq j \leq n-1$. Seja $\mathbf{r} = \left(0, 0, \cdots, \beta^k, \cdots, 0, 0\right)$ a palavra recebida. Assim, a síndrome S é dada por

$$S = H\mathbf{r}^t = \begin{pmatrix} \beta^{j+k} \\ \beta^{7j+k} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_7 \end{pmatrix}.$$

Logo,

$$\beta^{j+k} = S_1 \Rightarrow j + k \equiv L_1 \left(\mathrm{mod}(p-1)\right),$$

$$\beta^{7j+k} = S_7 \Rightarrow 7j + k \equiv L_2 \left(\mathrm{mod}(p-1)\right).$$

O sistema

$$\begin{cases} j + k \equiv L_1 \left(\mathrm{mod}\,(p-1)\right) \\ 7j + k \equiv L_2 \left(\mathrm{mod}\,(p-1)\right) \end{cases},$$

possui uma única solução:

$$\begin{cases} j \equiv \dfrac{L_2 - L_1}{6} \left(\mathrm{mod}\, n\right) \\ k \equiv L_1 - j \left(\mathrm{mod}(p-1)\right) \end{cases}$$

Desse modo, temos que na posição j ocorreu o erro cuja magnitude é β^k. ■

Exemplo 4.5 *Seja* $p = 37 = 6 \cdot 6 + 1$, *logo* $n = 6$. *Sejam* $\mathcal{A}$ *e* $\beta = 2$, *como no Exemplo e) da Seção* 3.2.2. *Portanto, os rótulos* $l \in GF(37)$ *dos elementos* $x + \omega y$ *de* $\mathcal{A}$ *são dados por* $l \equiv x + 27y \left(\mathrm{mod}\, 37\right)$. *Seja* $\mathbf{r} = (0, 0, 0, 0, \beta^{15}, 0)$ *a palavra recebida, onde* $\beta^{15} = 3 - 2\omega$, $w^M(\mathbf{r}) = 5$. *Seja* H *a matriz verificação de paridade,*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^6 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} & \beta^{35} \end{pmatrix}.$$

Então a síndrome da palavra recebida é dada por

$$S = H\mathbf{r}^t = \begin{pmatrix} \beta^{19} \\ \beta^{43} \end{pmatrix},$$

logo,

$$\begin{cases} j+k \equiv 19 (\mathrm{mod}\, 36) \\ 7j+k \equiv 7 (\mathrm{mod}\, 36) \end{cases}.$$

Portanto, $j \equiv \frac{7-19}{6} \equiv -2 \equiv 4 \,(\mathrm{mod}\, 6)$ *e* $k \equiv 19-4 \equiv 15 \,(\mathrm{mod}\, 36)$. *Assim, o erro ocorreu na* $5^{\underline{a}}$ *posição e seu valor é* β^{15}, *isto é,* $\mathbf{e} = (0,0,0,0,\beta^{15},0)$ *foi o erro cometido. Logo,* $\mathbf{c} = (0,0,0,0,0,0)$ *foi a palavra transmitida. Neste caso,* $d^M(\mathcal{C}) \geq 2 \cdot 2 + 1 = 5$.

A seguir veremos códigos que corrigem dois erros de Mannheim de peso um.

Teorema 4.9 *Seja* $\mathcal{C}$ *o código definido pela matriz verificação de paridade* H,

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \beta^{14} & \cdots & \beta^{7(n-1)} \\ 1 & \beta^{13} & \beta^{26} & \cdots & \beta^{13(n-1)} \end{pmatrix}.$$

Então $\mathcal{C}$ *é capaz de corrigir todo padrão de erro da forma* $e(x) = e_i x^i + e_j x^j$, *onde* $w^M(e_i) = w^M(e_j) = 1$, $0 \leq i \neq j \leq n-1$. *Portanto,* $d^M(\mathcal{C}) \geq 5$.

Demonstração: Sejam $\mathbf{v} \in \mathcal{C}$ a palavra transmitida, $\mathbf{e}$ o erro cometido e $\mathbf{r}$ a palavra recebida. Suponhamos que os erros ocorreram nas posições j e k, $0 \leq j, k \leq n-1$ e que suas magnitudes sejam, respectivamente, β^{un} e β^{vn}, $0 \leq u, v \leq 5$. Sejam ainda

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^j & \cdots & \beta^k & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \cdots & \beta^{7j} & \cdots & \beta^{7k} & \cdots & \beta^{7(n-1)} \\ 1 & \beta^{13} & \cdots & \beta^{13j} & \cdots & \beta^{13k} & \cdots & \beta^{13(n-1)} \end{pmatrix}$$

a matriz verificação de paridade e $\mathbf{r} = \begin{pmatrix} 0 & 0 & \cdots & \beta^{un} & \cdots & \beta^{vn} & \cdots & 0 \end{pmatrix}$ a palavra recebida. Então,

$$S = H\mathbf{r}^t = \begin{pmatrix} \beta^{j+un} + \beta^{k+vn} \\ \beta^{7j+un} + \beta^{7k+vn} \\ \beta^{13j+un} + \beta^{13k+vn} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_7 \\ S_{13} \end{pmatrix}$$

é a síndrome. Como $\beta^{6n} = 1$, segue que, $\beta^{un} = \beta^{6un}\beta^{un} = \beta^{7un} = \beta^{12un}\beta^{un} = \beta^{13un}$ (analogamente $\beta^{vn} = \beta^{7vn} = \beta^{13vn}$), e portanto, temos o sistema de equações:

$$\begin{cases} \beta^{j+un} + \beta^{k+vn} = S_1 \\ \beta^{7(j+un)} + \beta^{7(k+vn)} = S_7 \\ \beta^{13(j+un)} + \beta^{13(k+vn)} = S_{13} \end{cases}.$$

Fazendo: $\beta^{j+un} = x$, $\beta^{k+vn} = y$, $S_1 = a$, $S_7 = b$ e $S_{13} = c$ temos:

$$\begin{cases} x + y = a \\ x^7 + y^7 = b \\ x^{13} + y^{13} = c \end{cases}. \tag{4}$$

O código $\mathcal{C}$ será capaz de corrigir toda palavra com dois erros de Hamming, cada um com peso de Mannheim igual a um se, e somente se, o sistema (4) acima admitir somente duas soluções.

Como estamos admitindo que ocorreram dois erros, então temos os seguintes casos a considerar.

1) $a \neq 0$,

2) O sistema em (4) admite pelo menos duas soluções.

1) Mostremos que $a \neq 0$. De fato, suponhamos por absurdo, que ocorreram pelo menos dois erros e que $a = 0$. Mas $a = \beta^{j+un} + \beta^{k+vn} = 0 \Rightarrow \beta^{j+un} = -\beta^{k+vn} \Rightarrow b = \beta^{7(j+un)} + \beta^{7(k+vn)} = (\beta^{j+un})^7 + (\beta^{k+vn})^7 = (-\beta^{k+vn})^7 + (\beta^{k+vn})^7 = 0$.

Portanto, $b = 0$. De modo análogo mostramos que $c = 0$. Mas então a síndrome $S = (a, b, c) = (0, 0, 0)$ e portanto não ocorreram erros, o que é uma contradição.

2) Seja agora (x_0, y_0) uma solução de (5); mostraremos que $x_0 \neq y_0$. De fato : Se $x_0 = \beta^{j+un} = \beta^{k+vn} = y_0$, então $\beta^{k-j+n(v-u)} = 1$, mas $k - j + n(v-u) \leq n - 1 + n \cdot (5) = 6n - 1 < 6n = o(\beta)$, o que é uma contradição. Assim, $x_0 \neq y_0$. Como o sistema (4) é simétrico em relação a x e y, temos então que (y_0, x_0) também é uma solução. Sendo assim, as soluções de (4) ocorrem sempre aos pares.

No sistema (4), fazendo $y = a - x$, teremos os polinômios :

$$f(x) = x^{13} + (a-x)^{13} - c,$$

$$g(x) = x^7 + (a-x)^7 - b,$$

$f, g \in GF(p)[x]$. Seja x_0 uma raiz de $f(x)$, isto é, $f(x_0) = 0$. Agora, $f(a-x_0) = (a-x_0)^{13} + (a-a+x_0)^{13} - c = x_0^{13} + (a-x_0)^{13} - c = f(x_0) = 0$.

Então, $f(x_0) = 0 \Leftrightarrow f(a-x_0) = 0$. Analogamente, este desenvolvimento se aplica para $g(x)$. Portanto, as raízes de $f(x)$ e $g(x)$ ocorrem sempre aos pares. Considerando então os polinômios f e g e usando o Algoritmo de Euclides temos: $\exists\ q,\ h \in GF(p)[x]$ tais que $f(x) = q(x)g(x) + h(x)$, com $\partial(h) \leq 5$. Neste caso $h(x) = \frac{a^2}{7}(b-a^7)[39x^4 - 78ax^3 + 65a^2x^2 - 26a^3x] + \frac{1}{49a}(-29a^{14} + 65a^7b + 13b^2 - 49ac)$. Como as raízes ocorrem sempre aos pares, temos então quatro possibilidades: $h = 0$, $\partial(h) = 2$, $\partial(h) = 3$ ou $\partial(h) = 4$.

Se $\partial(h) = 2$ ou 3 então $b = a^7 \Rightarrow h(x) = a^{13} - c$. Mas como $f(x)$ e $g(x)$ possuem ao menos duas raízes em comum, então $h(x)$ também as possui, logo $h(x)$ é identicamente nulo e portanto, $c = a^{13}$. Assim, estes casos são equivalentes ao caso a) a seguir.

a) Se $\partial(h) = 0$, segue que $h(x)$ é o polinômio identicamente nulo. Mas $h(x) \equiv 0 \Rightarrow a = 0$ ou $b = a^7$ e $c = a^{13}$. Mas $a \neq 0$, pois estamos admitindo que houve pelo menos dois erros. Se $b = a^7$, então $c = a^{13}$ e com isso

$$g(x) = x(x-a)\left(x - \frac{a(1-\sqrt{-3})}{2}\right)^2\left(x - \frac{a(1+\sqrt{-3})}{2}\right)^2 = x(x-a)(x-a\omega)^2\left(x+a\omega^2\right)^2.$$

Assim, as raízes distintas de $g(x)$ são: $x = 0$, $x = a$, $x = \frac{a(1-\sqrt{-3})}{2} = -a\omega^2$ e $x = \frac{a(1+\sqrt{-3})}{2} = a\omega$. Mas $x = 0$ implica em $\beta^{j+un} = 0$, o que é impossível, Também $x = a$ implica em $y = 0$, isto é, $\beta^{k+vn} = 0$ o que também é impossível. Portanto, $g(x)$ possui somente duas raízes distintas. Logo, $f(x)$ e $g(x)$ possuem apenas duas raízes distintas em comum que são $x_1 = a(\omega - 1)$ e $x_2 = a\omega$.

b) Se $\partial(h) = 4$, então aplicando o algoritmo de Euclides aos polinômios g e h, existem

polinômios $s, k \in GF(p)[x]$ tais que $g(x) = s(x)h(x) + k(x)$, onde $\partial(k) \leq 3$. Ora, como as raízes de $f(x)$ e $g(x)$ (consequentemente de $h(x)$ e $k(x)$) ocorrem aos pares, temos que:

c) $\partial(k) = 2$

d) $\partial(k) = 0$

c) Se $\partial(k) = 2$, então $g(x)$ e $h(x)$ (e também $f(x)$) possuem duas raízes em comum, que são exatamente as duas raízes de $k(x)$.

d) Se $\partial(k) = 0$, então $k(x)$ é identicamente nulo, pois estamos admitindo que ocorreram pelo menos dois erros, e portanto, os polinômios $f(x)$, $g(x)$ e $h(x)$ possuem pelo menos duas raízes distintas em comum. Suponhamos $k(x) = k_0 + k_1x + k_2x^2$. Logo,

$$k_0 = 0 \Rightarrow c = \frac{a^{14} + 26a^7b + 169b^2}{196a}, \tag{5}$$

$$k_1 = 0 \Rightarrow c = \frac{4a^{14} + 104a^7b + 39b^2}{147a}, \tag{6}$$

$$k_2 = 0 \Rightarrow c = \frac{4a^{14} + 104a^7b + 39b^2}{147a}. \tag{7}$$

Igualando (6) e (7) temos a seguinte equação do 2^{o} grau em b:

$$m(b) = 637a^{14} + 16562a^7b - 17199b^2.$$

Resolvendo a equação $m(b) = 0$, temos as raízes, $b = a^7$ e $b = \frac{-a^7}{27}$.

