Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Diagonal forms over the unramified quadratic extension of $\mathbb{Q}_2$

por

Bruno de Paula Miranda

Orientador: Hemar Teixeira Godinho

Brasília

2018

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

dd de Paula Miranda, Bruno
Diagonal forms over the unramified quadratic extension of Q_2. / Bruno de Paula Miranda; orientador Hemar Teixeira Godinho. -- Brasília, 2018.
69 p.

Tese (Doutorado - Doutorado em Matemática) -- Universidade de Brasília, 2018.

1. Formas diagonais. 2. Conjectura de Artin. 3. Extensões não ramificadas. 4. Corpos locais. 5. Corpos p ádicos. I. Teixeira Godinho, Hemar , orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Diagonal Forms Over The Unramified Quadratic Extension of $\mathbb{Q}_2$

por

Bruno de Paula Miranda*

Tese apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática-UnB, como requisito parcial para obtenção do grau de

DOUTOR EM MATEMÁTICA

Brasília, 09 de março de 2018.

Comissão Examinadora:

Prof. Dr. Hemar Teixeira Godinho – Orientador (MAT-UnB)

Prof. Dr. Diego Marques Ferreira (MAT-UnB)

Prof. Dr. Michael Knapp (LUM)

Prof. Dr. Paulo Henrique de Azevedo Rodrigues (UFG)

*O autor foi bolsista PICME durante a elaboração deste trabalho.

Aos meus pais,

João Batista de Miranda e

Lindalva Soares de Paula.

Agradecimentos

Antes de tudo e todos, aos meus pais (João e Lindalva), um gigantesco OBRIGADO. Devo tudo aos dois. Ao meu irmão, Breno, também devo muito por tantos momentos de descontração, sempre que chegava de viagem em Goiânia.

Terei eterna gratidão por todo acolhimento, incentivo e ensinamento que obtive no decorrer de toda minha vida acadêmica por pessoas que, além de bons profissionais, são/eram excelentes seres humanos: Professor Walterson Pereira Ferreira (RIP), Professora Shirlei Serconeck, Professor José Hilário da cruz, Professor Rogério Chaves de Queiroz, Professor Paulo Henrique de Azevedo Rodrigues , Professor Michael P. Knapp e Professor Hemar teixeira Godinho.

Sinto-me muito feliz por ter percorrido esses quatro anos rodeado de amigos verdadeiros, que me ajudaram a carregar diversos fardos e tornaram os dias de trabalho mais alegres: Yerko, Josimar, Jean, Lucimeire (pereirão), Danilo, Carol, Daiane, Filipe, Gérsica, Elaine, Alessandra, Lais, Teló, Camila, Eduardo e outros muitos, Muito obrigado!

Finalmente, um salve aos meus amigos: Fábio Júnior, Jhonatan, Danillo e Diógenes que tem me aturado por mais de 12 anos.

"Fazer da queda um passo de dança, do medo uma escada, do sono uma ponte, da procura um encontro."

Fernando Sabino

Resumo

Em 1963, e Lewis provaram que se a forma diagonal $\mathscr{F}(x) = a_1x_1^d + \cdots + a_Nx_N^d$ com coeficientes em $\mathbb{Q}_p$, o corpo dos números p-ádicos, satisfizer $N > d^2$, então existe solução não trivial para $\mathscr{F}(x) = 0$. Muito estudo tem sido realizado a fim de generalizar esse resultado para extensões finitas de $\mathbb{Q}_p$. Aqui, estudamos o caso $\mathscr{F}(x) \in K[x]$ com K sendo a extensão quadrática não ramificada de $\mathbb{Q}_2$ e provamos dois resultados: Se d não é potência de 2, então $N > d^2$ garante a existência de solução não trivial para $\mathscr{F}(x) = 0$. Além disso, se $d = 6$, $N = 29$ garante existência de solução não trivial para $\mathscr{F}(x) = 0$.

Palavras-chave: Formas diagonais ;Extensões não ramificadas; Conjectura de Artin; Corpos locais; Corpos p-ádicos.

Abstract

In 1963, Davenport and Lewis proved that if the diagonal form $\mathscr{F}(x) = a_1x_1^d + \cdots + a_Nx_N^d$ with coefficients in $\mathbb{Q}_p$, the field of p-adic numbers, satisfies $N > d^2$, then there exists non-trivial solution for $\mathscr{F}(x) = 0$. Since then, there has been a lot of study in order to generalize this result to finite extensions of $\mathbb{Q}_p$. Here, we study the case $\mathscr{F}(x) \in K[x]$ where K is the quadratic unramified extension of $\mathbb{Q}_2$ and we prove two results: if d is not a power of 2 , then $N > d^2$ guarantees non-trivial solution for $\mathscr{F}(x) = 0$. Furthermore, if $d = 6$, $N = 29$ guarantees non-trivial solution for $\mathscr{F}(x) = 0$.

Keywords: Diagonal forms; Unramified extensions; Artin's conjecture; Local fields; p-adic fields.

Table of contents

Introduction

In 1951, in his doctoral thesis [8], Serge Lang defined the C_i property of fields: *A field F satisfies the C_i property if any homogeneous form $f \in F[x_1, \cdots, x_N]$ of degree d in $N > d^i$ variables admits non-trivial zero.* In 1952, Lang [9] showed that $\mathbb{F}_q((X))$, the field of meromorphic series over a finite field, satisfies the C_2 property. The austrian mathematician Emil Artin conjectured that if F is a local field, then it satisfies the C_2 property. However, in 1966, Guy Terjanian presented a homogeneous form with coefficients in $\mathbb{Q}_2$, the field of 2-adic numbers, with degree 4 in 18 variables ($> 4^2 + 1$) having no non-trivial zero in $\mathbb{Q}_2$ (see [14]). On the other side, one year before Terjanian's result, Ax and Kochen [2] proved that given a finite extension $F/\mathbb{Q}_p$ of degree n, and $d \in \mathbb{N}$, there exists a natural number $p(d, n)$ such that F satisfies the C_2 property provided $p > p(d, n)$.

Although Terjanian's counterexample invalidates Artin's conjecture, an interesting fact occurs: until now the conjecture remains opened if we include the hypothesis that the form is diagonal. In fact, great results have been achieved on this direction. In 1963, Davenport and Lewis [6] proved:

Theorem. *Let p be a prime number and let*

$$f = a_1 x_1^d + \cdots + a_N x_N^d$$

where $a_i \in \mathbb{Q}_p$, $i = 1, \cdots, N$. If $N > d^2$, then f admits non-trivial zero. Moreover, for $d = p - 1$, there exists forms in d^2 variables with no non-trivial zero.

So, Davenport and Lewis proved Artin's conjecture for diagonal forms over $\mathbb{Q}_p$. Since then, a lot of research has been made in order to generalize this result to finite extensions of $\mathbb{Q}_p$.

Let K be a finite extension of $\mathbb{Q}_p$. Let $\Gamma(K,d)$ denote the smallest positive integer such that if a diagonal form of degree d and coefficients in K has $N \geq \Gamma(K,d)$ variables, then it admits non-trivial zero. With this notation, the result of Davenport and Lewis can be expressed as $\Gamma(\mathbb{Q}_p,d) \leq d^2+1$, and if $d = p-1$ we have $\Gamma(\mathbb{Q}_p,d) = d^2+1$.

In 1964, Birch [3] proved that if K is a finite extension of $\mathbb{Q}_p$ with inertial degree f and $d = p^\tau \cdot m$ with $(m,p) = 1$, then

$$\Gamma(K,d) \leq (2\tau+3)^d(\delta^2 d)$$

where $\delta = (d, p^f - 1)$.

In 1987, Alemu [1] proved that if K is a finite extension of $\mathbb{Q}_p$ of degree n and $p \geq 3$, we have

$$\Gamma(K,d) \leq \max\,\{3nd^2 - nd + 1, 2d^3 - d^2\}$$

and if $p = 2$

$$\Gamma(K,d) \leq 4nd^2 - nd + 1.$$

In 2006, Skinner [12] proved that if K is a finite extension of $\mathbb{Q}_p$ and $d = p^\tau \cdot m$ with $(m,p) = 1$, then

$$\Gamma(K,d) \leq d(p^{3\tau}m^2)^{2\tau+1} + 1.$$

This result has the advantage of not depending on the degree of the extension.

In 2008, Brink, Godinho and Rodrigues [4] proved that if K is a finite extension of $\mathbb{Q}_p$ with degree n and $d = p^\tau \cdot m$ with $(m,p) = 1$, then

$$\Gamma(K,d) \leq d^{2\tau+5} + 1$$

and

$$\Gamma(K,d) \leq 4nd^2 + 1.$$

Here, the first estimate for $\Gamma(K,d)$ does not depend on the degree n and is an improvement on Skinner's result. The second estimate is, to the best of the author's knowledge, the optimal result depending on the degree n of the extension.

In 2017, Miranda Moore proved [10] that if K is a finite extension of $\mathbb{Q}_p$ and $d = p^\tau \cdot m$ with $(m, p) = 1$, then for $p \geq 3$ we have

$$\Gamma(K, d) \leq d(md+1)^{\tau+1}$$

and for $p = 2$

$$\Gamma(K, d) \leq d(md+1)^{\tau+2}.$$

This is an improvement on the result of Brink, Godinho and Rodrigues.

Also in 2017, Luis Sordo proved [13] that if K is a finite unramified extension of $\mathbb{Q}_p$ where $p \geq 3$, then

$$\Gamma(K, d) \leq d^2 + 1.$$

This is another important step on the direction of Artin's conjecture.

On this thesis, we study diagonal forms over the quadratic unramified extension of $\mathbb{Q}_2$. We prove two results:

Theorem 1. *Let $K = \mathbb{Q}_2(\sqrt{5})$ be the only unramified quadratic extension of $\mathbb{Q}_2$. Let $d \in \mathbb{N}$ not power of 2. Then $\Gamma(d, K) \leq d^2 + 1$.*

This is a first step on the case not treated by Sordo.

Theorem 2. *Let $K = \mathbb{Q}_2(\sqrt{5})$ be the only unramified quadratic extension of $\mathbb{Q}_2$. Then $\Gamma(6, K) \leq 29$.*

The problem treated in Theorem 2 was proposed by Knapp. In a recent work of his [7], he proved:

Theorem. *Let $\mathbb{Q}_2(\sqrt{\pm 2})$, $\mathbb{Q}_2(\sqrt{\pm 10})$, $\mathbb{Q}_2(\sqrt{-5})$ e $\mathbb{Q}_2(\sqrt{-1})$ be the ramified extensions of $\mathbb{Q}_2$.*

- *for $K = \mathbb{Q}_2(\sqrt{\pm 2}), \mathbb{Q}_2(\sqrt{\pm 10})$ we have $\Gamma(6, K) = 9$.*
- *for the other cases $\Gamma(6, K) \leq 9$.*

So, only the case where K is the unramified quadratic extension of $\mathbb{Q}_2$ remained untreated.

In the first chapter of this thesis we give a brief approach on Local fields. We give examples and properties of such fields. We define the concepts of ramified and unramified extensions of local fields and we prove that given a local field F and a natural number n, there is only one unramified extension of F having degree n.

In the sencond chapter we give some preliminary results that are the guidelines of our strategies on the proofs of theorems 1 and 2.

Chapter 3 contains a series of combinatorial Lemmas that will be used on the proofs of theorems 1 and 2.

Chapter 4 is entirely devoted to the proof of theorem 1. Finally, in chapter 5 we prove theorem 2 and present a lower bound for $\Gamma(\mathbb{Q}_2(\sqrt{5}), 6)$ that was obtained by Knapp.

Chapter 1

Local Fields

1.1 Definition and basics

Let K be a field and $|\cdot|$ a non-trivial non-archimedean absolute value on K. Let $O_K = \{a \in K \; ; \; |a| \leq 1\}$. It is easy to see that O_K is an integral domain. We call it the *ring of integers* of K. Let $O_K^\times = \{a \in K \; ; \; |a| = 1\}$. We show that $O_K^\times$ is the group of units of O_K. Indeed, If $a \in O_K$ is invertible, let $b \in O_K$ with $|ab| = 1$. If $a \notin O_K^\times$ then $|b| > 1$, which is a contradiction. Remains to be shown that every element of $O_K^\times$ is a unit. If $a \in O_K^\times$ and $b \in K$ is such that $|ab| = 1$, then $|b| = 1$ and $b \in O_K$ proving that a is a unit and we are done. Let $\mathfrak{p}_K = \{a \in K \; ; \; |a| < 1\}$. $\mathfrak{p}_K$ is an ideal of O_K. In fact, it is the unique maximal ideal of O_K. Indeed, every element $a \notin \mathfrak{p}_K$ is invertible. Let $k = O_K/\mathfrak{p}_K$. This field is called the *residue field* of K.

Example 1.1. *Take $K = \mathbb{Q}$ the set of rational numbers, and $|\cdot| = |\cdot|_p$ the p-adic absolute value given by*

$$|a/b|_p = p^{-(\nu_p(a) - \nu_p(b))}$$

where $a/b \in \mathbb{Q}$ with $(a, b) = 1$ and $\nu_p(a)$ is the p-adic valuation of the integer a, defined by $a = p^{\nu_p(a)} \cdot m$, $(m, p) = 1$. Clearly, $|\cdot|_p$ is a non-trivial non-archimedian absolute value on $\mathbb{Q}$. In this case the ring of integers is $O_\mathbb{Q} = \{a/b \in \mathbb{Q} \; ; \; |a/b|_p \leq 1\} = \{a/b \in \mathbb{Q} \; ; \; p \nmid b\}$. The maximal ideal is $\mathfrak{p}_\mathbb{Q} = \{a/b \in \mathbb{Q} \; ; \; p|a\} = p\mathbb{Z}$ and it is easy to see that the residue field $k_\mathbb{Q}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ the finite field with p elements.

