Universidade de Brasília

Formas de grau $3m$ sobre extensões quadráticas de $\mathbb{Q}_3$

Bruna Maria Frutuoso

Orientador: Hemar Teixeira Godinho

Departamento de Matemática

Universidade de Brasília

Brasília

2024

À minha mãe.

Seu apoio e sua fé em mim foram minha maior força.

Esta tese é para você, com todo meu amor e gratidão.

Agradecimentos

Agradeço primeiramente a Deus, por abençoar minha trajetória desde o início, por me dar a coragem para ir atrás dos meus sonhos e a certeza do caminho que escolhi.

À minha família, que sempre acreditou em mim e não mediu esforços para me apoiar, vibrou comigo a cada conquista no caminho e me levantou quando as coisas não iam bem. Eu estou aqui, hoje, por causa de vocês!

Ao meu orientador, Professor Hemar Godinho, por guiar meus primeiros passos no universo da pesquisa. Obrigada por me animar nos momentos difíceis e me ensinar tanto sobre a matemática e sobre a vida.

Aos professores que eu tive ao longo da minha trajetória, por me darem os exemplos e repertórios certos para que eu possa também ser uma professora que inspira meus alunos.

Aos meus amigos, aqueles da época da OBMEP, aos bons da UFV e aos que fiz em Brasília e na UnB, que me inspiram tanto e que eu tenho o privilégio de compartilhar a caminhada acadêmica.

À OBMEP, que há 12 anos despertou em mim o brilho nos olhos pela matemática e proporcionou, através do PICME, que eu chegasse tão longe quanto eu quisesse.

"Ninguém pode crescer se não aceitar que é pequeno."
Papa Francisco

Resumo

Sejam K uma extensão finita de $\mathbb{Q}_p$, o corpo nos números p-ádicos, e $\mathcal{O}_K$ o anel de inteiros de K. Seja

$$f = a_1 x_1^d + \cdots + a_s x_s^d$$

com $a_1, \ldots, a_s \in \mathcal{O}_K$. Defina $\Gamma_K^*(d)$ como sendo o menor inteiro positivo tal que $f = 0$ tem solução não trivial em K sempre que $s \geq \Gamma_K^*(d)$, independentemente da escolha dos coeficientes de f. Em 2021, Duncan e Leep estudaram formas de grau $2m$ com $m \geq 3$ ímpar sobre extensões quadráticas ramificadas de $\mathbb{Q}_2$ e mostraram que

$$\Gamma_K^*(d) = \begin{cases} \frac{3}{2}d & \text{para} \quad K \in \{\mathbb{Q}_2(\sqrt{\pm 2}), \mathbb{Q}_2(\sqrt{\pm 10}\}, \\ d+1 & \text{para} \quad K \in \{\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{-5})\}. \end{cases}$$

Neste trabalho, estudamos o caso em que K é uma extensão quadrática de $\mathbb{Q}_3$ e $d = 3m$ com $(3, m) = 1$ e $m \geq 2$. Obtemos que $\Gamma_K^*(d) \leq 3d+1$ quando d é ímpar e $\Gamma_K^*(d) \leq 14d+1$ quando d é par. Obtemos também uma estimativa para $\Gamma_K^*(d)$ com K extensão quadrática de $\mathbb{Q}_p$ e $d = pm$ com $(p, m) = 1$ e $m \geq 2$. Como aplicação, determinamos limitantes para $\Gamma_K^*(15)$ e $\Gamma_K^*(6)$ com $K/\mathbb{Q}_p$ quadrática.

Palavras-chave: Formas diagonais, extensões quadráticas, corpos p-ádicos.

Abstract

Let K be a finite extension of $\mathbb{Q}_p$, the field of the p-adic numbers, and $\mathcal{O}_K$ the ring of integers of K. Let

$$f = a_1 x_1^d + \cdots + a_s x_s^d$$

with $a_1, \ldots, a_s \in \mathcal{O}_K$. Let $\Gamma_K^*(d)$ denote the smallest positive integer such that $f = 0$ has nontrivial solution in K whenever $s \geq \Gamma_K^*(d)$, regardless of the choice of coefficients from K. In 2021, Duncan and Leep studied forms of degree $2m$, $m \geq 3$ odd over the ramified quadratic extensions of $\mathbb{Q}_2$ and showed that

$$\Gamma_K^*(d) = \begin{cases} \frac{3}{2}d & \text{for} \quad K \in \{\mathbb{Q}_2(\sqrt{\pm 2}), \mathbb{Q}_2(\sqrt{\pm 10}\}, \\ d+1 & \text{for} \quad K \in \{\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{-5})\}. \end{cases}$$

In this thesis, we study the case where K is a quadratic extension of $\mathbb{Q}_3$ and $d = 3m$ with $(3, m) = 1$ and $m \geq 2$. We obtain $\Gamma_K^*(d) \leq 3d+1$ for d odd and $\Gamma_K^*(d) \leq 14d+1$ for d even. We also obtain an estimate for $\Gamma_K^*(d)$ for K a quadratic extension of $\mathbb{Q}_p$ and $d = pm$ with $(p, m) = 1$ and $m \geq 2$. As an application, we determine bounds for $\Gamma_K^*(15)$ and $\Gamma_K^*(6)$ with $K/\mathbb{Q}_p$ quadratic.

Keywords: Diagonal forms, quadratic extensions, p-adic fields.

Sumário

Introdução

Em 1933, Tsen [30] mostrou que se f é uma forma (polinômio homogêneo) em s variáveis e grau d com coeficientes no corpo K de funções em uma variável sobre um corpo algebricamente fechado, então $f = 0$ tem solução não trivial em K quando $s > d$. Pouco depois, em 1935, Chevalley [3] mostrou que corpos finitos satisfazem a mesma propriedade.

As técnicas usadas na prova do resultado de Tsen podem ser estendidas para mostrar que se K é um corpo de funções em i variáveis sobre um corpo finito, então toda forma de grau d em mais de d^{i+1} variáveis tem zero não trivial em K (veja [10]). Com a terminologia introduzida em 1951 por Lang em sua tese de doutorado [16], corpos que satisfazem a condição acima são chamados C_{i+1}. Em 1952, Lang [17] mostrou que $\mathbb{F}_q((X))$, o corpo das séries meromórficas sobre $\mathbb{F}_q$, é C_2.

Na década de 1930, Emil Artin conjecturou que se K é um corpo p-ádico (uma extensão finita de $\mathbb{Q}_p$), então K é C_2. A conjectura permaneceu em aberto até 1966, quando Terjanian [27] mostrou que a forma

$$g(\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{t},\mathbf{u},\mathbf{v}) = f(\mathbf{x}) + f(\mathbf{y}) + f(\mathbf{z}) + 4(f(\mathbf{t}) + f(\mathbf{u}) + f(\mathbf{v}))$$

onde

$$f(\mathbf{x}) = x_1^4 + x_2^4 + x_3^4 - (x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2) + x_1x_2x_3(x_1 + x_2 + x_3)$$

é uma forma de grau 4 em $18 > 4^2 + 1$ variáveis que não possui zero não trivial em $\mathbb{Q}_2$. Depois disso, outros contraexemplos surgiram (veja, por exemplo, em [10]), mas nenhum deles é uma forma diagonal. Assim, ao impor a diagonalidade sobre a forma f, a conjectura de Artin ainda é um problema em aberto e tem intrigado muitos matemáticos mundo afora. É a essa versão da conjectura que nos referimos quando mencionamos a conjectura de Artin.

Sejam K uma extensão finita de $\mathbb{Q}_p$ e

$$f = a_1 x_1^d + \cdots + a_s x_s^d$$

com $a_i \in K$ para $i = 1, \ldots, s$. Defina $\Gamma_K^*(d)$ como sendo o menor inteiro positivo tal que $f = 0$ tem solução não trivial em K sempre que $s \geq \Gamma_K^*(d)$. Com essa notação, a conjectura de Artin afirma que $\Gamma_K^*(d) \leq d^2 + 1$. A conjectura foi provada ser verdadeira para vários casos particulares e, em alguns desses casos, limitantes melhores que o conjecturado foram determinados.

Para $K = \mathbb{Q}_p$, a conjectura foi estabelecida para todo grau d por Davenport e Lewis [4]. Eles também mostraram que esse limitante é o melhor possível quando $d+1$ é primo. Além disso, eles introduziram o método de *contração de variáveis* que desde então tem sido útil para estudar a solubilidade de formas diagonais não só em $\mathbb{Q}_p$, mas também em suas extensões finitas e, inclusive, é uma das ferramentas do nosso trabalho. Quando d é ímpar, o trabalho de Tietäväinen [29] estabelece que

$$\limsup_{d \to \infty} \frac{\Gamma_{\mathbb{Q}_p}^*(d)}{d \log d} = \frac{1}{\log 2},$$

indicando um limitante assintoticamente da ordem $d \log_2 d$ para $\Gamma_{\mathbb{Q}_p}^*(d)$ e, portanto, limitantes bem menores que o da conjectura são esperados quando d é ímpar. Valores exatos para $\Gamma_{\mathbb{Q}_p}^*(d)$ são conhecidos para $d \leq 64$ (veja [13] e [1] para mais detalhes).

Quando K é uma extensão finita arbitrária de $\mathbb{Q}_p$, em 1923, Siegel [25] mostrou que $\Gamma_K^*(2) = 5$ e em 1957, Lewis [19] mostrou que $\Gamma_K^*(3) = 7$. Dois anos depois, Gray, então aluno de Lewis, [9] generalizou seu resultado para $d = p$ primo ímpar, obtendo

$$\Gamma_K^*(p) \leq p(p-1) + 1$$

e, exceto no caso em que K é uma extensão finita de $\mathbb{Q}_5$, mostrou que $\Gamma_K^*(5) = 16$. Quando p não é um divisor de d, o Lema de Hensel [11] em conjunto com o resultado de Chevalley [3] prova que $\Gamma_K^*(d) \leq d^2 + 1$ e o limitante conjecturado é atendido. A dificuldade surge quando p é um divisor de d. Até os dias atuais, o resultado geral que chegou mais perto da conjectura foi obtido em 2020 por Skinner [26]. Ele mostrou, para d e K arbitrários, que

$$\Gamma_K^*(d) \leq \begin{cases} 8d^2+1 & \text{se } p=2, \\ 3d^2+1 & \text{se } p>2. \end{cases}$$

Ao especificar a ramificação da extensão $K/\mathbb{Q}_p$, resultados importantes na direção da conjectura de Artin foram obtidos. Em 2018, Leep e Vieira [18] mostraram que a conjectura é verdadeira para K uma extensão finita não ramificada de $\mathbb{Q}_p$ com $p \geq 3$. Em 2022, Miranda, Godinho e Knapp [5] garantiram a conjectura para $K/\mathbb{Q}_2$ quadrática não ramificada quando d não é potência de 2. No outro extremo, para K totalmente ramificada, há resultados interessantes quando $K/\mathbb{Q}_2$ é quadrática. Knapp [14] mostrou em 2019 que

$$\Gamma_K^*(6) = 9 \text{ para } K \in \{\mathbb{Q}_2(\sqrt{\pm 2}), \mathbb{Q}_2(\sqrt{\pm 10})\} \text{ e}$$

$$7 \leq \Gamma_K^*(6) \leq 9 \text{ para } K \in \{\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{-5}\},$$

conjecturando que $\Gamma_K^*(6) = 7$ para os últimos dois casos. Em 2021, Duncan e Leep [6, 7] mostraram que a conjectura de Knapp é verdadeira e estenderam esse resultado para $d = 2m$ com $m \geq 3$ ímpar, obtendo que

$$\Gamma_K^*(d) = \begin{cases} \frac{3}{2}d & \text{para} \quad K \in \{\mathbb{Q}_2(\sqrt{\pm 2}), \mathbb{Q}_2(\sqrt{\pm 10}\}, \\ d+1 & \text{para} \quad K \in \{\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{-5})\}. \end{cases}$$

Motivados, em especial, pelo trabalho de Duncan e Leep, nesta tese, nos dedicamos a formas de grau $3m$ com $(m,3) = 1$ e $m \geq 2$ em extensões quadráticas de $\mathbb{Q}_3$. Nossos resultados se resumem nos seguintes teoremas:

Teorema 1. *Sejam $K/\mathbb{Q}_3$ uma extensão quadrática e $d = 3m$ com $m > 1$ ímpar e $(3,m) = 1$. Então*

$$\Gamma_K^*(d) \leq \begin{cases} \left\lfloor \frac{5}{2}d \right\rfloor + 1 & \textit{se } K = \mathbb{Q}_3(\sqrt{3}), \\ 3d+1 & \textit{se } K = \mathbb{Q}_3(\sqrt{-3}), \\ \left\lfloor \frac{3}{2}d \right\rfloor + 1 & \textit{se } K \textit{ é não ramificada.} \end{cases}$$

Teorema 2. *Sejam $K/\mathbb{Q}_3$ uma extensão quadrática e $d = 3m$ com m par e $(3.m) = 1$. Então*

$$\Gamma_K^*(d) \leq \begin{cases} 6d+1 & \text{se } K = \mathbb{Q}_3(\sqrt{3}), \\ \frac{31}{3}d+1 & \text{se } K = \mathbb{Q}_3(\sqrt{-3}), \\ 14d+1 & \text{se } K \text{ é não ramificada.} \end{cases}$$

Esta tese está dividida da seguinte forma: começamos com um capítulo com as principais características dos corpos locais, dando uma atenção especial àqueles que são extensões totalmente ramificadas ou não ramificadas de $\mathbb{Q}_p$. Terminamos com uma caracterização das extensões quadráticas. O leitor que já tem familiaridade com a teoria pode omitir esse capítulo. A quem interessar aprender mais sobre corpos locais e extensões de $\mathbb{Q}_p$, sugerimos os livros de Greenberg [10], Cassels [2] e Gouvêa [8].

No Capítulo 2, apresentamos as ferramentas para a obtenção dos nossos resultados. Explicamos como reduzir o problema da solubilidade de formas sobre o corpo K ao estudo de congruências módulo potências do uniformizador π e detalhamos o método de contração de variáveis usado para resolver as tais congruências.

Os capítulos 3 e 4 são dedicados às provas dos teoremas 1 e 2. Começamos com o caso $K/\mathbb{Q}_3$ totalmente ramificada no capítulo 3 e o caso $K/\mathbb{Q}_3$ não ramificada é tratado no capítulo 4. A diferença fundamental entre os dois casos é a estrutura do corpo de resíduos, por isso a separação se faz necessária.

No capítulo 5, damos os primeiros passos na direção de estender os resultados obtidos nos capítulos anteriores, estudando o caso $K/\mathbb{Q}_p$ quadrática $d = pm$ com $(m,p) = 1$. Como aplicação, obtemos que os limitantes para $\Gamma_K^*(15)$ e $\Gamma_K^*(6)$ conhecidos no caso $K = \mathbb{Q}_p$ valem também para quase toda $K/\mathbb{Q}_p$ quadrática, restando apenas um caso em aberto.

Capítulo 1

Preliminares

1.1 Corpos locais

Um anel A é chamado *anel de valoração discreta* ou *anel local* se A é domínio de ideais principais e tem um único ideal primo não nulo $\mathfrak{p}(A)$. O corpo $A/\mathfrak{p}(A)$ é chamado *corpo de resíduos de* A. Como $\mathfrak{p}(A)$ é o único ideal maximal de A (lembre-se que em um domínio de ideais principais os ideais primos não nulos são precisamente os ideais maximais), o conjunto das unidades de A é $A \setminus \mathfrak{p}(A)$. As unidades formam um grupo multiplicativo denotado por $A^\times$ ou $U(A)$. Uma vez que A é domínio de ideais principais, $\mathfrak{p}(A)$ é da forma (π), onde π é um elemento irredutível chamado *uniformizador* de A. Como $\mathfrak{p}(A)$ é o único ideal primo não nulo, segue que quaisquer dois uniformizadores são associados, ou seja, se π e π' são uniformizadores, então $\pi = \pi' u$ onde $u \in A^\times$.

Os ideais não nulos de A são da forma (π^n), onde π é um uniformizador. Daí, se $x \neq 0$ é elemento de A, existem únicos $n \in \mathbb{N}$, $u \in A^\times$ tais que $x = \pi^n u$. O número n é chamado *valoração de* x, denotada por $v(x)$ e não depende da escolha do uniformizador π.

Seja K o corpo de frações de A. Então $K^\times$ é o grupo multiplicativo dos elementos não nulos de K. Se $x = a/b \in K^\times$, então podemos escrever

$$x = \pi^{v(x)} u \tag{1.1.1}$$

com $u \in A^\times$ e $v(x) = v(a) - v(b)$. Isso define uma função v sobre $K^\times$ com imagem no grupo aditivo $\mathbb{Z}$ que satisfaz as condições abaixo:

a) $v(xy) = v(x) + v(y)$ (v é homomorfismo de grupos)

b) $v(x+y) \geq \min(v(x), v(y))$

para quaisquer $x, y \in K^\times$. Por convenção, tomamos $v(0) = +\infty$ e v passa a ser uma função de K em $\mathbb{Z} \cup \{+\infty\}$.

No geral, uma função $v : K \longrightarrow \mathbb{R} \cup \{+\infty\}$ com as propriedades a) e b) acima, é chamada uma *valoração*. Quando $v(K^\times)$ é discreto, v é dita uma *valoração discreta*.

Se A é anel de valoração discreta e v é definida como em (1.1.1), observe que

$$A = \{x \in K : v(x) \geq 0\} \text{ e } \mathfrak{p}(A) = \{x \in K : v(x) > 0\}.$$

Assim, o conhecimento da função v determina o anel A. Daí vem o nome *anel de valoração discreta* e dizemos que v é a *valoração associada a* A.

Uma valoração v em um corpo K define um valor absoluto não-arquimediano $|\cdot|$ em K fazendo

$$|x| = \begin{cases} \alpha^{v(x)} & \text{se } x \neq 0, \\ 0 & \text{se } x = 0 \end{cases}$$

onde $\alpha \in (0,1)$. Escolhas diferentes para α levam a valores absolutos equivalentes.

O conjunto $\mathcal{V}(K) = \{v(x) : x \in K^\times\} \subseteq \mathbb{R}$ é um subgrupo aditivo de $\mathbb{R}$ chamado *grupo de valores de* K. Quando a valoração v é discreta, $\mathcal{V}(K)$ é discreto e dizemos que o valor absoluto $|\cdot|$ é discreto.

Exemplo 1.1.1. *Fixe um primo $p \in \mathbb{Z}$. Para cada $n \in \mathbb{Z}$, $n \neq 0$, seja $v_p(n)$ o único inteiro não negativo satisfazendo $n = p^{v_p(n)}u$ com $p \nmid u$. Além disso, tome $v_p(0) = +\infty$. Para $x = a/b \in \mathbb{Q}^\times$, fazemos $v_p(x) = v_p(a) - v_p(b)$. Isso define uma valoração discreta $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{+\infty\}$, chamada valoração p-ádica. A partir de v_p, definimos o valor absoluto p-ádico de $x \in \mathbb{Q}^\times$ por*

$$|x|_p = p^{-v_p(x)} \text{ e } |0|_p = 0.$$

O valor absoluto $|\cdot|_p$ assim definido é não-arquimediano e discreto sobre $\mathbb{Q}$.

Reciprocamente, se $|\cdot|$ é um valor absoluto não-arquimediano discreto definido em um corpo K, escolha uma constante $c \in (0,1)$ e considere a função $v : K \longrightarrow \mathbb{R} \cup \{+\infty\}$ definida por $|x| = c^{v(x)}$ para $x \in K^\times$ e $v(0) = +\infty$. v assim definida é uma valoração discreta em K. O conjunto

$$\mathcal{O}_K = \{x \in K : |x| \leq 1\} = \{x \in K : v(x) \geq 0\}$$

é um anel de valoração discreta que tem v como valoração associada e K é o corpo de frações de $\mathcal{O}_K$. Além disso, o conjunto

$$\mathfrak{p}_K = \{x \in K : |x| < 1\} = \{x \in K : v(x) > 0\}$$

é o ideal primo não nulo de $\mathcal{O}_K$ e

$$k = \mathcal{O}_K/\mathfrak{p}_K$$

é o corpo de resíduos de $\mathcal{O}_K$.

Concluímos portanto que todo corpo munido com um valor absoluto não-arquimediano discreto é o corpo de frações de um anel de valoração discreta. Frequentemente, nos referimos a um uniformizador de $\mathcal{O}_K$ como uniformizador de K e ao corpo de resíduos de $\mathcal{O}_K$ como corpo de resíduos de K.

Exemplo 1.1.2. *Se $K = \mathbb{Q}$ e $|\cdot|_p$ é o valor absoluto p-ádico, o anel de valoração de $\mathbb{Q}$ é $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b\}$ com ideal primo $p\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b \text{ e } p \mid a\}$ e p é um uniformizador de $\mathbb{Z}_{(p)}$. O corpo de resíduos de $\mathbb{Q}$ é*

$$\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p.$$

Veremos a seguir que o fato do corpo de resíduos de $\mathbb{Q}$ ser finito é uma propriedade especial dos chamados corpos locais.

Agora, se K é um corpo munido de um valor absoluto $|\cdot|$, então existe um único corpo $\overline{K} \supseteq K$ que completa K, ou seja, $\overline{K}$ tem um valor absoluto $\|\cdot\|$ que estende o valor absoluto de K, K é denso em $\overline{K}$ e $\overline{K}$ é um corpo completo em relação a $\|\cdot\|$. Quando $|\cdot|$ é discreto e não-arquimediano, $\|\cdot\|$ também o é.

Definição 1.1.3. Um corpo K é chamado *corpo local* se K é localmente compacto com respeito a um valor absoluto não trivial $|\cdot|$ em K, ou seja, o conjunto

$$\{x \in K : |x| \leq c\}$$

é compacto para todo $c > 0$.

Essa condição dá a K várias propriedades interessantes. Por exemplo, todo corpo local K é completo (toda sequência de Cauchy em K é convergente). A proposição a seguir determina que corpos locais munidos de um valor absoluto não trivial e não-arquimediano,

são precisamente os corpos completos, com valor absoluto discreto e com corpo de resíduos finito. Uma prova pode ser encontrada em [20], Capítulo 25, Proposição F1.

Proposição 1.1.4. *Se K é um corpo local com respeito a um valor absoluto não trivial e não-arquimediano $|\cdot|$, então*

a) K é completo com respeito a $|\cdot|$

b) $|\cdot|$ é discreto

c) O corpo de resíduos de K é finito.

Reciprocamente, se $|\cdot|$ é um valor absoluto não trivial e não-arquimediano em um corpo K satisfazendo a), b) e c), então K é corpo local.

Exemplo 1.1.5. *$\mathbb{Q}$ munido do valor absoluto p-ádico não é completo. O completamento de $\mathbb{Q}$ em relação a $|\cdot|_p$ é chamado corpo dos números p-ádicos e denotado por $\mathbb{Q}_p$. O anel de valoração de $\mathbb{Q}_p$ é denotado por $\mathbb{Z}_p$ e chamado anel dos inteiros p-ádicos, cujo ideal maximal é $p\mathbb{Z}_p$ e o corpo de resíduos é $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$. Pela proposição anterior, $\mathbb{Q}_p$ é um corpo local.*

Observação 1.1.6. Uma propriedade especial dos corpos K completos com respeito a um valor absoluto não-arquimediano é que uma série $\sum a_n$ em K é convergente quando $\lim_{n\to\infty} |a_n| = 0$. Isso acontece porque a propriedade não-arquimediana garante que a sequência das somas parciais da série seja de Cauchy (e, portanto, convergente em K) quando $|a_n|$ tende a zero. Isso é útil para obtermos um importante resultado em corpos locais exibido na proposição abaixo.

Proposição 1.1.7. *Sejam K um corpo local com uniformizador π e $\mathcal{R}$ um conjunto de representantes de $k = \mathcal{O}_K/(\pi)$. Então, todo elemento $a \in \mathcal{O}_K$ pode ser escrito de forma única como*

$$a = \sum_{n\geq 0} a_n \pi^n$$

com $a_n \in \mathcal{R}$. Além disso, toda série da forma $\sum_{n\geq 0} a_n \pi^n$ com $a_n \in \mathcal{R}$ converge a um elemento de $\mathcal{O}_K$.

Demonstração. Seja $a \in \mathcal{O}_K$. Então existe um único $a_0 \in \mathcal{R}$ tal que $a - a_0 \in (\pi)$, ou seja, $a = a_0 + b_1\pi$, com $b_1 \in \mathcal{O}_K$. Da mesma forma, b_1 pode ser escrito de forma única como

$b_1 = a_1 + b_2\pi^2$ com $a_2 \in \mathcal{R}$ e $b_2 \in \mathcal{O}_K$ e logo $a = a_0 + a_1\pi + b_2\pi^2$. Repetindo esse processo recursivamente, obtemos para cada $n \in \mathbb{N}$,

$$a = a_0 + a_1\pi + \cdots + a_n\pi^n + b_{n+1}\pi^{n+1}$$

com $a_i \in \mathcal{R}$ para $i = 0, \ldots, n$ e $b_{n+1} \in \mathcal{O}_K$. Isso define uma soma parcial $S_n = \sum_{i=0}^{n} a_i\pi^i$ tal que

$$|\, a - S_n \,| = \left| b_{n+1}\pi^{n+1} \right| \leq \left| \pi^{n+1} \right|$$

já que $|\, b_{n+1} \,| \leq 1$. Como $\lim_{n\to\infty} |\, \pi^{n+1} \,| = 0$, segue da Obervação 1.1.6 que a série $\sum_{n\geq 0} a_n\pi^n$ converge para a. Isso mostra a primeira afirmação da proposição.