O caso $b = a^7$ já examinamos.

Se $b = \frac{-a^7}{27}$ então $c = \frac{a^{13}}{729}$, e neste caso $f(x)$ e $g(x)$ possuem somente as raízes $x_1 = \frac{a\left(3+\sqrt{-3}\right)}{6} = \frac{a}{3}(1+\omega)$ e $x_2 = \frac{a\left(3-\sqrt{-3}\right)}{6} = \frac{a}{3}(2-\omega)$ em comum.

De fato:

$g(x) = \left(x - \frac{a\left(3-\sqrt{-3}\right)}{6}\right)^2\left(x - \frac{a\left(3+\sqrt{-3}\right)}{6}\right)^2\left(x - \frac{a\left(3-\sqrt{-39}\right)}{6}\right)\left(x - \frac{a\left(3+\sqrt{-39}\right)}{6}\right)$ e

$f\left(\frac{a\left(3\pm\sqrt{-39}\right)}{6}\right) \neq 0$, pois $f\left(\frac{a\left(3\pm\sqrt{-39}\right)}{6}\right) = \frac{-a^{13}}{729} + 2\left[\frac{a\left(3\pm\sqrt{-39}\right)}{6}\right]^{13} = a^{13}\left\{\frac{-1}{729} + 2\left[\frac{\left(3\pm\sqrt{-39}\right)}{6}\right]^{13}\right\}$

$= 0 \Leftrightarrow a = 0$, o que é impossível. ■

Obs. 4.3 *Vamos mostrar que este procedimento também se aplica no caso de ocorrer apenas um erro de peso um de Mannheim.*

De fato, suponhamos então que tenha ocorrido um erro de peso um na posição j, $0 \leq j \leq n-1$. *Então:*

$$\begin{cases} x = \beta^{j+un} = a \\ x^7 = \beta^{7(j+un)} = b = a^7 \\ x^{13} = \beta^{13(j+un)} = c = a^{13} \end{cases},$$

ou seja,

$$\begin{cases} x + y = a \\ x^7 + y^7 = b \\ x^{13} + y^{13} = c \end{cases} \tag{8}$$

Analisando o sistema em (8) *temos:*

De $b = a^7$ *e* $c = a^{13}$ *temos que* $h(x)$ *é identicamente nulo. Assim, como vimos no caso a) as raízes comuns a* $f(x)$ *e* $g(x)$ *são* $x = 0$, $x = a$, $x = a(\omega - 1)$ *e* $x = a\omega$. *Portanto, as soluções de* (8) *são* $(a, 0)$, $(0, a)$, $(-a\omega^2, a\omega)$ *e* $(a\omega, -a\omega^2)$.

a) Se $x = 0$, *então* $y = a = \beta^{j+un} = \beta^{L_1}$, *logo,* $j + un = L_1 \equiv j \pmod{n}$. *Portanto, ocorreu um erro na posição* j.

b) Se $x = a$, *então* $y = 0$, *logo* $x = \beta^{j+un} = \beta^{L_1}$, *daí* $j + un = L_1 \equiv j \pmod{n}$. *Portanto, ocorreu um erro na posição* j.

c) Se $x = a\omega$, *então,* $x = \beta^{j+un}\beta^n = \beta^{j+n(u+1)} = \beta^{L_2}$, *logo* $j + n(u+1) = L_2 \equiv j \pmod{n}$. *Portanto, ocorreu um erro na posição* j.

d) Se $x = -a\omega^2$, *temos* $x = \beta^{3n}\beta^{j+un}\beta^{2n} = \beta^{j+n(u+5)} = \beta^{L_3}$, *logo* $j + n(u+5) = L_3 \equiv j \pmod{n}$. *Portanto ocorreu um erro na posição* j.

Assim, se $b = a^7$, *então ocorreu um erro na posição* j.

Com isso, a afirmação fica demonstrada.

Obs. 4.4 *O código $\mathcal{C}$ definido pela matriz verificação de paridade H, do Teorema* 4.9, *também é capaz de corrigir todo padrão de erro do forma $e(x) = e_i x^i + e_j x^j$, onde $w^M(e_i) \leq 2$, $w^M(e_j) \leq 2$, $0 \leq i \neq j \leq n-1$, desde que e_i e e_j sejam raízes sextas da unidade. Assim, eventualmente, $d^M(\mathcal{C}) \geq 9$.*

A seguir fornecemos um procedimento de correção de erros para os códigos do Teorema 4.9.

Algoritmo de decodificação para os códigos definidos no Teorema 4.9

1. Se $a = 0$, então não ocorreram erros, então $\mathbf{v} = \mathbf{r}$.

2. Se $b = a^7$, então ocorreu apenas um erro e procedemos como no Teorema 4.8.

3. Se $b \neq a^7$, então ocorreram dois erros e procedemos como na demonstração do Teorema 4.6, isto é, resolvendo $h(x) = 0$, (ou $g(x) = 0$, ou $k(x) = 0$ conforme o caso), temos as raízes:

$$x_1 = \beta^{j+un} = \beta^{L_1},$$

$$x_2 = \beta^{k+vn} = \beta^{L_2},$$

então

$$j \equiv L_1 \pmod{n},$$

$$k \equiv L_2 \pmod{n},$$

e isto nos dá a localização dos erros.

4. As magnitudes dos erros são dadas por:

$$\beta^{L_1 - j} \quad \text{e} \quad \beta^{L_2 - k}.$$

5. Obtemos a palavra $\mathbf{v} \in \mathcal{C}$ transmitida calculando a diferença: $\mathbf{v} = \mathbf{r} - \mathbf{e}$.

Exemplo 4.6 *Consideremos* $p = 37 = 6 \cdot 6 + 1$, *logo* $n = 6$. *Sejam* $\mathcal{A}$ *e* $\beta = 2$ *como no Exemplo e) da Seção* 3.2.2, *assim os rótulos* $l \in GF(37)$ *dos elementos* $x + \omega y$ *de* $\mathcal{A}$ *são dados por* $l \equiv x + 27y \pmod{37}$.

Sejam $\mathcal{C}$ *o código definido pela matriz verificação de paridade*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} & \beta^{35} \\ 1 & \beta^{13} & \beta^{26} & \beta^3 & \beta^{16} & \beta^{29} \end{pmatrix}$$

e $\mathbf{r} = (0, \beta^6, 0, 0, 0, \beta^{18})$ *a palavra recebida, onde* $\beta^6 = \omega$, $\beta^{18} = -1$; $w^M(\beta^6) = w^M(\beta^{18}) = 1$. *A síndrome* S *é dada por*

$$S = H\mathbf{r}^t = \begin{pmatrix} \beta^7 + \beta^{23} \\ \beta^{13} + \beta^{17} \\ \beta^{19} + \beta^{11} \end{pmatrix} \equiv \begin{pmatrix} 17 + 5 \\ 15 + 18 \\ 35 + 13 \end{pmatrix} (\mathrm{mod}\,(\pi)) = \begin{pmatrix} 22 \\ -4 \\ 11 \end{pmatrix} (\mathrm{mod}\,(\pi)).$$

Portanto,

$$a = 22, \quad b = -4 \quad e \quad c = 11$$

Logo,

$$a^7 = 22^7 = 2 \neq -4 = b,$$

$$-a^7/27 = -2/27 = -2 \cdot 11 = 15 \neq -4 = b.$$

Sejam então:

$$f(x) = x^{13} + (22 - x)^{13} - 11,$$

$$g(x) = x^7 + (22 - x)^7 + 4$$

e $h(x)$ *o resto da divisão de* $f(x)$ *por* $g(x)$. *Então* $h(x) = 29x^4 + 30x^3 + 34x^2 + 32x + 32$. *Dividindo* $g(x)$ *por* $h(x)$ *obtemos o polinômio* $k(x) = 9(x - 17)(x - 5)$.

Agora

$$k(x) = 0 \Leftrightarrow \begin{cases} x_1 = 17 \equiv \beta^7 \pmod{(\pi)} \\ x_2 = 5 \equiv \beta^{23} \pmod{(\pi)} \end{cases},$$

logo,

$$j = L_1 \pmod 6 \equiv 7 \pmod 6 = 1 \,(2^{\underline{a}} \textit{ posição}),$$

$$k = L_2 \pmod 6 \equiv 23 \pmod 6 = 5 \,(6^{\underline{a}} \textit{ posição}).$$

Portanto, os erros ocorreram nas posições $j = 1$ $(2^{\underline{a}})$ *e* $k = 5$ $(6^{\underline{a}})$ *e suas magnitudes são, respectivamente:* $\beta^{7-1} = \beta^6$ *e* $\beta^{23-5} = \beta^{18}$, *e portanto* $\mathbf{c} = (0,0,0,0,0,0)$ *foi a palavra transmitida.*

Finalizando esta seção, veremos códigos que corrigem dois erros de Mannheim de qualquer peso.

Teorema 4.10 *Seja* $\mathcal{C}$ *o código definido pela matriz verificação de paridade* H,

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^7 & (\beta^7)^2 & \cdots & (\beta^7)^{n-1} \\ 1 & \beta^{13} & (\beta^{13})^2 & \cdots & (\beta^{13})^{n-1} \\ 1 & \beta^{19} & (\beta^{19})^2 & \cdots & (\beta^{19})^{n-1} \end{pmatrix}.$$

Então $\mathcal{C}$ *é capaz de corrigir todo padrão de erro da forma* $e(x) = e_i x^i + e_j x^j$, *onde* $1 \leq w^M(e_i), w^M(e_j) \leq d^M_{\max}(\mathcal{A})$, $0 \leq i \neq j \leq n-1$. *Portanto,* $d^M(\mathcal{C}) \geq 4d^M_{\max}(\mathcal{A}) + 1$.

Demonstração: Sejam $\mathbf{v} \in \mathcal{C}$ a palavra transmitida, $\mathbf{e}$ o erro cometido e $\mathbf{r}$ a palavra recebida. Suponhamos que os erros ocorreram nas posições i e j, $0 \leq i, j \leq n-1$ e que seus

valores sejam, respectivamente, β^k e β^l, $0 \leq k, l \leq p-1 = 6n$. Sejam então:

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^i & \cdots & \beta^j & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \cdots & (\beta^7)^i & \cdots & (\beta^7)^j & \cdots & (\beta^7)^{n-1} \\ 1 & \beta^{13} & \cdots & (\beta^{13})^i & \cdots & (\beta^{13})^j & \cdots & (\beta^{13})^{n-1} \\ 1 & \beta^{19} & \cdots & (\beta^{19})^i & \cdots & (\beta^{19})^j & \cdots & (\beta^{19})^{n-1} \end{pmatrix}$$

a matriz verificação de paridade e $\mathbf{r} = \begin{pmatrix} 0 & 0 & \cdots & \beta^k & \cdots & \beta^l & \cdots & 0 \end{pmatrix}$ a palavra recebida. Então,

$$S = H\mathbf{r}^t = \begin{pmatrix} \beta^{i+k} + \beta^{j+l} \\ \beta^{7i+k} + \beta^{7j+l} \\ \beta^{13i+k} + \beta^{13j+l} \\ \beta^{19i+k} + \beta^{19j+l} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_7 \\ S_{13} \\ S_{19} \end{pmatrix}$$

é a síndrome.

Fazendo $x = \beta^{i+k}$ e $y = \beta^{j+l}$, temos o seguinte sistema de equações:

$$\begin{cases} x + y = S_1 \\ \beta^{6i}x + \beta^{6j}y = S_7 \\ \beta^{12i}x + \beta^{12j}y = S_{13} \\ \beta^{18i}x + \beta^{18j}y = S_{19} \end{cases} \tag{9}$$

O código $\mathcal{C}$ será capaz de corrigir dois erros se, e somente se, o sistema acima admitir somente duas soluções. Como estamos supondo que ocorreram pelo menos dois erros, então o sistema admite pelo menos duas soluções. Vamos mostrar que existem somente duas.