In the example above, we have the maximal ideal $\mathfrak{p}_{\mathbb{Q}}$ being principal. We now characterize the cases for which this happens. Let $\mathcal{V}(K) = \{|a|;\ a \in K^*\}$. This is a multiplicative subgroup of the positive real numbers. We call it the *group of values* of K.

Proposition 1.2. *The maximal ideal $\mathfrak{p}_K$ is principal if, and only if, the group of values $\mathcal{V}(K)$ is a discrete subgroup of $(\mathbb{R}^*_+, \cdot)$, that is, if there exists $\delta > 0$ such that $1-\delta < |a| < 1+\delta \Rightarrow |a| = 1$.*

Proof. First we assume $\mathfrak{p}_K = (\pi)$. If $a \in k$ is such that $|a| < 1$, then we have $|a| \leq |\pi| < 1$. On the other hand, if $|a| > 1$, we have $|a^{-1}| < 1$ and $|a|^{-1} \leq |\pi|$ which gives us $|a| > |\pi|^{-1} > 1$. So, if we take $\delta = \min\{1-|\pi|, |\pi|^{-1}-1\}$ we have $1-\delta < |a| < 1+\delta \Rightarrow |a| = 1$.

Now we assume the absolute value being discrete. We want to find $\pi \in \mathfrak{p}_K$ satisfying $\mathfrak{p}_K = (\pi)$. It is sufficient to find $\pi \in \mathfrak{p}_K$ for which $|\pi| \geq |a|$ for every $a \in \mathfrak{p}_K$. Indeed, we would have for any given $a \in \mathfrak{p}_K$, $|a/\pi| \leq 1$ and so $a/\pi = b \in O_K$ and then $\mathfrak{p}_K = (\pi) = \pi O_K$.

Let $A = \{|a|;\ a \in \mathfrak{p}_K\}$. The set A is a limited subset of $\mathbb{R}$, so there exists its supremum S. From the definition of S, for any natural number n, there exists $|a_n| \in A$ satisfying $|a_n| \geq S - 1/n$. Take $n_0 \in \mathbb{N}$ sufficiently large so we have $\delta > 1/(Sn_0 - 1)$. So, for any $n, m \geq n_0$ we have

$$\frac{|a_n|}{|a_m|} - 1 \leq \frac{S}{S - 1/m} - 1 = \frac{1}{Sm - 1} \leq \frac{1}{Sn_0 - 1} < \delta \Longrightarrow \frac{|a_n|}{|a_m|} < 1 + \delta$$

and

$$\frac{|a_n|}{|a_m|} - 1 \geq \frac{S - 1/n}{S} - 1 = -\frac{1}{Sn} \geq -\frac{1}{Sn_0 - 1} > -\delta \Longrightarrow \frac{|a_n|}{|a_m|} > 1 - \delta$$

and we conclude that $|a_n| = |a_m|$ (remember that we are assuming the absolute value being discrete) for every $n, m \geq n_0$. So $S \geq |a_{n_0}| = |a_n| \geq S - 1/n$ for every $n \geq n_0$, we conclude that $|a_{n_0}| = S$. So, for $\pi = a_{n_0}$ we have $|\pi| \geq |a|$ for every $a \in \mathfrak{p}_K$ and we are done.

Definition 1.3 (Local field)**.** *A field K complete with respect to a non-trivial, non-archimedian, discrete absolute value, with finite residue field is called a local field.*

Let $\overline{K} \supseteq K$ be the completion of K, i.e. $\overline{K}$ has an absolute value which extends the absolute value of K, $\overline{K}$ is complete with respect to this absolute value, and K is dense in $\overline{K}$. It is known that every field K with a non-trivial absolute value admits a unique completion, see [5] for more details. Let $\Psi : O_K \longrightarrow O_{\overline{K}}/\mathfrak{p}_{\overline{K}}$ given by $a \longmapsto a + \mathfrak{p}_{\overline{K}}$. Since $O_K = K \bigcap O_{\overline{K}}$ and $\mathfrak{p}_K = \mathfrak{p}_{\overline{K}} \bigcap K$, it is easy to see that Ψ is injective. We assert that it is also surjective. Let $\alpha \in O_{\overline{K}}$. Take $a \in K$ such that $|\alpha - a| < 1$ (K is dense in $\overline{K}$) so $a - \alpha \in \mathfrak{p}_{\overline{K}}$. We have

$$|a| \leq \max\{|a - \alpha|, |\alpha|\} \leq 1$$

so $a \in O_K$ and we have $\Psi(a) = \alpha + \mathfrak{p}_{\overline{K}}$. We have just proved

Proposition 1.4. *If $\overline{K}$ is the completion of K, then $k_K = k_{\overline{K}}$.*

Example 1.5. *(Local Field) Recall that $\mathbb{Q}_p$, the field of p-adic numbers, is obtained from $\mathbb{Q}$ by means of Cauchy sequences. Moreover, if $a \in \mathbb{Q}_p$ is the limit of the Cauchy sequence $(x_n)_{n\in\mathbb{N}}$ of elements of $\mathbb{Q}$, then $|a|_p = \lim |x_n|_p$. And since there exists $N \in \mathbb{N}$ such that $|x_n|_p = |x_m|_p$ for all $n, m > N$, we conclude that the group of values of $\mathbb{Q}_p$ coincides with the group of values of $\mathbb{Q}$. Hence, it is discrete (the maximal ideal of $O_{\mathbb{Q}}$ is principal). By Proposition 1.4 we have the residue field $k_{\mathbb{Q}_p} = \mathbb{F}_p$. This shows us that $\mathbb{Q}_p$ is a local field.*

1.2 Generator of a local field

Let K be a local field. Let $\pi \in K$ be such that $\mathfrak{p}_K = (\pi)$, we call π a *generator of* K. The term *uniformizer* is also commonly used to designate π.

Proposition 1.6. *Let $a \in K^*$. There exists $n \in \mathbb{Z}$ and $b \in O_K^\times$ such that $a = \pi^n \cdot b$.*

Proof. Let $a \in K^*$ and $n \in \mathbb{Z}$ such that

$$|\pi|^n \leq |a| < |\pi|^{n-1}.$$

We have $|a/\pi^n| \in [1, |\pi|^{-1})$. By proposition 1.2 we have $|a/\pi^n| = 1$. So, we have $|a/\pi^n| = 1$, and there must exist an element $b \in O_K^\times$ such that $a = \pi^n \cdot b$.

□

Corollary 1.7. *π is the only prime (up to associates) in O_K.*

Proof. Proposition 1.6 implies that if $a, b \in O_K$ and $\pi | ab$, then either $\pi | a$ of $\pi | b$. So π is a prime in O_K. The uniqueness follows from the fact that $\mathfrak{p}_K$ is the only maximal ideal of O_K.

□

The above corollary and Proposition 1.6 give us a fundamental theorem of arithmetic for O_K: *every integer of K can be written as a product of primes of O_K in a unique manner, up to associates.* But we can say more, we will show that every element of O_K can be written uniquely as a power series in π. We clear this up in the next proposition.

Proposition 1.8. *Let K be a local field with generator π and let $\mathscr{R}$ be a set of representatives of the residue field $k_K = O_K/(\pi)$. Every element $a \in O_K$ can be written uniquely as*

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

where $a_i \in \mathscr{R}$ for every $i \geq 0$. Moreover, every series $\sum a_n \pi^n$ converges to an element of O_K.

Proof. Let $a \in O_K$. There exists a unique $a_0 \in \mathscr{R}$ such that $a - a_0 \in \mathfrak{p}_K$. Hence, there exists $b_1 \in O_K$ such that $a = a_0 + \pi \cdot b_1$. Similarly, there exists a unique $a_1 \in \mathscr{R}$ such that $b_1 - a_1 \in \mathfrak{p}_K$. So there is an element $b_2 \in O_K$ such that $b_1 = a_1 + \pi \cdot b_2$. Consequently $a = a_0 + a_1\pi + b_2\pi^2$. Following this process we get for every $N \in \mathbb{N}$

$$a = a_0 + a_1\pi + a_2\pi^2 + \cdots + a_N\pi^N + b_{N+1}\pi^{N+1}$$

where $a_i \in \mathscr{F}, \; i = 1, \cdots, N$ and $b_{N+1} \in O_K$. Since

$$|a - (a_0 + a_1\pi + a_2\pi^2 + \cdots + a_N\pi^N)| = |b_{N+1}\pi^{N+1}| = |\pi|^{N+1}$$

and $|\pi|^{N+1}$ goes to zero as N tends to infinity, we conclude that the series converges to a.

Now we prove the second part of the proposition. Consider a series $\sum a_n\pi^n$ where $a_i \in \mathscr{F}$ for every $i \geq 0$. Since the general term of the series is $a_n\pi^n$ and $|a_n\pi^n| = |\pi|^n$ goes to zero as n tends to infinity, we conclude that the series converges to some $a \in K$ (remember that this is true only for non-archimedean absolute values). We will show that $a \in O_K$. Observe that for every $n \in \mathbb{N}$ we have $|a_0 + a_1\pi + \cdots + a_n\pi^n| \leq \max\{|a_0|, |a_1\pi|, \cdots, |a_n\pi^n|\} \leq 1$. Since the series converges to a, there exists $N \in \mathbb{N}$ such that $|a - (a_0 + \cdots + a_N\pi^N)| \leq 1$. Then

$$|a| \leq \max\{|a - (a_0 + \cdots + a_N\pi^N)|, |a_0 + \cdots + a_N\pi^N|\} \leq 1$$

and we conclude that $a \in O_K$.

$\square$

Proposition 1.6 can be used to extend this result to all elements of K: *Every element $a \in K$ can be written in a unique manner as a series $\sum_{n \geq n_0(a)} a_n\pi^n$, where $a_i \in \mathscr{R}$ for all $i \geq n_0(a)$ and $n_0(a) \in \mathbb{Z}$.*

1.3 Ramification

Let F be a local field with a non-archimedean absolute value $|\cdot|_F$ and E a finite extension of F of degree n. The following theorem ([5] chapter 7, theorem 1.1) shows us that we can extend the absolute value of F to E in such a way that E is complete with respect to this new absolute value.

Theorem. *Let F be complete with respect to the absolute value $|\cdot|_F$ and E be an extension of F of degree $[E : F] = n$. Then there is precisely one extension $|\cdot|_E$ of $|\cdot|_F$ to E. It is given by*

$$|a|_E = \sqrt[n]{|N_{E/F}(a)|_F}, \quad \forall a \in E$$

where $N_{E/F} : E \longrightarrow F$ is the norm from E to F. Further, E is complete with respect to $|\cdot|_E$.

The Norm from E to F is a natural way to go down from elements of E to F. It can be defined in several ways:

1 - E is a finite-dimensional F-vector space. Take $\alpha \in E$ and consider the F-linear map $\psi : E \longrightarrow E$ given by $\psi(\beta) = \alpha\beta$, $\forall \beta \in E$. $N_{E/F}(\alpha)$ can be defined as the determinant of the matrix of ψ.

2 - Take $\alpha \in E$ and consider the sub-extension $F(\alpha)$. Set $r = [E : F(\alpha)]$ and let

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

be the minimal polynomial of α over F. Then we can define $N_{E/F}(\alpha) = (-1)^{nr} \cdot a_0^r$.

3 - Suppose E/F is normal. Then we can define $N_{E/F}(\alpha)$ to be the product of all $\sigma(\alpha)$, where σ runs through all elements of the Galois group of the extension E/F.

From these definitions it is easy to see that if $a \in F$, then $N_{E/F}(a) = a^n$. So it becomes clear that $|a|_E = |a|_F$ for all elements $a \in F$. Also, it is immediate that the norm is multiplicative. It is also clear that the absolute value $|\cdot|_E$ is discrete and non-archimedean. This implies that E is a local field with the absolute value $|\cdot|_E$.

Let O_F and O_E be the ring of integers of F and E, $\mathfrak{p}_F = (\pi_F)$ and $\mathfrak{p}_E = (\pi_E)$ their maximal ideals, and k_F and k_E their residue fields. Since the absolute value $|\cdot|_E$ is an extension of $|\cdot|_F$ we have $\mathcal{V}_F \leq \mathcal{V}_E$.

Definition 1.9 (Ramification index). *We set $[\mathcal{V}_E : \mathcal{V}_F] = e(E/F)$ and call it the ramification index of the extension E/F.*

Remember that $\mathcal{V}_E = (|\pi_E|)$ and $\mathcal{V}_F = (|\pi_F|)$. So, there exists $m \in \mathbb{Z}$ such that $|\pi_F| = |\pi_E|^m$. Since π_E^m generates $\mathcal{V}_F$ we conclude that $m = [\mathcal{V}_E : \mathcal{V}_F] = e(E/F)$.

Observe that $O_F = F \bigcap O_E$ and $\mathfrak{p}_F = F \bigcap \mathfrak{p}_E$. The map $\Psi : O_F \longrightarrow O_E/\mathfrak{p}_E$ given by $\Psi(a) = a + \mathfrak{p}_E$ has kernel $\mathfrak{p}_F$, so there is a natural inclusion $k_F \hookrightarrow k_E$.

Definition 1.10 (Degree of the residue class). *Set $[k_E : k_F] = f(E/F)$. We call it the degree of the residue class of E/F.*

Whenever it is clear by the context which extension we are dealing with, we will simply denote $e = e(E/F)$ and $f = f(E/F)$. The ramification index e and the degree of the residue class f relate in an interesting way:

Theorem 1.11. *Let E/F be a finite extension of degree n of the local field F. Then $n = ef$.*

Proof. Let π_E a generator of E and $\alpha_1, \cdots, \alpha_f \in O_E$ such that modulo $\mathfrak{p}_E$ they constitute a k_F-basis for k_E. We are going to show that the set

$$B = \{\alpha_i \pi_E^j \ ; \ 1 \leq i \leq f, \ 0 \leq j \leq e-1\}$$

is an F-basis for E.