Agora, se $\sum_{n\geq 0} a_n\pi^n$ é uma série com $a_i \in \mathcal{R}$, uma vez que

$$\lim_{n\to\infty} |\, a_n\pi^n \,| = \lim_{n\to\infty} |\, \pi \,|^n = 0$$

e $|\cdot|$ é não-arquimediano, usamos a Observação 1.1.6 mais uma vez e $\sum_{n\geq 0} a_n\pi^n$ converge para $a \in K$.

Como $a_i \in \mathcal{O}_K^{\times}$ para todo i, temos $|\, a_i \,| = 1$ e $|\, a_i\pi^i \,| < 1$ para $i > 0$. Daí, para cada $n \in \mathbb{N}$,

$$|\, S_n \,| = |\, a_s + a_1\pi + \cdots + a_n\pi^n \,| \leq \max_{0\leq i\leq n} \left\{ |\, a_i\pi^i \,| \right\} = 1.$$

Como S_n converge para a, existe $n_0 \in \mathbb{N}$ tal que $|\, a - S_n \,| \leq 1$ para $n \geq n_0$. Assim,

$$|\, a \,| = |\, a - S_{n_0} + S_{n_0} \,| \leq \max\{ |\, a - S_{n_0} \,|, |\, S_{n_0} \,| \} \leq 1.$$

Isso mostra que $a \in \mathcal{O}_K$ e conclui a prova. □

1.2 Extensões finitas de $\mathbb{Q}_p$

Seja K/E uma extensão de corpos de grau n. Dado $\alpha \in K$, considere

$$f(x) = x^s + a_{s-1}x^{s-1} + \cdots + a_0 \in E[x]$$

o polinômio minimal de α sobre E. Defina a norma de α em E como sendo

$$N_{K/E}(\alpha) = (-1)^{sr} a_0^r$$

onde $r = [K : E(\alpha)]$. Isso determina uma função $N_{K/E} : K \longrightarrow E$ chamada *norma de K em E*. Essa função tem várias definições equivalentes e propriedades interessantes que não vamos abordar aqui. No nosso estudo, ela é usada para estender o valor absoluto de E para K no teorema abaixo.

Teorema 1.2.1. *Seja E um corpo completo com respeito a um valor absoluto $|\cdot|$. Se K/E é uma extensão de grau n, podemos estender $|\cdot|$ a um único valor absoluto em K fazendo, para $\alpha \in K$,*

$$|\alpha| = \sqrt[n]{|N_{K/E}(\alpha)|},$$

com respeito ao qual K é completo.

Demonstração. Veja [20], Capítulo 23, Teorema 4. □

Se K/E é uma extensão finita e E é corpo local, K é, naturalmente, munido de um valor absoluto não-arquimediano discreto pelo teorema anterior. Daí, $\mathcal{O}_K$ é anel de valoração discreta com ideal primo $\mathfrak{p}_K$ e o corpo de resíduos de K é uma extensão do corpo de resíduos de E. É fácil ver que essa extensão tem grau menor ou igual a $[K : E]$ (basta notar que uma combinação linear não trivial de elementos de K sobre E determina uma combinação linear não trivial de elementos de $\mathcal{O}_K/\mathfrak{p}_K$ sobre $\mathcal{O}_E/\mathfrak{p}_E$). Assim, extensões de corpos locais são também corpos locais. O teorema abaixo nos diz que todo corpo local de característica zero é uma extensão finita de $\mathbb{Q}_p$.

Teorema 1.2.2. *Seja K um corpo local com um valor absoluto $|\cdot|$ não-arquimediano. Se K tem característica zero, então K é uma extensão finita de $\mathbb{Q}_p$ onde p é a característica do corpo de resíduos de K e $|\cdot|$ é equivalente à única extensão do valor absoluto p-ádico $|\cdot|_p$ em K.*

Demonstração. Veja [20], Capítulo 25, Teorema 1. □

Extensões finitas de $\mathbb{Q}_p$ são chamadas *corpos p-ádicos* e é sobre eles que nossos objetos de estudo serão definidos. A partir de agora vamos explorar algumas das propriedades dos corpos p-ádicos que serão úteis nos capítulos seguintes.

Se $K/\mathbb{Q}_p$ é uma extensão de grau n, podemos usar o Teorema 1.2.1 para estender o valor absoluto p-ádico a K. Dado $\alpha \in K$, como $N_{K/\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p$ existe um único $v \in \mathbb{Z}$ tal que $|N_{K/\mathbb{Q}_p}(\alpha)|_p = p^{-v}$. Daí,

$$|\alpha| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(\alpha)|_p} = \sqrt[n]{p^{-v}} = p^{-\frac{v}{n}}$$

Isso nos leva a definir a valoração p-ádica em K: para $x \in K$, $x \neq 0$, definimos $v_p(x)$ como o único racional satisfazendo $|x| = p^{-v_p(x)}$ e $v_p(0) = \infty$. v_p assim definida é uma valoração discreta. Observe que $v_p(K^\times) = \mathcal{V}(K)$ é um subgrupo de $\frac{1}{n}\mathbb{Z}$. Daí, existe um inteiro positivo e que divide n tal que $v_p(K^\times) = \frac{1}{e}\mathbb{Z}$. O número e assim determinado é um invariante da extensão $K/\mathbb{Q}_p$ e recebe um nome na definição abaixo.

Definição 1.2.3. Seja $K/\mathbb{Q}_p$ uma extensão de grau n. Definimos o *índice de ramificação de K sobre $\mathbb{Q}_p$* como sendo o único inteiro positivo $e = e(K/\mathbb{Q}_p)$ dividindo n tal que $v_p(K^\times) = \frac{1}{e}\mathbb{Z}$.

Os uniformizadores de K são, precisamente, os elementos com valoração p-ádica $1/e$. De fato, seja $\pi \in K$ um uniformizador. Então $\mathfrak{p}_K = (\pi)$. Se $\alpha \in K^\times$ é tal que $v_p(\alpha) = \frac{1}{e} > 0$, então $\alpha \in \mathfrak{p}_K$ e logo, π divide α. Daí, $v_p(\pi) \leq v_p(\alpha) = \frac{1}{e}$. Como $v_p(K^\times) = \frac{1}{e}\mathbb{Z}$, segue que $v_p(\pi) = 1/e$. Reciprocamente, como elementos com mesma valoração são associados (se $v_p(a) = v_p(b)$, então $v_p(a/b) = 0$, ou seja, $a/b \in \mathcal{O}_K^\times$) segue que se $\alpha \in K$ é tal que $v_p(\alpha) = 1/e$, então α também é um uniformizador.

Pelo Teorema 1.2.2, $k = \mathcal{O}_K/(\pi)$ é uma extensão finita de $\mathbb{F}_p$ e definimos um outro invariante de K com base nessa extensão.

Definição 1.2.4. O grau da extensão $k/\mathbb{F}_p$ é chamado *grau de resíduos* de K e é denotado por $f = f(K/\mathbb{Q}_p)$.

Sempre que não houver risco de confusão, vamos escrever apenas e e f para denotar o índice de ramificação e o grau de resíduos, respectivamente. O teorema abaixo relaciona os invariantes e e f com o grau da extensão $K/\mathbb{Q}_p$.

Teorema 1.2.5. *Seja $K/\mathbb{Q}_p$ uma extensão de grau n. Então $n = ef$.*

Demonstração. Seja π um uniformizador de K. Como $k = \mathcal{O}_K/(\pi) \simeq \mathbb{F}_{p^f}$, podemos escolher $\beta = \{a_1, \ldots, a_f\} \subseteq \mathcal{O}_K$ tal que $\overline{\beta} = \{\overline{a}_1, \ldots, \overline{a}_f\} \subseteq k$ é uma base de k sobre $\mathbb{F}_p$, onde $\overline{x} \in k$ é a imagem de $x \in \mathcal{O}_K$ pela projeção natural $x \mapsto x + (\pi)$.

Primeiramente, mostremos que β é *l.i.* sobre $\mathbb{Q}_p$. De fato, se β é um conjunto *l.d.*, em particular, existem $\lambda_i \in \mathbb{Z}_p$ com pelo menos um deles em $\mathbb{Z}_p^\times$ tais que

$$a_1\lambda_1 + \cdots + a_f\lambda_f = 0.$$

Módulo π, isso determina uma combinação linear não trivial dos $\overline{a}_i$'s sobre $\mathbb{F}_p$, o que contradiz a independência linear $\overline{\beta}$ sobre $\mathbb{F}_p$.

Vamos agora mostrar que

$$\beta' = \{a_i \pi^j : 1 \leq i \leq f, 0 \leq j \leq e-1\}$$

é uma base de K sobre $\mathbb{Q}_p$ e isso é suficiente para obter $n = ef$ e concluir a prova do teorema.

- β' é *l.i.* sobre $\mathbb{Q}_p$.

  Se $e = 1$, $\beta' = \beta$ e nada temos a fazer. Suponha que $e > 1$. Similarmente ao que fizemos para β, se β' é um conjunto *l.d.* sobre $\mathbb{Q}_p$, então existem $\lambda_{ij} \in \mathbb{Z}_p$ com pelo menos um deles em $\mathbb{Z}_p^\times$ tais que

  $$\sum_{i,j} \lambda_{ij} a_i \pi^j = 0. \tag{1.2.1}$$

  Módulo π, temos

  $$\sum_i \overline{\lambda}_{i_0} \overline{a}_i = 0 \Rightarrow \overline{\lambda}_{i0} = 0, \ \forall\, i \in \{1, \ldots, f\}$$

  já que $\overline{\beta}$ é base de k sobre $\mathbb{F}_p$. Daí, $\lambda_{i0} \in (p) = (\pi^e)$. Dividindo a equação (1.2.1) por π, obtemos

  $$0 = \sum_{i,j} \lambda_{ij} a_i \pi^{j-1} = \sum_i (\lambda_{i0} \pi^{-1}) a_i + \sum_i \lambda_{i1} a_i + \sum_i \sum_{j \geq 2} \lambda_{ij} a_i \pi^{j-1}.$$

  Como $e > 1$, $\lambda_{i0} \pi^{-1} \in (\pi)$. Daí, módulo π, temos

  $$\sum_i \overline{\lambda}_{i1} \overline{a}_i = 0$$

  e, de novo, pela independência linear de $\overline{\beta}$ sobre $\mathbb{F}_p$, temos $\overline{\lambda}_{i1} = 0$ em $\mathbb{F}_p$, ou seja, $\lambda_{i1} \in (p)$ para todo $i \in \{1, \ldots, f\}$.

  Repetindo o argumento acima $e-1$ vezes, obtemos $\lambda_{ij} \in (p)$ para todo i e j, o que contradiz o que assumimos em (1.2.1).

- β' gera K sobre $\mathbb{Q}_p$.

  Seja $x \in \mathcal{O}_K$. Então, para $\overline{x} \in k$, existem $\lambda_{10}, \ldots, \lambda_{f0} \in \mathbb{Z}_p$ tais que

  $$\overline{x} = \sum_{i=1}^{f} \overline{\lambda}_{i0} \overline{a}_i \Rightarrow x = \sum_{i=1}^{f} \lambda_{i0} a_i + b_1 \pi$$

com $b_1 \in \mathcal{O}_K$. Fazendo o mesmo para b_1, obtemos

$$b_1 = \sum_{i=1}^{f} \lambda_{i1} a_i + b_2\pi \;\Rightarrow\; x = \sum_{i=1}^{f} \lambda_{i0} a_i + \pi \sum_{i=1}^{f} \lambda_{i1} a_i + b_2\pi^2$$

$$= \sum_{i=1}^{f} a_i(\lambda_{i0} + \pi\lambda_{i1}) + b_2\pi^2$$

com $b_2 \in \mathcal{O}_K$. Repetindo esse processo, obtemos

$$x = \sum_{i=1}^{f} a_i \sum_{j=0}^{\infty} \lambda_{ij} a_i \pi^j.$$

Agora note que, para cada i fixo,

$$\sum_{j=0}^{\infty} \lambda_{ij}\pi^j = \sum_{j=0}^{e-1} \lambda_{ij}\pi^j + \pi^e \sum_{j=e}^{2e-1} \lambda_{ij}\pi^{j-e} + \cdots$$

$$= \sum_{k=0}^{\infty} \pi^{ke} \sum_{j=ke}^{(k+1)e-1} \lambda_{ij}\pi^{j-ke}.$$

Fazendo a mudança de índices $j' = j - ke$, temos

$$\sum_{j=0}^{\infty} \lambda_{ij}\pi^j = \sum_{k=0}^{\infty} p^k \sum_{j'=0}^{e-1} \lambda_{i(j'-ke)}\pi^{j'}.$$

Como $\lambda_{i(j'-ke)} \in \mathbb{Z}_p$, temos $\sum_{j'=0}^{e-1} \lambda_{i(j'-ke)}\pi^{j'} = b_{ik} \in \mathcal{O}_K$ pela Proposição 1.1.7. Daí,

$$\sum_{k=0}^{\infty} p^k \sum_{j'=0}^{e-1} \lambda_{i(j'-ke)}\pi^{j'} = \sum_{k=0}^{\infty} p^k b_{ik}$$

é uma série convergente pela Proposição 1.1.7. Assim, podemos trocar a ordem dos somatórios e temos

$$\sum_{k=0}^{\infty} p^k \sum_{j'=0}^{e-1} \lambda_{i(j'-ke)}\pi^{j'} = \sum_{j'=0}^{e-1} \pi^{j'} \sum_{k=0}^{\infty} p^k \lambda_{i(j'-ke)} = \sum_{j'=0}^{e-1} \pi^{j'} y_{ij'}$$

com $y_{ij'} \in \mathbb{Z}_p$. Assim,

$$x = \sum_{i=1}^{f} a_i \sum_{j=0}^{\infty} \lambda_{ij} a_i \pi^j = \sum_{i,j} a_i \pi^j y_{ij}.$$

Isso mostra que β' gera $\mathcal{O}_K$. Por fim, se $x \in K \setminus \mathcal{O}_K$, existe $n \in \mathbb{N}$ tal que $xp^n \in \mathcal{O}_K$. A combinação linear de β' sobre $\mathbb{Z}_p$ que gera xp^n determina uma combinação linear sobre $\mathbb{Q}_p$ que gera x.

Isso conclui a prova do teorema. □

Definição 1.2.6. Seja $K/\mathbb{Q}_p$ uma extensão de grau n com índice de ramificação e. Dizemos que K é *ramificada* se $e > 1$ e *não ramificada* se $e = 1$. Se $e = n$, K é dita *totalmente ramificada*.

Sabemos da teoria de corpos que se $K/\mathbb{Q}_p$ é uma extensão finita, então existe $\alpha \in K$ tal que $K = \mathbb{Q}_p(\alpha)$. Identificar o elemento α a ser adjuntado pode nos ajudar a entender mais sobre como são os elementos dessas extensões. Veremos que quando K é não ramificada ou totalmente ramificada, podemos obter mais informações sobre qual $\alpha \in K$ escolher.

Vamos começar com as extensões totalmente ramificadas.

Proposição 1.2.7. *Seja $K/\mathbb{Q}_p$ uma extensão finita totalmente ramificada. Então $K = \mathbb{Q}_p(\pi)$ onde π é um uniformizador. Além disso, π é raiz do polinômio*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$$

que satisfaz as condições do critério de Eisenstein, ou seja, $p \mid a_i$ para $0 \leq i < n$ e $p^2 \nmid a_0$. Reciprocamente, se uma extensão $K/\mathbb{Q}_p$ é obtida adjuntando uma raiz π de um polinômio de Eisenstein de grau n sobre $\mathbb{Q}_p$ então K é totalmente ramificada e π é um uniformizador.

Demonstração. Sejam π um uniformizador de K e $r = [K : \mathbb{Q}_p(\pi)]$. Como K é totalmente ramificada, temos $|\pi| = p^{-\frac{1}{n}}$. Seja $f(x) = x^s + a_{s-1}x^{s-1} + \cdots + a_0$ o polinômio minimal de π sobre $\mathbb{Q}_p$. Pelo Teorema 1.2.1, temos:

$$p^{-\frac{1}{n}} = |\pi| = \sqrt[n]{|(-1)^n a_0^r|} = \sqrt[n]{|a_0|^r} = \sqrt[s]{|a_0|}.$$

Como $a_0 \in \mathbb{Q}_p$, $|\,a_0\,|$ é uma potência inteira de p, digamos $p^{r'}$. Daí,

$$p^{-\frac{1}{n}} = p^{\frac{r'}{s}} \Rightarrow -\frac{1}{n} = \frac{r'}{s} \Rightarrow s = -nr'$$

e como $s \mid n$ devemos ter $s = n$, $|\,a_0\,| = p^{-1}$ e $K = \mathbb{Q}_p(\pi)$.

Agora, para mostrar que $f(x)$ satisfaz o critério de Eisenstein, sejam $\pi_1 = \pi, \pi_2, \ldots, \pi_n \in \overline{\mathbb{Q}}_p$ (o fecho algébrico de $\mathbb{Q}_p$) as raízes de $f(x)$. Como $f(x) = \mathrm{irr}_{\mathbb{Q}_p}(\pi_i)$ para todo $i \in \{1, \ldots, n\}$, segue que $N_{K/\mathbb{Q}_p}(\pi_i) = N_{K/\mathbb{Q}_p}(\pi)$ e, portanto, $|\,\pi_i\,| = |\,\pi\,| < 1$ para todo i. Como $f(x) = (x - \pi_1)\cdots(x - \pi_n)$, os coeficientes de f são somas de produtos dos π_i's e logo, devemos ter $|\,a_i\,| < 1$ para $1 \geq i < n$. Concluímos, portanto, que $a_i \in \mathbb{Z}_p$ para $0 \leq i < n$ e

- $|\,a_0\,| = p^{-1} \Rightarrow p \mid a_0$ e $p^2 \nmid a_0$,
- $|\,a_i\,| < 1 \Rightarrow p \mid a_i$ para $1 \geq i < n$.

Isso mostra que $f(x)$ satisfaz as condições do critério de Eisenstein.

Reciprocamente, seja π raiz de um polinõmio $f(x) \in \mathbb{Z}[x]$ de grau n satisfazendo o critério de Eisenstein. Então f é irredutível e daí $K = \mathbb{Q}_p(\pi)$ tem grau n.

Agora, se a_0 é o termo independente de f,

$$\begin{aligned} |\,\pi\,| = \sqrt[n]{|\,a_0\,|} = \sqrt[n]{p^{-1}} \quad &\Rightarrow \quad v_p(\pi) = \tfrac{1}{n} \\ &\Rightarrow \quad \tfrac{1}{n} \in v_p(K^\times) \\ &\Rightarrow \quad v_p(K^\times) = \tfrac{1}{n}\mathbb{Z} \end{aligned}$$

e $K/\mathbb{Q}_p$ é totalmente ramificada. □

No caso particular em que $p \nmid n$, podemos ir mais longe e determinar o polinômio de Eisenstein em questão.

Observação 1.2.8. Explorando um pouco das propriedades analíticas de $\mathbb{Q}_p$, pode-se mostrar que se $\alpha \in \mathbb{Z}_p$ e $|\,x\,|_p < 1$ (ou seja, $x \in p\mathbb{Z}_p$), a série

$$\mathfrak{B}(\alpha, x) = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n$$

onde $\binom{\alpha}{n} = \dfrac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$ é convergente em $\mathbb{Q}_p$ e podemos definir

$$(1+x)^\alpha := \mathfrak{B}(\alpha, x)$$

(veja [8], Seção 5.9 para mais detalhes). Com isso, podemos computar potências inteiras p-ádicas dos elementos de $1+p\mathbb{Z}_p$. Isso vai ser importante na prova da proposição abaixo.

Proposição 1.2.9. *Seja $K/\mathbb{Q}_p$ uma extensão totalmente ramificada de grau n e suponha que $p \nmid n$. Então K pode ser obtida adjuntando a $\mathbb{Q}_p$ uma raiz de um polinômio da forma $x^n - pu$ onde $u \in \mathbb{Z}_p^\times$.*

Demonstração. Como K é totalmente ramificada, pela Proposição 1.2.7, $K = \mathbb{Q}_p(\beta)$, onde β é tal que $v_p(\beta) = 1/n$ e é raiz de

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

com $v_p(a_0) = 1$ e $v_p(a_i) \geq 1$ para $i = 1, \ldots, n-1$. Podemos escrever $-a_0 = pu$ com $u \in \mathbb{Z}_p^\times$ e temos

$$\beta^n - pu = \beta^n + a_0 = -\beta^{n-1}a_{n-1} - \cdots - \beta a_1.$$

Como $p \mid a_i$ para $i = 1, \ldots, n-1$ e $\beta \in \mathcal{O}_K$, podemos escrever $\beta^n - pu = \beta p\alpha$ com $\alpha \in \mathcal{O}_K$. Daí,

$$\begin{aligned} v_p(\beta^n - pu) &= v_p(\beta) + v_p(p) + v_p(\alpha) \geq \tfrac{1}{n} + 1 \\ &\Rightarrow |\beta^n - pu| \leq p^{-\frac{1}{n}-1} \\ &\Rightarrow \left|\tfrac{pu}{\beta^n} - 1\right| \leq p^{-\frac{1}{n}} < 1 \\ &\Rightarrow \tfrac{pu}{\beta^n} \in 1 + p\mathbb{Z}_p. \end{aligned}$$

Como $\frac{1}{n} \in \mathbb{Z}_p$ (pois $p \nmid n$ por hipótese), pela Observação 1.2.8, temos

$$\left(\frac{pu}{\beta^n}\right)^{\frac{1}{n}} = \beta' \in \mathbb{Z}_p.$$

Assim, $\beta\beta' \in K$ é tal que

$$(\beta\beta')^n = \beta^n \cdot \frac{pu}{\beta^n} = pu.$$

Como $\beta' \in \mathbb{Z}_p$, temos $K = \mathbb{Q}_p(\beta) = \mathbb{Q}_p(\beta\beta')$. Isso conclui a prova. □

Observação 1.2.10. Extensões satisfazendo as hipóteses da proposição anterior são chamadas *monotonamente ramificadas*.

No caso de extensões não ramificadas, conseguimos uma descrição mais simples. De fato, para cada n inteiro positivo, existe uma única extensão não ramificada de $\mathbb{Q}_p$ de grau n, a saber, o corpo de decomposição do polinômio $x^q - x$ onde $q = p^n$. Para mostrar isso, precisamos de alguns resultados auxiliares.

Teorema 1.2.11 (Hensel)**.** *Sejam K uma extensão finita de $\mathbb{Q}_p$ e π um uniformizador. Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathcal{O}_K[x]$. Suponha que exista $\alpha_1 \in \mathcal{O}_K$ tal que*

$$f(\alpha_1) \equiv 0 \pmod{\pi} \text{ e } f'(\alpha_1) \not\equiv 0 \pmod{\pi}$$

onde f' é a derivada formal de f. Então existe $\alpha \in \mathcal{O}_K$ tal que $\alpha \equiv \alpha_1 \pmod{\pi}$ e $f(\alpha) = 0$.

Demonstração. Vamos usar indução para construir uma sequência de Cauchy $(\alpha_n)_{n\geq 1}$ em $\mathcal{O}_K$ de modo que o limite da sequência $\alpha \in \mathcal{O}_K$ satisfaça as condições do teorema.

Mais especificamente, queremos $(\alpha_n)_{n\geq 1}$ em $\mathcal{O}_K$ tal que, para cada n,

(i) $f(\alpha_n) \equiv 0 \pmod{\pi^n}$,

(ii) $\alpha_{n+1} \equiv \alpha_n \pmod{\pi^n}$.

Por hipótese, α_1 é o primeiro termo da sequência. Suponha já determinados α_i para $i \leq n$. Em particular, existe $\alpha_n \in \mathcal{O}_K$ tal que $f(\alpha_n) \equiv 0 \pmod{\pi^n}$ e $\alpha_n \equiv \alpha_{n-1} \pmod{\pi^{n-1}}$. Vamos encontrar $t \in \mathcal{O}_K$ tal que $\alpha_{n+1} = \alpha_n + t\pi^n$ seja o próximo termo da sequência.