De fato: de $x + y = S_1$ temos $y = S_1 - x$, assim o sistema (9) transforma-se em:

$$\begin{cases} y = S_1 - x \\ \beta^{6i}x + \beta^{6j}S_1 - \beta^{6j}x = S_7 \\ \beta^{12i}x + \beta^{12j}S_1 - \beta^{12j}x = S_{13} \\ \beta^{18i}x + \beta^{18j}S_1 - \beta^{18j}x = S_{19} \end{cases},$$

logo,

$$\begin{cases} (\beta^{6i} - \beta^{6j})x = S_7 - \beta^{6j}S_1 \\ (\beta^{12i} - \beta^{12j})x = S_{13} - \beta^{12j}S_1 \\ (\beta^{18i} - \beta^{18j})x = S_{19} - \beta^{18j}S_1 \end{cases},$$

portanto,

$$(\beta^{6i} - \beta^{6j)}x = S_7 - \beta^{6j}S_1, \tag{XI}$$

$$(\beta^{6i} - \beta^{6j})(\beta^{6i} + \beta^{6j})x = S_{13} - \beta^{12j}S_1, \tag{XII}$$

$$(\beta^{6i} - \beta^{6j})\left(\beta^{12i} + \beta^{6i}\beta^{6j} + \beta^{12j}\right)x = S_{19} - \beta^{18j}S_1. \tag{XIII}$$

Agora substituindo (XI) em (XII) e em (XIII) temos:

$$(\beta^{6i} + \beta^{6j})\left(S_7 - \beta^{6j}S_1\right) = S_{13} - \beta^{2j}S_1, \tag{XIV}$$

$$\left(\beta^{12i} + \beta^{6i}\beta^{6j} + \beta^{12j}\right)\left(S_7 - \beta^{6j}S_1\right) = S_{19} - \beta^{18j}S_1. \tag{XV}$$

Sejam $\beta^{6i} + \beta^{6j} = S$ e $\beta^{6i}\beta^{6j} = P$, então temos:

$$S\left(S_7 - \beta^{6j}S_1\right) = S_{13} - \beta^{12j}S_1,$$

$$\left(S^2 - P\right)\left(S_7 - \beta^{6j}S_1\ \right) = S_{19} - \beta^{18j}S_1,$$

daí,

$$SS_7 - \beta^{6j}\beta^{6i}S_1 - \beta^{12j}S_1 = S_{13} - \beta^{12j}S_1, \tag{XVI}$$

$$\left(S^2 - P\right)\left(S_7 - \beta^{6j}S_1\right) = S_{19} - \beta^{18j}S_1. \tag{XVII}$$

De (XVI) temos,

$$SS_7 - PS_1 = S_{13},$$

logo,

$$P = \frac{SS_7 - S_{13}}{S_1}. \tag{XVIII}$$

($S_1 \neq 0$, pois estamos assumindo que ocorrem pelo menos dois erros).

De (XVII) temos:

$$S_7\left(S^2 - P\right) - \beta^{6j} S_1\left(\beta^{12i} + \beta^{6i+6j} + \beta^{12j}\right) = S_{19} - \beta^{18j} S_1 \Rightarrow$$

$$S_7\left(S^2 - P\right) - \beta^{6j+12i} S_1 - \beta^{12j+6i} S_1 - \beta^{18j} S_1 = S_{19} - \beta^{18j} S_1 \Rightarrow$$

$$S_7\left(S^2 - P\right) - \beta^{6j+6i} S_1\left(\beta^{6i} + \beta^{6j}\right) = S_{19} \Rightarrow$$

$$S_7\left(S^2 - P\right) - PSS_1 = S_{19}. \tag{XIX}$$

Substituindo (XVIII) em (XIX) temos:

$$S_7\left(S^2 - \frac{SS_7 - S_{13}}{S_1}\right) - S_1 S \frac{SS_7 - S_{13}}{S_1} = S_{19} \Rightarrow$$

$$S_1 S_7 S^2 - S_7^2 S + S_7 S_{13} - S_1 S_7 S^2 + S_1 S_{13} S = S_1 S_{19} \Rightarrow$$

$$S\left(S_1 S_{13} - S_7^2\right) = S_1 S_{19} - S_7 S_{13} \Rightarrow$$

$$S = \frac{S_1 S_{19} - S_7 S_{13}}{S_1 S_{13} - S_7^2}. \qquad (*) \tag{XX}$$

(*) No Lema 4.2 mostraremos que $S_1 S_{13} - S_7^2 \neq 0$.

Substituindo (XX) em (XVIII) temos:

$$P = \frac{S_7 S_{19} - S_{13}^2}{S_1 S_{13} - S_7^2}.$$

Resolvendo a equação: $X^2 - SX + P = 0$, determinamos suas raízes,

$$X_1 = \beta^{6i}, \quad X_2 = \beta^{6j},$$

e consequentemente, determinamos i e j.

Por outro lado, usando as duas primeiras equações de (9) temos,

$$\begin{cases} x + y = S_1 \\ \beta^{6i}x + \beta^{6j}y = S_7 \end{cases},$$

ou seja

$$\begin{cases} x = \dfrac{S_7 - \beta^{6j}S_1}{\beta^{6i} - \beta^{6j}} \\ y = \dfrac{S_7 - \beta^{6i}S_1}{\beta^{6j} - \beta^{6i}} \end{cases}.$$

Assim, determinamos k e l pois $x = \beta^{i+k}$ e $y = \beta^{j+l}$. ■

Lema 4.2 *Com a notação acima adotada temos:*

a) $S_1S_{13} - S_7^2 \neq 0$, *a não ser que tenha ocorrido somente um erro.*

b) $\beta^{6j} - \beta^{6i} \neq 0$, *onde* $i, j \in \mathbb{Z}$, $0 \leq i, j \leq 6n$.

Demonstração: *a)* Suponhamos que $S_1S_{13} - S_7^2 = 0$.

Mas,

$$S_1S_{13} - S_7^2 = 0, \text{ isto é, } S_1S_{13} = S_7^2,$$

logo,

$$\beta^{12i}S_1x + \beta^{12j}S_1^2 - \beta^{12j}S_1x = (\beta^{6i} - \beta^{6j})^2x^2 + \beta^{12j}S_1^2 + 2\beta^{6j}\left(\beta^{6i} - \beta^{6j}\right)S_1x,$$

então,

$$(\beta^{6i} - \beta^{6j})^2x^2 + 2\beta^{6j+6i}S_1x - 2\beta^{12j}S_1x - \beta^{12i}S_1x = 0,$$

ou seja,

$$(\beta^{6i} - \beta^{6j})^2x^2 + 2\beta^{6j+6i}S_1x - \beta^{12j}S_1x - \beta^{12i}S_1x = 0,$$

portanto,

$$\begin{cases} x = 0 \\ \text{ou} \\ (\beta^{6i} - \beta^{6j})^2 x + 2\beta^{6j+6i} S_1 - \beta^{12j} S_1 - \beta^{12i} S_1 = 0. \end{cases}$$

$$x = 0 \text{ impossível pois } \beta^{i+k} \neq 0.$$

Se

$$(\beta^{6i} - \beta^{6j})^2 x + 2\beta^{6j+6i} S_1 - \beta^{12j} S_1 - \beta^{12i} S_1 = 0,$$

então

$$\frac{(\beta^{12j} + \beta^{12i} - 2\beta^{6i+6j}) S_1}{(\beta^{6i} - \beta^{6j})^2} = \frac{(\beta^{6i} - \beta^{6j})^2 x}{(\beta^{6i} - \beta^{6j})^2},$$

e temos,

$$x = S_1 \text{ logo, } y = 0, \text{ e portanto, } \beta^{j+l} = 0,$$

o que é uma contradição, a não ser que tenha ocorrido apenas um erro. Portanto, $S_1 S_{13} - S_7^2 \neq 0$ sempre que ocorrerem dois erros.

b) Suponhamos, por absurdo, que $\beta^{6i} - \beta^{6j} = 0$

De $\beta^{6i} - \beta^{6j} = 0$, temos $\beta^{6i} = \beta^{6j}$, isto é, $\beta^{6(i-j)} = 1$, portanto, $6n \mid 6(i-j)$ mas como $6(i-j) \leq 6(n-1) < 6n$ temos uma contradição. ■

A seguir apresentamos um procedimento de correção de erros para os códigos do Teorema 4.10.

Algoritmo de decodificação para os códigos definidos no Teorema 4.10

1. Se $S_1 = 0$, então não ocorreram erros, logo $\mathbf{r} = \mathbf{v}$.

2. Se $S_1 S_{13} - S_7^2 = 0$, então ocorreu apenas um erro de magnitude β^k, na posição i. Determinamos i e k como no Teorema 4.8.

3. Se $S_1S_{13} - S_7^2 \neq 0$, logo ocorreram dois erros, então procedemos como segue:

   a) Resolvemos a equação $X^2 - SX + P = 0$, onde $S = \dfrac{S_1S_{19} - S_7S_{13}}{S_1S_{13} - S_7^2}$ e $P = \dfrac{S_7S_{19} - S_{13}^2}{S_1S_{13} - S_7^2}$, cujas raízes são $X_1 = \beta^{6i}$ e $X_2 = \beta^{6j}$, determinamos assim, as posições i e j onde ocorreram os erros.

   b) Para determinarmos as magnitudes β^k e β^l dos erros, primeiro resolvemos o sistema,

$$\begin{cases} x + y = S_1 \\ \beta^{6i}x + \beta^{6j}y = S_7 \end{cases},$$

   determinando

$$x = \frac{S_7 - \beta^{6j}S_1}{\beta^{6i} - \beta^{6j}},$$

   e

$$y = \frac{S_7 - \beta^{6i}S_1}{\beta^{6j} - \beta^{6i}}.$$

   Agora, usando o fato que $x = \beta^{i+k}$ e $y = \beta^{j+l}$, calculamos as magnitudes β^k e β^l dos erros ocorridos.

4. Obtemos a palavra $\mathbf{v} \in \mathcal{C}$ transmitida calculando a diferença: $\mathbf{v} = \mathbf{r} - \mathbf{e}$.

Exemplo 4.7 *Seja* $p = 37 = 6 \cdot 6 + 1$, *logo* $n = 6$. *Sejam* $\mathcal{A}$ *e* $\beta = 2$ *como no Exemplo e) da Seção* 3.2.2. *Assim, os elementos* $x + \omega y$ *de* $\mathcal{A}$ *são rotulados por* $l \in GF(37)$, *onde* $l \equiv x + 27y (\mathrm{mod}\, 37)$.

Sejam $\mathcal{C}$ *o código definido pela matriz verificação de paridade* H,

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} & \beta^{35} \\ 1 & \beta^{13} & \beta^{26} & \beta^3 & \beta^{16} & \beta^{29} \\ 1 & \beta^{19} & \beta^2 & \beta^{21} & \beta^4 & \beta^{23} \end{pmatrix}$$

e $\mathbf{r} = (0, \beta^{11}, 0, 0, 0, \beta^2)$, *a palavra recebida, onde* $\beta^{11} = 3 - \omega$ *e* $\beta^2 = -3 + 3\omega$, $w^M(\beta^{11}) = 4$, $w^M(\beta^2) = 6$.