First we show that B is a linear independent set. Suppose not, that is, assume there exist $a_{ij} \in F$, $1 \leq i \leq f$, $0 \leq j \leq e-1$, with at least one of them not being trivial, satisfying

$$\sum a_{ij} \alpha_i \pi_E^j = 0 \tag{1.1}$$

We divide both sides of this equation by the coefficient with larger absolute value. So we can assume all $a_{ij} \in O_F$ and we can choose indices I, J such that $|a_{IJ}| = 1$ and if $j < J$ then $|a_{ij}| \leq |\pi_F|$ (equivalently $|a_{ij}| < 1$) for all $1 \leq i \leq f$; we just take the smallest j for which there exists i with $|a_{ij}| = 1$.

Fix J and look at the summation $\sum\limits_i a_{iJ}\alpha_i$. Since modulo $\mathfrak{p}_E$ the α's are independent, this sum can not be zero modulo $\mathfrak{p}_E$ ($|a_{IJ}| = 1$). Hence, we have $\sum\limits_i a_{iJ}\alpha_i \in O_E^\times$, that is, $|\sum\limits_i a_{iJ}\alpha_i| = 1$.

It follows that

- if $j = J$

  $|\sum\limits_i a_{iJ}\alpha_i\pi_E^J| = |\pi_E|^J |\sum\limits_i a_{iJ}\alpha_i| = |\pi_E|^J$

- if $j < J$

  $|\sum\limits_i a_{ij}\alpha_i\pi_E^j| = |\pi_E|^j |\sum\limits_i a_{iJ}\alpha_i| \leq \max\{|a_{ij}|, |\alpha_i|\} \leq \max\{|a_{ij}|\} \leq |\pi_F| = |\pi_E|^e$

- if $j > J$

  $|\sum\limits_i a_{ij}\alpha_i\pi_E^j| = |\pi_E|^j |\sum\limits_i a_{iJ}\alpha_i| \leq |\pi_E|^j \max\{|a_{ij}|, |\alpha_i|\} \leq |\pi_E|^j \leq |\pi_E|^{J+1}$

Set $b_j = \sum\limits_i a_{ij}\alpha_i\pi_E^j$. Then, equation 1.1 give us $\sum\limits_j b_j = 0$. Then,

$$|\pi_E|^J = |b_J| = |\sum_{j \neq J} b_j| \leq \max\{|b_j|, \ j \neq J\} \leq |\pi_E|^{J+1}$$

which is a contradiction. We conclude that the set B is linearly independent.

Now we prove that B generates E. Take $x \in E$, we want to find $c_{ij} \in F$, $i = 1, \cdots, f$ and $j = 0, \cdots, e-1$, such that $x = \sum c_{ij}\alpha_i \pi_E^j$. Without loss of generality we may assume $x \in O_E$, if not, just multiply by an appropriate power or π_F. We will use a bar to indicate that we are working modulo $\mathfrak{p}_E$. Since $\{\overline{\alpha_1}, \ldots, \overline{\alpha_f}\}$ is a k_F-basis for k_E, there exist $\overline{c}_{0i},\ i = 1, \cdots, f$ in k_F, such that

$$\overline{x} = \sum_i \overline{c}_{0i}\overline{\alpha_i}.$$

Then, there exist $c_{0i} \in O_F, 1 \leq i \leq f$ and $x_1 \in O_E$ such that

$$x - \sum_{1 \leq i \leq f} c_{0i}\alpha_i = x_1 \pi_E.$$

Repeating the same argument for x_1 we obtain $c_{1i} \in O_F, 1 \leq i \leq f$ and $x_2 \in O_E$ such that

$$x - \sum_{1 \leq i \leq f} c_{0i}\alpha_i - \sum_{1 \leq i \leq f} c_{1i}\alpha_i \pi_E = x_1 \pi_E^2.$$

We apply this procedure e times and obtain

$$x - \sum_{1 \leq i \leq f} \sum_{0 \leq j \leq e-1} c_{ji}^{(0)} \alpha_i \pi_E^j = x^{(1)} \pi_E^e = x^{(1)} \pi_F$$

where $c_{ji}^{(0)} \in O_F$ and $x^{(1)} \in O_E$.

We set $C^{(0)} = \sum\limits_{1 \leq i \leq f} \sum\limits_{0 \leq j \leq e-1} c_{ji}^{(0)} \alpha_i \pi_E^j$. We repeat this procedure with $x^{(1)}$ instead of x, and so on. Then, for each natural number N we get

$$x - C^{(0)} - C^{(1)}\pi_F - \cdots - C^{(N)}\pi_F^N = x^{(N+1)}\pi_F$$

where each $C^{(l)} \in O_E$ and $x^{(N+1)} \in O_E$. By Proposition 1.8 we conclude that

$$x = \sum_{l \geq 0} C^{(l)} \pi_F^l \tag{1.2}$$

We are almost there. Now, for each $1 \leq i \leq f$ and $0 \leq j \leq e-1$, consider the sub-series $\sum\limits_{l \geq 0} c_{ji}^{(l)} \alpha_i \pi_E^j \pi_F^l = \alpha_i \pi_E^j \cdot \sum\limits_{l \geq 0} c_{ji}^{(l)} \pi_F^l$. By Proposition 1.8, we now that $\sum\limits_{l \geq 0} c_{ji}^{(l)} \pi_F^l$ represents an element $c_{ij} \in O_F$. But then equation 1.2 give us $x = \sum\limits_{1 \leq i \leq f} \sum\limits_{0 \leq j \leq e-1} c_{ij}\alpha_i \pi_E^j$ and we are done.

□

Definition 1.12. *We say that the extension E/F of degree $n \geq 2$ is ramified if $e > 1$ (equivalently $f < n$). Otherwise we say it is unramified. When $e = n$ we say that the extension is totally ramified.*

Note that an extension is ramified or unramified according to the ramification of the prime π_F of O_F. In an unramified extension, the prime π_F of O_F continues being prime in O_E. The same does not happen in ramified extensions.

Given a local field F, for each $n \in \mathbb{N}$ there exists a unique unramified extension E/F of degree n. Moreover, E is the decomposition field over F of the polynomial $x^q - x$ where $q = (\#k_F)^n$. In order to prove this statement we are going to need a series of lemmas.

Lemma 1.13 (Hensel I)**.** *Let F be a field complete with respect to a non-archimedean absolute value and let $f(x) \in O_F[x]$. If there exists $a \in O_F$ such that*

$$|f(a)| < |f'(a)|^2$$

where $f'(x)$ is the formal derivative of $f(x)$, then there exists $\alpha \in O_F$ such that $f(\alpha) = 0$. Moreover, α is the unique solution to $f(x) = 0$ that satisfies

$$|a - \alpha| < \frac{|f(a)|}{|f'(a)|}.$$

Proof. See [5], Lemma 3.1.

□

Lemma 1.14. *Let F be a field complete with respect to a non-archimedean absolute value $|\cdot|_F$ and with residue field k_F with $q = p^m$ elements, $p = char(k_F)$. Then F contains all $(q-1)th$ roots of unity.*

Proof. Let $\overline{a} \in k_F$ and choose $a \in O_F^\times$ such that $\overline{a} = a + \mathfrak{p}_F$. Set $f(x) = x^{q-1} - 1 \in O_F[x]$. We have

$$f(a) = a^{q-1} - 1 \equiv (\overline{a})^{q-1} - 1 \equiv 0 \bmod \mathfrak{p}_F$$

and we conclude that $|f(a)| < 1$. If $|f'(a)| = 1$ we are done. Indeed, in this case we can apply Lemma 1.13 and obtain $\alpha \in O_F$ such that $f(\alpha) = 0$ with $\alpha \equiv a \mod \mathfrak{p}_F$. And since a is arbitrary we conclude that F contains all $(q-1)th$ roots of unity. But

$$|f'(a)| = |(q-1)||a|^{q-2} = |q-1|.$$

Suppose $|q-1| < 1$. Since $char(k_F) = p$ we have $|p| < 1$. Then

$$1 = |-1| = |(q-1) - p^m| \leq \max\{|p^m|, |(q-1)|\} < 1$$

which is a contradiction. Then, we have $|f'(a)| = 1$ as we wanted.

□

Proposition 1.15. *Let E/F be a finite extension of the local field F. Let $\overline{\alpha} \in k_E$. There exists $\alpha \in O_E$ such that $\alpha \equiv \overline{\alpha} \mod \mathfrak{p}_E$ and $[F(\alpha) : F] = [k_F(\overline{\alpha}) : k_F]$. Moreover, if $\alpha_0 \in O_E$, $\alpha_0 \equiv \overline{\alpha} \mod \mathfrak{p}_E$ and $[F(\alpha_0) : F] = [k_F(\overline{\alpha}) : k_F]$, then $F(\alpha_0) = F(\alpha)$.*

Proof. Let $\phi(x) \in k_F[x]$ be the minimal polynomial of $\overline{\alpha}$ over k_F. Since every finite field is perfect, we conclude that $\phi(x)$ has no repeated roots. Set $\psi(x) \in F[x]$ a lift of $\phi(x)$, that is, $\phi(x)$ and $\psi(x)$ have the same degree and $\psi(x) \equiv \phi(x) \mod \mathfrak{p}_E$. Let $\alpha_0 \in O_E$ be such that $\overline{\alpha} = \alpha_0 + \mathfrak{p}_E$. Since $\psi(\alpha_0) \equiv \phi(\alpha_0) \equiv 0 \mod \mathfrak{p}_E$ and $\psi'(\alpha_0) \equiv \phi'(\alpha_0) \not\equiv 0 \mod \mathfrak{p}_E$ we have $|\psi(\alpha_0)| < 1$ and $|\psi'(\alpha_0)| = 1$. Setting $K = F(\alpha_0)$ and applying Lemma 1.13 we conclude that there exists $\alpha \in K = F(\alpha_0)$ such that $\psi(\alpha) = 0$ and $|\alpha - \alpha_0| < 1$. Since $\psi(x)$ is irreducible (its roots are in distinct classes modulo $\mathfrak{p}_E$), we have

$$[F(\alpha) : F] = \text{degree of } \psi = \text{degree of } \phi = [k_F(\overline{\alpha}) : k_F].$$

This concludes the first part of the theorem. Now, if $\alpha_0 \in O_E$ is such that $\alpha_0 \equiv \overline{\alpha} \mod \mathfrak{p}_E$ and $[F(\alpha_0) : F] = [k_F(\overline{\alpha}) : k_F]$, then since Lemma 1.13 implies $\alpha \in F(\alpha_0)$ we must have

$$[F(\alpha) : F] \leq [F(\alpha_0) : F] = [k_F(\overline{\alpha}) : k_F] = [F(\alpha) : F]$$

and $F(\alpha) = F(\alpha_0)$.

□

The equality $[F(\alpha) : F] = [k_F(\overline{\alpha}) : k_F]$ in proposition 1.15 makes one think that the extension $F(\alpha)/F$ is unramified. This would be the case if $k_F(\overline{\alpha}) = k_{F(\alpha)}$. Fortunately this is actually true. Indeed, since $\overline{\alpha} \in k_{F(\alpha)}$ we have $k_F(\overline{\alpha}) \subseteq k_{F(\alpha)}$, then

$$[k_F(\overline{\alpha}) : k_F] \leq [k_{F(\alpha)} : k_F] \leq [F(\alpha) : F] = [k_F(\overline{\alpha}) : k_F]$$

and we are done. We have just proved:

Corollary 1.16. *There is a bijection between the fields $F \subseteq K \subseteq E$ which are unramified extensions of F and the fields $k_F \subseteq k \subseteq k_E$. The bijection is given by $K \longrightarrow k_K$.*

Finally we are able to prove:

Theorem 1.17. *Let F be a local field. For each $n \in \mathbb{N}$ there exists a unique unramified extension E/F of degree n. Moreover, E is the decomposition field over F of the polynomial $x^q - x$ where $q = (\#k_F)^n$.*

Proof. Let $\overline{F}$ be the algebraic closure of F and $\overline{k_F}$ the algebraic closure of k_F. We show that $k_{\overline{F}} = \overline{k_F}$. Indeed, let $\phi(x) \in k_F[x]$ irreducible and $\psi(x) \in F[x]$ a lift of $\phi(x)$ to $F[x]$. Since $\overline{F}$ contains all roots of $\psi(x)$, its residue class field contains all roots of $\phi(x)$ and we are done. Now, take an extension of k_F of degree n (which is unique up to isomorphism). By Corollary 1.16 there exists a unique (up to isomorphism) unramified extension E/F of degree n. Lemma 1.14 shows us that E is precisely the decomposition field over F of the polynomial $x^q - x$.