Uma vez determinado t, por construção, α_{n+1} já satisfaz a condição (ii). Para a condição (i), primeiro observe que dados $x, y \in \mathcal{O}_K$, podemos escrever

$$f(x+y) = f(x) + f'(x)y + c(x,y)y^2$$

(para ver isso, basta computar $f(x+y)$ usando a expansão binomial e agrupar os termos de forma conveniente). Daí temos:

$$\begin{aligned} f(\alpha_{n+1}) = f(\alpha_n + t\pi^n) &= f(\alpha_n) + f'(\alpha_n)t\pi^n + c(\alpha_n, t\pi^n)t^2\pi^{2n} \\ &\equiv f(\alpha_n) + f'(\alpha_n)\pi^n t \pmod{\pi^{n+1}}. \end{aligned}$$

Como as duas parcelas da soma acima são divisíveis por π^n, α_{n+1} satisfaz a condição (i) quando

$$\frac{f(\alpha_n)}{\pi^n} + f'(\alpha_n)t \equiv 0 \pmod{\pi} \;\Rightarrow\; t \equiv -\frac{f(\alpha_n)}{f'(\alpha_n)\pi^n} \pmod{\pi}.$$

É fácil ver que existe $t \in \mathcal{O}_K$ satisfazendo a equação acima, uma vez que

$$\alpha_i \equiv \alpha_{i-1} \pmod{\pi^i} \;\Rightarrow\; \alpha_i \equiv \alpha_1 \pmod{\pi} \text{ para todo } i \leq n$$

$$\Rightarrow\; f'(\alpha_n) \equiv f'(\alpha_1) \not\equiv 0 \pmod{\pi}.$$

Isso mostra que a sequência $(\alpha_n)_{n\geq 1}$, como queríamos, pode ser construída.
Agora, dado $\epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $\dfrac{1}{p^{en_0}} < \epsilon$. Daí, por (ii),

$$\alpha_{n+1} \equiv \alpha_n \pmod{\pi^n} \Rightarrow |\alpha_{n+1} - \alpha_n| \leq \frac{1}{p^{en}} < \epsilon.$$

para todo $n \geq n_0$ e $(\alpha_n)_{n\geq 1}$ é uma sequência de Cauchy, cujo limite α é tal que $f(\alpha) = 0$ pela continuidade de f e $\alpha \in \mathcal{O}_K$, pois cada $\alpha_i \in \mathcal{O}_K$.

Por fim, $\alpha \equiv \alpha_1 \pmod{\pi}$ por construção e isso conclui a prova do teorema. □

O Teorema 1.2.11 é uma das várias versões do conhecido *Lema de Hensel* que foi provado originalmente por Hensel [11] em 1908 e desde então tem sido uma ferramenta para vários resultados importantes na Teoria dos Números. No capítulo seguinte, vamos ver uma versão diferente que será usada na prova dos resultados dessa tese.

Corolário 1.2.12. *Seja K uma extensão finita de $\mathbb{Q}_p$ com grau de resíduos f. Então $\mathcal{O}_K$ contém o grupo cíclico das raízes $(p^f - 1)$-ésimas da unidade.*

Demonstração. Seja $0 \neq \overline{\alpha} \in k = \mathcal{O}_K/(\pi)$. Como $k^\times$ é um grupo cíclico de ordem $q-1$ com $q = p^f$, a ordem de $\overline{\alpha}$ divide $q-1$ e logo, $\overline{\alpha}$ é raiz de

$$f(x) = x^{q-1} - 1 \in k[x]. \tag{1.2.2}$$

Escolha $\alpha_1 \in \mathcal{O}_K^\times$ tal que $\alpha_1 \equiv \overline{\alpha} \pmod{\pi}$. Então:

$$f(\alpha_1) \equiv 0 \pmod{\pi} \text{ e } f'(\alpha_1) = (q-1)\alpha_1^{q-2} \not\equiv 0 \pmod{\pi}.$$

pois $q-1,\ \alpha_1 \notin (\pi)$. Pelo Teorema 1.2.11, existe $\alpha \in \mathcal{O}_K$ tal que $f(\alpha)=0$, ou seja, $\alpha^{q-1}=1$. Percorrendo todos os elementos $\overline{\alpha} \in k$, obtemos p^f-1 elementos distintos em $\mathcal{O}_K$ (pois são diferentes módulo π) satisfazendo (1.2.2). Isso mostra o corolário. □

Proposição 1.2.13. *Para cada n há exatamente uma extensão não-ramificada de grau n que é obtida adjuntando a $\mathbb{Q}_p$ uma raiz primitiva (p^n-1)-ésima da unidade.*

Demonstração. Seja β um gerador do grupo multiplicativo $\mathbb{F}_q^\times$ com $q=p^n$ e

$$\overline{f}(x) = x^n + \overline{a}_{n-1}x^{n-1} + \cdots + \overline{a}_0 \in \mathbb{F}_p[x]$$

o polinômio minimal de β sobre $\mathbb{F}_p$. Para cada i, escolha $a_i \in \mathbb{Z}_p$ tal que $a_i \equiv \overline{a}_i \pmod{p}$ e escreva $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_s \in \mathbb{Z}_p[x]$. É claro que f é irredutível sobre $\mathbb{Q}_p$, pois uma fatoração de f em $\mathbb{Q}_p$ determina uma fatoração de $\overline{f}$ módulo p.

Seja $\alpha \in \overline{\mathbb{Q}}_p$ uma raiz de f. Então $K=\mathbb{Q}_p(\alpha)$ é uma extensão de grau n de $\mathbb{Q}_p$. Se π é o uniformizador de K, então a redução de α módulo π é uma raiz $\overline{f}$ módulo π. Daí, $[\mathcal{O}_K/(\pi):\mathbb{F}_p]=n$ e K é não ramificada. Falta mostrar que podemos escolher α como sendo uma raiz primitiva (p^n-1)-ésima da unidade.

Pelo corolário anterior, K contém todas as raízes (p^n-1)-ésimas da unidade. Daí, se ζ é raiz primitiva (p^n-1)-ésima da unidade, então

$$\mathbb{Q}_p \subseteq \mathbb{Q}_p(\zeta) \subseteq K.$$

Como $\overline{\zeta}$ é um gerador de $\mathbb{F}_q^\times$, o corpo de resíduos de $\mathbb{Q}_p(\zeta)$ sobre $\mathbb{Q}_p$ deve conter $\mathbb{F}_q$. Assim, $n=[K:\mathbb{Q}_p] \geq [\mathbb{Q}_p(\zeta):\mathbb{Q}_p] \geq n$. Isso mostra que $K=\mathbb{Q}_p(\zeta)$. □

Vamos fechar essa seção com um importante resultado que determina uma forma de obter uma extensão qualquer de grau n através de uma torre de extensões, uma não ramificada e uma totalmente ramificada. Para entender a prova, precisamos estender a noção de extensão totalmente ramificada para K/E uma extensão de corpos locais qualquer (fizemos apenas no caso $E=\mathbb{Q}_p$). E a noção é análoga: K/E é dita totalmente ramificada se o corpo de resíduos de K é igual o corpo de resíduos de E.

Teorema 1.2.14. *Seja $K/\mathbb{Q}_p$ uma extensão de grau n, índice de ramificação e e grau de resíduos f.*

a) Se K_0 é a única extensão de $\mathbb{Q}_p$ não ramificada de grau f, então $\mathbb{Q}_p \subset K_0 \subset K$ e K/K_0 é totalmente ramificada de grau e.

b) $K = K_0(\pi)$ *onde* π *é um uniformizador de* K *sobre* K_0.

Demonstração. a) Pelo Corolário 1.2.12, K contém as raízes $(p^f - 1)$-ésimas da unidade. Em particular, K contém $K_0 = \mathbb{Q}_p(\beta)$, a única extensão não ramificada de grau f de $\mathbb{Q}_p$. Daí, $\mathbb{Q}_p \subseteq K_0 \subseteq K$ e $[K_0 : \mathbb{Q}_p] = f$. Isso implica que $[K : K_0] = e$ e K/K_0 é totalmente ramificada já que K e K_0 possuem corpos de resíduos iguais.

b) Sejam π um uniformizador de K e $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K_0[x]$ o polinômio minimal de π sobre K_0. Seguindo os mesmos passos que demos na prova da primeira parte da Proposição 1.2.7, mostramos que $d = e$ e $K = K_0[\pi]$. □

Observação 1.2.15. K_0 conforme o teorema acima é chamado *subcorpo maximal não ramificado de* K e de fato, é o maior subcorpo de K não ramificado sobre $\mathbb{Q}_p$.

Usando o teorema anterior e o Lema de Krasner ([8], Teorema 6.8.2) é possível mostrar que dado n um inteiro positivo, há uma quantidade finita de extensões de $\mathbb{Q}_p$ de grau n e, de fato, determinar todas elas em função dos polinômios geradores (cujas raízes geram a extensão K). Para mais detalhes, veja [8].

1.3 Caracterização das extensões quadráticas

O objetivo dos próximos capítulos será estudar formas diagonais sobre extensões quadráticas de $\mathbb{Q}_p$ com p ímpar. Os resultados da seção anterior nos permitem uma caracterização completa dessas extensões.

Seja p um primo ímpar. Considere a composição das projeções canônicas

$$\varphi : \mathbb{Z}_p^\times \xrightarrow{(\text{mod } p)} \mathbb{F}_p^\times \xrightarrow{(\text{mod } (\mathbb{F}_p^\times)^2)} \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2.$$

Como φ é sobrejetiva (pois é composição de funções sobrejetivas), pelo Teorema dos Isomorfismos de Grupos, temos

$$\mathbb{Z}_p^\times/\ker\varphi \simeq \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2.$$

É fácil ver que $(\mathbb{Z}_p^\times)^2 \subseteq \ker\varphi$. Por outro lado, dado $b \in \ker\varphi$, existe $\overline{b} \in (\mathbb{F}_p^\times)^2$ tal que $b \equiv \overline{b} \pmod p$. Daí, existe $\alpha_1 \in \mathbb{F}_p^\times$ raiz de $f(x) = x^2 - b$ módulo p. Como

$$f(\alpha_1) \equiv 0 \pmod p \text{ e } f'(\alpha_1) = 2\alpha_1 \not\equiv 0 \pmod p,$$

pelo Teorema 1.2.11, existe $\alpha \in \mathbb{Z}_p^\times$ tal que $\alpha^2 = b$. Assim, $b \in (\mathbb{Z}_p^\times)^2$ e $\ker\varphi = (\mathbb{Z}_p^\times)^2$.

Agora, como $\mathbb{F}_p^\times$ é grupo cíclico de ordem par, $x \in \mathbb{F}_p^\times$ é quadrado se, e somente se, é uma potência par de um gerador e, portanto, $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z}$. Com isso, concluímos que

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z}$$

e qualquer $u \in \mathbb{Z}_p^\times$ tal que $u \pmod p$ não é resíduo quadrático e é um representante para a a classe não trivial de $\mathbb{Z}/2\mathbb{Z}$.

Vamos usar a discussão acima para determinar os quadrados em $\mathbb{Q}_p^\times$.

Lema 1.3.1. *Seja $p \neq 2$ um primo. O grupo quociente $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ tem ordem 4 e dado $u \in \mathbb{Z}_p^\times$ tal que $u \pmod p$ não é resíduo quadrático, o conjunto $\{1, p, u, up\}$ é um sistema completo de representantes de $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.*

Demonstração. Sabemos que todo $x \in \mathbb{Q}_p$ pode ser escrito de forma única como $p^n u$ com $n \in \mathbb{Z}$ e $u \in \mathbb{Z}_p^\times$. Isso determina um isomorfismo

$$\phi : \mathbb{Q}_p^\times \longrightarrow \mathbb{Z}_p^\times \times \mathbb{Z} \text{ definido por } \phi(p^n u) = (u, n).$$

É fácil ver que $x \in (\mathbb{Q}_p^\times)^2$ se, e somente se, n é par e $u \in (\mathbb{Z}_p^\times)^2$. Daí,

$$(\mathbb{Q}_p^\times)^2 \simeq (\mathbb{Z}_p^\times)^2 \times 2\mathbb{Z}.$$

Assim,

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \simeq \left(\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2\right) \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Dado $u \in \mathbb{Z}_p^\times$ que não é resíduo quadrático módulo p, um conjunto de representantes para o termo do meio da expressão acima é $\{(1,0), (1,1), (u,0), (u,1)\}$, o que, em $\mathbb{Q}_p^\times$, determina um conjunto da forma $\{1, p, u, up\}$, como queríamos. □

Sejam p um primo ímpar e $K/\mathbb{Q}_p$ de grau 2. Então $K = \mathbb{Q}_p(\sqrt{d})$ onde $d \in \mathbb{Q}_p$ não é um quadrado em $\mathbb{Q}_p$ (isso é verdade para qualquer corpo de característica zero, não só para $\mathbb{Q}_p$). Pelo Lema 1.3.1, se d não é um quadrado, ele assume uma das seguintes três formas:

$$p\alpha^2, \ u\alpha^2 \text{ ou } pu\alpha^2$$

onde $u, \alpha \in \mathbb{Z}_p^\times$ e u não é resíduo quadrático módulo p. Assim, uma vez escolhida a unidade u, as extensões quadráticas de $\mathbb{Q}_p$ serão

$$\mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{u}) \text{ e } \mathbb{Q}_p(\sqrt{pu}).$$

Vamos agora determinar a ramificação das extensões quadráticas de $\mathbb{Q}_p$. Primeiramente, como $n=2$, temos $e=1$ ou $e=2$, ou seja, $K/\mathbb{Q}_p$ ou é não ramificada ou é totalmente ramificada. Da Proposição 1.2.13, exatamente uma delas é não ramificada.

Quando $e=2$, temos $p \nmid e$ pois p é ímpar. Daí, as extensões totalmente ramificadas quadráticas de $\mathbb{Q}_p$ são, na verdade, monotonamente ramificadas e podemos aplicar a Proposição 1.2.9 para determiná-las: são da forma $\mathbb{Q}_p(\sqrt{\alpha})$ onde α é a raiz de x^2-pu, com $u \in \mathbb{Z}_p^\times$, ou seja, $K=\mathbb{Q}_p(\sqrt{pu})$. Se u é quadrado em $\mathbb{Z}_p$, então $K=\mathbb{Q}_p(\sqrt{p})$ e se u não é quadrado em $\mathbb{Z}_p$, então podemos supor que $u \pmod p$ não é resíduo quadrático e $K=\mathbb{Q}_p(\sqrt{pu})$.

Assim, a terceira extensão, $\mathbb{Q}_p(\sqrt{u})$ com $u \pmod p$ não resíduo quadrático, é, necessariamente, a extensão não ramificada de $\mathbb{Q}_p$.

Exemplo 1.3.2. *Fixe $p=3$. Então $-1 \in \mathbb{Z}_3^\times$ não é resíduo quadrático módulo 3. Assim, existem exatas três extensões quadráticas de $\mathbb{Q}_3$, a saber, as totalmente ramificadas $\mathbb{Q}_3(\sqrt{3})$ e $\mathbb{Q}_3(\sqrt{-3})$ e a não ramificada $\mathbb{Q}_3(\sqrt{-1})$. Pela Proposição 1.2.13, $\mathbb{Q}_3(\sqrt{-1}) \simeq \mathbb{Q}_3(\xi)$ onde ξ é uma raiz 8-ésima primitiva da unidade.*

Observação 1.3.3. Quando $p=2$, usando uma versão do Lema de Hensel um pouco diferente da apresentada no Teorema 1.2.11, mostra-se de forma análoga ao que fizemos no caso p ímpar que $u \in \mathbb{Z}_2^\times$ é quadrado em $\mathbb{Z}_2$ se, e somente se, $u \equiv 1 \pmod{2^3}$. Daí, $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \simeq \mathbb{Z}/8\mathbb{Z}$ e $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^3$ é um grupo com oito elementos gerado por três classes, representadas, por exemplo, por 1, 5, e 2. Assim, existem sete extensões quadráticas de $\mathbb{Q}_2$, a saber,

$$\mathbb{Q}_2(\sqrt{-1}),\ \mathbb{Q}_2(\sqrt{\pm 2}),\ \mathbb{Q}_2(\sqrt{\pm 5}),\ \text{e}\ \mathbb{Q}_2(\sqrt{\pm 10}).$$

Para mais detalhes, veja [8], Seção 4.6.

Capítulo 2

Resultados auxiliares

Seja $K/\mathbb{Q}_p$ uma extensão de grau n, com anel de valoração $\mathcal{O}_K$, uniformizador π, índice de ramificação e e corpo de resíduos $k \simeq \mathbb{F}_{p^f}$. Considere a forma diagonal

$$f = a_1 x_1^d + \cdots + a_s x_s^d \tag{2.0.1}$$

com coeficientes $a_i \in \mathcal{O}_K$ e escreva $d = p^\tau m$ com $(p,m) = 1$.

Nosso trabalho se resume a estudar a solubilidade de $f = 0$ em K sob condições pré-estabelecidas. Nesse capítulo, vamos explorar importantes resultados já conhecidos na literatura que servirão como ferramentas para os resultados subsequentes.

2.1 O Lema de Hensel

O primeiro resultado é uma versão do Lema de Hensel diferente da que vimos no Teorema 1.2.11 e mais específica para o nosso trabalho. Ele pode ser obtido como corolário do teorema a seguir.

Teorema 2.1.1. *Sejam p um número primo, $d = p^\tau m$ com $(p,m) = 1$ e $b, c \in \mathcal{O}_K^\times$, onde K é uma extensão finita de $\mathbb{Q}_p$ com índice de ramificação e. Defina*

$$\gamma = \begin{cases} 1 & \text{se } \tau = 0; \\ \left\lfloor \dfrac{e}{p-1} \right\rfloor + e\tau + 1 & \text{se } \tau \geq 1. \end{cases}$$

Suponha que a congruência $cx^d \equiv b \pmod{\pi^\delta}$ tem uma solução $a \in \mathcal{O}_K$ para algum $\delta \geq \gamma$. Então a congruência $cx^d \equiv b \pmod{\pi^{\delta+1}}$ tem uma solução t onde $t \equiv a \pmod{\pi^{\delta - e\tau}}$. Consequentemente, a equação $cx^d = b$ tem solução em $\mathcal{O}_K$.

Demonstração. Veja [18], Teorema 2.3. □

Definição 2.1.2. Sejam $f = a_1x_1^d + \cdots + a_sx_s^d$, com $a_i \in \mathcal{O}_K$ e t um inteiro positivo. Dizemos que uma solução $(b_1, \ldots, b_s)$ com $b_1, \ldots b_s \in \mathcal{O}_K$ para $f \equiv 0 \pmod{\pi^t}$ é *não-singular*, se $a_ib_i \not\equiv 0 \pmod{\pi}$ para algum $i \in \{1, \ldots, s\}$.

Suponha que $(b_1, \ldots, b_s)$ seja uma solução não-singular para $f \equiv 0 \pmod{\pi^\gamma}$. Sem perda de generalidade, podemos supor $a_1b_1 \not\equiv 0 \pmod{\pi}$. Tome $c = -(a_2b_2^d + \cdots + a_sb_s^d)$. Então $b_1 \in \mathcal{O}_K^\times$ é solução de $a_1x^d \equiv c \pmod{\pi^\gamma}$. Pelo Teorema 2.1.1, existe $b \in \mathcal{O}_K$ tal que $a_1b^d = c$ em $\mathcal{O}_K$. Daí, $(b, b_2, \ldots, b_s)$ é solução para $f = 0$ em $\mathcal{O}_K$. Isso mostra o corolário abaixo.

Corolário 2.1.3 (Lema de Hensel)**.** *Sejam $f = a_1x_1^d + \cdots + a_sx_s^d$, $a_i \in \mathcal{O}_K$ com d e γ definidos como no Teorema 2.1.1. Se $f \equiv 0 \pmod{\pi^\gamma}$ tem uma solução não-singular, então $f = 0$ tem solução não trivial em K.*

Isso reduz nosso estudo à solubilidade de congruências módulo potências do uniformizador π.

2.2 π-normalização

Como queremos resolver uma congruência módulo π^γ, é de grande utilidade sermos capazes de estimar quantos dos coeficientes de f não são divisíveis por π^γ. O processo de π-normalização, introduzido por Davenport e Lewis em [4], nos permite obter essa informação.

O método consiste em agrupar as formas diagonais

$$f = a_1x_1^d + \cdots + a_sx_s^d$$

com $a_i \in \mathcal{O}_K$, em classes de equivalência, destacando um representante especial que possui a estimativa sobre os coeficientes que procuramos.

Dizemos que duas formas f e g são equivalentes se existe uma mudança de variáveis $x_i = l_ix_i'$, com $l_i \in \mathcal{O}_K$ que transforma f em um múltiplo de g, ou seja,

$$f(l_1x_1, \ldots, l_sx_s) = Lg(x_1, \ldots, x_s)$$

com $L \in \mathcal{O}_K$. Naturalmente, se $f = 0$ tem solução não trivial em $\mathcal{O}_K$, o mesmo acontece com $g = 0$ para toda forma g equivalente a f. É fácil ver que essa é uma relação de equivalência.

Vamos agora determinar um representante conveniente. Sejam x uma variável de uma forma diagonal f e $a \in \mathcal{O}_K$ o coeficiente de x. Vimos no Capítulo 1 que a pode ser escrito unicamente como $a = \pi^r u$ com $u \in \mathcal{O}_K^\times$ e $r \geq 0$ (essa é uma propriedade de anéis de valoração discreta). Se $r \geq d$, então existem $q \in \mathbb{Z}$ e $0 \leq r' < d$ tais que $r = dq + r'$. Fazendo a mudança de variáveis $y = \pi^q x$ obtemos

$$ax^d = u\pi^r x^d = u\pi^{dq+r'} x^d = u\pi^{r'}(\pi^q x)^d = u\pi^{r'} y^d.$$

Como essa substituição transforma f numa forma equivalente via a relação que definimos acima, vamos escolher um representante para a classe de f cujos coeficientes sejam todos da forma $a_i = \pi^r u_i$, $0 \leq r < d$ e $u_i \in \mathcal{O}_K^\times$.

Seja m_i o número de variáveis de um tal representante g cujo coeficiente é da forma $\pi^i u$ com $u \in \mathcal{O}_K^\times$. Então $m_0 + \cdots + m_{d-1} = s$ e podemos escrever

$$g = g_0 + \pi g_1 + \cdots + \pi^{d-1} g_{d-1}$$

onde g_i é uma forma diagonal de grau d e m_i variáveis, com coeficientes em $\mathcal{O}_K^\times$. Vamos nos referir a i como o *nível* das variáveis de g_i. Se $c \in \mathcal{O}_K$ é o coeficiente de f que acompanha uma variável x no nível i, pela Proposição 1.1.7 podemos escrever

$$c = \pi^i(c_0 + c_1\pi + c_2\pi^2 + \cdots)$$

com $c_j \in \mathcal{R}$, o conjunto de representantes de $\mathcal{O}_K/(\pi)$. c_0 é chamado 0-*coeficiente de* x e cada c_j é o π^j-*coeficiente de* x.

Podemos fazer uma mudança de variáveis que permuta ciclicamente as g_i's da seguinte forma:

$$g' = \frac{1}{\pi} g(\pi x_1, \ldots, \pi x_{m_0}, x_{m_0+1}, \ldots, x_s).$$

Essa mudança leva as variáveis do nível 0 ao nível $d-1$ e todas as outras variáveis passam a pertencer ao nível anterior ao que pertenciam. O lema a seguir nos garante que podemos executar uma certa quantidade de mudanças desse tipo a fim de obter uma forma na qual os m_i's satisfazem um sistema de desigualdades especial.

Lema 2.2.1. *Seja $f = a_1 x_1^d + \cdots + a_s x_s^d$ com $a_i \in \mathcal{O}_K$. Então existe g equivalente a f tal que*

$$g = g_0 + \pi g_1 + \pi^2 g_2 + \cdots + \pi^{d-1} g_{d-1}$$

onde g_i é uma forma diagonal de grau d em m_i variáveis e coeficientes em $\mathcal{O}_K^\times$, com $m_0,\dots,m_{d-1}$ satisfazendo

$$m_0+\cdots+m_{j-1}\geq \frac{js}{d},\ j=1,\dots,d.$$

Demonstração. Veja [21], Teorema 2.3. □

Uma forma g satisfazendo o lema anterior é dita *π-normalizada*.

2.3 Contração de variáveis

Sejam $K/\mathbb{Q}_p$ uma extensão finita e $f=a_1x_1^d+\cdots+a_sx_s^d$ com $a_i\in\mathcal{O}_K$. Uma vez que nosso objetivo é determinar a solubilidade de $f=0$ em K, pelo Lema 2.2.1, podemos assumir f π-normalizada.

Em [4], Davenport e Lewis introduziram uma operação sobre as variáveis de f chamada *contração* que consiste em substituir uma subforma de f por um único termo envolvendo uma variável em algum nível acima das variáveis substituídas.

Suponha que $x_{j_1},\dots,x_{j_t}$ são variáveis de f num nível l e que existam $b_1,\dots,b_t\in\mathcal{O}_K$ tais que

$$a_{j_1}b_1^d+\cdots+a_{j_t}b_t^d=\pi^j b,$$

com $b\in\mathcal{O}_K^\times$ e $j>l$. Naturalmente, devemos ter $b_i\in\mathcal{O}_K^\times$ para algum i. A mudança de variáveis $x_{j_i}=b_iy$ transforma a subforma $a_{j_1}x_{j_1}^d+\cdots+a_{j_t}x_{j_t}^d$ no termo π^jby^d. Descartamos, então, as variáveis $x_{j_1},\dots,x_{j_t}$ e incluímos o termo π^jby^d em f de modo a obter uma nova forma g cuja variável y está no nível j. Observe que y determina os x_{j_i}'s pela igualdade $x_{j_i}=b_iy$. Ao realizar esse processo, dizemos que y é o resultado da contração de $x_{j_1},\dots,x_{j_t}$. Se y participa de uma nova contração, então uma nova mudança de variáveis do tipo $y=b_kz$ com $b_k\in\mathcal{O}_K$ vai acontecer. Suponha que, após determinar um valor para z, queiramos traçar o caminho de volta de z à x_{j_i}. Nesse caso, obtemos $x_{j_i}=b_iy=b_ib_kz$. Assim, se após uma sequência de contrações, for atribuído um valor à variável resultante, esse valor e os coeficientes usados nos sucessores das variáveis iniciais x_{j_i} em cada uma das etapas determinam o valor de x_{j_i}.