Temos assim, a síndrome,

$$S = H\mathbf{r}^t = \begin{pmatrix} \beta^{12} + \beta^7 \\ \beta^{18} + \beta \\ \beta^{24} + \beta^{31} \\ \beta^{30} + \beta^{25} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_7 \\ S_{13} \\ S_{19} \end{pmatrix}.$$

Então,

$$S_1 = \beta^{12} + \beta^7 \equiv 26 + 17 \equiv 6 \,(\mathrm{mod}\,(\pi)),$$

$$S_7 = \beta^{18} + \beta \equiv 36 + 2 \equiv 1 \,(\mathrm{mod}\,(\pi)),$$

$$S_{13} = \beta^{24} + \beta^{31} \equiv 10 + 22 \equiv 32 \,(\mathrm{mod}\,(\pi)),$$

$$S_{19} = \beta^{30} + \beta^{25} \equiv 11 + 20 \equiv 31 \,(\mathrm{mod}\,(\pi)).$$

Logo,

$$P = \frac{S_7 S_{19} - S_{13}^2}{S_1 S_{13} - S_7^2} \equiv \frac{1 \cdot 31 - 32^2}{6 \cdot 32 - 1^2} \equiv \frac{6}{6} \equiv 1(\mathrm{mod}\,(\pi)),$$

$$S = \frac{S_1 S_{19} - S_7 S_{13}}{S_1 S_{13} - S_7^2} \equiv \frac{6 \cdot 31 - 1 \cdot 32}{6 \cdot 32 - 1^2} \equiv \frac{6}{6} \equiv 1 \,(\mathrm{mod}\,(\pi)).$$

Portanto,

$$X^2 - SX + P = 0 \text{ ou seja, } X^2 - X + 1 = 0, \text{ assim,}$$

$$X_1 = 27 \equiv \beta^6 \,(\mathrm{mod}\,(\pi)), \text{ logo } \beta^{6i} = \beta^6, \; i = 1 \text{ portanto } (2^{\underline{a}} \text{ posição}),$$

$$X_2 = 11 \equiv \beta^{30} \,(\mathrm{mod}\,(\pi)), \text{ então } \beta^{6j} = \beta^{30}, \text{ assim } j = 5 \;\; (6^{\underline{a}} \text{ posição}).$$

Determinação dos valores dos erros:

$$x = \frac{S_7 - \beta^{6j} S_1}{\beta^{6i} - \beta^{6j}} \equiv \frac{1 - 6 \cdot 11}{27 - 11} \equiv \frac{9}{16} \equiv 26 \equiv \beta^{12} \,(\mathrm{mod}\,(\pi)),$$

$$y = \frac{S_7 - \beta^{6i} S_1}{\beta^{6j} - \beta^{6i}} \equiv \frac{1 - 27 \cdot 6}{27 - 11} \equiv \frac{24}{-4} \equiv 17 \equiv \beta^7 \,(\mathrm{mod}\,(\pi)),$$

ou seja,

$$\begin{array}{l} x = \beta^{i+k} = \beta^{1+k} \equiv \beta^{12} \pmod{(\pi)} \\ y = \beta^{j+l} = \beta^{5+l} \equiv \beta^{7} \pmod{(\pi)} \end{array},$$

logo,

$$k = 11 \quad e \quad l = 2.$$

Portanto, ocorreu um erro de magnitude β^{11} *na* $2^{\underline{a}}$ *posição e um erro de magnitude* β^2 *na* $6^{\underline{a}}$ *posição. Logo,* $\mathbf{v} = (0,0,0,0,0,0)$ *foi a palavra transmitida.*
Neste caso $d^M(\mathcal{C}) \geq 2 \cdot 8 + 1 = 17$.

4.5 Comparação entre códigos sobre $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$

Faremos aqui uma comparação entre códigos sobre $\mathbb{Z}[\omega]$ e $\mathbb{Z}[i]$ quando os alfabetos em consideração possuem o mesmo número de elementos.

Por exemplo, quando $p \equiv 1 \pmod{12}$, temos também que $p \equiv 1 \pmod{4}$ e $p \equiv 1 \pmod{6}$. Neste caso, um código $\mathcal{C}_1$ sobre $\mathbb{Z}[\omega]$ tem comprimento $n_1 = \frac{p-1}{6}$ e um código $\mathcal{C}_2$ sobre $\mathbb{Z}[i]$ tem comprimento $n_2 = \frac{p-1}{4}$. (de acordo com o exposto nas Seções 4.3).

Assim, se as dimensões k_1 e k_2 dos códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ forem iguais a k, (isto é $\mathcal{C}_1$ e $\mathcal{C}_2$ possuem o mesmo número de palavras código), então a taxa $R_{\mathcal{C}_1}$ de $\mathcal{C}_1$ é sempre maior do que a taxa $R_{\mathcal{C}_2}$ de $\mathcal{C}_2$, pois $R_{\mathcal{C}_1} = \frac{6k}{p-1}$ e $R_{\mathcal{C}_2} = \frac{4k}{p-1}$. Dessa forma, o código $\mathcal{C}_1$ irá ocupar uma faixa menor que o código $\mathcal{C}_2$, isto é, $\frac{p-1}{6k} \cdot w$.

Com relação à capacidade de correção temos a seguinte comparação. Se $k = 1$, os códigos sobre $\mathbb{Z}[i]$ são perfeitos, cf [15], isto é, corrigem todo padrão de erro com peso de Mannheim menor ou igual a um e nenhum outro. Por outro lado, os códigos sobre $\mathbb{Z}[\omega]$ com $k = 1$ corrige todo padrão de erro com peso de Mannheim igual a um e alguns outros padrões de erro com peso dois. (Ver Teorema 4.7 e Exemplo 4.4 *b*))

Finalmente, pelo fato de que a constelação de sinais associada a códigos sobre $\mathbb{Z}[i]$ ser um subconjunto do reticulado $\mathbb{Z}^2$ e a constelação de sinais associada a códigos sobre $\mathbb{Z}[\omega]$ ser um subconjunto do reticulado A_2, e sendo A_2 mais denso do que $\mathbb{Z}^2$, temos que a energia

$GF(13)$	Taxa	Energia média
$\mathbb{Z}[\omega]$	$k/2$	1.85
$\mathbb{Z}[i]$	$k/3$	2.15

Tabela 4.1: Comparação entre os códigos sobre $\mathbb{Z}[\omega]$ e $\mathbb{Z}[i]$

$GF(37)$	Taxa	Energia média
$\mathbb{Z}[\omega]$	$k/6$	5.03
$\mathbb{Z}[i]$	$k/9$	6.16

Tabela 4.2: Comparação entre os códigos sobre $\mathbb{Z}[\omega]$ e $\mathbb{Z}[i]$

média gasta para constelações com mesmo número de sinais, é menor no caso $\mathbb{Z}[\omega]$ do que no caso $\mathbb{Z}[i]$. (Ver Tabelas 4.1, 4.2, e 4.3)

4.6 Propriedades da Distância de Hamming dos Códigos sobre $\mathbb{Z}[\omega]$

Sejam $p \equiv 1 \pmod 6$ e $n = \dfrac{p-1}{6}$. Suponhamos $r, t \in \mathbb{Z}$ tais que $0 \leq r < n, t < p-1$ e $(t, p-1) \leq 6$.

$GF(61)$	Taxa	Energia média
$\mathbb{Z}[\omega]$	$k/10$	8.36
$\mathbb{Z}[i]$	$k/15$	10.82

Tabela 4.3: Comparação entre os códigos sobre $\mathbb{Z}[\omega]$ e $\mathbb{Z}[i]$

Considere a matriz H :

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^{t+1} & (\beta^{t+1})^2 & \cdots & (\beta^{t+1})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^{rt+1} & (\beta^{rt+1})^2 & \cdots & (\beta^{rt+1})^{n-1} \end{pmatrix}_{(r+1)\times n},$$

onde β é um elemento primitivo de $\mathcal{A}$, conforme definido na seção anterior. Então temos,

Lema 4.3 *Quaisquer $r+2$ colunas de H são linearmente dependentes (l.d.).*

Demonstração: Imediato, pelo fato de H possuir apenas $r+1$ linhas. ■

Teorema 4.11 *Quaisquer $r+1$ colunas de H são linearmente independentes (l.i.).*

Demonstração: Seja $h_{i_j} = (\beta^{i_j}\ (\beta^{t+1})^{i_j} \cdots (\beta^{rt+1})^{i_j})$, $j = 1, 2, \cdots, r+1$, a $j-$ésima coluna de H.

Considere L a matriz formada pelas colunas $i_1, \cdots, i_{r+1}$ de H, isto é,

$$L = \begin{pmatrix} \beta^{i_1} & \beta^{i_2} & \cdots & \beta^{i_{r+1}} \\ (\beta^{t+1})^{i_1} & (\beta^{t+1})^{i_2} & \cdots & (\beta^{t+1})^{i_{r+1}} \\ \vdots & \vdots & \cdots & \vdots \\ (\beta^{rt+1})^{i_1} & (\beta^{rt+1})^{i_2} & \cdots & (\beta^{rt+1})^{i_{r+1}} \end{pmatrix}.$$

Provar que as $r+1$ colunas de H são l.i. equivale a provar que $\det L \neq 0$.

Mas

$$\det L = \beta^{i_1}\beta^{i_2} \cdots \beta^{i_{r+1}} \det L_1 = \beta^{\sum_{j=1}^{r+1} i_j} \det L_1,$$

onde

$$L_1 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta^{ti_1} & \beta^{ti_2} & \cdots & \beta^{ti_r} \\ \vdots & \vdots & \cdots & \vdots \\ \beta^{rti_1} & \beta^{rti_2} & \cdots & \beta^{rti_r} \end{pmatrix}.$$

Portanto,

$$\det L = 0 \Leftrightarrow \det L_1 = 0.$$

Sabemos que

$$\det L_1 = \pm \prod_{0 \leq j < k \leq r+1} \left(\beta^{ti_j} - \beta^{ti_k}\right)$$

pois $\det L_1$ é um determinante de Vandermonde.

Logo,

$$\det L_1 = 0 \Leftrightarrow \exists j, k \in \mathbb{Z} \text{ com } j < k \text{ tal que } \beta^{ti_j} = \beta^{ti_k}.$$

Agora,

$$\beta^{ti_j} = \beta^{ti_k} \Leftrightarrow \beta^{t(i_j - i_k)} = 1 \Leftrightarrow t\,(i_j - i_k) \equiv 0 \,(\mathrm{mod}\, 6n)\,.$$

Mas,

$$(t, 6n) = s \leq 6 \Rightarrow \left(\frac{t}{s}, \frac{6n}{s}\right) = 1.$$

Suponhamos $t\,(i_j - i_k) \equiv 0 \,(\mathrm{mod}\, 6n)$; disto concluímos que
$6n \mid t\,(i_j - i_k)$, logo, $\dfrac{6n}{s} \mid \dfrac{t}{s}\,(i_j - i_k)$ e daí, $\dfrac{6n}{s} \mid (i_j - i_k)$, pois $\left(\dfrac{t}{s}, \dfrac{6n}{s}\right) = 1$.
Como $6 \geq s$ e $(i_j - i_k) \leq n - 1$, então $\dfrac{6n}{s} \geq n$, e portanto $\dfrac{6n}{s} > (i_j - i_k)$, ou seja, é impossível que $\dfrac{6n}{s} \mid (i_j - i_k)$. Logo $t\,(i_j - i_k) \not\equiv 0 (\mathrm{mod}\, 6n)$ conduzindo a $\beta^{i_j} \neq \beta^{i_k}$ para $i < k$.
Assim, $\det L_1 \neq 0$, e conclui-se que as $r + 1$ colunas de H são $l.i.$ ■

Corolário 4.1 *Seja C o código definido pela matriz verificação de paridade H,*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^{t+1} & (\beta^{t+1})^2 & \cdots & (\beta^{t+1})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^{rt+1} & (\beta^{rt+1})^2 & \cdots & (\beta^{rt+1})^{n-1} \end{pmatrix},$$

com $(t, p-1) \leq 6$, $0 \leq r < \frac{p-1}{6}$, $t < p-1$. Então a distância mínima de Hamming de $\mathcal{C}$ é $d^H(\mathcal{C}) = r+2$. Portanto, $\mathcal{C}$ corrige $\lfloor \frac{r+1}{2} \rfloor$ erros de Hamming.

Corolário 4.2 *Os códigos definidos pela matriz verificação de paridade H, nas condições do Corolário 4.1, são códigos MDS, em relação à distância de Hamming.*

Obs. 4.5 *Todos os resultados desta seção continuam válidos, se considerarmos o número primo $p \equiv 1 \pmod 4$, $n = \frac{p-1}{4}$ e $(t, p-1) \leq 4$ e $\mathbb{A} = \mathbb{Z}[i]$, o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-1}\right)$.*

A demonstração destes fatos é totalmente análoga aos casos anteriores, (Lema 4.1, Teorema 4.3 e Corolários 4.4 e 4.5).