□

Example 1.18. *Let $F = \mathbb{Q}_2$. We are going to show that $F(\sqrt{5})$ is the only quadratic unramified extension of F.*

First, we have to show that 5 is not a square in $\mathbb{Z}_2$. We assert more: $\beta \in \mathbb{Z}_2^\times$ is a square if, and only if, $\beta \equiv 1 \bmod 2^3$. Suppose that $\beta \in \mathbb{Z}_2^\times$ satisfies $\beta \equiv 1 \bmod 2^3$. Consider the polynomial $f(x) = x^2 - \beta \in \mathbb{Z}_2[x]$. We have $f(1) = 1 - \beta \equiv 0 \bmod 2^3$ which implies $|f(1)| \leq 2^{-3}$. Further, $f'(1) = 1$ and so we have $|f'(1)| = 2^{-1}$. Hence, by Lemma 1.13 we conclude that there exists $\alpha \in \mathbb{Z}_2$ such that $\alpha^2 = \beta$ and β is a square. Conversely, let $\alpha \in \mathbb{Z}_2^\times$ such that $\alpha^2 = \beta$. We write α as a series in 2, and work modulo 2^3.

$$\alpha = 1 + 2\alpha_1 + 2^2\alpha_2$$

where $\alpha_1, \alpha_2 \in \{0,1\}$. *Then*

$$\beta = \alpha^2 = (1 + 2\alpha_1 + 2^2\alpha_2)^2 \equiv 1 \bmod 2^3.$$

So, 5 is not a square in $\mathbb{Z}_2$ *and* $\mathbb{Q}_2(\sqrt{5})$ *is indeed a quadratic extension.*

One way to verify that it is unramified is to show that 2 *is a generator of* $\mathbb{Q}_2(\sqrt{5})$, *that is, the prime 2 does not ramify. Remember (Theorem 1.3) that the absolute value in* $\mathbb{Q}_2(\sqrt{5})$ *is given by*

$$|a| = \sqrt[n]{|N(a)|_2}, \ \forall a \in \mathbb{Q}_2(\sqrt{5})$$

where $N : \mathbb{Q}_2(\sqrt{5}) \longrightarrow \mathbb{Q}_2$ *is the norm from* $\mathbb{Q}_2(\sqrt{5})$ *to* $\mathbb{Q}_2$. *One way to compute this norm is by means of the automorphisms of the Galois group of the extension. In this case there are only two of them, namely:* $\sigma_1 : \mathbb{Q}_2(\sqrt{5}) \longrightarrow \mathbb{Q}_2(\sqrt{5})$ *the identity automorphism and* $\sigma_2 : \mathbb{Q}_2(\sqrt{5}) \longrightarrow \mathbb{Q}_2(\sqrt{5})$ *given by* $\sigma_2(a+b\sqrt{5}) = a - b\sqrt{5}$, $a, b \in \mathbb{Q}_2$. *Hence the norm of an element* $a + b\sqrt{5}$ *of* $\mathbb{Q}_2(\sqrt{5})$ *is given by*

$$N(a + b\sqrt{5}) = \sigma_1(a + b\sqrt{5})\sigma_2(a + b\sqrt{5}) = a^2 - 5b^2.$$

Then, given $a + b\sqrt{5} \in \mathbb{Q}_2(\sqrt{5})$ *we have*

$$|a + b\sqrt{5}| = \sqrt{|a^2 - 5b^2|_2}$$

where $|\cdot|_2$ *is the 2-adic absolute value.*

If we verify that $|a + b\sqrt{5}|$ *is always a power of* 2 *with integer exponent, then we are done. Indeed, This would give us* $\mathcal{V}_{\mathbb{Q}_2(\sqrt{5})} = (|2|)$ *and we would have* $e = [\mathcal{V}_{\mathbb{Q}_2(\sqrt{5})} : \mathbb{Q}_2] = 1$ *and 2 as a generator of* $\mathbb{Q}_2(\sqrt{5})$.

We analyse $a^2 - 5b^2 \bmod 2^2$. *We know that* $a^2, b^2 \equiv 0, 1 \bmod 2^3$.

- *If both* $a^2, b^2 \equiv 1 \bmod 2^3$, *then* $a^2 - b^2 5 \equiv -4 \bmod 8$ *which implies that* $\nu_2(a^2 - 5b^2) = 2$ *and so*

$$|a + b\sqrt{5}| = \sqrt{|a^2 - 5b^2|_2} = \sqrt{2^{-2}} = 2^{-1}.$$

- *If both* $a^2, b^2 \equiv 0 \bmod 8$, *then* $a, b \equiv 0 \bmod 2$ *and* $\nu_2(a^2 - 5b^2) = min\{\nu_2(a^2), \nu_2(b^2)\}$. *Suppose without loss of generality that* $min\{\nu_2(a^2), \nu_2(b^2)\} = \nu_2(a^2) = 2\nu_2(a)$. *Then*

$$|a + b\sqrt{5}| = \sqrt{|a^2 - 5b^2|_2} = \sqrt{2^{-2\nu_2(a)}} = 2^{-\nu_2(a)}.$$

- *Finally, if only* $a^2 \equiv 0 \bmod 8$ *(without loss of generality). Then* $\nu_2(a^2 - 5b^2) = 0$ *and we have*
$$|a + b\sqrt{5}| = 2^0.$$

This concludes the proof that $\mathbb{Q}_2(\sqrt{5})$ *is an unramified quadratic extension of* $\mathbb{Q}_2$*. Theorem 1.17 guarantees it is the only one.*

Let $K = \mathbb{Q}_2(\sqrt{5})$. We have just seen that K is the only unramified extension of $\mathbb{Q}_2$. Hence 2 is a generator of K. It follows by Proposition 1.8 that every $a \in O_K$ can be written uniquely as
$$a = \sum_{i \geq 1} a_i \cdot 2^i$$
where $a_i \in \mathscr{R}$ a set of representatives of $O_K/(2) = k_K$. It is easy to see that the residue field k_K is isomorphic to $\mathbb{F}_4$. In the next example we explicit a set of representatives for k_K.

Example 1.19. $\mathscr{R} = \left\{0, 1, \frac{1+\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}\right\}$ *is a set of representatives for* k_K*.*

It is sufficient to show that 1 *and* $\frac{1+\sqrt{5}}{2}$ *are elements of* $O_K^\times$ *that represent distinct classes modulo* (2)*. Indeed, we would have* $1 + \frac{1+\sqrt{5}}{2} = \frac{3+\sqrt{5}}{2}$ *being the third non-trivial representative of* k_K

That $1 \in O_K^\times$ *is immediate. To show that* $\frac{1+\sqrt{5}}{2} \in O_K^\times$ *we evaluate* $\left|\frac{1+\sqrt{5}}{2}\right|$*. We have*
$$\left|\frac{1+\sqrt{5}}{2}\right| = \sqrt{\left|N\left(\frac{1+\sqrt{5}}{2}\right)\right|_2}$$
and since $N\left(\frac{1+\sqrt{5}}{2}\right) = \frac{1}{4} - 5 \cdot \frac{1}{4} = -1$ *we have*
$$\left|\frac{1+\sqrt{5}}{2}\right| = \sqrt{|-1|_2} = \sqrt{2^0} = 1$$
and we have $\frac{1+\sqrt{5}}{2} \in O_K^\times$*.*

Now we only have to verify that 1 *and* $\frac{1+\sqrt{5}}{2}$ *are in distinct classes modulo* (2)*. But* $1 - \frac{1+\sqrt{5}}{2} = \frac{1-\sqrt{5}}{2}$ *and*
$$\left|\frac{1-\sqrt{5}}{2}\right| = \sqrt{\left|N\left(\frac{1-\sqrt{5}}{2}\right)\right|_2} = \sqrt{\left|\frac{1}{4} - 5 \cdot \frac{1}{4}\right|_2} = \sqrt{|N(-1)|_2} = \sqrt{2^0} = 1$$
and we have $1 \neq \frac{1+\sqrt{5}}{2}$ *modulo* (2)*.*

Chapter 2

Preliminary results

Our goals in this thesis are Theorems 1 and 2. Theorem 1 says that if we have a diagonal form $\mathscr{F}(x) = a_1x_1^d + \cdots + a_Nx_N^d \in \mathbb{Q}_2(\sqrt{5})[x]$ with d not a power of 2, then $N > d^2$ guarantees the existence of non-trivial zero for $\mathscr{F}(x)$. In theorem 2 we set $d = 6$ and prove that $N > 28$ guarantees non-trivial zero for $\mathscr{F}(x)$. In this chapter we give the main strategies that we will adopt in order to prove theorems 1 and 2. First we present the process of normalization, introduced by Davenport and Lewis in [6]. This process consists in defining an equivalence relation on the set of diagonal forms so we can restrict our attention to class representatives. Moreover, it gives us some control on the variables of some special representatives. Then we enunciate another form of Hensel's lemma. This lemma allows us to work modulo a specific power of the generator $\pi = 2$ of $\mathbb{Q}_2(\sqrt{5})$. Finally, we present the concept of contraction of variables, which is a method to solve the congruences in the hypothesis of Hensel's lemma.

2.1 Normalization

Let F be a local field with generator π. Consider $\mathcal{A}$ the set of additive forms of degree d in N variables and with coefficients in F. We say that two elements $\mathscr{F}(x), \mathscr{G}(x) \in \mathcal{F}$ are equivalent, denoting it by $\mathscr{F}(x) \backsim \mathscr{G}(x)$, if we can turn $\mathscr{F}$ into a multiple of $\mathscr{G}$ by means of substitutions $x_i = l_ix_i'$, where $l_i \in O_F$.

Proposition 2.1. *The relation $\mathscr{F} \backsim \mathscr{G}$ is an equivalence relation on the set $\mathcal{A}$.*

Proof. That it is reflexive is immediate. Suppose $\mathscr{F} \backsim \mathscr{G}$. Then, there exists $\alpha \in F$ and $l_1, \cdots, l_N \in O_F$ such that

$$\alpha(b_1 x_1^d + \cdots b_N x_N^d) = \alpha\mathscr{G}(x_1, \cdots, x_N) = \mathscr{F}(l_1 x_1, \cdots, l_N x_N) = a_1 l_1^d x_1^d + \cdots + a_N l_N^d x_N^d$$

which implies

$$\mathscr{G}(x_1, \cdots, x_N) = \frac{1}{\alpha} \cdot (a_1 l_1^d x_1^d + \cdots + a_N l_N^d x_N^d).$$

Consequently,

$$\mathscr{G}(l_1^{-1} x_1, \cdots, l_N^{-1} x_N) = \frac{1}{\alpha} \cdot (a_1 l_1^d l_1^{-d} x_1^d + \cdots + a_N l_N^d l_N^{-d} x_N^d) = \frac{1}{\alpha}\mathscr{F}(x_1, \cdots, x_N)$$

and we have $\mathscr{G} \backsim \mathscr{F}$ which implies that the relation is commutative.

Now, let $\mathscr{F}, \mathscr{G}, \mathscr{H} \in \mathcal{A}$ such that $\mathscr{F} \backsim \mathscr{G}$ and $g \backsim h$. There exists $\alpha_1, \alpha_2 \in F$ and $l_1, \cdots, l_N, l_1', \cdots, l_N' \in O_F$ such that

$$\alpha_1 \mathscr{G}(x_1, \cdots, x_N) = \mathscr{F}(l_1 x_1, \cdots, l_N x_N)$$

and

$$\alpha_2 \mathscr{H}(x_1, \cdots, x_N) = g(l_1' x_1, \cdots, l_N' x_N).$$

Hence,

$$\alpha_1 \alpha_2 h(x_1, \cdots, x_N) = \mathscr{F}(l_1 l_1' x_1, \cdots, l_N l_N' x_N)$$

and we have $\mathscr{F} \backsim \mathscr{H}$ which implies that the relation is transitive.

$\square$

It is immediate to see that to find non-trivial zero for a polynomial $\mathscr{F} \in \mathcal{A}$ is equivalent to find non-trivial zero for any $\mathscr{G} \in \mathcal{A}$ with $\mathscr{F} \backsim \mathscr{G}$. Hence, we can choose in each equivalence class, any representative we want and restrict our attention to it. The next lemma will help us on the task of choosing a "good representative". This is Lemma 2 of [6].

Lemma 2.2. *Let $m_1, m_2, \cdots, m_{d-1}$ be real numbers and put $m_{j+d} = m_j$ for all j. Let*

$$m_0 + \cdots + m_{d-1} = s.$$

Then, there exists r such that

$$m_r + m_{r+1} + \cdots + m_{r+t-1} \geq \frac{ts}{d}$$

for $t = 1, \cdots, d$.

Proof. We can assume $s = 0$. If not, just set $m_i' = m_i - \frac{s}{d}$.

Assume there is not such r, that is, assume that for every given $a \in \mathbb{N}$ there exists an integer $b \geq a$ such that $m_a + m_{a+1} + \cdots + m_b < 0$. Let a_1, b_1 be two such integers. Take $a_2 = b_1 + 1$ and find the corresponding b_2. Continuing this way, we'll get $a_1 \equiv a_n \bmod d$ for some $n \in \mathbb{N}$(pigeonhole principle). Then,

$$\sum_{a_1}^{a_n - 1} m_i < 0$$

but this is a contradiction since

$$\sum_{a_1}^{a_n - 1} m_i = \frac{a_n - a_1}{k} s = 0$$

and this concludes the proof.

$\square$

Theorem 2.3. *Let F be a local field with generator π. Let $\mathcal{A}$ be the set additive forms of degree d in N variables and coefficients in F. Let $\mathscr{G} \in \mathcal{A}$. Then, there exists $\mathscr{F} \backsim \mathscr{G}$ such that*

$$\mathscr{F} = \mathscr{F}^{(0)} + \pi \mathscr{F}^{(1)} + \pi^2 \mathscr{F}^{(2)} + \cdots + \pi^{d-1} \mathscr{F}^{(d-1)}$$

where $\mathscr{F}^{(i)}$ is an additive form of degree d in m_i variables (the variables in distinct forms $\mathscr{F}^{(i)}$ being distinct) with all coefficients being $\not\equiv 0 (\bmod \pi)$ and where $m_0, \cdots, m_{d-1}$ satisfy

$$m_0 + \cdots + m_{j-1} \geq \frac{jN}{d}, \ j = 0, \cdots, d. \tag{2.1}$$

We say that $\mathscr{F}$ is a normalized form.