As variáveis de f_0 e variáveis resultantes de contrações envolvendo variáveis de f_0 são chamadas *primárias*. As demais variáveis são chamadas *secundárias*.

Suponha que, após uma série de contrações, obtemos uma variável w primária num nível $j>\gamma$ definido no Lema 2.1.1. Se g é a forma que resultou dessas mudanças, fazendo

$w = 1$ e atribuindo 0 a todas as demais variáveis de g, é claro que isso determina uma solução para $g \equiv 0 \pmod{\pi^\gamma}$. Ao traçar o caminho de volta às variáveis de f, obtemos uma solução para $f \equiv 0 \pmod{\pi^\gamma}$. Se formos capazes de garantir que os coeficientes usados nas etapas de contrações de pelo menos uma variável do nível 0 sejam todos unitários, então o valor determinado a essa variável é uma unidade e a solução obtida é não-singular. Pelo Corolário 2.1.3, isso é suficiente para garantir que $f = 0$ tenha solução não trivial em K.

Assim, a partir de agora, nossa estratégia é garantir que uma variável primária no nível γ ou maior seja criada. Além disso, precisamos que essa variável determine uma solução não-singular. O lema abaixo resume os casos em que isso vai acontecer.

Lema 2.3.1. *Sejam $K/\mathbb{Q}_p$ uma extensão finita, f uma forma diagonal π-normalizada com coeficientes em $\mathcal{O}_K$ e γ definido no Teorema 2.1.1. Suponha que uma variável primária no nível γ ou maior foi obtida após uma série de contrações satisfazendo uma das condições abaixo:*

(i) todos os coeficientes não nulos usados nas etapas de contrações são unitários;

(ii) todas as etapas de contrações envolveram apenas variáveis primárias;

(iii) apenas uma contração foi realizada.

Então, $f \equiv 0 \pmod{\pi^\gamma}$ tem solução não-singular e, portanto, $f = 0$ tem uma solução não trivial em K.

Para determinar quando uma variável no nível γ pode ser criada, vamos precisar estudar inúmeros casos de acordo com o valor dos m_i's. O lema abaixo nos ajuda a reduzir o número de casos a serem estudados em algumas situações que vamos nos deparar no capítulo seguinte.

Lema 2.3.2. *Sejam $K/\mathbb{Q}_p$ uma extensão finita com $\mathcal{O}/(\pi) \simeq \mathbb{F}_q$ e f uma forma diagonal sobre $\mathcal{O}_K$ de grau d ímpar. Suponha f π-normalizada. Se f possui $\lfloor \gamma \log_2 q \rfloor + 1$ variáveis no mesmo nível, então elas podem ser usadas numa contração a uma variável pelo menos γ níveis acima.*

Demonstração. Sem perda de generalidade, podemos supor que as variáveis estão no nível 0. Quando d é ímpar, -1 é d-ésima potência módulo π^γ para todo γ. Considere as 2^{m_0} possíveis somas dos coeficientes de f_0:

$$0, a_i, a_i + a_j, \ldots, a_1 + \cdots + a_{m_0}.$$

Suponha que $m_0 > \gamma \log_2 q$. Então $2^{m_0} > q^\gamma$. Se uma das somas acima é 0 módulo π^γ, então fazendo $x_i = 1$ para as variáveis correspondentes aos coeficientes da soma e $x_i = 0$ para as demais variáveis, obtemos uma solução para $f_0 \equiv 0 \pmod{\pi^\gamma}$. Se todas as somas são não nulas módulo π^γ, como $\mathcal{O}/(\pi^\gamma)$ tem q^γ elementos, duas delas precisam ser iguais módulo π^γ. Removendo os elementos repetidos, essa igualdade determina dois conjuntos disjuntos de coeficientes, digamos, $a_1, \ldots, a_r$ e $a_{r+1}, \ldots, a_l$, cujas somas são iguais módulo π^γ. Tomando $x_i = 1$ para $i \in \{1, \ldots, r\}$, $x_i = \eta$ para $i \in \{r+1, \ldots, l\}$ onde $\eta^d = -1$ e $x_i = 0$ para $i > l$ obtemos uma solução $(x_1, \ldots, x_{m_0})$ para $f_0 \equiv 0 \pmod{\pi^\gamma}$. Isso mostra que $m_0 \geq \lfloor \gamma \log_2 q \rfloor + 1$ variáveis no nível 0 permitem obter uma variável primária no nível γ ou maior. □

2.4 Formas diagonais sobre corpos finitos

O tipo de contração de variáveis mais básico é o que gera uma variável no nível imediatamente acima ao das variáveis contraídas. Pelo que vimos na seção anterior, determinar contrações desse tipo significa garantir que uma certa equação diagonal tenha solução não trivial módulo π. Como $\mathcal{O}_K/(\pi)$ é um corpo finito, nos deparamos com equações sobre corpos finitos. Vamos relembrar os principais fatos sobre esses tipos de corpos.

Seja $\mathbb{F}_q$ o corpo finito de ordem $q = p^f$ onde p é um primo e $f \geq 1$. Sabemos que $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ é um grupo multiplicativo cíclico com $q-1$ elementos.

Escreva $\delta = (d, q-1)$. O fato de $\mathbb{F}_q^*$ ser cíclico, nos dá a seguinte caracterização das d-ésimas potências em $\mathbb{F}_q^*$.

Teorema 2.4.1. *Seja $\alpha \in \mathbb{F}_q^*$. Então $x^d = \alpha$ tem solução em $\mathbb{F}_q^*$ se, e somente se, $\alpha^{(q-1)/\delta} = 1$. Se existe uma solução, então existem exatamente δ soluções.*

Demonstração. Veja [12], Proposição 7.2.1. □

Dado $d \in \mathbb{N}$, defina $\gamma_q^*(d)$ como sendo o menor inteiro positivo tal que toda forma diagonal

$$f = a_1 x_1^d + \cdots + a_s x_s^d$$

com $a_1, \ldots, a_s \in \mathbb{F}_q^*$, tem um zero não trivial em $\mathbb{F}_q$ sempre que $s \geq \gamma_q^*(d)$.

Pelo Teorema 2.4.1, temos $(\mathbb{F}_q^*)^d = (\mathbb{F}_q^*)^\delta$. Daí, $a_1 x_1^d + \cdots + a_s x_s^d = 0$ tem solução não trivial em $\mathbb{F}_q$ se, e somente se, $a_1 x_1^\delta + \cdots + a_s x_s^\delta = 0$ tem solução não trivial em $\mathbb{F}_q$ e, portanto, $\gamma_q^*(d) = \gamma_q^*(\delta)$.

Corolário 2.4.2. *$\gamma_q^*(\delta) = 2$ se, e somente se, $\delta = 1$.*

Demonstração. Quando $\delta = 1$, f é linear e duas variáveis são suficientes para garantir uma solução não trivial para $f = 0$ em $\mathbb{F}_q$. Daí, $\gamma_q^*(1) = 2$. Reciprocamente, se $\gamma_q^*(\delta) = 2$, então dados $a_1, a_2 \in \mathbb{F}_q^*$, existem $x_1, x_2 \in \mathbb{F}_q^*$ tais que

$$a_1 x_1^\delta + a_2 x_2^\delta = 0 \Rightarrow -\frac{a_2}{a_1} = \left(\frac{x_1}{x_2}\right)^\delta.$$

Daí, todo elemento de $\mathbb{F}_q^*$ é δ-ésima potência, e pelo Teorema 2.4.1, $\delta = 1$. □

A seguir, vamos reunir uma série de resultados sobre estimativas para $\gamma_q^*(d)$ que serão úteis quando formos executar as contrações de variáveis nos capítulos 4 e 5. Começamos com dois resultados gerais. O primeiro deles é o clássico teorema mostrado por Chevalley [3]. Depois, o de Tietäväinen [28], que reduz o limitante de Chevalley quase pela metade quando f é uma forma diagonal, exceto em alguns casos.

Teorema 2.4.3 (Chevalley)**.** *Sejam $f_1, \ldots, f_r$ polinômios homogêneos de graus $d_1, \ldots, d_r$, respectivamente, sobre $\mathbb{F}_q$ em s variáveis. Se $s > \sum_{i=1}^r d_i$, então o sistema $f_i = 0, i = 1, \ldots, r$ tem solução não trivial em $\mathbb{F}_q$.*

Demonstração. Veja [12], Capítulo 10, Teorema 1. □

Teorema 2.4.4 (Tietäväinen)**.** *Seja q uma potência de primo qualquer e d um inteiro positivo tal que $d \neq p-1$ no caso em que $q = p$. Então a equação $\sum_{i=1}^s c_i x_i^d = 0$ tem solução não trivial em $\mathbb{F}_q$ sempre que $s \geq \frac{d+3}{2}$.*

Demonstração. Veja [24], Teorema 5.2.1. □

Em particular, o Teorema de Chevalley nos dá que $\gamma_q^*(\delta) \leq \delta + 1$ e o de Tietäväinen que $\gamma_q^*(\delta) \leq \frac{\delta+3}{2}$ quando $(\delta, q) \neq (p-1, p)$.

Suponha agora d ímpar. Então $\delta \mid (q-1)/2$ e $(q-1)/\delta$ é um número par. Daí, $(-1)^{(q-1)/\delta} = 1$ e -1 é d-ésima potência em $\mathbb{F}_q$ pelo Teorema 2.4.1. O lema a seguir é uma consequência direta do Lema 2.3.2.

Lema 2.4.5. *Seja $f = a_1 x_1^d + \cdots + a_s x_s^d$ com $a_i \in \mathbb{F}_q^*$. Se d é ímpar então a equação $f = 0$ tem solução não trivial em $\mathbb{F}_q$ quando $2^s > q$.*

Observe que

$$2^s > q \Leftrightarrow s > \log_2 q \Leftrightarrow s \geq \lfloor \log_2 q \rfloor + 1.$$

Daí, o lema anterior nos dá que $\gamma_q^*(d) \leq \lfloor \log_2 q \rfloor + 1$ quando d é ímpar. Note que esse limitante não depende de d.

Teorema 2.4.6 (Tietäväinen). *Seja* $f = a_1x_1^d + \cdots + a_sx_s^d$ *com* $a_i \in \mathbb{F}_q^*$. *Se* $2 \leq \delta \mid \frac{q-1}{2}$, *então* $f = 0$ *tem solução não trivial em* $\mathbb{F}_q$ *quando* $s \geq \lceil 2\log_2\delta - \log_2\log_2\delta \rceil + 1$.

Demonstração. Veja [24], Teorema 4.4.7. □

Teorema 2.4.7 (Tietäväinen). *Seja* $f = a_1x_1^d + \cdots + a_sx_s^d$ *com* $a_i \in \mathbb{F}_q^*$ *com* $s \geq 3$. *Se* d *é ímpar e* $q \geq s^{-1}d(d-1)^{\frac{s}{s-2}}$, *então* $f = 0$ *tem solução não trivial em* $\mathbb{F}_q$.

Demonstração. Veja [24], Teorema 4.4.4. □

Alguns casos particulares para δ vão ser necessários nos capítulos 4 e 5. O lema abaixo pode ser encontrado em [24], Apêndice A.

Lema 2.4.8. *Suponha que* $\delta \mid \frac{q-1}{2}$.

a) Se $\delta = 2, 3$ *ou* 4, *então* $\gamma_q^*(\delta) = 3$.

b) Se $\delta = 5$ *ou* 6, *então* $\gamma_q^*(\delta) = 4$.

Por fim, se $\delta = q-1$, então $x^\delta = 0$ ou 1 em $\mathbb{F}_q$ e a equação $f \equiv 0 \pmod{\pi}$ se resume a uma soma de elementos de $\mathbb{F}_q$. Daí, podemos aplicar o resultado de Olson [23] sobre problemas de soma-zero sobre grupos abelianos finitos.

Lema 2.4.9 (Olson). *Se* $\delta = q-1$ *e* $q = p^2$, *então* $\gamma_q^*(\delta) \leq 2p-1$.

Capítulo 3

Formas de grau $3m$ sobre $K/\mathbb{Q}_3$ quadrática ramificada

Na Seção 1.3 vimos que se $K/\mathbb{Q}_3$ é quadrática totalmente ramificada, então $K = \mathbb{Q}_3(\sqrt{3})$ ou $K = \mathbb{Q}_3(\sqrt{-3})$. Temos $\mathcal{O}_K/(\pi) \simeq \mathbb{F}_3$ e $\mathcal{R} = \{-1, 0, 1\}$ é um conjunto de representantes para $\mathcal{O}_K/(\pi)$. Além disso, $3 = \pm\pi^2$.

Seja f uma forma diagonal sobre $\mathcal{O}_K$ de grau $d = 3m$ com $(3.m) = 1$. Quando $m = 1$, Lewis [18] mostrou que sete variáveis são suficientes para que $f = 0$ tenha solução não trivial em K, onde K é uma extensão finita qualquer de $\mathbb{Q}_p$. Em nosso trabalho vamos supor $m \geq 2$.

Suponha f π-normalizada. Na notação do Teorema 2.1.1, temos $p = 3$, $e = 2$ e $\tau = 1$. Pelo Lema 2.3.1, $f = 0$ tem solução não trivial em K quando uma variável primária pode ser obtida no nível

$$\gamma = \left\lfloor \frac{e}{p-1} \right\rfloor + e\tau + 1 = 4.$$

Vimos na Seção 2.3 que uma etapa de contração de variáveis depende da existência de solução primitiva para uma equação do tipo

$$c_1 x_1^d + \cdots + c_t x_t^d \equiv 0 \pmod{\pi^j}$$

com $c_i \in \mathcal{O}_K$ (uma solução $(b_1, \ldots, b_s)$ é dita *primitiva* quando $b_i \not\equiv 0 \pmod{\pi}$ para algum $i \in \{1, \ldots, s\}$). Usando a descrição dos elementos de $\mathcal{O}_K$ dada pela Proposição 1.1.7, vamos determinar as d-ésimas potências em $\mathcal{O}_K/(\pi^4)$ e isso vai nos permitir encontrar contrações mais eficientes em alguns casos, ou seja, contrações onde temos certo controle do coeficiente da variável resultante. Uma vez determinadas essas contrações, vamos

estudar como combiná-las em cada possibilidade para os coeficientes da forma f. Nosso objetivo é determinar o menor número de variáveis possível, para o qual conseguimos contrações que geram uma variável primária no nível 4 em qualquer configuração possível dos coeficientes de f.

Precisamos estudar os casos m par e m ímpar separadamente pois as d-ésimas potências são diferentes em cada caso. A principal diferença está no fato de -1 ser d-ésima potência em $\mathcal{O}_K^\times$ quando d é ímpar e isso nem sempre acontece quando d é par. Na Seção 2.4, vimos como os limitantes para $\gamma_q^*(\delta)$ são significantemente menores quando δ é ímpar. Daí, é de se esperar que menos variáveis sejam necessárias para garantir solução não trivial para $f=0$ nesse caso.

Vamos assumir que as variáveis resultantes das contrações estejam no nível mais baixo possível, ou seja, se uma contração garante uma variável num certo nível l ou acima, vamos supor que ela está exatamente no nível l. Se formos capazes de garantir uma variável primária no nível necessário dessa forma, então claro que é mais fácil conseguir isso se alguma contração produzir uma variável num nível mais alto.

3.1 Caso m ímpar

Lema 3.1.1. *Seja $d=3m$, m ímpar e $(3,m)=1$. Se $K=\mathbb{Q}_3(\sqrt{3})$, as d-ésimas potências em $\mathcal{O}_K^\times/(\pi^4)$ são da forma $a+b\pi^3$ com $a,b\in\{0,1,-1\}$ e $a\neq 0$. Se $K=\mathbb{Q}_3(\sqrt{-3})$, então 1 e -1 são as únicas d-ésimas potências em $\mathcal{O}_K^\times/(\pi^4)$.*

Demonstração. Seja $x\in\mathcal{O}_K^\times$. Pela Proposição 1.1.7, temos

$$x\equiv a+b\pi+c\pi^2+d\pi^3 \pmod{\pi^4}$$

onde $a,b,c,d\in\mathcal{R}=\{0,1,-1\}$, $a\neq 0$. Daí, módulo π^4,

$$\begin{aligned} x^3 &\equiv ((a+b\pi)+\pi^2(c+d\pi))^3 \\ &\equiv (a+b\pi)^3+3(a+b\pi)^2\pi^2(c+d\pi)+3(a+b\pi)\pi^4(c+d\pi)^2+\pi^6(c+d\pi)^3 \\ &\equiv (a+b\pi)^3\equiv a^3+3a^2b\pi+3ab^2\pi^2+b^3\pi^3 \\ &\equiv a^3+3a^2b\pi+b^3\pi^3. \end{aligned}$$

Como $a \in \{1,-1\}$, temos $a^3 = a$ e $a^2 = 1$. Além disso, $3 = \pm\pi^2$ e logo $3b\pi = \pm b\pi^3$. Assim,

$$x^3 \equiv a \pm b\pi^3 + b\pi^3 \equiv \begin{cases} a & (\text{mod } \pi^4) \quad \text{se } \pi = \sqrt{-3} \\ a + 2b\pi^3 \equiv a - b\pi^3 & (\text{mod } \pi^4) \quad \text{se } \pi = \sqrt{3}. \end{cases}$$

Agora, se $\pi = \sqrt{-3}$, então

$$x^d = (x^3)^m \equiv a^m \equiv a \pmod{\pi^4}$$

pois m é ímpar. Se $\pi = \sqrt{3}$, então

$$x^d \equiv (a - b\pi^3)^m \equiv a^m - ma^{m-1}b\pi^3 \equiv a - mb\pi^3 \pmod{\pi^4}.$$

Como $(3,m) = 1$, $m \equiv \pm 1 \pmod{\pi^2}$ e logo $x^d \equiv a \pm b\pi^3 \pmod{\pi^4}$. Como $b \in \{0,1,-1\}$ podemos assumir $x^d \equiv a + b\pi^3 \pmod{\pi^4}$. □

Observação 3.1.2. Como $\mathcal{O}_K/(\pi) \simeq \mathbb{F}_3$ e d é ímpar, temos $\delta = (3m,2) = 1$. Pelo Lema 2.4.2, duas variáveis quaisquer num mesmo nível podem ser contraídas a uma nova variável um nível acima. Quando $K = \mathbb{Q}_3(\sqrt{3})$, a natureza das d-ésimas potências em $\mathcal{O}_K/(\pi^4)$ nos permite conseguir uma contração especial que vai nos poupar um nível a ser alcançado.

Proposição 3.1.3. *Sejam $K/\mathbb{Q}_3$ uma extensão quadrática totalmente ramificada e f uma forma diagonal de grau d sobre $\mathcal{O}_K$. Então, duas variáveis de f no nível l podem ser contraídas a uma variável pelo menos um nível acima. Além disso, se $K = \mathbb{Q}_3(\sqrt{3})$, podemos escolher a contração de modo que se a nova variável estiver no nível*

- *$l+1$, podemos escolher o seu π^2-coeficiente;*
- *$l+2$, podemos escolher o seu π-coeficiente;*
- *$l+3$, podemos escolher o seu 0-coeficiente.*

Em particular, se a nova variável estiver no nível $l+3$, podemos escolher se queremos subi-la mais um nível.

Nota. Lembre-se da definição de π^i-coeficiente na Seção 2.2.

Demonstração. A primeira afirmação segue da Observação 3.1.2. Sejam x_1 e x_2 duas variáveis de f com coeficientes α_1 e α_2, respectivamente. Sem perda de generalidade, podemos assumir que x_1 e x_2 estão no nível 0. Pela Proposição 1.1.7, podemos escrever

$$\alpha_i \equiv a_i + \pi b_i + \pi^2 c_i + \pi^3 d_i \pmod{\pi^4}$$

com $a_i, b_i, c_i, d_i \in \{0, 1, -1\}$, $a_i \neq 0$ para $i = 1, 2$.

Suponha, primeiramente, que $a_1 \neq a_2$. Então $a_1 + a_2 = 0$. Sejam $\alpha, \beta \in \mathcal{O}_K^\times$ tais que

$$\begin{cases} \alpha^d \equiv 1 + \pi^3 \pmod{\pi^4} \\ \beta^d \equiv 1 - \pi^3 \pmod{\pi^4}. \end{cases}$$

Os elementos α e β existem pelo Lema 3.1.1.

Fazendo $x_1 = x_2 = y$, temos

$$\begin{aligned} \alpha_1 x_1^d + \alpha_2 x_2^d &= (\alpha_1 + \alpha_2) y^d \\ &\equiv \left[(a_1 + \pi b_1 + \pi^2 c_1 + \pi^3 d_1) + (a_2 + \pi b_2 + \pi^2 c_2 + \pi^3 d_2)\right] y^d \\ &\equiv \left[\pi(b_1 + b_2) + \pi^2(c_1 + c_2) + \pi^3(d_1 + d_2)\right] y^d \\ &\equiv \left[\pi((b_1 + b_2) + \pi(c_1 + c_2) + \pi^2(d_1 + d_2))\right] y^d \pmod{\pi^4}. \end{aligned}$$

Fazendo $x_1 = y$, $x_2 = \alpha y$, temos

$$\begin{aligned} \alpha_1 x_1^d + \alpha_2 x_2^d &= (\alpha_1 + \alpha\alpha_2) y^d \\ &\equiv \left[(a_1 + \pi b_1 + \pi^2 c_1 + \pi^3 d_1) + (a_2 + \pi b_2 + \pi^2 c_2 + \pi^3 d_2)(1 + \pi^3)\right] y^d \\ &\equiv \left[(a_1 + \pi b_1 + \pi^2 c_1 + \pi^3 d_1) + (a_2 + \pi b_2 + \pi^2 c_2 + \pi^3 d_2 + \pi^3 a_2)\right] y^d \\ &\equiv \left[\pi(b_1 + b_2) + \pi^2(c_1 + c_2) + \pi^3(d_1 + d_2 + a_2)\right] y^d \\ &\equiv \left[\pi((b_1 + b_2) + \pi(c_1 + c_2) + \pi^2(d_1 + d_2 + a_2))\right] y^d \pmod{\pi^4}. \end{aligned}$$

Fazendo $x_1 = y$, $x_2 = \beta y$, temos

$$\begin{aligned}
\alpha_1 x_1^d + \alpha_2 x_2^d &= (\alpha_1 + \beta\alpha_2) y^d \\
&\equiv \left[(a_1 + \pi b_1 + \pi^2 c_1 + \pi^3 d_1) + (a_2 + \pi b_2 + \pi^2 c_2 + \pi^3 d_2)(1 - \pi^3)\right] y^d \\
&\equiv \left[(a_1 + \pi b_1 + \pi^2 c_1 + \pi^3 d_1) + (a_2 + \pi b_2 + \pi^2 c_2 + \pi^3 d_2 - \pi^3 a_2)\right] y^d \\
&\equiv \left[\pi(b_1 + b_2) + \pi^2(c_1 + c_2) + \pi^3(d_1 + d_2 - a_2)\right] y^d \\
&\equiv \left[\pi((b_1 + b_2) + \pi(c_1 + c_2) + \pi^2(d_1 + d_2 - a_2))\right] y^d \pmod{\pi^4}.
\end{aligned}$$

Agora, como $d_1, d_2 \in \{0, 1, -1\}$ e $a_2 \in \{-1, 1\}$, temos

$$\{d_1 + d_2 - a_2, d_1 + d_2, d_1 + d_2 + a_2\} = \{0, 1, -1\}.$$

Daí, sendo i o nível da variável resultante, cada tipo de contração fornece um valor diferente para o seu π^{3-i}-coeficiente e podemos escolher a mais conveniente em cada caso. Em particular, se $i = 3$, podemos escolher a contração que anula o 0-coeficiente da variável resultante, fazendo com que, assim, ela esteja no nível 4 ou acima.

Se $a_1 = a_2$, então $a_1 - a_2 = 0$ e basta tomar $\alpha = -1 + \pi^3$, $\beta = -1 - \pi^3$. A prova é análoga. □

Observe que as contrações da proposição anterior satisfazem a condição (i) do Lema 2.3.1. Assim, obter uma variável primária no nível $\gamma = 4$ através dessas contrações garante solução não trivial para $f = 0$ em K.

Observação 3.1.4. Mesmo que a Proposição 3.1.3 trate do caso em que realizamos uma única contração, a mesma conclusão pode ser obtida quando a nova variável é resultado de mais de uma etapa de contrações, contando que ela esteja no nível indicado. Por exemplo, se w é uma variável no nível $l + 3$, resultado de uma série de contrações envolvendo variáveis no nível l, uma vez determinados os coeficientes das variáveis usadas na segunda etapa em diante, podemos mudar, se for conveniente, a contração usada na primeira etapa de modo a mudar o 0-coeficiente de w permitindo que esta alcance um nível acima. Qual contração escolher vai depender dos coeficientes das variáveis usadas nas etapas seguintes.