4.7 Correção de Erros Múltiplos

Nosso objetivo nesta seção é fazer uso do algoritmo de Berlekamp-Massey para decodificar códigos sobre anéis de inteiros algébricos, quando ocorrem erros múltiplos de Hamming.

Seja $\mathcal{C}$ o código definido pela matriz verificação de paridade H,

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \beta^{14} & \cdots & \beta^{7(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^{6t+1} & \beta^{2(6t+1)} & \cdots & \beta^{(n-1)(6t+1)} \end{pmatrix}, \tag{10}$$

onde $\beta \in \mathcal{A} \cong GF(p)$, p um inteiro primo, $p \equiv 1 \pmod 6$ e $o(\beta) = 6n$, $t < n$.

Lembremos que, pelo Corolário 4.4, $\mathcal{C}$ é capaz de corrigir $\left\lfloor \frac{t+1}{2} \right\rfloor$ erros de Hamming.

Vamos agora descrever o procedimento de decodificação para o código $\mathcal{C}$, definido pela matriz (10). Tal procedimento é uma adaptação daquele usado na decodificação de códigos BCH, conforme [25]. Como consequência, $\mathcal{C}$ será capaz de corrigir $\left\lfloor \frac{t+1}{2} \right\rfloor$ erros de qualquer peso.

Seja $e(x) = e_{j_1}x^{j_1} + e_{j_2}x^{j_2} + \ldots + e_{j_\nu}x^{j_\nu}$ o padrão de erro, onde $\nu \leq \left\lfloor \frac{t+1}{2} \right\rfloor$ representa o número de posições afetadas na palavra código transmitida.

Suponhamos que as síndromes sejam dadas por:

$T_i = S_{6i-5} = e(\beta^{6i-5}) = e_{j_1}(\beta^{6i-5})^{j_1} + e_{j_2}(\beta^{6i-5})^{j_2} + \ldots + e_{j_\nu}(\beta^{6i-5})^{j_\nu}$, $i = 1, 2, \cdots, t+1$.

Façamos:

$$Y_i = e_{j_i}, \quad i = 1, 2, \cdots, \nu,$$

$$X_i = \beta^{j_i}, \quad i = 1, 2, \cdots, \nu.$$

Então

$$T_i = \sum_{j=1}^{\nu} Y_j \cdot X_j^{6i-5}, \quad i = 1, 2, \cdots, t+1. \tag{11}$$

Seja agora $\sigma(x)$ o polinômio localizador de erros, definido por:

$$\sigma(X) = \prod_{j=1}^{\nu} \left(X - X_j^6\right) = X^\nu + \sigma_1 X^{\nu-1} + \ldots + \sigma_{\nu-1}X + \sigma_\nu, \tag{12}$$

onde $\sigma_1, \sigma_2, \ldots, \sigma_\nu$ são as funções simétricas elementares dos números de localização de erro $X_1^6, X_2^6, \ldots, X_\nu^6$.

Multiplicando-se a equação em (12) por $Y_j X_j^{6i-5}$ e substituindo X por X_j^6, temos:

$$Y_j X_j^{6(i+\nu)-5} + \sigma_1 Y_j X_j^{6(i+\nu-1)-5} + \cdots + \sigma_{\nu-1} Y_j X_j^{6(i+1)-5} + \sigma_\nu Y_j X_j^{6i-5}, \quad 1 \leq j \leq \nu. \tag{13}$$

Agora somando-se as equações em (13) para $1 \leq j \leq \nu$ e substituindo em (11), obtemos:

$$T_{i+\nu} + \sigma_1 T_{i+\nu-1} + \cdots + \sigma_{\nu-1} T_{i+1} + \sigma_\nu T_i = 0, \quad i = 1, 2, \cdots, t+1.$$

Este é o conjunto de equações lineares que relaciona as síndromes aos coeficientes de $\sigma(X)$. As primeiras ν equações podem ser escritas na forma matricial como:

$$\begin{pmatrix} T_1 & T_2 & \cdots & T_\nu \\ T_2 & T_3 & \cdots & T_{\nu+1} \\ \vdots & \vdots & \cdots & \vdots \\ T_\nu & T_{\nu+1} & \cdots & T_{2\nu-1} \end{pmatrix} \begin{pmatrix} \sigma_\nu \\ \sigma_{\nu-1} \\ \vdots \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -T_{\nu+1} \\ -T_{\nu+2} \\ \vdots \\ -T_{2\nu} \end{pmatrix}, \tag{14}$$

onde $T_i = S_{6i-5}$

Esta equação matricial possui solução única se a matriz de síndromes $(T_j)_{\nu\times\nu}$ for não singular.

Proposição 4.1 *A matriz de síndromes:*

$$M = \begin{pmatrix} T_1 & T_2 & \cdots & T_\mu \\ T_2 & T_3 & \cdots & T_{\mu+1} \\ \vdots & \vdots & \cdots & \vdots \\ T_\mu & T_{\mu+1} & \cdots & T_{2\mu-1} \end{pmatrix} = \begin{pmatrix} S_1 & S_7 & \cdots & S_{6\mu-5} \\ S_7 & S_{13} & \cdots & S_{6\mu+1} \\ \vdots & \vdots & \cdots & \vdots \\ S_{6\mu-5} & S_{6\mu+1} & \cdots & S_{12\mu-11} \end{pmatrix},$$

é não singular se $\mu = \nu$. Se $\mu > \nu$ então M é singular.

Demonstração: Consideremos as matrizes:

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ X_1^6 & X_2^6 & \cdots & X_\mu^6 \\ \vdots & \vdots & \cdots & \vdots \\ X_1^{6\mu-6} & X_2^{6\mu-6} & \cdots & X_\mu^{6\mu-6} \end{pmatrix} \text{ e } B = \begin{pmatrix} Y_1X_1 & 0 & \cdots & 0 \\ 0 & Y_2X_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & Y_\mu X_\mu \end{pmatrix}.$$

Calculando-se o produto ABA^T, onde A^T denota a transposta da matriz A, temos $M = ABA^T$. Portanto,

$$\det(M) = \det(A)\det(B)\det(A).$$

Se $\mu = \nu$, então $\det(B) = \prod_{i=1}^{\nu} Y_i X_i$, é não nulo pois os elementos Y_i e X_i são todos não nulos, $i = 1, 2, \cdots, \nu$. Também $\det(A)$ é não nulo, pois A é uma matriz de Vandermonde e os elementos X_i, $i = 1, 2, \cdots, \nu$, são distintos e não nulos. Assim, $\det(M)$ é não nulo, e portanto, M é não singular.

Se $\mu > \nu$, então $X_i = 0$, $i = 1, 2, \cdots, \nu$; logo $\det(B) = 0$, e portanto, $\det(M) = 0$, e assim, a matriz M é singular. ■

Portanto, sempre que ν ou menos posições forem afetadas, o algoritmo será capaz de fazer a correção, resolvendo as equações em (14).

Tais equações nas variáveis $\sigma_1, \sigma_2, \cdots, \sigma_\nu$, podem ser resolvidas eficientemente pelo algoritmo de Berlekamp-Massey. A partir do conhecimento de $\sigma_1, \sigma_2, \cdots, \sigma_\nu$, determinamos o polinômio localizador de erros, como na equação em (12). Suas raízes são $X_1^6, X_2^6, \cdots, X_\nu^6$, onde $X_i = \beta^{j_i}$, $i = 1, 2, \cdots, \nu$ são os números localizadores de erros.

Agora, a partir do conhecimento das variáveis $X_1, X_2, \cdots, X_\nu$, determinamos as magnitudes dos erros através das equações em (11), que na forma matricial são dadas por:

$$\begin{pmatrix} T_1 \\ T_2 \\ \vdots \\ T_{t+1} \end{pmatrix} = \begin{pmatrix} X_1 & X_2 & \cdots & X_\nu \\ X_1^7 & X_2^7 & \cdots & X_\nu^7 \\ \vdots & \vdots & \cdots & \vdots \\ X_1^{6t+1} & T_2^{6t+1} & \cdots & X_\nu^{6t+1} \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_\nu \end{pmatrix}. \tag{15}$$

Ao invés de invertermos a matriz em (15) para encontrar as magnitudes $Y_1, Y_2, \cdots, Y_\nu$, usaremos o procedimento de Forney, como a seguir.

Primeiro definimos as funções simétricas elementares σ_{jl} dos números de localização de

erro $X_1^6, X_2^6, \cdots, X_{j-1}^6, X_{j+1}^6, \cdots, X_\nu^6$ por:

$$\prod_{i \neq j} \left(X - X_i^6\right) = \sum_{l=0}^{\nu-1} \sigma_{jl} \cdot X^{\nu-1-l}. \tag{15}$$

De (12) temos:

$$\prod_{\mu=1}^{\nu} \left(X - X_\mu^6\right) = \sum_{\mu=0}^{\nu-1} \sigma_\mu \cdot X^{\nu-\mu}, \tag{16}$$

onde $\sigma_0 = \sigma_{j,0} = 1$.

De (15) e (16) temos:

$$\left(X - X_j^6\right) \sum_{l=0}^{\nu-1} \sigma_{jl} \cdot X^{\nu-1-l} = \sum_{\mu=0}^{\nu-1} \sigma_\mu \cdot X^{\nu-\mu}. \tag{17}$$

Disso obtemos:

$$\sum_{l=0}^{\nu-1} \sigma_{jl} \cdot X^{\nu-l} - \sum_{l=0}^{\nu-1} \sigma_{jl} \cdot X_j^6 X^{\nu-1-l} = \sum_{\mu=0}^{\nu-1} \sigma_\mu \cdot X^{\nu-\mu} \tag{18}$$

Igualando os coeficientes em (18), temos que os elementos σ_{jl} podem ser obtidos recursivamente, através de X_i e σ_i, por:

$$\sigma_{ji} = \sigma_i + X_j^6 \cdot \sigma_{j,i-1}, \tag{19}$$

para $0 \leq i \leq \nu - 1$, com $\sigma_0 = \sigma_{j,0} = 1$. Assim, denotando a magnitude do l-ésimo erro por Y_l, temos:

$$\sum_{l=0}^{\nu-1} \sigma_{jl} T_{\nu-l} = \sum_{l=0}^{\nu-1} \sigma_{jl} \cdot \sum_{k=1}^{\nu} Y_k X_k^{-5+6(\nu-l)} = \sum_{k=1}^{\nu} Y_k X_k^{-5+6} \cdot \sum_{l=0}^{\nu-1} \sigma_{jl} \cdot X_k^{6(\nu-l-1)}. \tag{20}$$

Usando (15) em (20) , temos:

$$\sum_{l=0}^{\nu-1} \sigma_{jl} T_{\nu-l} = \sum_{k=1}^{\nu} Y_k X_k^{-5+6} \prod_{i \neq j} \left(X_k^6 - X_i^6\right) = Y_j X_j^{-5+6} \cdot \prod_{i \neq j} \left(X_j^6 - X_l^6\right), \tag{21}$$

onde a última igualdade em (21) vale pois na soma mais à direita, somente o termo para o

qual $k = j$ é não nulo. Portanto,

$$\sum_{l=0}^{\nu-1} \sigma_{jl} T_{\nu-l} = Y_j X_j^{-5} \cdot \sum_{l=0}^{\nu-1} \sigma_{jl} \cdot X_j^{6(\nu-l)}. \tag{22}$$

Assim, cada magnitude de erro Y_j, $1 \leq j \leq \nu$, é determinada por:

$$Y_j = \frac{\sum_{l=0}^{\nu-1} \sigma_{jl} \cdot T_{\nu-l}}{X_j^{-5} \cdot \sum_{l=0}^{\nu-1} \sigma_{jl} \cdot X_j^{6(\nu-l)}}, \tag{23}$$

para $1 \leq j \leq \nu$, e onde os σ_{jl} são obtidos recursivamente por:

$$\sigma_{ji} = \sigma_i + X_j^6 \cdot \sigma_{j,i-1}.$$

Exemplo 4.8 *Sejam* $n = 9$, $p = 61$, $\pi = 5 + 4\omega$, $\omega = \frac{1+\sqrt{-3}}{2}$, $\beta = 17$, $o(\beta) = 60$ *e* $\mathcal{A}$ *como no Exemplo f) da Seção* 3.2.2, *logo os elementos* $x + \omega y \in \mathcal{A}$ *são rotulados por* $l \in GF(61)$, *onde* $l \equiv x + 14y \pmod{61}$.