Proof. Let $\alpha \in F$ be the coefficient of the variable x_i of the form $\mathscr{G}$. By Proposition 1.6, we know that $\alpha = \pi^n \cdot \beta$ for some integer n and some unit β. Write $n = q \cdot d + r$ with $q \in \mathbb{Z}$ and $0 \leq r < d$. Then $\alpha = \beta(\pi^r)(\pi^q)^d$. Set $x_i' = (\pi^q)x_i$ and we get that the coefficient of the new variable is $\beta\pi^r$. Proceeding this way with the other variables we find an equivalent form $\mathscr{H}$ for which the power of π of any given coefficient is π^i with $0 \leq i \leq d-1$. Then we can write

$$\mathscr{H} = \mathscr{H}^{(0)} + \pi\mathscr{H}^{(1)} + \pi^2\mathscr{H}^{(2)} + \cdots + \pi^{d-1}\mathscr{H}^{(d-1)}$$

where $\mathscr{H}^{(i)}$ is an additive form of degree d in $m_i^{(\mathscr{H})}$ variables (the variables in distinct forms $\mathscr{H}^{(i)}$ being distinct) with all coefficients being $\not\equiv 0(\bmod \pi)$. We have $\sum_{i=0}^{d-1} m_i^{(\mathscr{H})} = N$. Then, Lemma 2.2 says that we can choose $l \in \{0, 1, \cdots, d-1\}$ such that

$$m_l^{(\mathscr{H})} + m_{l+1}^{(\mathscr{H})} + \cdots + m_{l+j-1}^{(\mathscr{H})} \geq \frac{jN}{d}, \ j = 0, \cdots, d.$$

If we set $x_i' = \pi x_i$ for the variables of $\mathscr{H}^{(0)}$ and then divide $\mathscr{H}$ by π we effect a cyclic permutation of $\mathscr{H}^{(0)}, \mathscr{H}^{(1)}, \cdots, \mathscr{H}^{(d-1)}$. Repeat this process l times and the new equivalent form $\mathscr{F}$ will satisfy (2.1).

□

2.2 Hensel's Lemma and contraction of variables

Definition 2.4. *Let F be a local field with generator π. Let $\mathscr{F}(x) = a_1x_1^d + \cdots + a_Nx_N^d \in F[x]$ an additive form. We say that a solution $\overline{x}$ to $\mathscr{F} = 0$ is non-singular if there exists $i \in \{1, \cdots, N\}$ such that $a_i\overline{x}_i \not\equiv 0 \bmod \pi$. Similarly, if $\overline{x}$ is a solution to $\mathscr{F} \equiv 0(\mathrm{mod}\pi^j)$ such that there exists $i \in \{1, \cdots, N\}$ with $a_i\overline{x}_i \not\equiv 0 \bmod \pi$, then we say that $\overline{x}$ is a non-singular solution modulo π^j.*

Next we give another version of Hensel's lemma. It is Lemma 1 of [4]. In fact, in [4] the authors work with systems of diagonal forms and present a version of Hensel's lemma that can be applied to these systems. Here we enunciate a simplified version.

Lemma 2.5 (Hensel's Lemma II). *Let F be an extension of $\mathbb{Q}_p$ of degree n. Let e be its ramification index. Set $d = p^\tau \cdot m$ with $(m, p) = 1$ and define*

$$\gamma = \begin{cases} 1 & \text{for } \tau = 0, \\ e(\tau+1) & \text{for } p > 2, \ \tau > 0, \\ e(\tau+2) & \text{for } p = 2, \ \tau > 0. \end{cases}$$

Let $\mathscr{F}(x) = a_1x_1^d + \cdots + a_Nx_N^d \in F[x]$*. If* $\mathscr{F} \equiv 0 \bmod \pi^\gamma$ *admits a non-singular solution modulo* π^γ*, then* f *admits non-trivial zero in* F*.*

Let F be an extension of $\mathbb{Q}_p$ with generator π. When we have

$$\mathscr{F} = \mathscr{F}^{(0)} + \pi\mathscr{F}^{(1)} + \pi^2\mathscr{F}^{(2)} + \cdots + \pi^{d-1}\mathscr{F}^{(d-1)} \in F[x] \tag{2.2}$$

with $\mathscr{F}^{(i)}$ an additive form of degree d in m_i variables with all coefficients being $\not\equiv 0(\bmod \pi)$, we are going to say that a variable of $\mathscr{F}^{(i)}$ is at *level* i. That is, the variable x_j of $\mathscr{F}(x)$ is at level i if π^i divides the coefficient of x_j but π^{i+1} does not. When $\alpha \in F$ is the coefficient of a variable at level i, we say the α is at level i.

Consider a form as in (2.2). Let $x_1, \cdots, x_t$ be variables of this form at levels less than j. If we can find $b_1, \cdots, b_t \in O_F$ such that

$$a_1b_1^d + \cdots + a_tb_t^d = \pi^l \cdot c$$

with $c \not\equiv 0 \bmod \pi$, then, setting $x_i = b_iT$ we obtain a new variable T of level $l \geq j$ and coefficient $\pi^l \cdot c$. This process is called a *contraction of variables to a new variable at level* l.

So, if we can use a variable at level zero in a series of contractions and get a new variable T at level γ, Lemma 2.5 says that there exists a non-trivial solution for $\mathscr{F} = 0$. Indeed, we just have to assign the value 1 to variables that were used on the series of contractions and 0 to the ones that were not used. The solution will be non-singular for we have used a variable at level 0.

Variables at level zero, or variables at higher levels that were obtained by contractions containing variables at level zero, will be called *primary.* More precisely, (i)-*primary* if it is primary and is at level i. The other variables will be called (i)-*secondary.* We denote by p_i the number of primary variables at level i and by s_i the number o secondary variables at level i. That being said, using the aforementioned version of Hensel's lemma, it is sufficient to construct a (γ)-primary variable in order to guarantee non-trivial zero for $\mathscr{F}$.

Chapter 3

Combinatorial lemmas

In this section we state a number of preliminary lemmata that will be used in the proofs of theorems 1 and 2. Here we will set $K = \mathbb{Q}_2(\sqrt{5})$ the only unramified extension of $\mathbb{Q}_2$ (see example 1.18). We have 2 being the generator of K. Remember (Proposition 1.8) that every $a \in O_K$ can be written as

$$a = \sum_{i \geq 0} a_i 2^i \tag{3.1}$$

where $a_i \in \mathscr{R}$, and $\mathscr{R}$ is a set of representatives for $k_K = O_K/(2)$. In Example 1.19 we saw that $\mathscr{R} = \left\{0, 1, \frac{1+\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}\right\}$ is a set of representatives for k_K. But we know that k_K is isomorphic to $\mathbb{F}_4$ and sometimes we will simply write $\mathscr{R} = \{0, 1, \alpha, 1+\alpha\}$ and use the additive structure of $\mathbb{F}_4$. Observe that the integer a written as in (3.1) is at level l if, and only if, l is the first index satisfying $a_l \neq 0$. When a is at level l we can write

$$a = 2^l(a_0 + a_1 \cdot 2 + \cdots + a_n \cdot 2^n + \cdots) \tag{3.2}$$

where $a_i \in \mathscr{R}$ for all i and $a_0 \neq 0$. Then we will call a_0 the *zeroterm* of a. Similarly we will call a_1 and a_2 the *oneterm* and the *twoterm* of a.

Lemma 3.1. *a) Suppose we have four variables at level l. Then we can contract two of them to a variable T at level at least $l+1$.*

b) If we have three variables at level l, then we can contract three (maybe two) of them to a variable T at level at least $l+1$.

c) If we have three variables at level l with the same zeroterm, then we can contract exactly two variables to a new variable at level exactly $l+1$.

Proof. The first two statements follow directly from [11]. We prove the last statement. Without loss of generality, we suppose $l = 0$ and that the zeroterm is $a_0 = 1$. Since we are interested in contract variables to level 1, we can work modulo 2^2. Consider three coefficients (modulo 2^2)

$$a_1 = 1 + 2b_1, \quad a_2 = 1 + 2b_2, \quad a_3 = 1 + 2b_3$$

where b_1, b_2 and b_3 are elements of $\mathscr{R}$.
If $a_1 + a_2 \equiv 0 \bmod 2^2$, we have $(1 + b_1 + b_2) \equiv 0 \bmod 2$. It is easy to see (remember that $(O_K, +) \cong (C_2 \times C_2, +))$ that this occurs just in the four following cases.

- If $b_1 = 1, b_2 = 0$ $(b_1 = 0, b_2 = 1)$. In this case, we look for b_3. If $b_3 = 0$, then $a_2 + a_3$ has level exactly 1. If $b_3 = 1$, then $a_1 + a_3$ has level exactly 1. And if $b_3 \notin \{0, 1\}$ we have $b_1 + b_3$ and $b_2 + b_3$ both with level exactly 1.

- If $b_1 = a \notin \{0, 1\}, \beta_2 = a + 1$ $(b_2 = a \notin \{0, 1\}, b_1 = a + 1)$. If $b_3 = a$, then $b_1 + b_3$ has level exactly 1. If $b_3 = a + 1$, then $b_2 + b_3$ has level exactly 1. And if $b_3 \in \{0, 1\}$, $b_1 + b_3$ and $b_2 + b_3$ both have level exactly 1.

□

Observation. If we have two (l)-primary variables and one (l)-secondary, part (b) of Lemma 3.1 says that we can contract some of these variables to obtain a (j)-primary with $j \geq l + 1$. Indeed, at least one of the (l)-primary must be used in this contraction.

If the reader is interested only on Theorem 1, he can skip the remaining of this chapter. In theorem 2 we work with diagonal forms of degree 6. So we have a lot more tools at hand. Indeed, we can use the structure of the sixth powers of O_K. The next lemma characterizes these sixth powers modulo 2^3. But why modulo 2^3? If we want to find non-trivial zero for a diagonal f of degree 6, then it is sufficient (Hensel's Lemma II) to create a (γ)-primary, and in this case $\gamma = 3$. Hence, we can restrict our attention to modulo 2^3, which we will do from now on; for example, if $a \in O_K$, we will simply write

$$a = a_0 + a_1 \cdot 2 + a_2 \cdot 4$$

with $a_0, a_1, a_2 \in \mathscr{R}$.

Lemma 3.2. *The only non-zero* $6th$ *power in* $O_K/(2^2)$ *is 1. However, there are two non-zero* $6th$ *powers in* $O_K/(2^3)$*. These are 1 and 1* $+ 1 \cdot 4$*.*

Proof. This can be proven by direct calculation. First we deal with the sixth powers of the nonzero representatives. Clearly $1^6 \equiv 1 \bmod 8$. For $\left(\frac{1+\sqrt{5}}{2}\right)$ we have

$$\begin{aligned} &\left(\frac{1+\sqrt{5}}{2}\right)^2 = \left(\frac{3+\sqrt{5}}{2}\right) \\ \Longrightarrow &\left(\frac{1+\sqrt{5}}{2}\right)^4 = \left(\frac{1+\sqrt{5}}{5}\right) + 2\cdot\left(\frac{3+\sqrt{5}}{2}\right) \\ \Longrightarrow &\left(\frac{1+\sqrt{5}}{2}\right)^6 \equiv 1+2^2 \bmod 8 \end{aligned} \tag{3.3}$$

and proceeding in the same way we conclude that $\left(\frac{3+\sqrt{5}}{2}\right)^6 \equiv 1 \bmod 8$. Now consider a general $x \in O_K$. Write $x = a + 2\cdot b + 2^2 \cdot c(\text{mod} 8)$ with $a, b, c, d \in \mathscr{R}$ and $a \neq 0$. Then $x^6 \equiv a^6 + 4a^4 b(a+b)(\text{mod}8)$. If either b or $(a+b) \equiv 0 \bmod 2$ we get $x^6 \equiv a^6$ and we are done. If not, a simple calculation shows us that $4a^4b(a+b) \equiv 1(\text{mod}2)$ and we have $x^6 \equiv a^6 + 4(\text{mod}8)$ and the result follows immediately.

$\square$

From now on, ζ will denote an element of O_K for which $\zeta^6 \equiv 1 + 1\cdot 4(\text{mod}8)$. Let x be a variable with coefficient $a + 2b + 4c$. If we set $T = \zeta x$, then we get a new variable T with coefficient $a+2b+4(c+a)$. If we simply set $T = x$, the coefficient of the new variable would still be $a+2b+4c$. For each $a \in \mathscr{R} - \{0\}$ we define δ_a to be a number which can be either 0 or a. In these terms, if we have a variable x with coefficient $a + 2b + 4c$, we can make a change of variables and get a new variable T with coefficient $a+2b+4(c+\delta_a)$. The point of this is that we can talk about all the possible ways to contract all at once without needing to make special cases for whether we set $T = x$ or $T = \zeta x$ in the contraction. The benefits of this approach will become clear in the lemmas that follow.

Lemma 3.3. *Suppose we have 3 variables at level 0 which all have different zeroterms. If we contract these variables to a new variable* T *at level 2, then we can also contract* *them to a variable at level 3. If we contract them to a variable T at level 1, then we can contract in such a way that the oneterm of T has any value that we choose.*

Proof. Suppose that the variables in question are x_1, x_2, x_3 and that they appear in our form as

$$(1 + 2b_1 + 4c_1)x_1^6 + (\alpha + 2b_2 + 4c_2)x_2^6 + (1 + \alpha + 2b_3 + 4c_3)x_3^6.$$

Contracting the three variables we get a new variable T with coefficient $2(1 + \alpha + b_1 + b_2 + b_3) + 4(c_1 + c_2 + c_3 + \delta_1 + \delta_\alpha + \delta_{1+\alpha})$. If $1 + \alpha + b_1 + b_2 + b_3 \equiv 0(\bmod 2)$ (that is, if we can contract the three variables to a new variable at level 2), then the coefficient of our new variable would be

$$4(d + c_1 + c_2 + c_3 + \delta_1 + \delta_\alpha + \delta_{1+\alpha})$$

for some $d \in \mathscr{R}$. But we can choose the $\delta_i' s$ in such a way that $\delta_1 + \delta_2 + \delta_3$ equals whichever element of $\mathscr{R}$. In particular, we can choose them to satisfy

$$d + c_1 + c_2 + c_3 + \delta_1 + \delta_\alpha + \delta_{1+\alpha} = 0$$

and we can get T at level at least 3. If, on the other hand, we have $1 + \alpha + b_1 + b_2 + b_3 \not\equiv 0(\bmod 2)$, our variable T would be at level exactly 1, but, proceeding as above, we would be able to choose its oneterm freely.

$\square$

Observation. Remember that Hensel's Lemma II says that to find nontrivial zero for our form, it is sufficient to use a variable of level l in contractions in order to produce a new variable of level at least $l + 3$. So, whenever we contract three variables at level l having distinct zeroterms, we'll assume that the new variable has level exactly $l + 1$, moreover, we'll be able to choose its zeroterm.