3.1.1 Teorema para $K = \mathbb{Q}_3(\sqrt{3})$

O lema a seguir é corolário da Proposição 3.1.3 específico para $K = \mathbb{Q}_3(\sqrt{3})$.

Lema 3.1.5. *Sejam $K = \mathbb{Q}_3(\sqrt{3})$ e f uma forma de diagonal sobre $\mathcal{O}_K$ de grau d e s variáveis. Se, após contrações, uma das condições abaixo é satisfeita, então $f = 0$ tem solução não trivial em K.*

a) Há uma variável primária no nível 3.

b) Há duas variáveis no nível 2*, uma delas primária.*

c) Há duas variáveis no nível 1*, uma delas primária, e uma variável no nível* 2.

d) Há quatro variáveis no nível 1*, duas delas primárias.*

e) Há oito variáveis no nível 0.

Demonstração. Basta observar que, em cada uma das condições acima, somos capazes de obter uma variável primária no nível 4 usando as contrações da Proposição 3.1.3.

a) Segue imediatamente da Proposição 3.1.3 e da Observação 3.1.4.

b) As duas variáveis do nível 2 podem ser contraídas a uma variável primária no nível 3 e o resultado segue do item a).

c) As duas variáveis do nível 1 podem ser contraídas a uma variável primária no nível 2 e o resultado segue do item b).

d) Podemos formar dois pares, cada um contendo uma variável primária, que podem ser contraídos a duas variáveis primárias no nível 2 e o resultado segue do item b).

e) Oito variáveis do nível 0 podem ser contraídas a quatro variáveis no nível 1 e o resultado segue do item d).

□

Agora estamos prontos para provar nosso primeiro teorema!

Teorema 3.1.6. *Se $K = \mathbb{Q}_3(\sqrt{3})$ e $d = 3m$ com $m > 1$ ímpar e $(3, m) = 1$, então*

$$\Gamma_K^*(d) \leq \left\lfloor \tfrac{5}{2} d \right\rfloor + 1.$$

Demonstração. Sejam $f = a_1x_1^d + \cdots + a_sx_s^d$ com $a_i \in \mathcal{O}_K$ e $s = \left\lfloor \frac{5}{2}d \right\rfloor + 1$. Como f é π-normalizada, temos

$$m_0 \geq 3,$$
$$m_0 + m_1 \geq 6,$$
$$m_0 + m_1 + m_2 \geq 8,$$
$$m_0 + m_1 + m_2 + m_3 \geq 11 \text{ e}$$
$$m_0 + m_1 + m_2 + m_3 + m_4 \geq 13.$$

Pela definição de $\Gamma_K^*(d)$, basta mostrarmos que $f = 0$ tem solução não trivial em K. Vamos estudar os casos de acordo com o valor de m_0.

- Se $m_0 \geq 8$, o resultado segue do Lema 3.1.5 e).
- Se $m_0 = 7$ ou 6, então $m_1 + m_2 \geq 1$. Daí, $m_1 \geq 1$ ou $m_2 \geq 1$. Sete variáveis no nível 0 podem ser contraídas a três variáveis primárias no nível 1. Se $m_1 \geq 1$, o resultado segue do Lema 3.1.5 d). Se $m_1 = 0$, então há três variáveis no nível 1 e duas delas podem ser contraídas a uma variável primária no nível 2. Como $m_2 \geq 1$, o resultado segue do Lema 3.1.5 b).
- Se $m_0 = 5$ ou 4, então $m_1 \geq 1$ e $m_1 + m_2 \geq 3$. Cinco variáveis no nível 0 podem ser contraídas a duas variáveis primárias no nível 1. Se $m_1 \geq 2$, o resultado segue do Lema 3.1.5 d). Se $m_1 = 1$, então $m_2 \geq 2$ e o resultado segue do Lema 3.1.5 c).
- Se $m_0 = 3$, então $m_1 \geq 3$ e $m_1 + m_2 \geq 5$.

  Suponha primeiro, que $m_2 \geq 1$. Três variáveis no nível 0 podem ser contraídas a uma variável primária no nível 1. Essa variável pode ser contraída com alguma secundária do nível 1 para obtermos uma nova variável no nível 2 e o resultado segue do Lema 3.1.5 b).

  Suponha agora $m_2 = 0$. Temos as seguintes informações:

$$3 + m_1 \geq 6 \Rightarrow m_1 \geq 3,$$
$$3 + m_1 + 0 \geq 8 \Rightarrow m_1 \geq 5,$$
$$3 + m_1 + 0 + m_3 \geq 11 \Rightarrow m_3 \geq 11 - m_1 - 3 = 8 - m_1.$$

Podemos fazer uma mudança de variáveis que transforma f em uma outra forma f' onde as variáveis do nível 0 de f estão no nível $d-1$ em f' e todas as outras variáveis estão um nível abaixo, de modo que

$$f' = \frac{1}{\pi} f(\pi x_1, \ldots, \pi x_{m_0}, x_{m_{0+1}}, \ldots, x_s)$$

Seja m_i' o número de variáveis no nível i em f'. É fácil ver que

$$\begin{aligned} m_0' &= m_1 \geq 5, \\ m_1' &= m_2 = 0, \\ m_2' &= m_3 \geq 11 - m_1 = 8 - m_0'. \end{aligned}$$

Se $m_0' \geq 8$, então $f' = 0$ (e, portanto, $f = 0$) tem solução não trivial pelo Lema 3.1.5 e).

Se $m_0' = 7$ ou 6, como $m_2' \geq 1$, o resultado segue análogo ao caso $m_0 = 7$ ou 6.

Se $m_0' = 5$, então $m_2' \geq 3$. Cinco variáveis no nível 0 podem ser contraídas a duas variáveis primárias no nível 1 e o resultado segue do Lema 3.1.5 c), já que $m_2 \geq 1$.

□

3.1.2 Teorema para $K = \mathbb{Q}_3(\sqrt{-3})$

O lema a seguir é corolário da Proposição 3.1.3 específico para $K = \mathbb{Q}_3(\sqrt{-3})$. A prova é análoga à do Lema 3.1.5.

Lema 3.1.7. *Sejam $K = \mathbb{Q}_3(\sqrt{-3})$ e f uma forma diagonal sobre $\mathcal{O}_K$ de grau d e s variáveis. Se, após contrações, uma das condições abaixo é satisfeita, $f = 0$ tem solução não trivial em K.*

a) Há duas variáveis no nível 3, uma delas primária.

b) Há duas variáveis no nível 2, uma delas primária, e uma variável no nível 3.

c) Há quatro variáveis no nível 2, duas delas primárias.

d) Há duas variáveis no nível 1, uma delas primária, e uma variável em cada um dos níveis 2 e 3.

Lema 3.1.8. *Se há sete variáveis no nível* 0*, então* $f = 0$ *tem solução não trivial.*

Demonstração. Fazendo $\gamma = 4$ e $q = 3$ na prova do Lema 2.3.2, obtemos uma variável primária no nível 4 quando $m_0 \geq \lfloor 4\log_2 3 \rfloor + 1 = 7$. □

Teorema 3.1.9. *Se* $K = \mathbb{Q}_3(\sqrt{-3})$ *e* $d = 3m$ *com* $m > 1$ *ímpar e* $(3, m) = 1$*, então*

$$\Gamma_K^*(d) \leq 3d + 1.$$

Demonstração. Sejam $f = a_1 x_1^d + \cdots + a_s x_s^d$ com $a_i \in \mathcal{O}_K$ e $s = 3d + 1$. Como f é π-normalizada, temos

$$m_0 \geq 4,$$
$$m_0 + m_1 \geq 7,$$
$$m_0 + m_1 + m_2 \geq 10 \text{ e}$$
$$m_0 + m_1 + m_2 + m_3 \geq 13.$$

Vamos estudar os casos de acordo com o valor de m_0.

- Se $m_0 \geq 7$, o resultado segue do Lema 3.1.8.
- Se $m_0 = 6$, então $m_1 \geq 1$ e $m_1 + m_2 \geq 4$. Seis variáveis no nível 0 podem ser contraídas a três variáveis no nível 1. Se $m_1 \geq 4$, então há sete variáveis no nível 1. Por uma mudança de variáveis como a que fizemos na prova do Teorema 3.1.6, podemos obter uma forma f' com sete variáveis no nível 0. Pelo Lema 3.1.8, $f' = 0$ (e, portanto, $f = 0$) tem solução não trivial. Suponha que $m_1 = 3$. Então podemos formar três pares, cada um contendo uma variável primária, que podem ser contraídas a três variáveis primárias no nível 2. Como $m_2 \geq 1$, o resultado segue do Lema 3.1.7 c). Agora, se $m_1 \in \{1, 2\}$, há pelo menos quatro variáveis no nível 1, duas delas primárias. Isso implica duas primárias no nível 2. Como $m_2 \geq 2$, o resultado segue do Lema 3.1.7 c).
- Se $m_0 = 5$ ou 4, então $m_1 \geq 2$, $m_1 + m_2 \geq 5$ e $m_1 + m_2 + m_3 \geq 8$. Cinco variáveis no nível 0 podem ser contraídas a duas variáveis no nível 1. Daí, há pelo menos quatro variáveis no nível 1, duas delas primárias. Isso implica duas primárias no nível 2. Se $m_2 \geq 2$, o resultado segue do Lema 3.1.7 c). Se $m_2 = 1$ e $m_3 \geq 1$, o resultado segue do Lema 3.1.7 b). Se $m_2 = 1$ e $m_3 = 0$, então $m_1 \geq 7$ e o resultado segue do Lema 3.1.8 através de uma mudança de variáveis, como fizemos no caso $m_0 = 6$.

Por fim, se $m_2 = 0$ e $m_3 \geq 1$, o resultado segue do Lema 3.1.7 b) e se $m_2 = m_3 = 0$, então $m_1 \geq 8$ e o resultado segue do Lema 3.1.8.

□

3.2 Caso m par

Vamos seguir as mesmas etapas da seção anterior: descrever as d-ésimas potências e os tipos de contrações que podemos performar para, depois, estudar caso a caso como combinar essas contrações usando o menor número de variáveis possível para chegar ao nível 4. Como observamos no início do capítulo, quando m é par, -1 não é d-ésima potência e os tipos de contrações são mais restritos.

Lema 3.2.1. *Seja $d = 3m$, com m par e $(3,m) = 1$. Se $K = \mathbb{Q}_3(\sqrt{3})$, as d-ésimas potências em $\mathcal{O}_K/(\pi^4)$ são da forma $1+b\pi^3$ com $b \in \{0,1,-1\}$. Se $K = \mathbb{Q}_3(\sqrt{-3})$, então 1 é a única d-ésima potência em $\mathcal{O}_K/(\pi^4)$.*

Demonstração. A prova é praticamente a mesma do Lema 3.1.1. Dado $x \in \mathcal{O}_K$, temos

$$x^3 \equiv a \pm b\pi^3 + b\pi^3 \equiv \begin{cases} a & (\text{mod } \pi^4) \quad \text{se } \pi = \sqrt{-3}, \\ a + 2b\pi^3 \equiv a - b\pi^3 & (\text{mod } \pi^4) \quad \text{se } \pi = \sqrt{3}. \end{cases}$$

Agora, se $\pi = \sqrt{-3}$, então $x^d = (x^3)^m \equiv a^m \equiv 1 \pmod{\pi^4}$ pois m é par. Se $\pi = \sqrt{3}$, então

$$x^d \equiv (a - b\pi^3)^m \equiv a^m - ma^{m-1}b\pi^3 \equiv 1 - mab\pi^3 \pmod{\pi^4}.$$

Como $(3,m) = 1$, $m \equiv \pm 1 \pmod{\pi^2}$ e logo $x^d \equiv 1 \pm ab\pi^3$. Como $a,b \in \{0,1,-1\}$ podemos assumir $x^d \equiv 1 + b\pi^3 \pmod{\pi^4}$. □

Observação 3.2.2. Como $\mathcal{O}_K/(\pi) \simeq \mathbb{F}_3$ e d é par, temos $\delta = (3m,2) = 2$.

Proposição 3.2.3. *Sejam $K/\mathbb{Q}_3$ uma extensão quadrática totalmente ramificada e f uma forma diagonal de grau d sobre $\mathcal{O}_K$. Então duas variáveis de f no nível l com 0-coeficientes distintos podem ser contraídas a uma variável pelo menos um nível acima e três variáveis quaisquer no nível l podem ser contraídas a uma variável pelo menos um nível acima. Além disso, se $K = \mathbb{Q}_3(\sqrt{3})$, podemos escolher a contração de modo que se a nova variável estiver no nível*

- *$l+1$, podemos escolher o seu π^2-coeficiente;*
- *$l+2$, podemos escolher o seu π-coeficiente;*
- *$l+3$, podemos escolher o seu 0-coeficiente.*

Em particular, se $K=\mathbb{Q}_3(\sqrt{3})$ e a variável resultante estiver no nível $l+3$, podemos escolher se queremos subi-la mais um nível.

Demonstração. Os coeficientes de f módulo π estão em $\{1,-1\}$. Daí, duas variáveis com 0-coeficientes distintos podem ser contraídas a uma variável um nível acima fazendo a mudança $x_1=x_2=y$ e três variáveis com 0-coeficientes iguais podem ser contraídas a uma variável um nível acima fazendo a mudança $x_1=x_2=x_3=y$.

Suponha $K=\mathbb{Q}_3(\sqrt{3})$. Sejam x_1, x_2 e x_3 variáveis de f com coeficientes α_1, α_2 e α_3, respectivamente. Sem perda de generalidade, podemos assumir que x_1, x_2 e x_3 estão no nível 0. Pela Proposição 1.1.7, podemos escrever

$$\alpha_i \equiv a_i + \pi b_i + \pi^2 c_i + \pi^3 d_i \pmod{\pi^4}$$

com $a_i, b_i, c_i, d_i \in \{0,1,-1\}$, $a_i \neq 0$ para $i=1,2,3$.

Suponha, primeiramente, que entre os a_i's, dois deles são distintos. Sem perda de generalidade, podemos supor $a_1 \neq a_2$. Então $a_1+a_2=0$ e já vimos na Proposição 3.1.3 que podemos contrair x_1 e x_2 de três formas diferentes, cada uma delas fornecendo um π^3-coeficiente diferente para a variável resultante.

Suponha agora que $a_1=a_2=a_3$. Então $a_1+a_2+a_3=\pm 3 \equiv 0 \pmod{\pi^2}$.

Sejam $\alpha, \beta \in \mathcal{O}_K^\times$ tais que

$$\begin{cases} \alpha^d \equiv 1+\pi^3 \pmod{\pi^4} \\ \beta^d \equiv 1-\pi^3 \pmod{\pi^4}. \end{cases}$$

Os elementos α e β existem pela Proposição 3.2.3. Vamos analisar os efeitos das diferentes mudanças de variáveis em $\mathcal{O}_K/(\pi^4)$.

Fazendo $x_1=x_2=x_3=y$, temos

$$\begin{aligned} \alpha_1 x_1^d + \alpha_2 x_2^d + \alpha_3 x_3^d &= (\alpha_1+\alpha_2+\alpha_3) y^d \\ &= \left[\pi(b_1+b_2+b_3) + \pi^2(c_1+c_2+c_3 \pm 1) + \pi^3(d_1+d_2+d_3)\right] y^d \\ &= \left[\pi((b_1+b_2+b_3) + \pi(c_1+c_2+c_3 \pm 1) + \pi^2(d_1+d_2+d_3))\right] y^d. \end{aligned}$$

Fazendo $x_1 = x_2 = y$ e $x_3 = \alpha y$, temos

$$\begin{aligned}\alpha_1 x_1^d + \alpha_2 x_2^d + \alpha_3 x_3^d &= (\alpha_1 + \alpha_2 + \alpha\alpha_3) y^d \\ &= \left[\pi(b_1 + b_2 + b_3) + \pi^2(c_1 + c_2 + c_3 \pm 1) + \pi^3(d_1 + d_2 + d_3 + a_3)\right] y^d \\ &= \left[\pi((b_1 + b_2 + b_3) + \pi(c_1 + c_2 + c_3 \pm 1) + \pi^2(d_1 + d_2 + d_3 + a_3))\right] y^d.\end{aligned}$$

Fazendo $x_1 = x_2 = y$ e $x_3 = \beta y$, temos

$$\begin{aligned}\alpha_1 x_1^d + \alpha_2 x_2^d + \alpha_3 x_3^d &= (\alpha_1 + \alpha_2 + \alpha\alpha_3) y^d \\ &= \left[\pi(b_1 + b_2 + b_3) + \pi^2(c_1 + c_2 + c_3 \pm 1) + \pi^3(d_1 + d_2 + d_3 - a_3)\right] y^d \\ &= \left[\pi((b_1 + b_2 + b_3) + \pi(c_1 + c_2 + c_3 \pm 1) + \pi^2(d_1 + d_2 + d_3 - a_3))\right] y^d.\end{aligned}$$

Assim como na Proposição 3.1.3, como $a_3 \in \{-1, 1\}$, cada tipo de contração acima fornece um valor diferente para o π^{3-i}-coeficiente da nova variável quando ela está no nível i e podemos escolher a mais conveniente em cada caso. Em particular, se $i = 3$, podemos escolher a contração que anula o 0-coeficiente da variável resultante, fazendo com que, assim, ela esteja no nível 4 ou acima. □

Como na Proposição 3.1.3, as contrações acima satisfazem a condição (i) do Lema 2.3.1 e obter uma variável primária no nível $\gamma = 4$ através desse tipo de contração, garante uma solução não trivial para $f = 0$ em K. Além disso, aqui vale também a Observação 3.1.4: obtemos a mesma conclusão se a nova variável é resultado de múltiplas contrações.

3.2.1 Lemas importantes de contrações

Usando as contrações de forma análoga ao que fizemos no caso m ímpar, acabamos precisando de variáveis demais para garantir uma variável primária no nível 4, uma vez que as contrações da Proposição 3.2.3, usam três variáveis em vez de duas como na Proposição 3.1.3. Para evitar isso, vamos explorar mais da descrição dos coeficientes de f.

Observe que, módulo π^2, nossas contrações consistem apenas em somar os coeficientes em pares ou trios. Veremos nos lemas a seguir que, a depender dos 0 e π-coeficientes das variáveis, vamos ser capazes de escolher os pares e/ou trios mais convenientes a fim de obter contrações mais eficientes.

Lema 3.2.4. *Três variáveis no nível l, uma delas primária, podem ser contraídas a uma variável primária no nível $l+1$.*

Demonstração. Seja x_0 a variável primária e fixe seu 0-coeficiente. Se as outras duas têm 0-coeficientes iguais ao de x_0, então elas formam um trio que pode ser contraído a uma variável no nível $l+1$. Caso contrário, o 0-coeficiente de uma delas é diferente do de x_0 e elas formam um par que podem ser contraídos a uma variável no nível $l+1$. Como ambas as contrações usam x_0, a variável resultante é primária. □

Lema 3.2.5. *Entre cinco variáveis no nível l com o mesmo 0-coeficiente, há três delas que podem ser contraídas a uma variável no nível $l+2$.*

Demonstração. Se há três variáveis com π-coeficientes iguais, elas formam um trio que pode ser contraído a uma variável no nível $l+2$. Caso contrário, há pelo menos três variáveis, cada uma com um π-coeficiente distinto. As três variáveis correspondentes formam um trio que pode ser contraído a uma variável no nível $l+2$. □

Lema 3.2.6. *Entre $5+3j$ variáveis no nível l com o mesmo 0-coeficiente, há $5+3j-2$ que podem ser contraídas a $j+1$ variáveis no nível $l+2$, onde $j \geq 0$.*

Demonstração. Separe cinco variáveis. Pelo Lema 3.2.5, três delas podem ser contraídas a uma variável no nível $l+2$. Sobram $5+3j-3 = 5+3(j-1)$. Repita esse processo j vezes. Sobram cinco variáveis no nível l. Aplique o lema anterior nas cinco que restaram. Obtemos no final $j+1$ variáveis no nível $l+2$ e sobram duas no nível l. □

Observação 3.2.7. Nas demonstrações abaixo vamos diferenciar as variáveis da seguinte forma: sabemos que os 0-coeficientes das variáveis de f são 1 ou -1. Vamos denotar por x_i variáveis com um mesmo 0-coeficiente e y_j variáveis com o outro. Não há necessidade de diferenciar os 0-coeficientes no geral. Mas vale a pena destacar os π-coeficientes. Vamos chamar a_i o π-coeficiente de x_i e b_j o π-coeficiente de y_j. Naturalmente, $a_i, b_j \in \{-1, 0, 1\}$.

Lema 3.2.8. *Quatro variáveis no nível l podem participar de contrações que fornecem um dos resultados abaixo, a depender dos seus π-coeficientes.*

a) uma variável no nível $l+2$,

b) uma variável no nível $l+1$ com o 0-coeficiente que quisermos ou

c) duas variáveis no nível $l+1$ com π-coeficientes iguais mas que não podemos escolher.

Demonstração. Vamos estudar as possibilidades para os 0 e π-coeficientes.
Caso 1. As quatro têm o mesmo 0-coeficiente.

Quatro variáveis com mesmo 0-coeficiente só podem ser contraídas de uma forma: através de um trio. Se há um trio com π-coeficientes iguais ou com um de cada, a variável correspondente está no nível $l+2$.

Suponha que há dois pares, cada um com um π-coeficiente diferente. Então, podemos escolher o trio que gera uma variável no nível $l+1$ com o 0-coeficiente que quisermos. De fato, sejam x_1, x_2, x_3, x_4 as variáveis em questão. De acordo com as notações da Observação 3.2.7, temos as seguintes possibilidades:

(i) Se $a_1 = a_2 = 0$, $a_3 = a_4 \neq 0$, o trio $x_1x_2x_3$ gera uma variável com 0-coeficiente igual a a_3 e o trio $x_1x_3x_4$ gera uma variável com 0-coeficiente igual a $-a_3$, ambas no nível $l+1$.

(ii) Se $a_1 = a_2 \neq 0$, $a_3 = a_4 = -a_1$, o trio $x_1x_3x_4$ gera uma variável com 0-coeficiente igual a a_1 e o trio $x_1x_3x_4$ gera uma variável com 0-coeficiente igual a $a_3 = -a_1$, ambas no nível $l+1$.

Caso 2. Três delas têm um 0-coeficiente e uma delas tem o outro.

Se as três com o mesmo 0-coeficiente compartilham também do mesmo π-coeficiente ou cada uma tem um π-coeficiente diferente, a variável resultante da contração dessas três está no nível $l+2$.

Suponha que duas delas tenham um π-coeficiente e a terceira tenha outro. Podemos escolher qual das variáveis irá formar um par com a variável de 0-coeficiente diferente. Sejam x_1, x_2, x_3 as variáveis com um mesmo 0-coeficiente e y_1 a variável com o outro. De acordo com as notações da Observação 3.2.7, temos as seguintes possibilidades:

(i) $a_1 = a_2 = 1$ e $a_3 = -1$

Se $b_1 = 0$, então o par x_1y_1 gera uma variável com 0-coeficiente igual a 1 e o par x_3y_1 gera uma variável com 0-coeficiente igual a -1, ambas no nível $l+1$.

Se $b_1 = 1$ ou $b_1 = -1$, formamos o par x_3y_1 ou x_1y_1, respectivamente. Ambos fornecem uma variável no nível $l+2$.

(ii) $a_1 = a_2 = 0$ e $a_3 \neq 0$.

Se $b_1 = 0$ ou $b_1 = -a_3$, formamos o par x_1y_1 ou x_3y_1, respectivamente, e obtemos uma variável no nível $l+2$. Se $b_1 = a_3$, então o par x_1y_1 gera uma variável com 0-coeficiente igual a a_3 e o par x_3y_1 gera uma variável com 0-coeficiente igual a $-a_3$, ambas no nível $l+1$.

(iii) $a_1 = a_2 \neq 0$ e $a_3 = 0$.

Se $b_1 = 0$ ou $b_1 = -a_1$, formamos o par x_3y_1 ou x_1y_1, respectivamente, e obtemos uma variável no nível $l+2$. Se $b_1 = a_1$, então o par x_1y_1 gera uma variável com 0-coeficiente igual a $-a_1$ e o par x_3y_1 gera uma variável com 0-coeficiente igual a a_1, ambas no nível $l+1$.

Em qualquer caso, conseguimos uma variável no nível $l+2$ ou uma no nível $l+1$ com o 0-coeficiente que quisermos.

Caso 3. Duas delas têm um 0-coeficiente e as outras duas têm o outro.

Se há um par com 0-coeficientes diferentes que também tenham π-coeficientes opostos ou ambos nulos, então esse par gera uma variável no nível $l+2$.

Suponha que o caso anterior não acontece. Sejam x_1, x_2 as variáveis com um mesmo 0-coeficiente e y_1, y_2 as variáveis com o outro. De acordo com as notações da Observação 3.2.7, temos as seguintes possibilidades:

(i) Se $a_1 = a_2 = 0$ e $b_1 \neq b_2 \neq 0$, podemos formar dois pares que geram variáveis no nível $l+1$ com 0-coeficientes diferentes e logo, podemos obter uma variável no nível $l+2$.