Seja $\mathcal{C}$ o código de comprimento $n = 10$ definido pela matriz verificação de paridade H,

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 & \beta^9 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} & \beta^{35} & \beta^{42} & \beta^{49} & \beta^{56} & \beta^3 \\ 1 & \beta^{13} & \beta^{26} & \beta^{39} & \beta^{52} & \beta^5 & \beta^{18} & \beta^{31} & \beta^{44} & \beta^{57} \\ 1 & \beta^{19} & \beta^{38} & \beta^{57} & \beta^{16} & \beta^{35} & \beta^{54} & \beta^{13} & \beta^{32} & \beta^{51} \\ 1 & \beta^{25} & \beta^{50} & \beta^{15} & \beta^{40} & \beta^5 & \beta^{30} & \beta^{55} & \beta^{20} & \beta^{45} \\ 1 & \beta^{31} & \beta^2 & \beta^{33} & \beta^4 & \beta^{35} & \beta^6 & \beta^{37} & \beta^8 & \beta^{39} \end{pmatrix}.$$

Este código $\mathcal{C}$ corrige até 3 erros de qualquer peso.

Sejam $\mathbf{c} = (0, 0, \ldots, 0)$ a palavra transmitida e $\mathbf{r} = (0, \beta^3, 0, 0, \beta^{36}, 0, 0, 0, \beta^5, 0)$ a palavra recebida, onde, $\beta^3 = -2\omega$, $\beta^5 = 2 - 3\omega$ e $\beta^{36} = 4 - 4\omega$, logo $w^M(\mathbf{r}) = 15$.

A matriz de síndromes M será:

$$M = \begin{pmatrix} T_1 & T_2 & T_3 \\ T_2 & T_3 & T_4 \\ T_3 & T_4 & T_5 \end{pmatrix} = \begin{pmatrix} S_1 & S_7 & S_{13} \\ S_7 & S_{13} & S_{19} \\ S_{13} & S_{19} & S_{25} \end{pmatrix} \equiv \begin{pmatrix} 33 & 43 & 48 \\ 43 & 48 & 31 \\ 48 & 31 & 6 \end{pmatrix} (\mathrm{mod}\, 61)\,.$$

Passo 1) Localização dos erros:

Como $\det(M) = 55 \,(\mathrm{mod}\, 61)$, o sistema (14) possui solução.

$$\begin{pmatrix} 33 & 43 & 48 \\ 43 & 48 & 31 \\ 48 & 31 & 6 \end{pmatrix} \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -T_4 \\ -T_5 \\ -T_6 \end{pmatrix} \equiv \begin{pmatrix} -31 \\ -6 \\ -9 \end{pmatrix} (\mathrm{mod}\, 61)\,, \tag{24}$$

Resolvendo (24) encontramos: $\sigma_1 = 39$, $\sigma_2 = 46$ e $\sigma_3 = -3$. Portanto, o polinômio localizador de erros será:

$$\sigma(X) = X^3 + 39X^2 + 46X - 3$$

$$\sigma(X) = (X+3)(X-52)(X-34)\,(\mathrm{mod}\, 61)\,,$$

$$\sigma(X) = \left(X - \beta^6\right)\left(X - \beta^{24}\right)\left(X - \beta^{48}\right)(\mathrm{mod}\,(\pi))\,.$$

Assim,

$$X_1 = \beta, \quad X_2 = \beta^4, \quad X_3 = \beta^8.$$

Portanto, os erros ocorreram na $2^{\underline{a}}$, $5^{\underline{a}}$ e $9^{\underline{a}}$ posições.

Passo 2) Determinação das magnitudes dos erros:

Sabemos que $T_1 = 33$, $T_2 = 43, T_3 = 48$. Neste caso a relação recursiva e a equação (23)

se apresentam como:

$$\sigma_{ji} = \sigma_i + X_j^6 \cdot \sigma_{j,i-1},\ 0 \leq j \leq 3,\ 1 \leq i \leq 2, \tag{25}$$

onde $\sigma_{j0} = 1$, $j = 1, 2$, e

$$Y_j = \frac{\sum\limits_{l=0}^{2} \sigma_{jl} \cdot T_{\nu-l}}{X_j^{-5} \cdot \sum\limits_{l=0}^{2} \sigma_{jl} \cdot X_j^{6(\nu-l)}},\ 0 \leq j \leq 3,\ 1 \leq i \leq 2. \tag{26}$$

Logo,

a) $j = 1$

$$\sigma_{11} = \sigma_1 + X_1^6 \sigma_{10} = 39 + 52 \equiv 30 (\mathrm{mod}\, 61),$$

$$\sigma_{12} = \sigma_2 + X_1^6 \sigma_{11} = 46 + 52 \cdot 30 \equiv 20 (\mathrm{mod}\, 61),$$

$$Y_1 = \frac{1 \cdot 48 + 30 \cdot 43 + 20 \cdot 33}{32\,(3 + 30 \cdot 20 + 20 \cdot 52)} \equiv 33 \equiv \beta^3\,(\mathrm{mod}\,(\pi))\,.$$

b) $j = 2$

$$\sigma_{21} = \sigma_1 + X_2^6 \sigma_{20} = 39 + 34 \equiv 12 (\mathrm{mod}\, 61),$$

$$\sigma_{22} = \sigma_2 + X_1^6 \sigma_{21} = 46 + 34 \cdot 12 \equiv 27 (\mathrm{mod}\, 61),$$

$$Y_2 = \frac{1 \cdot 48 + 43 \cdot 12 + 33 \cdot 27}{47\,(20 + 12 \cdot 58 + 27 \cdot 34)} \equiv 9 \equiv \beta^{36}\,(\mathrm{mod}\,(\pi))\,.$$

c) $j = 3$

$$\sigma_{31} = \sigma_1 + X_3^6 \sigma_{30} = 39 + 58 \equiv 36 (\mathrm{mod}\, 61),$$

$$\sigma_{32} = \sigma_2 + X_3^6 \sigma_{31} = 46 + 58 \cdot 36 \equiv -1 (\mathrm{mod}\, 61),$$

$$Y_3 = \frac{1 \cdot 48 + 43 \cdot 36 - 1 \cdot 33}{13\,(34 + 36 \cdot 9 - 58)} \equiv 21 \equiv \beta^5\,(\mathrm{mod}\,(\pi))\,.$$

Portanto, ocorreram erros na $2^{\underline{a}}$, $5^{\underline{a}}$ e $9^{\underline{a}}$ posições, com magnitudes β^3, β^{36} e β^5, respectivamente. Logo, $\mathbf{r} = (0, \beta^3, 0, 0, \beta^{36}, 0, 0, 0, \beta^5, 0)$ foi o erro cometido e assim, $\mathbf{c} = \mathbf{r} - e = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$, foi a palavra transmitida.

Exemplo 4.9 *O exemplo que segue visa mostrar o contraste entre o espectro de pesos de um código $\mathcal{C}$, quando consideramos as distâncias de Hamming e de Mannheim.*
Sejam então $p = 61$, $\beta = 3 + \omega \in \mathcal{A}$, como no Exemplo f), da Seção 3.2.2, assim, usando o rotulamento dado por $l \equiv x + 14y \pmod{61}$, temos que $l = 17$ é o rótulo de β.
Seja $\mathcal{C}$ o código definido pela matriz verificação de paridade H

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 & \beta^9 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} & \beta^{35} & \beta^{42} & \beta^{49} & \beta^{56} & \beta^3 \\ 1 & \beta^{13} & \beta^{26} & \beta^{39} & \beta^{52} & \beta^5 & \beta^{18} & \beta^{31} & \beta^{44} & \beta^{57} \\ 1 & \beta^{19} & \beta^{38} & \beta^{57} & \beta^{16} & \beta^{35} & \beta^{54} & \beta^{13} & \beta^{32} & \beta^{51} \\ 1 & \beta^{25} & \beta^{50} & \beta^{15} & \beta^{40} & \beta^5 & \beta^{30} & \beta^{55} & \beta^{20} & \beta^{45} \\ 1 & \beta^{31} & \beta^2 & \beta^{33} & \beta^4 & \beta^{35} & \beta^6 & \beta^{37} & \beta^8 & \beta^{39} \end{pmatrix},$$

ou, após efetuarmos o rotulamento,

$$H = \begin{pmatrix} 1 & 17 & 45 & 33 & 12 & 21 & 52 & 30 & 22 & 8 \\ 1 & 30 & 46 & 38 & 42 & 40 & 41 & 10 & 56 & 33 \\ 1 & 35 & 5 & 53 & 25 & 21 & 3 & 44 & 15 & 37 \\ 1 & 51 & 39 & 37 & 57 & 40 & 27 & 35 & 16 & 23 \\ 1 & 29 & 48 & 50 & 47 & 21 & 60 & 32 & 13 & 11 \\ 1 & 44 & 45 & 28 & 12 & 40 & 52 & 31 & 22 & 53 \end{pmatrix}.$$

O código $\mathcal{C}$ possui um total de 13.845.841 palavras. Segundo a distância de Hamming, C possui 7.200 palavras códigos com peso mínimo $w_{\min}^H(\boldsymbol{c}) = 7$, $\boldsymbol{c} \in \mathcal{C} = \left[10, 4, d^H\right]$, (que $w_{\min}^H(\boldsymbol{c}) = 7$ é uma consequência do Corolário 4.1). Por outro lado, segundo a distância de Mannheim, $\mathcal{C}$ possui 2 palavras códigos com peso mínimo $w_{\min}^M(\boldsymbol{v}) = 13$, $\boldsymbol{v} \in \mathcal{C} = \left[10, 4, d^M\right]$, (uma é a palavra $\boldsymbol{v} = (46, 14, 60, 51, 0, 1, 14, 0, 14, 47)$, a outra é $-\boldsymbol{v}$). Quanto ao peso máximo temos que: o peso máximo de Hamming de uma palavra de $\mathcal{C}$ é 10, enquanto que o peso máximo de Mannheim é 69.

4.8 Conclusões

Neste capítulo foram tratados códigos sobre os anéis de inteiros algébricos de $\mathbb{Q}\left(\sqrt{-1}\right)$ e $\mathbb{Q}\left(\sqrt{-3}\right)$, principalmente com enfoque sobre a distância de Mannheim. Mostramos que tais códigos são MDS com respeito a distância de Hamming.

Todos os códigos sobre $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$ foram caracterizados em termos de suas respectivas matrizes verificação de paridade. Propusemos algoritmos de decodificação para cada classe de códigos proposta. Em particular, o algoritmo de Berlekamp-Massey foi proposto para a decodificação de erros múltiplos de Hamming.

Estabelecemos uma comparação entre códigos sobre $\mathbb{Z}[i]$ e sobre $\mathbb{Z}[\omega]$, a qual mostrou serem os códigos sobre $\mathbb{Z}[\omega]$ *melhores* do que os códigos sobre $\mathbb{Z}[i]$, com relação aos aspectos, taxa, capacidade de correção e energia média.

Capítulo 5

Conclusões e Sugestões

5.1 Conclusões

Nossa proposta, neste trabalho, foi estender os resultados de Huber obtidos em [15], tanto no anel dos inteiros gaussianos, ali tratados, quanto no anel do inteiros algébricos de $\mathbb{Q}\left(\sqrt{d}\right)$, d um inteiro livre de quadrados, além de pesquisar novos resultados envolvendo conjuntos de sinais e a determinação de um alfabeto apropriado $\mathcal{A}$, sobre o qual foram projetados códigos, usando-se a distância de Mannheim.