Corollary 3.4. *Suppose that our form has two disjoint sets of 3 variables at level 0 such that each set has all 3 possible zeroterms represented. If both of these sets can be contracted to level 1, and there is one additional variable at level 1 (which can be either primary or secondary), then we can construct a primary variable at level at least 3.*

Proof. Contract both 3-variable sets obtaining two primary variables T_1 and T_2. If none of these variables are at a level higher than 1, then Lemma 3.3 guarantees that we can choose their oneterms γ_1 and γ_2 freely. Let x be the additional variable at level 1. Suppose first that two of the three variables have same zeroterm. Without loss of generality we assume one of these variables being T_1. Then we can write the coefficient of T_1 as $2b+4\gamma_1$. Suppose that the other variable has coefficient $2b+4c$. If we now set both variables equal to a new variable U, then its coefficient would be $4(b+\gamma_1+c)$. Since we can choose freely the value of γ_1 we can set $\gamma_1 = -(b+c)$ and then obtain a primary variable at level at least 3.

Suppose on the other hand that the three variables at level zero have distinct zeroterms. We may assume that they appear in our form as

$$(2b_1 + 4\gamma_1)T_1^6 + (2b_2 + 4\gamma_2)T_2^6 + (2b_3 + 4c)x^6$$

where $\{b_1, b_2, b_3\} = \{1, \alpha, 1+\alpha\}$ and we can choose γ_1, γ_2 to have any values we wish. Then setting $x = T_1 = T_2 = U$ produces a new variable U with coefficient $4(1+\alpha+c+\gamma_1+\gamma_2)$. Again, since we can choose freely the values of γ_1 and γ_2, we can make $-(1+\alpha+c+\gamma_1) = \gamma_2$ and obtain a primary variable at level at least 3.

$\square$

Corollary 3.5. *Suppose our form has one set of 3 variables at level 0 such that all 3 possible zeroterms are represented. If we have two variables at level 1 (wich can be either primary or secondary) with distinct zeroterms, then we can construct a primary variable at level at least 3.*

Proof. If these three variables can not be contracted to a primary variable at level at least 3, then Lemma 3.3 says that we can contract them to a (1)-primary having whichever oneterm γ we desire. We have two possibilities:

Possibility I. One of the (1)-secondary variables has the same zeroterm as the (1)-primary. Let $(2\beta + 2^2\gamma_1)x^6$ be the (1)-primary and $(2\beta + 2^2\gamma_2)y^6$ the (2)-secondary. We make $x = y = T$ and get a new variable T having coefficient $2^2(\beta+\gamma+\beta_2)$. And since we are free to choose any γ we want, we can do it so the new variable T has level at least 3.

Possibility II. If Possibility I does not happen, then the three variables will have distinct zeroterms and they can be contracted to a new variable of higher level. It is easy to see that here we can also choose γ so this new variable is at level at least 3.

□

Lemma 3.6. *Suppose that we have 4 variables at level 0 with the same zeroterm a. Then the following are true.*

a) If all four variables have the same oneterm, then they can be contracted to a variable T at level at least 2. Moreover, if T is at level exactly 2, then we can choose the zeroterm of T to be either possibility which is different from a.

b) If all four possible oneterms exist among the four variables, then we can contract some of these variables to a primary variable at level at least 3.

c) If exactly three different oneterms appear in the variables, then we can contract two of these variables to a variable at level at least 2, while the other two variables contract to a variable at level 1. Moreover, if the new variable at level at least 2 is in fact at level exactly 2, then we can choose its zeroterm to be anything other than a.

d) If exactly two different oneterms appear in the variables, with one of the oneterms appearing three times, then we can use these variables to create one primary variable at level exactly 1 and one primary variable which is at level at least 1. However, we cannot control the level of this second variable. If both variables are at level 1, then they have different zeroterms. Finally, for each variable, we can choose between two options for the coefficient of 4 in the variable's coefficient. However, we cannot control what options are possible.

e)If exactly two different oneterms appear in the variables, and each appears twice, then we can contract these four variables to a primary variable at level at least 2. If this new variable is forced to be at level exactly 2, then we can choose the zeroterm of this variable to be either possibility other than a.

Proof. To prove part (a), suppose that the variables are x_1, x_2, x_3, x_4 and that they appear in the form as

$$(a+2b+4c_1)x_1^6+(a+2b+4c_2)x_2^6+(a+2b+4c_3)x_3^6+(a+2b+4c_4)x_4^6.$$

We can contract these four variables to a new variable T with coefficient $4(a + c_1 + c_2 + c_3 + c_4 + \delta_a)$. If we can choose δ_a so the coefficient is $0 \pmod 2$, then we get a variable at level at least 3. If not, We have two possible oneterms $((a+c_1+c_2+c_3+c_4+\delta_a)$. If either of these oneterms is divisible by two, we have actually constructed a primary variable at level at least 3. If not, we note that the terms in parenthesis are different mod2 and if one is congruent to a mod2, then the other must be zero mod2. So we can choose the coefficient of T to have either zeroterm which is not a.

To prove part (b), suppose that the variables appear in the form as

$$(a + 2a + 4c_1)x_1^6 + (a + 4c_2)x_2^6 + (a + 2b_3 + 4c_3)x_3^6 + (a + 2b_4 + 4c_4)x_4^6$$

Where b_3 and b_4 are the two possible oneterms which are different from a and 0. We can contract these two variables to a new variable T with coefficient $4(c_1 + c_2 + \delta_a)$. If we can choose δ_a so the term in parenthesis is divisible by 2, then we are done. Otherwise, note that we can choose the zeroterm to be either possibility other than a (similar to what we have done in part (a)).

Next, if we contract x_3 and x_4 we obtain a variable U with coefficient $2(a + b_3 + b_4) + 4(c_3 + c_4 + \delta_a)$. However, we have $a + b_3 + b_4 = 1 + \alpha + (1 + \alpha) \equiv 0 \pmod 2$, and so we can rewrite this coefficient as $4(\beta + c_3 + c_4 + \delta_a)$. Again, if we can choose δ_a so the term in parenthesis is zero $\pmod 2$, then we get a primary variable at level at least 3. Otherwise, we can choose the zeroterm to be any possibility other than a. In particular, if we can not make either T or U a primary variable at level at least 3, then we can choose it's zeroterms being equal, and then contract these two variables setting $T = U = X$ we get a primary variable X at level at least 3.

To prove part (c), suppose that the variables appear in the form as

$$(a + 2b + 4c_1)x_1^6 + (a + 2b + 4c_2)x_2^6 + (a + 2b_3 + 4c_3)x_3^6 + (a + 2b_4 + 4c_4)x_4^6$$

where $b_3 \neq b_4$ and $b_3, b_4 \neq b$. If we contract some pairs of variables x_i, x_j setting $x_i = x_j = T$, then we get the following possibilities for the coefficient of T:

Variables contracted	Coefficient of T
x_1, x_2	$2a + 4(b + c_1 + c_2)$
x_1, x_3	$2(a + b + b_3) + 4(c_1 + c_3)$
x_1, x_4	$2(a + b + b_4) + 4(c_1 + c_4)$
x_3, x_4	$2(a + b_3 + b_4) + 4(c_3 + c_4)$

The conditions on b, b_3 and b_4 imply that the numbers $b + b_3, b + b_4$ and $b_3 + b_4$ are all different and nonzero (mod2). Then, exactly one of these ways to contract will yield a variable at level at least 2. Since x_1 and x_2 have the same oneterm, it is not possible to make two contractions which both go to level at least 2. Hence one of these contractions will end up at level exactly 1. For the contraction to level at least 2, the same reasoning shows that either we can contract the variables to level at least 3, or we can choose the zeroterm of the new variable to be either possibility other than a.

To prove part (d), suppose that the variables appear in the form as

$$(a + 2b_1 + 4c_1)x_1^6 + (a + 2b_2 + 4c_2)x_2^6 + (a + 2b_2 + 4c_3)x_3^6 + (a + 2b_2 + 4c_4)x_4^6.$$

If we set $x_1 = x_2 = T$, then the coefficient of T will be $2(a+b_1+b_2)+4(c_1+c_2)$. Similarly, if we set $x_3 = x_4 = U$, the coefficient of U will be $2a + 4(b_2 + c_2 + c_3)$. The variable U is at level exactly 1, while T will be at level 2 if $b_1 + b_2 \equiv a(\mathrm{mod}\,2)$ and at level exactly one otherwise. If T is at level exactly 1, then since $b_1 \neq b_2$, we know that $a+b_1+b_2 \not\equiv a \bmod 2$, and so the variables T and U have different zeroterms. That we have two options for the coefficient of 4 in these coefficients is proved as in previous parts of the lemma.

To prove part (e), suppose that the variables appear in the form as

$$(a + 2b_1 + 4c_1)x_1^6 + (a + 2b_1 + 4c_2)x_2^6 + (a + 2b_3 + 4c_3)x_3^6 + (a + 2b_3 + 4c_4)x_4^6.$$

We contract the four variables to a new variable T with coefficient $4(a + b_1 + b_3 + c_1 + c_2 + c_3 + c_4 + \delta_a)$. We have two possibilities for the coefficient of T. If either of these possibilities is a, then the other will be a primary variable at level at least 3. Hence, if both of these contractions leads to variables at level exactly 2, then the two possible zeroterms must be the two possibilities other than a.

$\square$

Corollary 3.7. *If we have five variables at level zero having the same zeroterm a, then we can contract four of them (or maybe two) to a primary variable at level at least 2. If it is at level exactly two, then we can choose its zeroterm to be either possibility other than a.*

Proof. We just have to analyse the possible distributions of the oneterms of these five variables. If all four possible oneterms are represented we are done by Part (b) of Lemma 3.6. So we can assume only three types of oneterms appearing. Let them be a, b, and c. The next table gives us all possible distributions (up to permutations) of the oneterms.

a	b	c
5	0	0
4	1	0
3	1	1
3	2	0
2	2	1

In the first two cases Part (a) of Lemma 3.6 gives us what we want. In the third case we use part (c) of Lemma 3.6. Finally, if the last two cases occur, then we use part (e) of Lemma 3.6.

□

Lemma 3.8. *Suppose that we have three variables at level 0 with the same zeroterm a. Then the following are true.*
a) If these variables have three different oneterms, then we can contract two of them to a variable T at level exactly 1 and we have a choice of two zeroterms for T. If it is not possible to contract to a variable at level at least 2, then we may arrange for T to have any zeroterm we like. If it is possible to contract to level 2, then either we can contract to level at least 3, or else we can arrange for T to have either possible zeroterm other than a.
b) If these variables have exactly two different oneterms, then we can contract two of them to a variable T at level at least 1. If it is not possible to contract to a variable at level at least 2, then we have a choice of two zeroterms for T, one of which is a.

c) If these variables all have the same oneterm, then we can contract two of them to a variable T at level 1 with zeroterm a. In this case, it is not possible to contract either to a variable at level 2 or to a variable at level 1 with any other zeroterm.

Proof. We denote our three variables by x_1, x_2, x_3. To prove part (a) we suppose the variables appear in the form as

$$(a + 2b_1 + 2c_1)x_1^6 + (a + 2b_2 + 2c_2)x_2^6 + (a + 2b_3 + 2c_3)x_3^6$$

with the $b_i's$ pairwise distinct. We analyse the following possibilities of contractions:

Variables contracted	Coefficient of T
$x_1,\ x_2$	$2(a + b_1 + b_2) + 4(c_1 + c_2 + \delta_a)$
$x_1,\ x_3$	$2(a + b_1 + b_3) + 4(c_1 + c_3 + \delta_a)$
$x_1,\ x_4$	$2(a + b_2 + b_3) + 4(c_2 + c_3 + \delta_a)$

Note that at most one of the contractions above gives us a variable at level at least 2. The other two possibilities yields variables at level exactly 1 and by the assumptions on the $b_{i's}$ it is easy to see that we can choose either zeroterm other than a. In the case where none of these contractions give us a variable at level at least 2, we can choose whichever zeroterm we want. Now, suppose one of these contractions results in a variable at level at least 2. Without loss of generality assume this contraction involving x_1 and x_2. Then we have $a + b_1 + b_2 \equiv 0(\bmod 2)$ and the coefficient of T is $4(\beta + c_1 + c_2 + \delta_a)$ for some $\beta \in \mathscr{R}$. So we can either obtain a variable at level at least 3, or a variable at level exactly 2 for which we can choose the zeroterm to be either possibility other than a.

To prove part (b) we suppose the variables appear in the form as

$$(a + 2b_1 + 2c_1)x_1^6 + (a + 2b_1 + 2c_2)x_2^6 + (a + 2b_3 + 2c_3)x_3^6$$

with the $b_1 \neq b_3$. We analyse the following possibilities of contractions:

Variables contracted	Coefficient of T
$x_1 = x_2 = T$	$2a + 4(b_1 + c_1 + c_2)$
$x_1 = x_3 = T$	$2(a + b_1 + b_3) + 4(c_1 + c_3)$

In the first contraction, the variable T has level exactly 1 and zeroterm a. If the second contraction also gives a variable at level 1, then, since $b_1 \neq b_2$ we must have (without loss of generality) $b_1 = a$. Indeed, if a, b_1, b_3 are pairwise distinct, their sum must be $\equiv 0 \bmod 2$. So, the zeroterm of T would be $b_3 \neq a$ and we have two options, one of them being a.

Finally we analyse part (c). We suppose the variables appear in the form as

$$(a + 2b_1 + 2c_1)x_1^6 + (a + 2b_1 + 2c_2)x_2^6 + (a + 2b_1 + 2c_3)x_3^6$$

and all possible ways of contracting two of these variables give us a variable T with coefficient $2a + 4(b_1 + c)$ for some c. This variable is at level 1 and have zeroterm a.