(ii) Se $a_1 = a_2 = 0$ e $b_1 = b_2 \neq 0$ podemos formar dois pares que geram variáveis no nível $l+1$ com 0-coeficientes iguais que dependem de b_1. Logo, conseguimos duas variáveis no nível $l+1$ mas sem controle sobre seus π-coeficientes, exceto pelo fato de sabermos que são iguais.

(iii) Se $a_1 = 0$, $a_2 \neq 0$ e $b_1 = b_2 = a_2$, então o par x_1y_1 gera uma variável com 0-coeficiente igual a a_2 e x_2y_2 gera uma variável com 0-coeficiente igual a $-a_2$ e podemos obter uma variável no nível $l+2$.

(iv) Por último, se $a_1 = a_2 = b_1 = b_2 \neq 0$, podemos formar dois pares que geram variáveis no nível $l+1$ com 0-coeficientes iguais que não podem ser escolhidos.

Isso cobre todos os casos e prova o resultado. □

Lema 3.2.9. *Cinco variáveis no nível l podem ser contraídas a uma variável no nível $l+2$.*

Demonstração. Vamos estudar as possibilidades para os 0 e π-coeficientes.

Caso 1. As cinco têm o mesmo 0-coeficiente. O resultado segue do Lema 3.2.5.

Caso 2. Quatro delas têm um 0-coeficiente e uma delas o outro.

Podemos formar um par e um trio nesse caso. Se, entre as quatro com mesmo 0-coeficiente, há um trio com π-coeficientes iguais ou com um de cada, a variável resultante da contração dessas três está no nível $l+2$.

Se há dois pares, cada um com um π-coeficiente diferente, podemos escolher qual das variáveis irá formar um par com a variável de 0-coeficiente diferente. Sejam x_1, x_2, x_3, x_4 as variáveis com um mesmo 0-coeficiente e y_1 a variável com o outro. De acordo com as notações da Observação 3.2.7, temos as seguintes possibilidades:

(i) $a_1 = a_2 = 1$ e $a_3 = a_4 = -1$

Se $b_1 = 0$, então o par x_1y_1 gera uma variável com 0-coeficiente igual a 1 e o trio $x_2x_3x_4$ gera uma variável com 0-coeficiente igual a -1. As duas variáveis resultantes estão no nível $l+1$ e podem ser contraídas a uma nova variável no nível $l+2$.

Se $b_1 = 1$ ou $b_1 = -1$, formamos o par x_3y_1 ou x_1y_1, respectivamente. Ambos fornecem uma variável no nível $l+2$.

(ii) $a_1 = a_2 = 0$ e $a_3 = a_4 \neq 0$.

Se $b_1 = 0$, formamos o par x_1y_1 e obtemos uma variável no nível $l+2$. Se $b_1 = a_3$, então o par x_1y_1 gera uma variável com 0-coeficiente igual a a_3 e o trio $x_2x_3x_4$ gera uma variável com 0-coeficiente igual a $-a_3$. As duas variáveis resultantes estão no nível $l+1$ e podem ser contraídas a uma nova variável no nível $l+2$.

Caso 3. Três delas têm um 0-coeficiente e duas dela o outro.

Nesse caso, podemos formar dois pares ou um trio.

Se as três com o mesmo 0-coeficiente compartilham também do mesmo π-coeficiente ou cada uma tem um π-coeficiente diferente, a variável resultante da contração dessas três está no nível $l+2$.

Se duas delas têm um π-coeficiente e a terceira um outro, podemos escolher qual delas irá formar um par com uma das variáveis de 0-coeficiente diferente. Sejam x_1, x_2, x_3 as variáveis com um mesmo 0-coeficiente e y_1, y_2 as variáveis com o outro. De acordo com as notações da Observação 3.2.7, temos as possibilidades:

(i) $a_1 = a_2 = 0$, $a_3 \neq 0$.

Se uma das y_i's tem π-coeficiente igual a 0, podemos formar um par com x_1.

Se uma das y_i's tem π-coeficiente igual a $-a_3$, podemos formar um par com x_3.

Se as duas têm π-coeficiente igual a a_3, podemos formar dois pares, x_1y_1 e x_3y_2 por exemplo, que geram variáveis no nível $l+1$ com 0-coeficientes diferentes e podem ser contraídas mais uma vez.

(ii) $a_1 = a_2 \neq 0$ e $a_3 = 0$.

Basicamente a mesma coisa:

Se uma das y_i's tem π-coeficiente igual a 0, podemos formar um par com x_3.

Se uma das y_i's tem π-coeficiente igual a $-a_1$, podemos formar um par com x_1.

Se as duas têm π-coeficiente igual a a_1, podemos formar dois pares, x_1y_1 e x_3y_2 por exemplo, que geram variáveis no nível $l+1$ com 0-coeficientes diferentes e podem ser contraídas mais uma vez.

(iii) $a_1 = a_2 \neq 0$ e $a_3 = -a_1$.

Se uma das y_i's tem π-coeficiente igual a a_1, podemos formar um par com x_3.

Se uma das y_i's tem π-coeficiente igual a $-a_1$, podemos formar um par com x_1.

Se as duas têm π-coeficiente igual a 0, podemos formar dois pares, x_1y_1 e x_3y_2, por exemplo, que geram variáveis no nível $l+1$ com 0-coeficientes diferentes e podem ser contraídas mais uma vez.

Isso cobre todos os casos e prova o lema. □

Corolário 3.2.10 (Dos Lemas 3.2.8 e 3.2.9)**.** *Cinco variáveis nos níveis l e $l+1$ podem ser contraídas a uma variável no nível $l+2$.*

Demonstração. Temos os seguintes casos:

- Se as cinco estão no nível l, o resultado segue do Lema 3.2.9.
- Se quatro delas estão no nível l, então pelo Lema 3.2.8, podemos obter uma variável no nível $l+2$ ou uma variável no nível $l+1$ com 0-coeficiente diferente da que já está no nível $l+1$ ou duas variáveis no nível $l+1$ que podem formar um par ou um trio com a que já está no nível $l+1$. Em qualquer caso, obtemos uma variável no nível $l+2$.
- Se três delas estão no nível l, então elas podem ser contraídas ao nível $l+1$, onde já há duas variáveis, e o resultado segue do Lema 3.2.4.

- Se há menos de três delas no nível l, então há três ou mais no nível $l+1$, e o resultado segue do Lema 3.2.4.

□

3.2.2 Teorema para $K = \mathbb{Q}_3(\sqrt{-3})$

Lembre-se que, pelo Lema 2.3.1, $f = 0$ tem solução não trivial em K quando uma variável primária no nível $\gamma = 4$ puder ser criada. Pelo Corolário 3.2.10, é suficiente garantirmos cinco variáveis nos níveis 2 e 3 com uma quantidade suficiente delas sendo primárias. Os lemas abaixo estudam casos em que isso é possível.

Vamos dividir as variáveis em dois grupos de acordo com o 0-coeficiente delas. Não há necessidade de especificar qual grupo tem um 0-coeficiente dado. Nossa estratégia será usar o Lema 3.2.6 para garantir o máximo de variáveis primárias no nível 2 e então usar as variáveis que sobrarem no nível 0 em contrações até o nível 1 quando for possível.

Lema 3.2.11. *Se $m_0 \geq 18$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos estudar os casos de acordo com o número de variáveis com cada 0-coeficiente.
Caso 1. Se todas ou 17 delas têm um mesmo 0-coeficiente, podemos obter cinco variáveis no nível 2 pelo Lema 3.2.6, e o resultado segue.

Caso 2. Se há 16, 15 ou 14 delas com um mesmo 0-coeficiente, podemos obter quatro variáveis no nível 2 e sobram seis variáveis no nível 0 pelo Lema 3.2.6. Cinco delas podem ser contraídas a mais uma variável no nível 2 usando o Lema 3.2.9 e a conclusão é a mesma do Caso 1.

Caso 3. Se há 13, 12 ou 11 delas com um mesmo 0-coeficiente, então há pelo menos cinco variáveis com o outro 0-coeficiente. Aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $3+1=4$ variáveis no nível 2 e sobram seis variáveis no nível 0. A conclusão é a mesma do Caso 2.

Caso 4. Se há dez ou nove delas com um mesmo 0-coeficiente, então há pelo menos oito variáveis com o outro 0-coeficiente. Aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $2+2=4$ variáveis no nível 2 e sobram seis variáveis no nível 0. A conclusão é a mesma do Caso 2. □

Lema 3.2.12. *Se $m_0 = 17$ e $m_1 \geq 2$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos seguir as linhas do Lema 3.2.11.
Caso 1. Se todas elas têm o mesmo 0-coeficiente, podemos obter cinco variáveis no nível 2 pelo Lema 3.2.6 e o resultado segue.

Caso 2. Se há 16, 15 ou 14 delas com um mesmo 0-coeficiente, podemos obter quatro variáveis no nível 2 pelo Lema 3.2.6 e sobram cinco variáveis no nível 0 que podem ser contraídas a mais uma variável no nível 2 pelo Lema 3.2.9. A conclusão é a mesma do Caso 1.

Caso 3. Se há 13 delas com um mesmo 0-coeficiente, podemos obter três variáveis no nível 2 pelo Lema 3.2.6 e sobram oito variáveis no nível 0. Cinco delas podem ser contraídas ao nível 2 e as três que restaram podem ser contraídas ao nível 1. Como $m_1 \geq 2$, podemos aplicar o Lema 3.2.4 e obter mais uma variável no nível 2. Terminamos com cinco variáveis no nível 2 e a conclusão é a mesma do Caso 1.

Caso 4. Se há 12 ou 11 delas com um mesmo 0-coeficiente, então há pelo menos cinco variáveis com o outro 0-coeficiente. Aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $3+1=4$ variáveis no nível 2 e sobram cinco variáveis no nível 0. A conclusão é a mesma do Caso 2.

Caso 5. Se há dez delas com um mesmo 0-coeficiente, então há sete variáveis com o outro 0-coeficiente. Aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $2+1=3$ variáveis no nível 2 e sobram oito variáveis no nível 0. A conclusão é a mesma do Caso 3.

Caso 6. Se há nove delas com um mesmo 0-coeficiente, então há oito variáveis com o outro 0-coeficiente. Aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $2+2=4$ variáveis no nível 2 e sobram cinco variáveis no nível 0. A conclusão é a mesma do Caso 2. □

Lema 3.2.13. *Se $m_0 = 16$ e $m_1 \geq 3$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos seguir as linhas do Lema 3.2.11.
Caso 1. Se todas, 15 ou 14 delas têm o mesmo 0-coeficiente, podemos obter quatro variáveis no nível 2 pelo Lema 3.2.6 e sobram quatro no nível 0. Aplicando o Lema 3.2.8 e usando que $m_1 \geq 1$, podemos obter mais uma variável no nível 2 e o resultado segue.

Caso 2. Se há 13 ou 12 delas com um mesmo 0-coeficiente, podemos obter três variáveis no nível 2 pelo Lema 3.2.6 e sobram sete variáveis no nível 0, quatro com um mesmo 0-coeficiente e três com o outro. Podemos formar três pares que podem ser contraídos ao nível 1. Como $m_1 \geq 3$, podemos formar dois trios, cada um deles contendo pelo menos

uma variável primária. Pelo Lema 3.2.4, obtemos mais duas variáveis no nível 2 e o resultado segue.

Caso 3. Se há 11 delas com um mesmo 0-coeficiente e cinco delas com o outro, aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $3+1=4$ variáveis no nível 2 e sobram quatro variáveis no nível 0. A conclusão é a mesma do Caso 1.

Caso 4. Se há dez ou nove delas com um mesmo 0-coeficiente, então há pelo menos seis variáveis com o outro 0-coeficiente. Aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $2+1=3$ variáveis no nível 2 e sobram sete variáveis no nível 0. A conclusão é a mesma do Caso 2.

Caso 5. Se há oito delas com um mesmo 0-coeficiente e oito com o outro, aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $2+2=4$ variáveis no nível 2 e sobram quatro variáveis no nível 0. A conclusão é a mesma do Caso 1. □

Lema 3.2.14. *Se $m_0=15$ e $m_1\geq 4$, então $f=0$ tem solução não trivial em K.*

Demonstração. Vamos seguir as linhas do Lema 3.2.11.
Caso 1. Se todas ou 14 delas têm o mesmo 0-coeficiente, podemos obter quatro variáveis no nível 2 pelo Lema 3.2.6 e sobram três variáveis no nível 0 que podem ser contraídas a uma variável no nível 1. Como $m_1\geq 2$, podemos usar o Lema 3.2.4 para garantir mais uma no nível 2 e o resultado segue.

Caso 2. Se há 13, 12 ou 11 delas com um mesmo 0-coeficiente, podemos obter três variáveis no nível 2 pelo Lema 3.2.6 e sobram seis variáveis no nível 0 que podem ser contraídas a duas variáveis no nível 1. Como $m_1\geq 4$, podemos formar dois trios contendo pelo menos uma variável primária e isso nos dá duas variáveis no nível 2 pelo Lema 3.2.4. O resultado segue.

Caso 3. Se há dez, nove ou oito delas com um mesmo 0-coeficiente, então há pelo menos cinco variáveis com o outro. Aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $2+1=3$ variáveis no nível 2 e sobram seis variáveis no nível 0. A conclusão é a mesma do Caso 2. □

Quando $m_0=14$, conseguimos no máximo quatro variáveis no nível 2 e em alguns casos não sobram variáveis suficientes no nível 0 para obtermos uma primária no nível 1 e assim podermos usar condições sobre m_1. Daí, precisamos acrescentar condições sobre m_2

Lema 3.2.15. *Se $m_0=14$, $m_1\geq 2$ e $m_2\geq 1$, então $f=0$ tem solução não trivial em K.*

Demonstração. Vamos seguir as linhas do Lema 3.2.11.
Caso 1. Se todas elas têm o mesmo 0-coeficiente, podemos obter quatro variáveis no nível 2 pelo Lema 3.2.6 e sobram duas variáveis no nível 0 que não podem ser contraídas. Como $m_2 \geq 1$, o resultado segue do Corolário 3.2.10.

Caso 2. Se há 13, 12 ou 11 delas com um mesmo 0-coeficiente, podemos obter três variáveis no nível 2 pelo Lema 3.2.6 e sobram cinco variáveis no nível 0 que podem ser contraídas a mais uma variável no nível 2. A conclusão é a mesma do Caso 1.

Caso 3. Se há dez delas com um mesmo 0-coeficiente e quatro delas com o outro, podemos obter duas variáveis no nível 2 pelo Lema 3.2.6 e sobram oito variáveis no nível 0 que podem ser contraídas a mais uma variável no nível 2 e uma no nível 1. Como $m_1 \geq 2$, podemos usar o Lema 3.2.4 para garantir mais uma no nível 2 e a conclusão é a mesma do Caso 2.

Caso 4. Se há nove ou oito delas com um mesmo 0-coeficiente, então há pelo menos cinco variáveis com o outro. Aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $2+1=3$ variáveis no nível 2 e sobram cinco variáveis no nível 0. A conclusão é a mesma do Caso 2.

Caso 5. Se há sete delas com um mesmo 0-coeficiente e sete com o outro, aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $1+1=2$ variáveis no nível 2 e sobram oito variáveis no nível 0. A conclusão é a mesma do Caso 3. □

Lema 3.2.16. *Se $m_0 = 13$, $m_1 \geq 3$ e $m_2 \geq 1$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos seguir as linhas do Lema 3.2.11.
Caso 1. Se todas, 12 ou 11 delas têm o mesmo 0-coeficiente, podemos obter três variáveis no nível 2 pelo Lema 3.2.6 e sobram quatro variáveis no nível 0 que podem ser contraídas ao nível 1 e como $m_1 \geq 2$, terminamos com pelo menos quatro variáveis no nível 2. Como $m_2 \geq 1$, o resultado segue do Corolário 3.2.10.

Caso 2. Se há dez ou nove delas com um mesmo 0-coeficiente, podemos obter duas variáveis no nível 2 pelo Lema 3.2.6 e sobram sete variáveis no nível 0 que podem ser contraídas a três variáveis no nível 1. Como $m_1 \geq 3$, podemos formar dois trios, cada um contendo uma variável primária e isso nos dá duas variáveis no nível 2. Como $m_2 \geq 1$, o resultado segue.

Caso 3. Se há oito delas com um mesmo 0-coeficiente e cinco delas com o outro, aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $2+1=3$ variáveis no nível 2 e sobram quatro variáveis no nível 0. A conclusão é a mesma do Caso 1.

Caso 4. Se há sete delas com um mesmo 0-coeficiente e seis delas com o outro, aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $1+1=2$ variáveis no nível 2 e sobram sete variáveis no nível 0. A conclusão é a mesma do Caso 2. □

Lema 3.2.17. *Se $m_0 = 12$, $m_1 \geq 4$ e $m_2 \geq 1$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos seguir as linhas do Lema 3.2.11.
Caso 1. Se todas ou 11 delas têm o mesmo 0-coeficiente, podemos obter três variáveis no nível 2 pelo Lema 3.2.6 e sobram quatro variáveis no nível 0 que podem ser contraídas ao nível 1. Como $m_1 \geq 2$, terminamos com pelo menos quatro variáveis no nível 2, e como $m_2 \geq 1$, o resultado segue do Corolário 3.2.10.

Caso 2. Se há dez, nove ou oito delas com um mesmo 0-coeficiente, podemos obter duas variáveis no nível 2 pelo Lema 3.2.6 e sobram seis variáveis no nível 0 que podem ser contraídas a duas variáveis no nível 1. Como $m_1 \geq 4$, podemos formar dois trios, cada um contendo uma variável primária, e isso nos dá mais duas variáveis no nível 2. Como $m_2 \geq 1$, o resultado segue do Corolário 3.2.10.

Caso 3. Se há sete ou seis delas com um mesmo 0-coeficiente, então há pelo menos cinco variáveis com o outro. Aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $1+1=2$ variáveis no nível 2 e sobram seis variáveis no nível 0. A conclusão é a mesma do Caso 2. □

Lema 3.2.18. *Se $m_0 = 11$, $m_1 \geq 4$ e $m_2 \geq 6$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos seguir as linhas do Lema 3.2.11.
Caso 1. Se todas elas têm o mesmo 0-coeficiente, podemos obter três variáveis no nível 2 pelo Lema 3.2.6 e sobram duas variáveis no nível 0 que não podem ser contraídas ao nível 1. Como $m_2 \geq 6$, podemos formar três trios, cada um contendo uma variável primária e pelo Lema 3.2.4, podemos obter três variáveis no nível ≥ 3 e o resultado segue.

Caso 2. Se há dez, nove ou oito delas com um mesmo 0-coeficiente, podemos obter duas variáveis no nível 2 pelo Lema 3.2.6 e sobram cinco variáveis no nível 0 que podem ser contraídas a mais uma variável no nível 2. A conclusão é a mesma do Caso 1.

Caso 3. Se há sete delas com um mesmo 0-coeficiente e quatro delas com o outro, podemos obter uma variável no nível 2 pelo Lema 3.2.6 e sobram oito variáveis no nível 0 que podem ser contraídas a mais uma variável no nível 2 e uma no nível 1. Como $m_1 \geq 2$, obtemos mais uma no nível 2 e a conclusão é a mesma do Caso 1.

Caso 4. Se há seis delas com um mesmo 0-coeficiente e cinco com o outro, aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $1+1=2$ variáveis no nível 2 e sobram cinco variáveis no nível 0. A conclusão é a mesma do Caso 2. □

Observação 3.2.19. Apesar dos lemas acima serem enunciados com condições sobre m_0, é claro que uma mudança de variáveis cíclica permite que encontremos solução não trivial para $f=0$ se as condições estão sobre qualquer nível, por exemplo, o Lema 3.2.11 nos diz que se f possui um nível com pelo menos 18 variáveis, então há solução não trivial. Usamos isso na prova do teorema abaixo.

Teorema 3.2.20. *Se* $K=\mathbb{Q}_3(\sqrt{-3})$ *e* $d=3m$ *com* m *par e* $(3,m)=1$*, então*

$$\Gamma_K^*(d)\leq \tfrac{31}{3}d+1.$$

Demonstração. Seja $f=a_1x_1^d+\cdots+a_sx_s^d$ com $a_i\in\mathcal{O}_K$ e $s=\frac{31}{3}d+1$. Como f é π-normalizada, temos

$$m_0\geq 11,$$
$$m_0+m_1\geq 21 \text{ e}$$
$$m_0+m_1+m_2\geq 32.$$

Vamos mostrar que $f=0$ tem solução não trivial em K. Os lemas anteriores já resolveram todos os casos:

- Se $m_0\geq 18$, o resultado segue do Lema 3.2.11.
- Se $m_0=17$, 16 ou 15, então $m_1\geq 4$ e o resultado segue dos Lemas 3.2.12, 3.2.13 ou 3.2.14, respectivamente.
- Se $m_0=14$, então $m_1\geq 7$ e $m_1+m_2\geq 18$.
  - Se $m_1\geq 18$, o resultado segue do Lema 3.2.11.
  - Se $m_1\leq 17$, então $m_2\geq 1$ e o resultado segue do Lema 3.2.15.
- Se $m_0=13$, então $m_1\geq 8$ e $m_1+m_2\geq 19$.
  - Se $m_1\geq 18$, o resultado segue do Lema 3.2.11.
  - Se $m_1\leq 17$, então $m_2\geq 1$ e o resultado segue do Lema 3.2.16.

- Se $m_0 = 12$, então $m_1 \geq 9$ e $m_1 + m_2 \geq 20$.
  - Se $m_1 \geq 18$, o resultado segue do Lema 3.2.11.
  - Se $m_1 \leq 17$, então $m_2 \geq 1$ e o resultado segue do Lema 3.2.17.
- Se $m_0 = 11$, então $m_1 \geq 10$ e $m_1 + m_2 \geq 21$.
  - Se $m_1 \geq 18$, o resultado segue do Lema 3.2.11.
  - Se $m_1 = 17$ ou 16, $m_2 \geq 4$ e o resultado segue dos Lemas 3.2.12, 3.2.13 respectivamente.
  - Se $m_1 \leq 15$, então $m_2 \geq 6$ e o resultado segue do Lema 3.2.18.

□

3.2.3 Teorema para $K = \mathbb{Q}_3(\sqrt{3})$

Como no caso m ímpar, quando $K = \mathbb{Q}_3(\sqrt{3})$, basta alcançarmos o nível 3 com as contrações da Proposição 3.2.3, pela Observação 3.1.4. Pelo Lema 3.2.4, é suficiente garantirmos três variáveis no nível 2, uma delas primária. Os lemas abaixo estudam casos em que isso é possível.

Lema 3.2.21. *Se $m_0 \geq 11$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Esse é, essencialmente, o Lema 3.2.18.
Caso 1. Se todas elas têm o mesmo 0-coeficiente, podemos obter três variáveis no nível 2 pelo Lema 3.2.6 e o resultado segue.

Caso 2. Se há dez, nove ou oito delas com um mesmo 0-coeficiente, podemos obter duas variáveis no nível 2 pelo Lema 3.2.6 e sobram cinco variáveis no nível 0 que podem ser contraídas a mais uma variável no nível 2. A conclusão é a mesma do Caso 1.

Caso 3. Se há sete delas com um mesmo 0-coeficiente e quatro delas com o outro, podemos obter uma variável no nível 2 pelo Lema 3.2.6 e sobram oito variáveis no nível 0, quatro com cada 0-coeficiente, que podem ser contraídas a quatro variáveis no nível 1. Aplicando o Lema 3.2.8, podemos obter uma ou duas variável no nível 2 que podem ser contraídas com a variável que já está no nível 2 e o resultado segue.

Caso 4. Se há seis delas com um mesmo 0-coeficiente e cinco variáveis com o outro, aplicando o Lema 3.2.6 aos dois grupos de variáveis, obtemos $1 + 1 = 2$ variáveis no nível 2 e sobram cinco variáveis no nível 0. A conclusão é a mesma do Caso 2. □

Lema 3.2.22. *Se $m_0 = 10$ e $m_1 \geq 1$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos estudar os casos de acordo com o valor de m_0.

Caso 1. Se todas, nove ou oito delas têm o mesmo 0-coeficiente, podemos obter duas variáveis no nível 2 pelo Lema 3.2.6 e sobram quatro no nível 0. Aplicando o Lema 3.2.8 e usando que $m_1 \geq 1$, podemos obter mais uma variável no nível 2 e o resultado segue.

Caso 2. Se há sete ou seis delas com um mesmo 0-coeficiente, podemos obter uma variável no nível 2 pelo Lema 3.2.6 e sobram sete variáveis no nível 0, quatro com um 0-coeficiente e três com o outro, que podem ser contraídas a três variáveis no nível 1. Como $m_1 \geq 1$, podemos aplicar o Lema 3.2.8 para obter uma ou duas variável no nível 2 que podem ser contraídas com a variável que já está no nível 2 e o resultado segue.

Caso 3. Se há cinco delas com cada 0-coeficiente, podemos obter duas variáveis no nível 2 pelo Lema 3.2.6 e sobram quatro variáveis no nível 0. A conclusão é a mesma do Caso 1. □

Lema 3.2.23. *Se $m_0 = 9$ e $m_1 \geq 2$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos estudar os casos de acordo com o valor de m_0.