Com este objetivo, o principal resultado obtido no Capítulo 3, foi a determinação de um procedimento que permite rotular os elementos de um conjunto de sinais $\mathcal{A}$, pelo grupo aditivo de $GF(p)$, onde $\mathcal{A}$ é um conjunto completo de representantes de um ideal primo $\mathfrak{p}$ no anel $\mathbb{A}$ dos inteiros algébricos de uma extensão de grau 2, $K = \mathbb{Q}\left(\sqrt{d}\right)$, d um inteiro livre de quadrados, onde $\mathfrak{p}$ é um ideal primo de $\mathbb{A}$, gerado por um elemento $\pi \in \mathbb{A}$ com norma $N(\pi)$ igual a um número primo p, isto é, $N(\pi) = p$ e p se decompõe completamente em $\mathbb{A}$. Em seguida estendemos o conceito de distância de Mannheim para $\mathcal{A}$, generalizando assim a proposta de Huber em [15]. Determinamos a distância máxima de Mannheim entre dois elementos quaisquer de $\mathcal{A}$, nos casos $d = -1$ e $d = -3$ e mostramos ainda que, quando consideramos $\mathbb{A}$ como um reticulado gerado por $\{1, \omega\}$, $\omega = i$ se $d = -1$ e $\omega = \frac{1+\sqrt{-3}}{2}$ se $d = -3$, este possui um subreticulado $\mathcal{S}$ gerado por $\{\omega, \omega\pi\}$. Determinamos a região de

Voronoi da origem de $\mathcal{S}$ e mostramos que o conjunto de sinais $\mathcal{A}$, rotulado por $GF(p)$, está contido na região de Voronoi da origem de $\mathcal{S}$.

No Capítulo 4, construímos códigos constacíclicos, (com métrica de Mannheim), sobre o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{d}\right)$, $d \in \mathbb{Z}$ livre de quadrados, gerados por um polinômio $g(x)$ que divide $x^n - \omega$, $\omega = i$ se $d = -1$ e $\omega = \frac{1+\sqrt{-3}}{2}$ se $d = -3$. Mostramos que estes códigos, sob a distância de Hamming, são códigos MDS. A seguir, estendemos o trabalho de Huber para códigos sobre um alfabeto $\mathcal{A} \simeq \mathbb{A}/(\pi)$, apresentando algoritmos de decodificação para as classes de códigos estudadas. Em seguida, propusemos códigos sobre $\mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-3}}{2}$, com a distância de Mannheim e apresentamos, também neste caso, quatro classes de códigos, a saber: uma classe proposta para corrigir um erro de Mannheim, outra capaz de corrigir todo padrão de erro que apresenta uma posição alterada, com qualquer peso de Mannheim, isto é, um erro de Hamming, uma outra classe projetada para corrigir dois erros de Mannheim e finalmente uma classe de códigos capaz de corrigir todo padrão de erro que apresenta duas posições alteradas, com qualquer peso de Mannheim, isto é, dois erros de Hamming. Apresentamos, a seguir, o algoritmo de Berlekamp-Massey, adaptado para estes códigos sobre o anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{d}\right)$, $d = -1, -3$. Na Seção 4.7, fizemos uma análise comparativa entre os códigos sobre $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, onde comparamos a taxa k/n do código e a energia média das respectivas constelações de sinais e notamos uma supremacia dos códigos construídos em $\mathbb{Z}[\omega]$ sobre aqueles projetados sobre $\mathbb{Z}[i]$, não somente em relação aos parâmetros acima, mas também quanto a capacidade de correção de erros.

5.2 Sugestões

Durante o desenvolvimento deste trabalho, nos deparamos com tópicos que despertaram nossa atenção e que podem ser objeto de pesquisas futuras. Dentre eles, podemos citar os seguintes:

1. Determinar a verdadeira distância mínima de Mannheim de um código $\mathcal{C}$, ou mesmo uma cota inferior para distância mínima de Mannheim de um código $\mathcal{C}$, $d^M(\mathcal{C})$.

2. Desenvolver um algoritmo de decodificação, do tipo Berlekamp-Massey para a distância de Mannheim.

3. Usar a distância de Mannheim para empacotamento esférico.

4. Construir códigos em extensões de grau 3 (ou maiores) de $\mathbb{Q}$.

5. Considerar o caso onde o ideal primo $\mathfrak{p}$ do anel de inteiros algébricos é inerte, por exemplo, em $\mathbb{Q}(\sqrt{d})$ considerar o conjunto de sinais $\mathcal{A} \simeq \mathbb{A}/\mathfrak{p}$.

6. Generalizar os trabalhos [12] e [5], de Giraud *et al.* e Boutros *et al.*, respectivamente, para uma extensão finita de $\mathbb{Q}$.

Apêndice

Teorema A (Teorema 90 de Hilbert) Sejam $K \supset k$ uma extensão cíclica finita, σ um gerador de $G = Gal(K/k)$ e $\alpha \in K$. Então $N_{K/k}(\alpha) = 1$ se, e somente se, existe $\beta \in K$, não nulo, tal que $\alpha = \frac{\beta}{\sigma(\beta)}$.

Com a notação das Seções 3.1 e 3.2, temos,

Lema A O elemento $\alpha_l \in \mathcal{A}$, $l = 0, 1, \cdots, p-1$, tal que $\alpha_l \equiv l \pmod{(\pi)}$ e $N(\alpha_l)$ mínimo, é único.

Demonstração: De fato, suponhamos que para um dado $l \in \{0, 1, \cdots, p-1\}$ existem α_{l_1}, $\alpha_{l_2} \in \mathcal{A}$ tais que $\alpha_{l_1} \equiv \alpha_{l_2} \pmod{(\pi)}$ e $N(\alpha_{l_1}) = N(\alpha_{l_2})$ mínimas. Se $l = 0$ então, pela minimalidade de $N(\alpha_0)$, $\alpha_0 = 0$ e a unicidade é verificada.

De $N(\alpha_{l_1}) = N(\alpha_{l_2})$, com $\alpha_{l_i} \neq 0$, $i = 1, 2$, temos pelo **Teorema A**,

$$\frac{\alpha_{l_1}}{\alpha_{l2}} = \frac{\beta}{\sigma(\beta)}, \tag{1}$$

para algum $\beta \in \mathbb{Q}(\omega)$.

É claro que se $c \in \mathbb{Q}^*$, então $c\beta$ também é uma solução de (1), de modo que podemos supor $\beta = a + b\omega$, com $a, b \in \mathbb{Z}$ e $(a, b) = 1$.

De (1) obtemos $\alpha_{l_1}\sigma(\beta) = \beta\alpha_{l_2}$, de modo que, se $\beta \in (\pi)$, então $\alpha_{l_1}\sigma(\beta) \in (\pi)$, ou seja, $\sigma(\beta) \in (\pi)$ pois (π) é um ideal primo e $\alpha_{l_1} \notin (\pi)$. Neste caso $\beta \in \sigma(\pi)$ e consequentemente $\beta \in (\pi)(\sigma(\pi)) = p\mathbb{A}$, ou seja, $p \mid (a, b)$, o que é uma contradição, isto é, $\alpha \notin (\pi)$. A condição $(a, b) = 1$ implica que na fatoração do ideal principal (α) não aparecem ideais primos inertes, nem pares de ideais primos distintos conjugados e nem potência maior do que um de ideais primos acima de primos que se ramificam. Assim sendo, podemos supor $\frac{\alpha_{l_1}}{\alpha_{l2}} = \varepsilon\frac{\beta_1}{\sigma(\beta_1)}$, onde os ideais (β_1) e $(\sigma(\beta_1))$ são relativamente primos e ε é uma unidade de $\mathbb{A}$, e portanto, $N(\beta_1)$ divide $N(\alpha_{l_1})$. Por outro lado,

$$N(\alpha_l) \leq \left(\frac{p-1}{2}\right)^2, \tag{2}$$

pela minimalidade de $N(\alpha_l)$; logo

$$N(\beta_1) \leq \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Agora suponhamos $\alpha_{l_1} = a_1 + b_1\omega$ e $\alpha_{l_2} = a_2 + b_2\omega$. De (1) temos, $\frac{a_1+b_1\omega}{a_2+b_2\omega} = \frac{a+b\omega}{\sigma(a+b\omega)}$, portanto, $a_1 + b_1\omega = (a_2 + b_2\omega)\frac{(a+b\omega)^2}{N(a+b\omega)}$.

Caso 1: $K = \mathbb{Q}\left(\sqrt{-1}\right)$, $\omega = i$.

$$\frac{a_1 + b_1 i}{a_2 + b_2 i} = \frac{(a^2 - b^2 + 2abi)}{a^2 + b^2} \Rightarrow$$

$$\begin{cases} a_1 = \frac{a_2\left(a^2-b^2\right)-2abb_2}{a^2+b^2} \\ \\ b_1 = \frac{b_2\left(a^2-b^2\right)+2aba_2}{a^2+b^2} \end{cases}. \tag{4}$$

De $a_1 + b_1 r \equiv a_2 + b_2 r \pmod{p}$ e $N(\alpha) \not\equiv 0 \pmod{p}$, temos:

$$a_2\left(a^2 - b^2\right) - 2abb_2 + \left[2aba_2 + b_2\left(a^2 - b^2\right)\right] r \equiv (a_2 + b_2 r)\left(a^2 + b^2\right) \pmod{p}$$

$$a_2a^2 - a_2b^2 - 2abb_2 + 2aba_2r + b_2a^2r - b_2b^2r \equiv a_2a^2 + a_2b^2 + b_2a^2r + b_2b^2r \pmod{p}$$

$$-2a_2b^2 - 2abb_2 + 2aba_2r - 2b_2b^2r \equiv 0 \pmod{p} \Rightarrow$$

$$a_2b^2 + abb_2 - aba_2r + b_2b^2r \equiv 0 \pmod{p}.$$

1) Se $b \not\equiv 0 \pmod{p}$, então dividindo por b a expressão acima temos

$$a_2b + ab_2 - aa_2r + b_2br \equiv 0 \pmod{p} \Rightarrow$$

$$b(a_2 + b_2r) + a(b_2 - a_2r) \equiv 0 \pmod{p} \Rightarrow$$

$$b(a_2 + b_2r) + \frac{a}{r}(a_2 + b_2r) \equiv 0 \pmod{p}, \text{ pois } r \equiv i \pmod{p},$$

logo

$$(a_2 + b_2 r)\left(\frac{a}{r} + b\right) \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$(a_2 + b_2 r)(a + br) \equiv 0 \,(\mathrm{mod}\, p),$$

portanto,

$$\begin{cases} a_2 + b_2 r \equiv 0 \,(\mathrm{mod}\, p) \\ \qquad\qquad \text{ou} \qquad\qquad \\ a + br \equiv 0 \,(\mathrm{mod}\, p) \end{cases},$$

e isto é um absurdo, pois $a_2 + b_2 r \equiv \alpha_{l_2} \,(\mathrm{mod}\,(\pi))$, $a + br \equiv \beta \,(\mathrm{mod}\,(\pi))$ e ambos são não nulos mod (π).

2) Se $b \equiv 0 \,(\mathrm{mod}\, p)$, temos dois casos a considerar:

i) Se $b = 0$, então de (3), tem-se $\alpha_{l_1} = \alpha_{l_2}$ e a unicidade está verificada.

ii) Se $b \neq 0$, digamos $b = pb'$, $b' \neq 0$, temos $\beta = a + pb'\omega$. É fácil ver que $\beta = \beta_1$ ou $\beta = (1 + i)\beta_1$, isto é, $N(\beta) = N(\beta_1)$ ou $N(\beta) = 2N(\beta_1)$. Visto que $N(\beta) = a^2 + p^2\left(b'\right)^2 \geq p^2$; tem-se que, $N(\beta_1) \geq p^2$ ou $N(\beta_1) \geq p^2/2$, conforme $\beta = \beta_1$ ou $\beta = (1 + i)\beta_1$. Em ambos os casos tem-se uma contradição com (3).

Caso 2: $K = \mathbb{Q}\left(\sqrt{-3}\right)$, $\omega = \frac{1+\sqrt{-3}}{2}$.