□

Corollary 3.9. *Suppose we have three variables at level 0 with the same zeroterm a. If at least two of the oneterms of these variables are equal, then we can contract two of them to a variable T at level exactly 1 and having zeroterm a. If not, then we can contract two of them to a variable T at level exactly 1 and we have a choice of two zeroterms for T but we can not assume that one of them is a. But if we can not create one with zeroterm a, then we can obtain a new variable at level at least 2.*

Proof. If at least two of the variables have the same oneterm, then by parts (b) and (c) of Lemma 3.8 we can create a new variable at level exactly 1 and having zeroterm a. If all oneterms are distinct, then by part (a) of Lemma 3.8, either we can create a variable at level at least 2, or we can obtain a variable at level 1 having zeroterm a.

□

Corollary 3.9 says that if we have three variables at level j all with the same zeroterm a, so if we are not able to contract two of them to a variable at level exactly $j+1$ having zero term a, then we can contract two of them to a variable at level at least $j+2$.

Chapter 4

Additive forms of degree d

In this chapter we prove theorem 1. We restate it here.

Theorem 1. *Let $K = \mathbb{Q}_2(\sqrt{5})$ be the only unramified quadratic extension of $\mathbb{Q}_2$. Let $d \in \mathbb{N}$ not power of 2. Then $\Gamma(d, K) \leq d^2 + 1$.*

Proof. Let $\mathscr{F}$ be a diagonal form of degree d in N variables and with coefficients in K. We want to prove that $\mathscr{F}$ admits non-trivial zero whenever $N > d^2$. We saw in Chapter 2 that we can choose freely in the class of $\mathscr{F}$ with respect to the equivalence relation " $\backsim$ " any representative we want. Here we will choose a representative that is normalized. So we assume that $\mathscr{F}$ satisfies all the properties presented in Theorem 2.3. In particular, if we set $d = 2^l \cdot m$, $m \geq 3$ odd, and assume $N \geq d^2 + 1$, we can write

$$\mathscr{F} = \mathscr{F}^{(0)} + 2\mathscr{F}^{(1)} + 2^2\mathscr{F}^{(2)} + \cdots + 2^{d-1}\mathscr{F}^{(d-1)}$$

where $\mathscr{F}^{(i)}$ is an additive form of degree d in m_i variables (the variables in distinct forms $\mathscr{F}^{(i)}$ being distinct) with all coefficients being $\not\equiv 0 (\text{mod} 2)$, and we have

$$m_0 + \cdots + m_j \geq (j+1) \cdot d + 1 = (j+1) \cdot 2^l \cdot m + 1 \geq (j+1) \cdot 2^l \cdot 3 + 1 \tag{4.1}$$

for $j = 1, \cdots, d-1$. In particular, $m_0 \geq 2^l \cdot 3 + 1$.

We will assume first that $l \geq 5$ and prove the theorem in this case. Later we will solve the rest of the cases. We have seen that it is sufficient to construct an $(l+2)$-primary variable. We divide the proof in cases according to the value of m_0.

- **Case $m_0 \geq 2^l \cdot 8 - 1$.**

  Remember that by Lemma 3.1 (parts (a) and (b)) we have that, given four variables at level j, we can contract two of them to a new variable at a level higher than j. And given three variables at level j, we can contract three of them (or maybe two) to a new variable at a level higher than j. We will assume that when we make these contractions the new variable will be at level exactly $j+1$. If we can produce a primary variable at level $l+2$ proceeding this way, then it would be easier to produce a primary variable at level $l+2$ if the jumps on the levels were higher. So, we have

  $$p_1 \geq \frac{2^l \cdot 8 - 1 - 3}{2} + 1 = 2^{l-1} \cdot 8 - 1$$

  and applying reasoning recursively we get $p_{l+1} = 2^{l-(l+1)} \cdot 8 - 1 = 3$. So we can contract these three variables to an $(l+2)$-primary and we are done.

  Observation From now on, unless stated otherwise, we will always assume that, when contracting primary variables at level j, the new variable will be at level exactly $j+1$. Furthermore, whenever we want to make reference to parts (a) and (b) of Lemma 3.1 we will simple cite Lemma 3.1. If we want to reference part (c) we will make it clear.

- **Case $2^l \cdot 6 - 1 \leq m_0 \leq 2^l \cdot 8 - 2$.**

  By Lemma 3.1 we have $p_1 \geq \frac{2^l \cdot 6 - 4}{2} + 1 = 2^{l-1} \cdot 6 - 1$. Recursively we obtain $p_l \geq 5$ which implies $p_{l+1} \geq 2$. If $m_{l+1} \geq 1$ we are done (just apply Lemma 3.1). If not, we must have

  $$\begin{aligned} m_0 + \cdots + m_{l+1} &\geq (l+2)d + 1 \\ m_0 + \cdots + m_l &\geq (l+2)d + 1 \\ m_1 + \cdots + m_l &\geq (l+2)d + 1 - m_0 \\ &\geq (l+2)d + 1 - 2^l \cdot 8 + 2 \\ &\geq 2^l \cdot 7 + 3 \text{ , since } l \geq 3. \end{aligned}$$

We want to produce an $(l+1)$-secondary and then proceed as in case $m_{l+1} \geq 1$. We assume the worst case: all secondary variables are at level 1. So we have

$$s_1 \geq 2^l \cdot 7 + 3 \geq 2^l \cdot 7 - 5.$$

By part (c) of Lemma 3.1 we have

$$s_2 \geq \frac{s_1 - 5}{2} = 2^{l-1} \cdot 7 - 5.$$

Continuing this way we obtain $s_{l+1} \geq 2$ and we are done.

Observation Usually when contracting secondary variables, we need to have absolute certainty of the levels of the new variables. For this reason, when contracting secondary variables we will always use Part (c) of Lemma 3.1.

- **Case** $2^l \cdot 5 - 1 \leq m_0 \leq 2^l \cdot 6 - 2$**.**

Proceeding as before, we use Lemma 3.1 and obtain $p_l \geq 4$. If $m_l \geq 1$ we can use the four (l)-primary variables and one (l)-secondary to obtain $p_{l+1} \geq 2$ and then proceed as we did in the last case. If not, we must have

$$\begin{aligned} m_0 + \cdots + m_l &\geq (l+1)d + 1 \\ m_0 + \cdots + m_{l-1} &\geq (l+1)d + 1 \\ m_1 + \cdots + m_{l-1} &\geq (l+1)d + 1 - m_0 \\ &\geq (l+1)d + 1 - 2^l \cdot 6 + 2 \\ &\geq 2^l \cdot 6 + 3 \ , \ \text{ since } l \geq 3. \end{aligned}$$

We want to produce a (l)-secondary variable so we can use the same idea used in case $m_l \geq 1$. We assume the worst case: all secondary variables are at level 1. So we have

$$s_1 \geq 2^l \cdot 6 + 3 \geq 2^l \cdot 6 - 5.$$

By Lemma 3.1 we have

$$s_2 \geq \frac{s_1 - 5}{2} = 2^{l-1} \cdot 6 - 5.$$

Continuing this way we obtain $s_l \geq 7$ and we are done.

- **Case** $2^l \cdot (\frac{9}{2}) - 1 \leq m_0 \leq 2^l \cdot 5 - 2$**.**

  Applying Lemma 3.1 recursively we get $p_{l-1} \geq 8$. If $m_{l-1} \geq 19$ we are done. Indeed, in this case we can use Lemma 3.1 and obtain $s_{l-1}, s_l, s_{l+1} \geq 1$ and eight $(l-1)$-primary and one $(l-1)$-secondary give us $p_l \geq 4$. Proceeding this way we get $p_{l+2} \geq 1$. Now, if $m_{l-1} \leq 18$ then $m_1 + \cdots + m_{l-2} \geq 2^l \cdot 7 + 21$ and then we can contract these variables to get $s_{l-1} \geq 19$.

- **Case** $2^l \cdot 4 + 1 \leq m_0 \leq 2^l \cdot (\frac{9}{2}) - 2$

  In this case we have $m_1 \geq 2^{l-1} \cdot 3 + 3$. We'll use this secondary variables to help create more primary variables. Observe that $s_1 \geq 2^{l-1} \cdot 3 - 5$ and this implies $s_{l-1} \geq 1$. Moreover, in the process of obtaining the $(l-1)$-secondary at least one (j)-secondary was left without being contracted for each $j \in \{1, 2, \cdots, l-2\}$.

  Now, we have $p_1 \geq \frac{2^l \cdot 4 + 1 - 1}{2} = 2^{l-1} \cdot 4$. With the $2^{l-1} \cdot 4$ primary variables at level 1 and one (1)-secondary we obtain $p_2 \geq 2^{l-2} \cdot 4$. Continuing like this we obtain $p_l \geq 4$. If $m_l \geq 7$ we are done. If not, then $m_1 + \cdots + m_{l-2} > 2^l \cdot 10 - 5$ and we can contract these variables to get $s_l \geq 7$.

- **Case** $2^l \cdot (\frac{7}{2}) + 1 \leq m_0 \leq 2^l \cdot 4$**.**

  In this case we have $m_1 \geq 2^l \cdot 2 + 1$. We use these variables to construct one (j)-seconadary for $j = 1, \cdots, l-3$. We contract the $2^{l-3} \cdot 28 + 1$ variables at level zero to $n = 2^{l-4} \cdot 28$ new variables at higher levels. We'll denote by n_i the number of the new variables that are at level i, so we have

  $$2^{l-4} \cdot 28 = n = n_1 + \cdots + n_{l+1}.$$

  Of course, we are not considering the case where $n_{l+2} \geq 1$ since if this happens we have nothing to do.

  Now we'll prove two auxiliary facts.

  Fact I. If $\sum_{i \geq 2} n_i \geq 2^{l-4} \cdot 4$, then we can obtain a $(l+2)$-primary variable.

  Suppose $\sum_{i \geq 2} n_i \geq 2^{l-4} \cdot 4$. We assume the worst case: $n_2 = 2^{l-4} \cdot 4$ and $n_1 = 2^{l-4} \cdot 24$. So we have $p_1 \geq 2^{l-4} \cdot 24$, $s_1 \geq 1$ and $p_2 \geq 2^{l-4} \cdot 4$. Then, we apply Lemma 3.1 and get

$$
\begin{aligned}
p_2 &\geq 2^{l-4} \cdot 4 + \frac{2^{l-4} \cdot 24 + 1 - 1}{2} \\
&= 2^{l-5} \cdot 8 + 2^{l-5} \cdot 24 \\
&= 2^{l-5} \cdot 32
\end{aligned}
$$

Again we use the (2)-primary variables and one (2)-secondary to obtain $p_3 \geq 2^{l-6} \cdot 32$. Continuing this way we obtain $p_{l-2} \geq 16$. Now, if $m_{l-2} \geq 43$, then we can contract variables and get $s_{l-2}, s_{l-1}, s_l, s_{l+1} \geq 1$. With sixteen $(l-2)$-primary and one $(l-2)$-secondary we get $p_{l-1} \geq 8$. Continuing this way we obtain $p_{l+2} \geq 1$. Then, we can assume $m_{l-2} \leq 42$. But in this case we have

$$
\begin{aligned}
m_0 + m_1 + \cdots + m_{l-3} + m_{l-2} &\geq (l-1)2^l \cdot 3 + 1 \quad \Rightarrow \\
m_1 + \cdots + m_{l-3} &\geq (l-1)2^l \cdot 3 + 1 - 2^l \cdot 4 - 42 \\
&\geq 2^l \cdot 12 - 2^l \cdot 4 - 41 \quad \text{since } l \geq 5 \\
&= 2^l \cdot 8 - 41
\end{aligned}
$$

and even assuming that all of these variables have level 1 we can contract them to obtain $s_{l-2} \geq 43$ and in this process at least one (j)-secondary is left behind so we can proceed exactly as we did above.

Fact II. If $\sum\limits_{i \geq 3} n_i \geq 2^{l-4} \cdot 2$, then we can obtain a $(l+2)$-primary variable.

Fact II can be proved in the same way as fact I has been proved.

By Fact I, we only have to consider the cases where

$$0 \leq \sum_{i \geq 2} n_i < 2^{l-4} \cdot 4.$$

We'll divide the demonstration in two parts.

Part I. $2^{l-4} \cdot 2 \leq \sum\limits_{i \geq 2} n_i < 2^{l-4} \cdot 4$

We will assume the worst case: $n_1 = 2^{l-4} \cdot 24$ and $n_2 = 2^{l-4} \cdot 2$.

Here we use a change of variables to get an equivalent form $\mathscr{F}^1$ and then we will try to find non-trivial zero for $\mathscr{F}^1$. The change of variables is obtained in the following way: Let $\mathscr{F}$ be our form with all the new variables obtained by the aforementioned contractions. We use Lemma 2.3 with the change of variables

$$\mathscr{F}^1 = \frac{1}{2}\mathscr{F}(2x_1, \cdots, 2x_{m_0}, x_{m_0+1}, \cdots, x_N).$$

to get the equivalent form $\mathscr{F}^1$. We will denote by $m_i^{(1)}$ the number of variables of $\mathscr{F}^1$ at level i, $i = 0, 1, \cdots, d-1$. It is easy to see that $\mathscr{F}^1$ satisfies

$$\begin{aligned} m_0^1 &\geq m_1 + n_1 \\ &= m_0 + m_1 - (m_0 - n_1) \\ &\geq 2^l \cdot 6 + 1 - \left(2^l \cdot 4 - 2^l \cdot \frac{24}{16}\right) \\ &= 2^l \cdot \left(\frac{7}{2}\right) + 1 \end{aligned} \tag{4.2}$$

$$\begin{aligned} m_0^1 + m_1^1 &\geq m_1 + n_1 + m_2 + n_2 \\ &= m_0 + m_1 + m_2 - (m_0 - n_1 - n_2) \\ &\geq 2^l \cdot 9 + 1 - \left(2^l \cdot 4 - 2^l \cdot \frac{26}{16}\right) \\ &= 2^l \cdot 6 + 1 + 2^l \cdot \left(\frac{5}{8}\right) \end{aligned} \tag{4.3}$$

and

$$m_0^1 + \cdots + m_j^1 \geq (j+1)2^l \cdot 3 + 1 + 2^l \cdot \left(\frac{5}{8}\right) \tag{4.4}$$

for $j = 2, \cdots, 2^l \cdot 3 - 1$.