Caso 1. Se todas ou oito delas têm o mesmo 0-coeficiente, podemos obter duas variáveis no nível 2 pelo Lema 3.2.6 e sobram três no nível 0 que podem ser contraídas a uma variável no nível 1. Como $m_1 \geq 2$, podemos obter mais uma variável no nível 2 e o resultado segue pelo Lema 3.2.4.

Caso 2. Se há sete, seis ou cinco delas com um mesmo 0-coeficiente, podemos obter uma variável no nível 2 pelo Lema 3.2.6 e sobram seis variáveis no nível 0 que podem ser contraídas a duas variáveis no nível 1. Como $m_1 \geq 2$, podemos aplicar o Lema 3.2.8 para obter uma ou duas variáveis no nível 2 que podem ser contraídas com a variável que já está no nível 2 e o resultado segue. □

Lema 3.2.24. *Se $m_0 = 8$ e $m_2 \geq 1$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos estudar os casos de acordo com o valor de m_0.

Caso 1. Se todas elas têm o mesmo 0-coeficiente, podemos obter duas variáveis no nível 2 pelo Lema 3.2.6 e sobram duas no nível 0 que não podem ser contraídas. Como $m_2 \geq 1$, o resultado segue do Lema 3.2.4.

Caso 2. Se há sete, seis ou cinco delas com um mesmo 0-coeficiente, podemos obter uma variável no nível 2 pelo Lema 3.2.6 e sobram cinco variáveis no nível 0 que podem ser contraídas a mais uma no nível 2. A conclusão é a mesma do Caso 1. □

Lema 3.2.25. *Se $m_0 = 7$, $m_1 \geq 1$ e $m_2 \geq 1$, então $f = 0$ tem solução não trivial em K.*

Demonstração. Vamos estudar os casos de acordo com o valor de m_0.

Caso 1. Se todas, seis ou cinco delas têm o mesmo 0-coeficiente, podemos obter uma variável no nível 2 pelo Lema 3.2.6 e sobram quatro no nível 0 que podem ser contraídas a uma ou duas variáveis no nível 1 que podem ser contraídas com a variável que já está no nível 1, uma vez que $m_1 \geq 1$. Terminamos com duas variáveis no nível 2 e como $m_2 \geq 1$, o resultado segue do Lema 3.2.4.

Caso 2. Se há quatro delas com um mesmo 0-coeficiente e três com o outro, podemos formar três pares que podem ser contraídos ao nível 1. Como $m_1, m_2 \geq 1$, terminamos com quatro variáveis no nível 1 e uma no nível 2. O resultado segue do Corolário 3.2.10. □

Teorema 3.2.26. *Se $K = \mathbb{Q}_3(\sqrt{3})$ e $d = 3m$ com m par e $(3,m) = 1$, então*

$$\Gamma_K^*(d) \leq 6d + 1.$$

Demonstração. Seja $f = a_1 x_1^d + \cdots + a_s x_s^d$ com $a_i \in \mathcal{O}_K$ e $s = 6d + 1$. Como f é π-normalizada, temos

$$m_0 \geq 7,$$
$$m_0 + m_1 \geq 13 \text{ e}$$
$$m_0 + m_1 + m_2 \geq 19.$$

Vamos mostrar que $f = 0$ tem solução não trivial em K. Os lemas anteriores já resolveram todos os casos:

- Se $m_0 \geq 11$, o resultado segue do Lema 3.2.21.
- Se $m_0 = 10$ ou 9, então $m_1 \geq 3$ e o resultado segue dos Lemas 3.2.22 ou 3.2.23, respectivamente.
- Suponha $m_0 = 8$. Então $m_1 \geq 5$ e $m_1 + m_2 \geq 11$.
  - Se $m_1 \geq 11$, o resultado segue do Lema 3.2.21.
  - Se $m_1 \leq 10$, então $m_2 \geq 1$ e o resultado segue do Lema 3.2.24.

- Por fim, se $m_0 = 7$, então $m_1 \geq 6$ e $m_1 + m_2 \geq 12$.
  - Se $m_1 \geq 11$, o resultado segue do Lema 3.2.21.
  - Se $m_1 \leq 10$, então $m_2 \geq 1$ e o resultado segue do Lema 3.2.25.

□

Capítulo 4

Formas de grau $3m$ sobre $K/\mathbb{Q}_3$ quadrática não ramificada

Quando K é quadrática não ramificada, temos $\mathcal{O}_K/(\pi) \simeq \mathbb{F}_9$ e $\pi = 3$. Seja f uma forma diagonal sobre $\mathcal{O}_K$ de grau $d = 3m$ com $m \geq 2$ e $(3, m) = 1$. Podemos supor f π-normalizada. Na notação do Teorema 2.1.1, temos $p = 3, e = 1$ e $\tau = 1$. Pelo Lema 2.3.1, $f = 0$ tem solução não trivial em K quando uma variável primária pode ser obtida no nível

$$\gamma = \left\lfloor \frac{e}{p-1} \right\rfloor + e\tau + 1 = 2.$$

Aqui também vamos assumir o "pior caso possível", ou seja, se uma contração garante uma variável num certo nível l ou acima, vamos supor que ela está no nível l.

4.1 Caso m ímpar

Como $\delta = (3m, 8) = 1$, pelo Lema 2.4.2, duas variáveis quaisquer num mesmo nível podem ser contraídas a uma nova variável pelo menos um nível acima.

Teorema 4.1.1. *Se $K/\mathbb{Q}_3$ é quadrática não ramificada e $d = 3m$ com m ímpar e $(3, m) = 1$, então*

$$\Gamma_K^*(d) \leq \left\lfloor \tfrac{3}{2}d \right\rfloor + 1.$$

Demonstração. Seja $f = a_1 x_1^d + \cdots + a_s x_s^d$ com $a_i \in \mathcal{O}_K$ e $s = \left\lfloor \frac{3}{2}d \right\rfloor + 1$. Como f é π-normalizada, temos $m_0 \geq 2$ e $m_0 + m_1 \geq 4$. Vamos mostrar que uma variável primária no nível 2 pode ser criada.

Pelo Lema 2.4.2, duas variáveis no nível 0 podem ser contraídas a uma variável primária no nível 1.

Se $m_0 \geq 4$, então duas variáveis primárias podem ser obtidas no nível 1 que, por sua vez, podem ser usadas numa contração para obter uma variável no nível 2.

Se $m_0 \in \{2,3\}$, então $m_1 \geq 1$. Duas ou três variáveis no nível 0 garantem uma variável primária no nível 1. Como $m_1 \geq 1$, há duas variáveis no nível 1 que podem ser contraídas a uma nova variável primária num nível 2.

Isso conclui a prova. □

4.2 Caso m par

Quando m é par, temos $\delta = (d, q-1) = (3m, 8) = 2$, 4 ou 8. Para lidar com os diferentes casos para δ, vamos precisar da definição do seguinte invariante.

Dado $d \in \mathbb{N}$, defina $l_q(d)$ como sendo o menor inteiro positivo tal que

$$x_1^d + \cdots + x_s^d = 0$$

tem solução não trivial em $\mathbb{F}_q$ sempre que $s \geq l_q(d)$. Pelo Teorema 2.4.1, temos $l_q(d) = l_q(\delta)$ e, como essa equação define um tipo particular de forma diagonal, temos $2 \leq l_q(\delta) \leq \gamma_q^*(\delta)$. Em [18], Leep e Vieira mostraram que l_q satisfaz as seguintes propriedades:

Lema 4.2.1 (Leep, Vieira)**.** *Seja $q = p^f$.*

a) $1 \leq l_q(\delta) \leq p$

b) Se $j \geq 2$ é um divisor de $q-1$ e $\delta \mid \frac{q-1}{j}$, então $l_q(\delta) \leq j$.

c) Se q é ímpar, então $l_q(\delta) = 2 \Leftrightarrow \delta \mid \frac{q-1}{2}$.

Demonstração. Veja [18], Lemas 3.6 e 3.8. □

Observação 4.2.2. O conjunto $(\mathbb{F}_q^*)/(\mathbb{F}_q^*)^\delta$ é um grupo cíclico de δ elementos gerado por $h(\mathbb{F}_q^*)^\delta$ onde $h \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^\delta$. Daí, se f é uma forma diagonal sobre $\mathbb{F}_q$ de grau $\delta \mid q-1$ e $a \in \mathbb{F}_q^*$ é um coeficiente de f, então $a \in h^i(\mathbb{F}_q^*)^\delta$ para algum $i \in \{0, \ldots, \delta-1\}$. Daí, $a = h^i b^\delta$ para algum $b \in \mathbb{F}_q^*$. Fazendo a mudança de variáveis $y = bx$, obtemos

$$ax^\delta = h^i b^\delta x^\delta = h^i y^\delta.$$

Fazendo uma mudança desse tipo em todos os coeficientes de f, obtemos uma forma g de grau δ e com coeficientes em $\{h^i : 0 \leq i \leq \delta-1\}$. Claro que uma solução não trivial

para $g=0$ determina uma solução não trivial para $f=0$ e vice versa. Assim, podemos assumir que os coeficientes de f estão entre os δ representantes de $(\mathbb{F}_q^*)/(\mathbb{F}_q^*)^\delta$.

Lema 4.2.3. *Seja $q=p^f$. Então*

$$\gamma_q^*(\delta) \leq \delta(l_q(\delta)-1)+1.$$

Se $\delta \nmid \frac{q-1}{2}$, então

$$\gamma_q^*(\delta) \leq \frac{\delta}{2}(l_q(\delta)-1)+1.$$

Demonstração. Seja $f=a_1x_1^\delta+\cdots+a_sx_s^\delta$ sobre $\mathbb{F}_q$. Pela Observação 4.2.2, podemos supor que os coeficientes de f estão entre os δ representantes de $(\mathbb{F}_q^*)/(\mathbb{F}_q^*)^\delta$. Pelo Princípio da casa dos pombos, se $s \geq \delta(l_q(\delta)-1)+1$, pelo menos $l_q(\delta)$ dos coeficientes de f são iguais e isso define uma solução não trivial para $f=0$ em $\mathbb{F}_q$ pela definição de l_q.

Agora, se $\delta \nmid \frac{q-1}{2}$, então -1 é elemento de alguma das $\delta-1$ classes não nulas de $\mathbb{F}_q^*/(\mathbb{F}_q^*)^\delta$ e, pelo Princípio da casa dos pombos, entre $\frac{\delta}{2}(l_q(\delta)-1)+1$ variáveis, há $l_q(\delta)$ delas com coeficientes iguais ou duas delas, digamos, x_i e x_j cujos coeficientes são tais que $a_i \equiv -a_j \pmod{\pi}$. Ambos os casos determinam uma solução para $f=0$ em $\mathbb{F}_q$. □

Para simplificar a notação, vamos escrever $l_q(\delta)=l$ e $\gamma_q^*(\delta)=\gamma^*$ de agora em diante.

Observação 4.2.4. O lema anterior pode ser expresso de forma geral no contexto de contração de variáveis como o seguinte.

a) Se $\delta \mid \frac{q-1}{2}$, então $l=2$ e entre $\delta+2(j-1)+1$ variáveis no mesmo nível, há j grupos com duas variáveis com coeficientes iguais que podem ser contraídas a j variáveis num nível acima e sobram, no mínimo, $\delta-1$ variáveis não utilizadas.

b) Agora, se $\delta \nmid \frac{q-1}{2}$, então entre $\frac{\delta}{2}(l-1)+l(j-1)+1$ variáveis no mesmo nível, há j grupos com l variáveis com coeficientes iguais ou com duas variáveis x_i, x_j cujos coeficientes são tais que $a_i \equiv -a_j \pmod{\pi}$, que podem ser contraídas a j variáveis num nível acima e sobram, no mínimo, $\frac{\delta}{2}(l-1)-l+1$ variáveis não utilizadas.

Vamos usar essas informações para obter o último caso do limitante para $\Gamma_K^*(d)$ que buscamos.

Teorema 4.2.5. *Se $K/\mathbb{Q}_3$ é quadrática não ramificada e $d=3m$ com m par e $(3,m)=1$, então*

a) $\Gamma_K^*(d) \leq 4d+1$ *se* $\delta=2$ *ou* 4.

b) $\Gamma_K^*(d) \leq 14d+1$ *se* $\delta=8$.

Demonstração. Vamos mostrar que uma variável primária no nível 2 pode ser obtida.

a) Seja $f = a_1x_1^d + \cdots + a_sx_s^d$ com $a_i \in \mathcal{O}_K$ e $s = 4d+1$. Como f é π-normalizada, temos $m_0 \geq 5$ e $m_0 + m_1 \geq 9$. Quando $\delta = 2$ ou 4, temos $l = 2$ pelo Lema 4.2.1 c) e $\gamma^* = 3$ pelo Lema 2.4.8.

Suponha $\delta = 2$. Se $m_0 \geq 7$, então podemos obter três variáveis primárias no nível 1 pela Observação 4.2.4 a), o que nos dá uma variável primária no nível 2. Se $m_0 = 6$ ou 5, então duas variáveis podem ser obtidas no nível 1 pela Observação 4.2.4 a). Como $m_1 \geq 3$, podemos usar uma das secundárias do nível 1 num trio e obter uma variável no nível 2. Isso conclui a prova nesse caso.

Suponha agora $\delta = 4$. Se $m_0 \geq 7$, podemos obter duas variáveis primárias no nível 1 pela Observação 4.2.4 a) e sobram $\delta - 1 = 3$ variáveis no nível 0 que podem ser contraídas a mais uma no nível 1 pelo Lema 2.4.8. Terminamos com três variáveis no nível 1 que, por sua vez, podem ser contraídas ao nível 2. Se $m_0 = 6$ ou 5, podemos obter uma variável no nível 1 pela Observação 4.2.4 a) e sobram no mínimo três variáveis no nível 0 que podem ser contraídas a mais uma no nível 1 pelo Lema 2.4.8. Terminamos com duas variáveis no nível 1. Como $m_1 \geq 3$, podemos usar uma das secundárias do nível 1 num trio e obter uma variável no nível 2.

b) Seja $f = a_1x_1^d + \cdots + a_sx_s^d$ com $a_i \in \mathcal{O}_K$ e $s = 14d+1$. Como f é π-normalizada, temos $m_0 \geq 15$ e $m_0 + m_1 \geq 29$. Quando $\delta = 8$, temos $l = 3$ pelo Lema 4.2.1 itens a) e c) e $\gamma^* \leq 5$ pelo Lema 2.4.9. Se $m_0 \geq 18$, então podemos obter quatro variáveis no nível 1 e sobram $\delta - 1 = 7$ variáveis no nível 0 pela Observação 4.2.4 b). Cinco delas podem ser contraídas a mais uma no nível 1 e o resultado segue aplicando o Lema 2.4.9 às variáveis no nível 1. Se $m_0 = 17, 16$ ou 15, então três variáveis podem ser obtidas no nível 1 pela Observação 4.2.4 b) e sobram seis variáveis no nível 0 que podem ser contraídas a mais uma no nível 1. Terminamos com quatro variáveis no nível 1. Como $m_1 \geq 12$, o resultado segue.

Isso conclui a prova do teorema. □

Observação 4.2.6. O Teorema 4.2.5 foi o primeiro resultado onde enxergamos a dependência entre $\Gamma_K^*(d)$ e os invariantes γ^* e l. Observe que usamos as contrações dadas pela Observação 4.2.4 e, quando as variáveis restantes ultrapassam γ^*, conseguimos mais uma variável. Ao estudar o caso $d = pm$ em $K/\mathbb{Q}_p$ quadrática, essa estratégia se faz necessária e a detalharemos no capítulo seguinte.

Capítulo 5

Formas de grau pm sobre $K/\mathbb{Q}_p$ quadrática

5.1 Caso K não ramificada

Se K é quadrática não ramificada, temos $\mathcal{O}_K/(\pi) \simeq \mathbb{F}_{p^2}$. Seja f uma forma diagonal sobre $\mathcal{O}_K$ de grau $d = pm$ com $(p,m) = 1$. Na notação do Teorema 2.1.1, temos $e = 1$ e $\tau = 1$. Pelo Lema 2.3.1, $f = 0$ tem solução não trivial em K quando uma variável primária pode ser obtida no nível

$$\gamma = \left\lfloor \frac{e}{p-1} \right\rfloor + e\tau + 1 = 2.$$

Seja $\delta = (d, p^2-1)$. Para simplificar a notação, vamos escrever $l_q(\delta) = l$ e $\gamma_q^*(\delta) = \gamma^*$.

Para alcançar o nível 2, primeiro, determinamos qual o menor número de variáveis necessário para realizar uma única contração. Depois, determinamos qual o jeito mais eficiente de obter essa quantidade de variáveis no nível 1 a partir de variáveis no nível 0, ou seja, precisaremos realizar múltiplas contrações e queremos as contrações que usam a menor quantidade de variáveis quando realizadas em sequência. Em resumo, queremos responder as duas perguntas abaixo:

1. Qual o menor número de variáveis num mesmo nível que garante uma variável um nível acima?
2. Qual a forma mais eficiente de conseguir esse número de variáveis no nível 1?

Os resultados da Seção 2.4 respondem à Pergunta 1. Precisamos de pelo menos γ^* variáveis num mesmo nível. Como não conseguimos controlar quantas das variáveis serão,

de fato, usadas na contração, precisamos que pelo menos γ^*-1 delas sejam primárias caso queiramos que a variável resultante seja primária.

Para a Pergunta 2, seja $w=\left\lfloor\frac{\delta(l-1)-1}{\gamma^*}\right\rfloor$. Suponha que queiramos obter j variáveis no nível 1. Vamos começar aplicando a Observação 4.2.4 a) para obter $j-w$ variáveis. Para isso, usamos $\delta(l-1)+l(j-w-1)+1$ variáveis e sobram, no mínimo, $\delta(l-1)-1$ no nível 0. Vamos chamar essas contrações de *contrações Tipo 1*. As variáveis que sobraram, separamos em w grupos de tamanho γ^* e cada grupo pode ser contraído a mais uma variável no nível 1. Sobram no máximo γ^*-1 variáveis que não podem mais ser usadas em contrações. Vamos chamar essa segunda forma de realizar contrações de *contrações Tipo 2*.

Para obter as γ^*-1 variáveis primárias necessárias no nível 1 usando o processo descrito acima, precisamos de pelo menos $\delta(l-1)-1$ variáveis no nível 0 se $w\geq\gamma^*-1$. Se $w\leq\gamma^*-2$, precisamos de

$$\delta(l-1)+l(\gamma^*-w-2)+1 \tag{5.1.1}$$

no nível 0. Isso nos dá o resultado abaixo.

Teorema 5.1.1. *Sejam $K/\mathbb{Q}_p$ uma extensão quadrática não ramificada e $d=pm$ com $(p,m)=1$. Seja $w=\left\lfloor\frac{\delta(l-1)-1}{\gamma^*}\right\rfloor$. Então*

$$\Gamma_K^*(d)\leq\begin{cases}(\delta(l-1)+l(\gamma^*-w-2))\,d+1 & \text{se } w\leq\gamma^*-2,\\ (\delta(l-1)-2)d+1 & \text{se } w\geq\gamma^*-1.\end{cases}$$

5.1.1 Caso $\delta\mid\frac{q-1}{2}$

Quando $\delta\mid\frac{q-1}{2}$, pelo Lema 4.2.1 c), temos $l=2$ e $\delta+1$ variáveis no nível 0 garantem que duas delas possam ser contraídas a uma variável primária no nível 1. Daí, as estimativas para $\Gamma_K^*(d)$ no teorema anterior são expressões mais simples. Por exemplo, para $\delta\leq 4$, temos os valores exatos para γ^* e podemos usá-las para obter os resultados abaixo.

Suponha primeiro que $(d,q-1)=1$. Então, módulo π, as equações que determinam as contrações de variáveis são lineares e $\gamma^*=2$. O resultado abaixo estende o caso $K/\mathbb{Q}_3$ não ramificada e d ímpar e a demonstração é exatamente a mesma do Teorema 4.1.1.

Lema 5.1.2. *Se $\delta=1$, então*

$$\Gamma_K^*(d)\leq\left\lfloor\tfrac{3}{2}d\right\rfloor+1.$$

Quando $\delta = 2$ ou 4, temos $\gamma^* = 3$ pelo Lema 2.4.8. De novo, o resultado abaixo estende o Teorema 4.2.5 a).

Lema 5.1.3. *Se $\delta = 2$ ou 4 então*

$$\Gamma_K^*(d) \leq 4d+1.$$

Quando $\delta = 3$, temos $\gamma^* = 3$ pelo Lema 2.4.8.

Lema 5.1.4. *Se $\delta = 3$, então*

$$\Gamma_K^*(d) \leq 4d+1.$$

Demonstração. Seja $f = a_1x_1^d + \cdots + a_sx_s^d$ com $a_i \in \mathcal{O}_K$ e $s = 4d+1$. Como f é π-normalizada, temos $m_0 \geq 5$ e $m_0 + m_1 \geq 9$.

Vamos mostrar que uma variável primária no nível 2 pode ser criada. Pelo Lema 2.4.8, basta obtermos três variáveis no nível 1 com pelo menos duas delas primárias.

Se $m_0 \geq 8$, três variáveis podem ser obtidas no nível 1 e o resultado segue.

Se $m_0 = 7$ ou 6, então conseguimos duas variáveis no nível 1. Como $m_0 + m_1 \geq 9$, temos $m_1 \geq 2$ e o resultado segue.

Se $m_0 = 5$, conseguimos uma variável no nível 1 ao contrair um par de variáveis com coeficientes iguais ou inversos módulo π. Sobram três no nível 0 que podem ser contraídas a mais uma no nível 1 aplicando o Lema 2.4.8. Daí, obtemos duas variáveis primárias no nível 1 e $m_1 \geq 4$.

Isso conclui a prova. □

Quando $\delta \geq 5$, temos $w \geq 1$. Como exemplo de como usar o limitante (5.1.1), temos o lema abaixo.

Lema 5.1.5. *Se $\delta \geq 5$, então*

$$\Gamma_K^*(d) \leq (\delta + 2(\gamma^* - 3))d + 1.$$

Demonstração. Seja $f = a_1x_1^d + \cdots + a_sx_s^d$ com $a_i \in \mathcal{O}_K$ e $s = (\delta + 2(\gamma^* - 3))d + 1$. Como f é π-normalizada, temos

$$m_0 \geq \frac{s}{d} = \delta + 2(\gamma^* - 3) + \frac{1}{d} \Rightarrow m_0 \geq \delta + 2(\gamma^* - 3) + 1 \text{ e}$$

$$m_0 + m_1 \geq \frac{2s}{d} = 2\delta + 4(\gamma^* - 3) + \frac{2}{d} \Rightarrow m_0 + m_1 \geq 2\delta + 4(\gamma^* - 3) + 1.$$

Vamos mostrar que uma variável primária no nível 2 pode ser criada. Para isso, precisamos de γ^* variáveis no nível 1, pelo menos γ^*-1 delas primárias.

Se $m_0 \geq \delta+2(\gamma^*-3)+3 = \delta+2(\gamma^*-2)+1$, pela Observação 4.2.4 a), podemos obter γ^*-1 variáveis no nível 1, sobram $\delta-1$ variáveis no nível 0. Como $\delta \geq 5$, temos $\frac{\delta+3}{2} \leq \delta-1$ e podemos aplicar o Teorema 2.4.4 para obter mais uma variável primária no nível 1, terminando assim com γ^* variáveis no nível 1.

Se $m_0 = \delta+2(\gamma^*-3)+2 = \delta+2(\gamma^*-2)$, pelo Lema 4.2.4 a), podemos obter γ^*-2 variáveis no nível 1, sobram δ variáveis no nível 0. De novo, podemos obter mais uma variável primária no nível 1 a partir das que sobraram no nível 0, totalizando γ^*-1 variáveis no nível 1. Agora, como $m_0+m_1 \geq 2\delta+4(\gamma^*-3)+1$, temos

$$m_1 \geq 2\delta+4(\gamma^*-3)+1-(\delta+2(\gamma^*-3)+2) = \delta+2(\gamma^*-3)-1 \geq 4$$

pois $\delta \geq 5$ por hipótese e $\gamma^* \geq 3$ pelo Lema 2.4.2. Daí, podemos usar uma das secundárias do nível 1 para completar as γ^* variáveis necessárias.

Por fim, se $m_0 = \delta+2(\gamma^*-3)+1$, o resultado segue análogo ao caso anterior. Isso conclui a prova. □

Pelo Lema 2.3.2, temos que $m_0 \geq \lfloor 2\log_2 q \rfloor + 1 = \lfloor 4\log_2 p \rfloor + 1$ garante uma variável primária no nível 2, fornecendo um forma diferente de chegar ao nível 2.

Lema 5.1.6. *Sejam $K/\mathbb{Q}_p$ quadrática não ramificada e $d = pm$ com $(p,m)=1$. Se $\delta \mid \frac{q-1}{2}$, então*

$$\Gamma_K^*(d) \leq \lfloor 4\log_2 p \rfloor d + 1.$$

Observe que como $p \leq d$, temos $\lfloor 4\log_2 p \rfloor \leq \lfloor 4\log_2 d \rfloor$. Em particular, quando $m > p^3$, temos $d > p^4$ e $\Gamma_K^*(d) \leq \lfloor \log_2 d \rfloor d + 1$.