De $\omega = \frac{1+\sqrt{-3}}{2}$ temos $\omega^2 = \omega - 1$, portanto $(a + b\omega)^2 = a^2 + 2ab\omega + b^2\omega^2 = a^2 - b^2 + (2ab + b^2)\omega$. Assim, de

$$a_1 + b_1\omega = (a_2 + b_2\omega)\frac{(a + b\omega)^2}{N(a + b\omega)},$$

temos

$$a_1 + b_1\omega = (a_2 + b_2\omega)\frac{a^2 - b^2 + (2ab + b^2)\omega}{a^2 + ab + b^2} \Rightarrow$$

$$a_1 + b_1\omega = \frac{a^2a_2 - b^2a_2 - 2abb_2 - b^2b_2 + (2aba_2 + 2abb_2 + b^2a_2 + a^2b_2)\omega}{a^2 + ab + b^2},$$

portanto,

$$\begin{cases} a_1 = \frac{a^2a_2 - b^2a_2 - 2abb_2 - b^2b_2}{a^2+ab+b^2} \\ \\ b_1 = \frac{2aba_2 + 2abb_2 + b^2a_2 + a^2b_2}{a^2+ab+b^2} \end{cases} . \tag{4}$$

De $a_1 + b_1 r \equiv a_2 + b_2 r \,(\mathrm{mod}\, p)$, e $N(\alpha) \not\equiv 0 \,(\mathrm{mod}\, p)$, temos

$$a^2a_2 - b^2a_2 - 2abb_2 - b^2b_2 + 2aba_2r + 2abb_2r + b^2a_2r + a^2b_2r \equiv$$

$$\equiv a^2a_2 + aba_2 + b^2a_2 + a^2b_2r + abb_2r + b^2b_2r \,(\mathrm{mod}\, p) \Rightarrow$$

$$b^2a_2r + abb_2r + 2aba_2r - b^2b_2 - 2abb_2 - b^2a_2 - aba_2 - b^2a_2 - b^2b_2r \equiv 0 \,(\mathrm{mod}\, p) .$$

1) Se $b \not\equiv 0 \,(\mathrm{mod}\, p)$, temos

$$ba_2r + ab_2r + 2aa_2r - bb_2 - 2ab_2 - ba_2 - aa_2 - ba_2 - bb_2r \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$ba_2(r-1) + ab_2(r-1) + aa_2(r-1) - bb_2(r+1) - ab_2 - ba_2 + aa_2r - aa_2 + aa_2 \equiv 0 \,(\mathrm{mod}\, p)$$

$$(r-1)(ba_2 + ab_2 + aa_2) - (ab_2 + ba_2 + aa_2) + aa_2 + aa_2r - bb_2r - bb_2 \equiv 0 \,(\mathrm{mod}\, p)$$

$$(ba_2 + ab_2 + aa_2)(r - 1 - 1) + aa_2(r+1) - bb_2(r+1) \equiv 0 \,(\mathrm{mod}\, p) .$$

Como $r \equiv \omega \,(\mathrm{mod}\,(\pi))$, temos $r^2 \equiv r - 1 \,(\mathrm{mod}\,(\pi))$, logo $r - 2 \equiv r^2 - 1 \,(\mathrm{mod}\,(\pi))$. Assim,

$$(ba_2 + ab_2 + aa_2)(r-1)(r+1) + aa_2(r+1) + (r+1)(aa_2 - bb_2) \equiv 0 \,(\mathrm{mod}\, p)$$

$$(r+1)\left[(ba_2 + ab_2 + aa_2)(r-1) + (aa_2 - bb_2)\right] \equiv 0 \,(\mathrm{mod}\, p) .$$

Visto que $p \equiv 1 \,(\mathrm{mod}\, 6)$ e $N(1+\omega) = 3$ segue que, $\omega + 1 \notin (\pi)$, isto é $r + 1 \not\equiv 0 \,(\mathrm{mod}\, p)$. Portanto,

$$(ba_2 + ab_2 + aa_2)(r-1) + (aa_2 - bb_2)] \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$ba_2r + ab_2r + aa_2r - ba_2 - ab_2 - aa_2 + aa_2 - bb_2 \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$ar\,(a_2 + b_2) - b\,(a_2 + b_2) + ba_2r - ab_2 \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$(a_2 + b_2)\,(ar - b) + ba_2r - ab_2 \equiv 0 \,(\mathrm{mod}\, p)\,.$$

Como ω é uma unidade de $\mathbb{A}$, temos $r \not\equiv 0 \,(\mathrm{mod}\, p)$. Logo, multiplicando-se a equação acima por r temos:

$$(a_2 + b_2)\,(ar - a - br) + ba_2r - ba_2 - ab_2r \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$-\,(a + br)\,(a_2 + b_2) + aa_2r + ab_2r + ba_2r - ba_2 - ab_2r \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$-\,(a + br)\,(a_2 + b_2) + a_2(ar - b) + ba_2r \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$-\,(a + br)\,(a_2 + b_2) + \frac{a_2}{r}(ar - a - br) + ba_2r \equiv 0 \,(\mathrm{mod}\, p)\,,\ \text{pois}\ \frac{1}{r} = 1 - r,$$

logo,

$$-\,(a + br)\,(a_2 + b_2) - \frac{a_2}{r}(a + br) + aa_2 + ba_2r \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$-\,(a + br)\left(a_2 + b_2 + \frac{a_2}{r}\right) + a_2(a + br) \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow$$

$$-\,(a + br)\,(a_2 + b_2 + a_2 - a_2r - a_2) \equiv 0 \,(\mathrm{mod}\, p)\,.$$

Como $a + br \not\equiv 0 \,(\mathrm{mod}\, p)$, temos

$$a_2 + b_2 - a_2r \equiv 0 \,(\mathrm{mod}\, p) \Rightarrow a_2(r - 1) \equiv b_2 \,(\mathrm{mod}\, p)\,.$$

Logo,

$$a_2 + b_2r \equiv a_2 + a_2\,(r - 1)\,r \equiv a_2 + a_2r^2 - a_2r \equiv a_2 + a_2r - a_{2\_}a_2r \equiv 0 \,(\mathrm{mod}\, p)\,.$$

Portanto,

$$a_2 + b_2r \equiv 0 \,(\mathrm{mod}\, p)\,,$$

o que é uma contradição.

2) Se $b \equiv 0 \pmod{p}$, temos dois casos a analisar:

i) Se $b = 0$, então de (4), tem-se $\alpha_{l_1} = \alpha_{l_2}$ e a unicidade está verificada.

ii) Se $b \neq 0$, digamos $b = pb'$, $b' \neq 0$, temos $\beta = a + pb'\omega$. É fácil ver que $\beta = \beta_1$ ou $\beta = (1+\omega)\beta_1$, isto é, $N(\beta) = N(\beta_1)$ ou $N(\beta) = 3N(\beta_1)$. Visto que $N(\beta) = a^2 + apb' + p^2\left(b'\right)^2 \geq \frac{3\left(pb'\right)^2}{4}$, tem-se que, $N(\beta_1) \geq \frac{3\left(pb'\right)^2}{4} \geq \left(\frac{p-1}{2}\right)^2$ ou $N(\beta_1) \geq \frac{\left(pb'\right)^2}{4} \geq \left(\frac{p-1}{2}\right)^2$, conforme $\beta = \beta_1$ ou $\beta = (1+\omega)\beta_1$. Em ambos os casos tem-se uma contradição com (3). ■

Bibliografia

[1] Berlekamp, E.R., *Algebraic Coding Theory,* New York: McGraw-Hill, 1968.

[2] Biglieri, E., Elia, M., "On the construction of group block codes", *Annales des Télécommunications*, Tome 50, n. 9-10, p. 817-823, Set.-Out. 1995.

[3] Blake, I.F., "Codes over certain rings", Inform. Contr. v. 20, p. 396-404, 1972.

[4] Blake I.F., "Codes over integer residue rings", Inform. Contr. v. 29, p. 295-300, 1975.

[5] Boutros J., Viterbo E., Castelo C., Belfiore J.-C., "Good lattice constellations for both Rayleigh fading and Gaussian channels", *IEEE Trans. Inform. Theory,* v. 42, n. 2, p. 502-518, Mar. 1996 .

[6] Conway J. H., Sloane N.J.A., *Sphere Packings, Lattices and Groups,* New York: Springer-Verlag, 1988.

[7] Engler, A.J., Brumatti P., *Anéis de Inteiros Quadráticos*, In: XII Escola de Álgebra, 1992, Diamantina, M.G., Campinas, IMECC-UNICAMP, 1995.

[8] Forney, Jr. G.D., "On decoding BCH codes", *IEEE Trans. Inform. Theory*, v. 11, p. 549-557, Out. 1965.

[9] Forney Jr., G.D., "Coset codes I: Introduction and geometrical classification", *IEEE Trans. Inform. Theory*, v. 34, p. 1123-1151, Set. 1988.

[10] Forney Jr., G.D., "Coset codes II: Binary lattices and related codes", *IEEE Trans. Inform. Theory*, v. 34, p. 1152-1187, Set. 1988.

[11] Forney Jr., G.D., "Geometrically uniform codes", *IEEE Trans. Inform. Theory*, v. 37, p. 1241-1260, Set. 1991.

[12] Giraud, X., Belfiore, J.-C., "Constellations matched to Rayleigh fading channel", *IEEE Trans. Inform. Theory,* v. 42, n. 1, p. 106-115, Jan. 1996.

[13] Gonçalves A., *Introdução à Álgebra,* Rio de Janeiro, Instituto de Matemática Pura e Aplicada, CNPq, 1979.

[14] Herstein I.N., *Tópicos de Álgebra*, São Paulo, Editora da Universidade de São Paulo e Editora Polígono, 1970.

[15] Huber, K., "Codes over Gaussian integers", *IEEE Trans. Inform. Theory*, v. 40, n. 1, p. 207-216, Jan. 1994.

[16] Interlando J.C., "Uma contribuição à construção e decodificação de códigos lineares sobre grupos abelianos via concatenação de códigos sobre anéis de inteiros residuais". Tese de Doutorado, FEE-Unicamp, Dez. 1994.

[17] Lang S., *Algebra,* Reading, Mass: Addison-Wesley, 1972.

[18] Lin. S., Costelo Jr. D.J., *Error Control Coding*, Prentice-Hall, Inc., 1983.

[19] van Lint, J.H., *Introduction to Coding Theory,* 2.ed., Berlim Heidelberg: Springer-Verlag, 1992.

[20] Loeliger, H.-A., "Signal sets matched to groups", *IEEE Trans. Inform. Theory*, v.. 37, n. 6, p. 1675-1682, Nov. 1991.

[21] MacWilliams, F.J., Sloane N.J.A., *The Theory of Error Correting Codes,* North-Holland Publishing Company, 1977.

[22] Marcus, D.A., *Number Fields*, New York: Springer Verlag, 1977.

[23] Massey, J.L., "Shift register synthesis and BCH decoding", *IEEE Trans. Inform. Theory*, v. IT-15, p. 122-127, Jan. 1969.

[24] Massey, J.L., Mittelholzer, T., Riedel, T., Vollenweider, M., "Ring convolutional codes for phase modulation", *IEEE Int. Symp. Inform. Theory*, San Diego, CA, Jan. 14-19, 1990.

[25] Peterson, W.W., Weldon Jr., E.J., *Error Correting Codes*, 2.ed., Cambridge, Mass: MIT Press, 1972.

[26] Samuel, P., *Algebraic Theory of Numbers*, Paris, France: Hermann, 1971.

[27] Shankar, P., "On BCH codes over arbitrary integer rings", *IEEE Trans. Inform. Theory*, v. IT-25, n. 4, p. 480-483, Jul. 1979.

[28] Slepian, D., "Groups codes for the Gaussian channel", Bell Syst. Tech. J., v. 37, p. 575-602, 1968.

[29] Spiegel, E., "Codes over $\mathbb{Z}_m$", *Inform. and Control*, n. 35, p. 48-51, 1977.

[30] Spiegel, E., "Codes over $\mathbb{Z}_m$, revisited", *Inform. and Control*, n. 37, p. 100-104, 1978.