Claro que, quando d é grande, um limitante da forma $Cd+1$ com C uma constante absoluta é mais interessante do que um com C que depende de d. Assim, uma vez fixos δ e γ^*, o Lema 5.1.5 é mais interessante que o Lema 5.1.6 para d suficientemente grande.

5.2 Caso K totalmente ramificada

Se K é totalmente ramificada, temos $\mathcal{O}_K/(\pi) \simeq \mathbb{F}_p$. Seja f uma forma diagonal sobre $\mathcal{O}_K$ de grau $d = pm$ com $(p,m)=1$. Na notação do Teorema 2.1.1, temos $e=2$ e $\tau=1$. Pelo Lema 2.3.1, $f=0$ tem solução não trivial em K quando uma variável primária pode

ser obtida no nível

$$\gamma = \left\lfloor \frac{e}{p-1} \right\rfloor + e\tau + 1 = 3.$$

O caso $\delta = 1$ é, essencialmente, o Teorema 3.1.6.

Lema 5.2.1. *Se $\delta = 1$, então*

$$\Gamma_K^*(d) \leq \left\lfloor \tfrac{5}{2} d \right\rfloor + 1.$$

Para o caso $\delta > 1$, vamos usar o mesmo raciocínio da seção anterior: pelo Teorema 5.1.1, precisamos de $M = \delta(l-1) + l(\gamma^* - w - 1) + 1$ variáveis no nível 1 para garantir uma variável primária no nível 3, onde $w = \left\lfloor \frac{\delta(l-1)-1}{\gamma^*} \right\rfloor$.

Com essas variáveis no nível 1, vamos executar γ^* contrações. As contrações do Tipo 1 produzem $\gamma^* - w$ variáveis e cada uma das contrações usam l variáveis com coeficientes iguais e todas elas recebem o coeficiente 1 na mudança de variáveis que define a contração. Isso quer dizer que basta que uma delas seja primária para garantir que a variável resultante seja primaria.

As contrações do Tipo 2 produzem as w variáveis restantes e como não conseguimos controlar os coeficientes da mudança de variáveis nesse caso, podemos ter apenas uma variável secundária em cada contração.

Isso quer dizer que não precisamos de tantas variáveis primárias! Mas manipular essas quantidades no caso geral não é fácil. Vamos enunciar o resultado considerando o número de variáveis que precisamos no nível zero sem a ajuda das variáveis secundárias nos níveis acima. Em casos particulares onde temos os valores de l e γ^*, podemos fazer as reduções cabíveis.

Teorema 5.2.2. *Se $\delta \mid q-1$, então*

$$\Gamma_K^*(d) \leq (\delta(l-1) + l(M - w - 1))\, d + 1$$

onde $M = (\delta(l-1) + l(\gamma^* - w - 1)) + 1$ e $w = \left\lfloor \frac{\delta(l-1)-1}{\gamma^*} \right\rfloor$.

Demonstração. Pelo Teorema 5.1.1, precisamos de $M = \delta(l-1) + l(\gamma^* - w - 1) + 1$ variáveis no nível 1, para garantir uma variável primária no nível 3. Daí, precisamos de

$\delta(l-1)+l(M-w-1)+1$ no nível 0. Em resumo, temos

$$\begin{array}{c}\text{uma variável no nível 3}\\ \Uparrow\\ \gamma^* \text{ variáveis no nível 2}\\ \Uparrow\\ M=\delta(l-1)+l(\gamma^*-w-1)+1 \text{ variáveis no nível 1}\\ \Uparrow\\ \delta(l-1)+l(M-w-1)+1 \text{ variáveis no nível 0.}\end{array}$$

Isso mostra o resultado. □

5.3 Exemplo: formas de grau particular

Valores exatos para $\Gamma_K^*(d)$ são conhecidos quando $K=\mathbb{Q}_p$ para vários $d\in\mathbb{N}$. Por exemplo, $\Gamma_{\mathbb{Q}_p}^*(15)=61$ e $\Gamma_{\mathbb{Q}_p}^*(6)=37$ (veja [14] e [4], respectivamente). Usando nossos resultados e alguns fatos já provados antes por outros autores, vamos comparar $\Gamma_K^*(15)$ e $\Gamma_K^*(6)$ quando K é extensão quadrática de $\mathbb{Q}_p$ com os valores citados acima. Exceto para uma extensão específica em cada caso, conseguimos alcançar o mesmo limitante determinado para $K=\mathbb{Q}_p$.

5.3.1 Formas de grau 15

Seja f uma forma diagonal de grau 15 sobre $K/\mathbb{Q}_p$ quadrática.

Primeiro, suponha $p=3$.

Se $K/\mathbb{Q}_3$ é não ramificada, então, pelo Teorema 4.1.1,

$$\Gamma_K^*(15)\leq\left\lfloor\tfrac{3}{2}\cdot 15\right\rfloor+1=22+1=23.$$

Se $K=\mathbb{Q}_3(\sqrt{3})$, então, pelo Teorema 3.1.6

$$\Gamma_K^*(15)\leq\left\lfloor\tfrac{5}{2}\cdot 15\right\rfloor+1=37+1=38.$$

Por fim, se $K=\mathbb{Q}_3(\sqrt{-3})$, então pelo Teorema 3.1.9

$$\Gamma_K^*(15)\leq 3\cdot 15+1=46.$$

Suponha agora $p = 5$.

Se $K/\mathbb{Q}_5$ é não ramificada, temos $\mathcal{O}_K \simeq \mathbb{F}_{25}$ e $\delta = (15, 24) = 3$. Pelo Lema 5.1.4, temos

$$\Gamma_K^*(15) \leq 4 \cdot 15 + 1 = 61.$$

Se $K/\mathbb{Q}_5$ é totalmente ramificada, temos $\mathcal{O}_K \simeq \mathbb{F}_5$ e $\delta = (15, 4) = 1$. Pelo Lema 5.2.1, temos

$$\Gamma_K^*(15) \leq \left\lfloor \tfrac{5}{2} \cdot 15 \right\rfloor + 1 = 38.$$

Para $p \neq 3, 5$, temos $(15, p) = 1$ e $\tau = 0$ na notação do Teorema 2.1.1. Daí, basta obter uma variável primária no nível 1 através de contrações pelo Lema 2.3.1. Observe que $\delta = (15, q-1) = 1, 3, 5$ ou 15.

Se $\delta = 1$ então, módulo π, f é linear e basta que $m_0 \geq 2$ pelo Lema 2.4.2. Se $\delta = 3$, basta que $m_0 \geq 3$ pelo Lema 2.4.8 e se $\delta = 5$, basta que $m_0 \geq 4$ pelo Lema 2.4.8. Isso mostra que

$$\Gamma_K^*(15) \leq \begin{cases} 15 + 1 = 16 & \text{se } \delta = 1, \\ 2 \cdot 15 + 1 = 31 & \text{se } \delta = 3, \\ 3 \cdot 15 + 1 = 46 & \text{se } \delta = 5. \end{cases}$$

Por fim, seja $\delta = 15$. Vamos mostrar que, exceto possivelmente para $K/\mathbb{Q}_{11}$ não ramificada, $m_0 \geq 5$ é suficiente para garantir uma variável primária no nível 1.

Cinco variáveis são suficientes para garantir solução não trivial de $f \equiv 0 \pmod{\pi}$, sempre que $q < 2^5 = 32$ pelo Lema 2.4.5 e

$$q \geq 5^{-1} \cdot 15 \cdot 14^{\frac{5}{5-2}} = 3 \cdot 14^{\frac{5}{3}} > 243$$

pelo Teorema 2.4.7. Daí, basta que estudemos os números da forma $q = p$ ou p^2 entre 32 e 243. Além disso, como $15 \mid \frac{q-1}{2}$, temos $q \equiv 1 \pmod{30}$. Os inteiros satisfazendo essas condições são:

$$61, 121, 151, 181, 211 \text{ e } 241.$$

Observe que nessa lista, apenas o 121 não é primo. Em [14], Knapp apresentou um argumento computacional que mostra que cinco variáveis são suficientes para que $f = 0$ em $\mathbb{F}_p$ tenha solução não trivial para uma lista de p primos que inclui os primos que precisamos verificar. Isso resolve nosso problema para todos os casos restantes, exceto para $q = 121 = 11^2$. Nesse último caso, o melhor limitante que temos é dado pelo Teorema 2.4.6: $\gamma_q^*(15) \leq \lceil 2\log_2 15 - \log_2 \log_2 15 \rceil + 1 = 7$.

Em resumo, obtemos o seguinte resultado.

Teorema 5.3.1. *Seja $K/\mathbb{Q}_p$ uma extensão quadrática com $\mathcal{O}_K/(\pi) \neq \mathbb{F}_{11^2}$. Então*

$$\Gamma_K^*(15) \leq 4 \cdot 15 + 1 = 61$$

Se $\mathcal{O}_K/(\pi) = \mathbb{F}_{11^2}$, então $\Gamma_K^*(15) \leq 6 \cdot 15 + 1 = 91$.

Agora, seguindo as ideias de Norton em [22], podemos exibir um exemplo que nos dá um limitante inferior para $\Gamma_K^*(15)$. Observe que $2 \cdot 15 + 1 = 31$ é primo. Se $K/\mathbb{Q}_{31}$ é totalmente ramificada, então $\mathcal{O}_K/(\pi) \simeq \mathbb{F}_{31}$. Para $\overline{x}_i = (x_i, y_i, z_i, t_i)$, defina $f(\overline{x}_i) = x_i^{15} + 2y_i^{15} + 4z_i^{15} + 8t_i^{15}$. É fácil ver que a equação $f(\overline{x}_i) \equiv 0 \pmod{31}$ não tem solução não trivial. Daí,

$$\mathcal{F} = \sum_{i=0}^{14} \pi^i f(\overline{x}_i)$$

é uma forma diagonal em 60 variáveis que não tem zero não trivial em K.

De fato, observe que se $(b_1, \ldots, b_{60})$ é uma solução não trivial de $\mathcal{F} = 0$ com, digamos, $b_i \neq 0$, então $b_i = \pi^a u$ com $u \in \mathcal{O}_K^\times$ e, como $\mathcal{F}$ é um polinômio homogêneo, $(b_1/\pi^a, \ldots, b_{60}/\pi^a)$ também é uma solução de $\mathcal{F} = 0$ com $b_i/\pi^a = u \in \mathcal{O}_K^\times$. Assim, se existe uma solução não trivial em K, então existe uma solução primitiva, ou seja, com alguma entrada coprima com π.

Agora, suponha que $\mathcal{F} \equiv 0 \pmod{\pi^{15}}$ tenha uma solução não trivial. Então, em particular, $f(\overline{x}_0) \equiv 0 \pmod{\pi}$. Como esta última congruência não tem solução não trivial módulo π, devemos ter $x_0 \equiv y_0 \equiv z_0 \equiv t_0 \equiv 0 \pmod{\pi}$. Com essa informação, temos

$$\begin{aligned} \mathcal{F} &= \sum_{i=1}^{14} \pi^i f(\overline{x}_i) = \pi \sum_{i=1}^{14} \pi^{i-1} f(\overline{x}_i) \equiv 0 \pmod{\pi^{15}} \\ \Rightarrow & \sum_{i=1}^{14} \pi^{i-1} f(\overline{x}_i) \equiv 0 \pmod{\pi^{14}}. \end{aligned}$$

Repetindo o mesmo argumento, obtemos $x_i \equiv y_i \equiv z_i \equiv t_i \equiv 0 \pmod{\pi}$ para $i = 0, \ldots, 14$. Assim, toda solução de $\mathcal{F} \equiv 0 \pmod{\pi^{15}}$ em K deve ser nula módulo π, impossível. Isso mostra que a única solução de $\mathcal{F} = 0$ em K é a trivial e $\Gamma_K^*(15) = 61$ quando $K/\mathbb{Q}_{31}$ é quadrática totalmente ramificada.

Observação 5.3.2. Fica a pergunta se cinco variáveis são suficientes para garantir uma solução não trivial para $f = 0$ em $\mathbb{F}_{11^2}$. Os métodos computacionais usados por Knapp usam fortemente o fato de $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ quando p é primo e portanto não se aplicam ao nosso caso.

5.3.2 Formas de grau 6

Seja f uma forma diagonal de grau 6 sobre $K/\mathbb{Q}_p$ quadrática.

Se $p=2$, os trabalhos de Knapp [15] e Duncan e Leep [7] determinam que $\Gamma_K^*(6)=9$ ou 7 quando K é totalmente ramificada, a depender da extensão.

Quando K é não ramificada, por Knapp [15] e Bruno [5] temos $19 \leq \Gamma_K^*(6) \leq 29$.

Seja $p=3$.

Se $K/\mathbb{Q}_3$ é não ramificada, como $\delta=(6,8)=2$, temos pelo Teorema 4.2.5,

$$\Gamma_K^*(6) \leq 4\cdot 6+1 = 24+1 = 25.$$

Se $K=\mathbb{Q}_3(\sqrt{3})$, então, pelo Teorema 3.2.26

$$\Gamma_K^*(6) \leq 6\cdot 6+1 = 36+1 = 37.$$

Por fim, se $K=\mathbb{Q}_3(\sqrt{-3})$, então pelo Teorema 3.2.20

$$\Gamma_K^*(6) \leq \frac{31}{3}\cdot 6+1 = 62+1 = 63.$$

Para $p\neq 2,3$, temos $(6,p)=1$ e $\tau=0$ na notação do Teorema 2.1.1. Daí, basta obter uma variável primária no nível 1 através de contrações pelo Lema 2.3.1. Observe que $\delta=(6,q-1)=1,2,3$ ou 6.

Se $\delta=1$ então, módulo π, f é linear e basta que $m_0\geq 2$ pelo Lema 2.4.2. Se $\delta=2$ ou 3, basta que $m_0\geq 3$ pelo Teorema 2.4.4 e pelo Lema 2.4.8, respectivamente. Se $\delta=6$ e $\delta \mid \frac{q-1}{2}$, basta que $m_0\geq 4$ pelo Lema 2.4.8. Caso contrário, precisamos que $m_0\geq 7$ pelo Teorema 2.4.3. Isso mostra que

$$\Gamma_K^*(6) \leq \begin{cases} 6+1=7 & \text{se } \delta=1, \\ 2\cdot 6+1=13 & \text{se } \delta=2 \text{ ou } 3, \\ 6\cdot 6+1=37 & \text{se } \delta=6. \end{cases}$$

Em resumo, obtemos o teorema abaixo.

Teorema 5.3.3. *Seja $K/\mathbb{Q}_p$ uma extensão quadrática com $K\neq\mathbb{Q}_3(\sqrt{-3})$. Então*

$$\Gamma_K^*(6) \leq 6^2+1 = 37.$$

Se $K=\mathbb{Q}_3(\sqrt{-3})$, então $\Gamma_K^*(6) \leq \frac{31}{6}\cdot 15+1 = 63$.

Analogamente ao que fizemos no caso $d = 15$, uma vez que $6+1 = 7$ é primo, temos $x^6 = 0$ ou 1 em $\mathbb{F}_7$ e é fácil ver que a forma

$$\mathcal{F} = \sum_{i=0}^{6} \pi^i f(\overline{x}_i)$$

onde $f(\overline{x}_i) = x_{i_1}^6 + x_{i_2}^6 + x_{i_3}^6 + x_{i_4}^6 + x_{i_5}^6 + x_{i_6}^6$ é uma forma diagonal em 36 variáveis que não tem zero não trivial em $K/\mathbb{Q}_7$ quadrática totalmente ramificada.

Observação 5.3.4. O fato de o limitante de $\Gamma_K^*(6)$ não ter alcançado o da conjectura de Artin quando $K = \mathbb{Q}_3(\sqrt{-3})$ ilustra bem as restrições que encontramos ao realizar as contrações de variáveis no Teorema 3.2.20. Como 1 é a única 6-ésima potência módulo π^4, não conseguimos realizar contrações tão eficientes.

Considerações finais

A conjectura de Artin para formas diagonais tem motivado o trabalho de muitos matemáticos nas últimas décadas. Além da expectativa de provar a conjectura no caso geral, há também a busca por limitantes superiores para $\Gamma_K^*(d)$ que se aproximem (e, idealmente, alcancem) o seu valor exato. Como vimos na introdução, em vários casos particulares, esse problema já foi resolvido. Mas inúmeros outros casos ainda podem ser abordados. São muitas possibilidades! Neste trabalho, escolhemos trabalhar com formas diagonais sobre extensões quadráticas de $\mathbb{Q}_p$, $p > 2$, inspirados nos trabalhos recentes sobre extensões quadráticas de $\mathbb{Q}_2$. Nosso objetivo era determinar um limitante da forma

$$\Gamma_K^*(d) \leq Cd + 1$$

onde C é uma constante absoluta. Um resultado desse tipo fornece um limitante melhor que o conjecturado por Artin sempre que $d > C$.

O método de contrações de variáveis é o padrão para trabalhar com problemas desse tipo. Ele funciona bem quando temos informações suficientes sobre o corpo de resíduos para garantir contrações eficientes. Por exemplo, no Capítulo 3, conhecer as d-ésimas potências em $\mathcal{O}_K/(\pi^4)$ quando m é ímpar nos permitiu um limitante melhor para uma das extensões totalmente ramificadas. Quando m é par, a análise dos π-coeficientes foi fundamental para conseguirmos um limitante não tão longe do obtido no caso m ímpar, apesar de ser maior (o que é esperado, uma vez que o fato de -1 ser d-ésima potência no caso m ímpar torna as contrações mais eficientes). Mas essa abordagem deixa de ser viável quando os representantes de $\mathcal{O}_K/(\pi)$ são muitos. Isso ilustra bem a limitação do método quando generalizamos o grau da extensão e/ou o grau das formas diagonais estudadas. Nesse aspecto, é necessário que novas estratégias sejam desenvolvidas para lidarmos com problemas mais gerais. Precisamos de ideias que nos permitam encontrar contrações eficientes, mesmo quando o grau da forma ou da extensão (e, logo, o nível a ser alcançado com as contrações) exigirem variáveis demais com as contrações que

já conhecemos. Leep e Vieira em [18], já lidaram com um problema do tipo, quando obtiveram um resultado válido para extensões de qualquer grau finito, desde que o índice de ramificação seja 1.

Os resultados que obtemos nos capítulos 3 e 4 fornecem limitantes melhores ou iguais ao conjecturado por Artin, exceto no caso $d = 6$ e $K = \mathbb{Q}_3(\sqrt{-3})$. No Capítulo 5, nos deparamos com a relação de dependência entre $\Gamma_K^*(d)$ e δ, e observamos como, por exemplo, o caso $d = 3m$ com m ímpar e $K/\mathbb{Q}_3$ não ramificada quadrática do Teorema 4.1.1 é um caso particular de $d = pm$ com $(d, p^2 - 1) = 1$ e $K/\mathbb{Q}_p$ não ramificada quadrática no Lema 5.1.2. Já o caso $d = 3m$ com m par e $(d, 8) = 2$ ou 4 e $K/\mathbb{Q}_3$ não ramificada quadrática (ítem a) do Teorema 4.2.5) é um caso particular de $d = pm$ com $(d, p^2 - 1) = 2$ ou 4 e $K/\mathbb{Q}_p$ não ramificada quadrática no Lema 5.1.3. Isso não é suspeito. O valor de δ (juntamente com o conhecimento de $\gamma_q^*(\delta)$ e de $l_q(\delta)$) e o número de níveis a subir são fatores determinantes na performance das contrações. Dois níveis são suficientes precisamente quando $e = \tau = 1$ e $p \geq 3$ (ou seja, quando $d = pm$ e $K/\mathbb{Q}_p$ é finita não ramificada). Melhorias podem ser obtidas aqui, se soubermos mais sobre as variantes envolvidas.

Muitas perguntas permanecem em aberto. As primeiras que queremos responder são:

- Quais ideias precisamos ter para resolver o caso excepcional onde nosso resultado não superou o limitante conjectura por Artin?
- Se mantermos as extensões quadráticas ramificadas de $\mathbb{Q}_3$ e o grau qualquer, será se vale a conjectura? (isso, junto com o resultado de Leep e Vieira, resolveria a conjectura para extensões quadráticas de $\mathbb{Q}_3$, o que seria bem legal!)
- O nosso resultado do Capítulo 5 não exibe uma relação direta com a conjectura de Artin. Quais os casos particulares onde esse resultado supera a conjectura? Será se conseguimos uma versão onde a conjectura é superada sempre?

Uma coisa é certa: tem muita coisa a ser feita. Nossa trajetória está apenas começando!

Referências Bibliográficas

[1] C. Broll, M. P. Knapp, J. A. Kuiper, P. H. Rodrigues, and D. Veras. More exact values of the function $\Gamma^*(k)$. *Journal of Number Theory*, 233:481–497, 2022.

[2] J. Cassels. *Local Fields*. London Mathematical Society Student Texts. Cambridge University Press, 1986.

[3] C. Chevalley. Démonstration d'une hypothèse de M. Artin. *Abh. Math. Sem. Hamburg*, 11:73–75, 1935.

[4] H. Davenport and D. J. Lewis. Homogeneous additive equations. *Proc. Roy. Soc. London Ser. A*, 274:443–460, 1963.

[5] B. de Paula Miranda, H. Godinho, and M. P. Knapp. Diagonal forms over quadratic extensions of $\mathbb{Q}_2$. *Publ. Math. Debrecen*, 101(1-2):63–101, 2022.

[6] D. Duncan and D. B. Leep. Solubility of additive forms of twice odd degree over ramified quadratic extensions of $\mathbb{Q}_2$. *Acta Arith.*, 201(2):149–164, 2021.

[7] D. Duncan and D. B. Leep. Solubility of additive sextic forms over $\mathbb{Q}_2(\sqrt{-1})$ and $\mathbb{Q}_2(\sqrt{-5})$. *Publ. Math. Debrecen*, 99(3-4):431–446, 2021.

[8] F. Gouvêa. *p-adic Numbers: An Introduction*. Universitext. Springer International Publishing, 2020.

[9] J. F. Gray. *Diagonal Forms of Prime Degree*. 1959. Thesis (Ph.D.)–University of Notre Dame.

[10] M. Greenberg and J. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 2013.

[11] K. Hensel. *Theorie der algebraischen Zahlen*, volume 1. BG Teubner, 1908.

[12] K. F. Ireland and M. I. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, revised edition, 1982.

[13] M. Knapp. Exact values of the function $\Gamma^*(k)$. *Journal of Number Theory*, 131:1901–1911, 2011.

[14] M. P. Knapp. Pairs of additive forms of odd degrees. *Michigan Math. J.*, 61(3):493–505, 2012.

[15] M. P. Knapp. Solubility of additive sextic forms over ramified quadratic extensions of $\mathbb{Q}_2$. *Publ. Math. Debrecen*, 95(1-2):67–91, 2019.

[16] S. Lang. *On quasi algebraic closure*. ProQuest LLC, Ann Arbor, 1951. Thesis (Ph.D.)–Princenton University.

[17] S. Lang. On quasi algebraic closure. *Ann. of Math*, 55:373–390, 1952.

[18] D. B. Leep and L. Sordo Vieira. Diagonal equations over unramified extensions of $\mathbb{Q}_p$. *Bull. Lond. Math. Soc.*, 50(4):619–634, 2018.

[19] D. J. Lewis. Cubic congruences. *Michigan Math. J.*, 4:85–95, 1957.

[20] F. Lorenz and S. Levy. *Algebra: Volume II: Fields with Structure, Algebras and Advanced Topics*. Universitext. Springer New York, 2007.

[21] B. Miranda. *Diagonal forms over the unramified quadratic extension of* $\mathbb{Q}_2$. 2018. Thesis (Ph.D.)-Universidade de Brasília.

[22] K. K. Norton. *On Homogeneous Diagonal Congruences of Odd Degree*. 1966. Thesis (Ph.D.)–University of Illinois at Urbana-Champaign.

[23] J. E. Olson. A combinatorial problem on finite abelian groups, I and II. *Journal of Number Theory*, 1:8–10 and 195–199, 1969.

[24] R. Petrik. *Solutions to Systems of Equations over Finite Fields*. 2020. Thesis (Ph.D.)-University of Kentucky.

[25] C. L. Siegel. Additive theorie der zahlenkörper II. *Ann. of Math*, 88:184–210, 1923.

[26] C. Skinner. Solvability of systems of diagonal equations over p-adic local fields. *Proc. Lond. Math. Soc. (3)*, 122(2):207–228, 2021.

[27] G. Terjanian. Un contre-exemple à une conjecture d'Artin. *C. R. Acad. Sci. Paris Sér. A-B*, 262:A612, 1966.

[28] A. Tietäväinen. On diagonal forms over finite fields. *Ann. Univ. Turku. Ser. A I*, 118:10, 1968.

[29] A. Tietäväinen. On a problem of chowla and shimura. *Journal of Number Theory*, 3:247–252, 1971.

[30] C. Tsen. Divisionsalgebren über funktionkörper. *Nachr. Ges. Wiss. Göttingen*, page 335, 1933.