Again we use the variables at level zero to produce $n^1 = 2^{l-4} \cdot 28$ new variables at higher levels. We denote by n_i^1 the number of these variables that have level i. By Fact I, we only have to consider the case $\sum_{i \geq 2} n_i^1 < 2^{l-4} \cdot 4$. So we assume $n_1^1 \geq 2^{l-4} \cdot 24$

and then consider the equivalent form $\mathscr{F}^2$ (obtained by the same change of variables that we did above, now applied to $\mathscr{F}^1$) that satisfy

$$\begin{aligned} m_0^2 &\geq m_1^1 + n_1^1 \\ &= m_0^1 + m_1^1 - (m_0^1 - n_1^1) \\ &\geq 2^l \cdot 6 + 1 + 2^l \cdot \left(\frac{5}{8}\right) - (2^l \cdot 4 - 2^l \cdot \frac{24}{16}) \\ &> 2^l \cdot 4 + 1 \end{aligned} \tag{4.5}$$

and

$$m_0^2 + \cdots + m_j^2 \geq (j+1)2^l \cdot 3 + 1$$

and since we have already treated the case $m_0 \geq 2^l \cdot 4 + 1$, we can find non-trivial zero for $\mathscr{F}^2$ and consequently, for $\mathscr{F}$.

Observation From now on, we will keep using the same change of variables used above. So keep in mind that whenever we say that we will get an equivalent form, it will be by means of this change of variables.

Part II. $\sum_{i \geq 2} n_i < 2^{l-4} \cdot 2$**.**

In this case we can assume $n_1 \geq 2^{l-4} \cdot 26$. We construct the equivalent form $\mathscr{F}^1$ that satisfy

$$\begin{aligned} m_0^1 &\geq m_1 + n_1 \\ &= m_0 + m_1 - (m_0 - n_1) \\ &\geq 2^l \cdot 6 + 1 - \left(2^l \cdot 4 - 2^l \cdot \frac{26}{16}\right) \\ &= 2^l \cdot 3 + 1 + 2^l \cdot \left(\frac{5}{8}\right) \end{aligned} \tag{4.6}$$

and

$$m_0^1 + \cdots + m_j^1 \geq (j+1)2^l \cdot 3 + 1 + 2^l \cdot \left(\frac{5}{8}\right).$$

Again we use the variables at level zero to obtain $n^1 = 2^{l-3} \cdot 28$ new variables at higher levels. By Fact I we only have to consider the case $\sum_{i \geq 2} n_i^1 < 2^{l-4}$. So we assume $n_1^1 \geq 2^{l-4} \cdot 24$ and then consider the equivalent form $\mathscr{F}^2$ satisfying

$$
\begin{aligned}
m_0^2 &\geq m_1^1 + n_1^1 \\
&= m_0^1 + m_1^1 - (m_0^1 - n_1^1) \\
&\geq 2^l \cdot 6 + 1 + 2^l \cdot \left(\frac{5}{8}\right) - \left(2^l \cdot 4 - 2^l \cdot \frac{24}{16}\right) \\
&> 2^l \cdot 4 + 1
\end{aligned}
\tag{4.7}
$$

and

$$m_0^2 + \cdots + m_j^2 \geq (j+1)2^l \cdot 3 + 1$$

and by the above cases we know that it is possible to find non trivial zero for $\mathscr{F}^2$.

- $2^l \cdot 3 + 1 \leq m_0 \leq 2^l \cdot (\frac{7}{2})$.

Observe that in this case we have $m_1 \geq 2^{l-1} \cdot 5 + 1$. We can contract these variables and get $s_j \geq 5$ for $j = 1, 2, \cdots, l-1$. We use the variables at level zero to construct $n = 2^{l-4} \cdot 24$ new variables at higher levels. We denote by n_i the number of these new variables that are at level i.

Affirmation. If $\sum\limits_{i \geq 2} n_i \geq 2^{l-4} \cdot 8$ then we can obtain a $(l+2)$-primary variable.

We assume the worst case: $n_1 = 2^{l-4} \cdot 16$ and $n_2 = 2^{l-4} \cdot 8$. Then, using one (1)-secondary variable and Lemma 3.1 we get

$$
\begin{aligned}
p_2 &\geq n_2 + \frac{n_1 + 1 - 1}{2} \\
&= 2^{l-4} \cdot 8 + 2^{l-5} \cdot 16 \\
&= 2^{l-5} \cdot 32
\end{aligned}
$$

Then, with one (2)-secondary and the (2)-primary variables, using Lemma 3.1 we get $p_3 \geq 2^{l-6} \cdot 32$. Continuing this way we obtain $p_l \geq 4$. It's easy to see that if $m_l \geq 7$ then we are done. If not we would have $m_1 + \cdots + m_{l-1} \geq 2^l \cdot 11 - 5$ and we would be able to construct seven (l)-secondary.

So we have the affirmation proved and remains to be analysed the case $\sum\limits_{i \geq 2} n_i < 2^{l-4} \cdot 8$. In this case we have $n_1 \geq 2^{l-4} \cdot 16 + 1$. We consider the equivalent form $\mathscr{F}^1$

satisfying

$$\begin{aligned} m_0^1 &\geq m_1 + n_1 \\ &= m_0 + m_1 - (m_0 - n_1) \\ &\geq 2^l \cdot 6 + 1 - \left(2^l \cdot \binom{7}{2} - 2^l - 1\right) \\ &= 2^l \cdot (\frac{7}{2}) + 2 \end{aligned} \tag{4.8}$$

and

$$m_0^1 + \cdots + m_j^1 \geq (j+1)2^l \cdot 3 + 1$$

and by the above cases we know that it is possible to find non trivial zero for $\mathscr{F}^1$.

Now we just have to analyse the cases $d = 2^l \cdot m$ with $l = 1, 2, 3, 4$.

- Case $d = 3 \cdot 2^4$

  By the proof we just gave for $l \geq 5$, we just have to analyse the cases $2^4 \cdot 3 + 1 \leq m_0 \leq 2^4 \cdot 4$ since for the remaining cases we only used the hypothesis $l \geq 3$. We divide in subcases.

  - Case $63 \leq m_0 \leq 64$.

    We have $m_1 \geq 33$ and, by Lemma 3.1, we can get $s_1, s_2, s_3 \geq 1$. We contract the variables at level zero to $n = 31$ new variables at higher levels. We denote by n_i the number of these new variables at level i so

    $$31 = n_1 + n_2 + \cdots + n_5.$$

    We affirm that if $n_2 + \cdots + n_5 \geq 16$ then we can create a (6)-primary. Indeed, assuming the worst case $n_2 = 16$, then with these (2)-primary and one (2)-secondary we obtain $p_3 \geq 8$ and repeating the argument, $p_4 \geq 4$. If $m_4 \geq 7$ we are done, since we can use Lemma 3.1 to obtain $s_4, s_5 \geq 1$ and then create a (6)-primary. But if $m_4 \leq 6$ we get a bigger m_1 and then we can create seven (4)-secondary.

    So we can assume $n_1 \geq 15$. Suppose $n_1 = 15$, then we can contract these variables to seven variables at higher levels. We get $n_2 + \cdots + n_5 \geq 15 + 7 =$

$22 \geq 16$ and we are done. If $n_1 = 16$ we use these variables and one (1)-secondary to get seven new variables and we are again in the situation just described. This same argument shows us that we only have to analyse the cases $n_1 = 31$.

So we consider the equivalent form $\mathscr{F}^1$ satisfying

$$\begin{aligned} m_0^1 &\geq m_1 + n_1 \\ &= m_0 + m_1 - (m_0 - n_1) \\ &\geq 2 \cdot 2^4 + 32 \\ &= 4 \cdot 2^4 \end{aligned} \tag{4.9}$$

and $m_0^1 + m_1^1 \geq 7 \cdot 2^4$, $m_0^1 + \cdots + m_i^1 \geq (i+1)3 \cdot 2^4 + 2^4$.

and it is sufficient to find non trivial solution for $\mathscr{F}^1$. By proof of the case $l \geq 5$ we can assume $m_0^1 = 64$. And repeating the argument we just used, we obtain an equivalent form $\mathscr{F}^2$ for which

$$\begin{aligned} m_0^2 &\geq m_1^1 + 31 \\ &= m_0^1 + m_1^1 - (m_0^1 - 31) \\ &\geq 5 \cdot 2^4 + 31 \end{aligned} \tag{4.10}$$

and $m_0^2 + \cdots + m_i^2 \geq (3i+1)2^4 + 31$. And for the form $\mathscr{F}^2$ we can find nontrivial solution.

– Case $61 \leq m_0 \leq 62$

Again we use the (1)-secondary variables to obtain $s_1, s_2, s_3 \geq 1$. We contract the variables at level zero to $n = 30$ primary variables at higher levels. The same argument used in the last case shows that we can assume $n_1 \geq 29$.

So we create the equivalent form $\mathscr{F}^1$ for which

$$\begin{aligned} m_0^1 &\geq m_1 + 29 \\ &= m_0 + m_1 - (m_0 - 29) \\ &\geq 6 \cdot 2^4 + 1 + 29 - (4 \cdot 2^4 - 2) \\ &= 4 \cdot 2^4 \end{aligned} \tag{4.11}$$

and for the form $\mathscr{F}^1$ we can find nontrivial solution.

- Case $57 \leq m_0 \leq 60$.

  We use the (1)-secondary variables to obtain $s_1, s_2, s_3 \geq 1$. We contract the variables at level zero to $n = 28$ primary variables at higher levels. The same argument used in the first case shows that we can assume $n_1 \geq 25$.

  So we create the equivalent form $\mathscr{F}^1$ for which

$$\begin{aligned} m_0^1 &\geq m_1 + 25 \\ &= m_0 + m_1 - (m_0 - 25) \\ &\geq 6 \cdot 2^4 + 1 + 25 - (4 \cdot 2^4 - 4) \\ &= 2 \cdot 2^4 + 2 \cdot 2^4 - 2 \\ &= 4 \cdot 2^4 - 2 \end{aligned} \tag{4.12}$$

  and for the form $\mathscr{F}^1$ we can find nontrivial solution.

- Case $49 \leq m_0 \leq 56$.

  We use the (1)-secondary variables to obtain $s_1, s_2, s_3 \geq 1$. We contract the variables at level zero to $n = 24$ primary variables at higher levels. The same argument used in the first case shows that we can assume $n_1 \geq 17$.

  So we create the equivalent form $\mathscr{F}^1$ for which

$$\begin{aligned} m_0^1 &\geq m_1 + 17 \\ &= m_0 + m_1 - (m_0 - 17) \\ &\geq 6 \cdot 2^4 + 1 + 17 - (4 \cdot 2^4 - 8) \\ &= 2 \cdot 2^4 + 2 \cdot 2^4 - 6 \\ &= 4 \cdot 2^4 - 6 \end{aligned} \tag{4.13}$$

  and for the form $\mathscr{F}^1$ we can find nontrivial solution.

- Case $d = 3 \cdot 2^3$ Our goal now is to obtain (5)-primary variables. By the proof we gave for $l \geq 5$, we just have to analyse the cases $2^3 \cdot 3 + 1 \leq m_0 \leq 2^3 \cdot 4$. We divide in subcases.

  - Case $31 \leq m_0 \leq 32$.

Here we have $m_1 \geq 17$ so we can guarantee $s_1, s_2 \geq 1$. We use the variables at level zero to create $n = 15$ new variables at higher levels. As usual we denote by n_i the number of these new variables that are at level i. Then

$$n = n_1 + \cdots + n_4.$$

We assert that if $n_2 + \cdots + n_4 \geq 8$, then we can create a (5)-primary. Indeed, assuming the worst case $n_2 = 8$, we use one (2)-secondary and the (2)-primary variables to get $p_3 \geq 4$. Assume $m_3 \geq 7$. This allows us to obtain $s_3, s_4 \geq 1$. Then with four (3)-primary and one (3)-secondary we get $p_4 \geq 2$. These two (4)-primary together with one (4)-secondary give us a (5)-primary. So, we can assume $m_3 \leq 6$. In this case we have

$$\begin{aligned} m_0 + \cdots + m_3 &\geq 12 \cdot 2^3 + 1 \\ \Rightarrow m_1 + m_2 &\geq 12 \cdot 2^3 + 1 - 32 - 6 \\ &= 8 \cdot 2^3 - 5 \end{aligned}$$

and we can use these variables to obtain $s_3 \geq 7$ and proceed as before.

So we can assume that $n_1 \geq 8$. If $n_1 = 8$, then we use one (1)-secondary and the (1)-primary to get four new variables at level at least 2. Then we stay with $n_2 + \cdots + n_4 \geq 7 + 4 = 11 > 8$ and we are done. Following this reasoning we conclude that the only delicate case is $n_1 = 15$.

For solve this case we consider the equivalent form $\mathscr{F}^1$ that satisfies

$$\begin{aligned} m_0^1 &\geq m_1 + 15 \\ &= m_0 + m_1 - (m_0 - 15) \\ &\geq 6 \cdot 2^3 + 1 + 15 - 32 \\ &= 4 \cdot 2^3 \end{aligned} \tag{4.14}$$

and $m_0^1 + \cdots + m_i^1 \geq (i+1)3 \cdot 2^3 + 2^3$ for $i = 1, \ldots, d-1$.

It is sufficient to find non trivial solution to $\mathscr{F}^1$. By our results for $l \geq 5$ we can assume $m_0^1 = 4 \cdot 2^3$ and use the exact same approach we used above. That is, use the variables at level zero to create $n = 15$ new variables at higher levels. Again we can assume $n_1 = 15$ and consider a second equivalent form $\mathscr{F}^2$ satisfying

$$\begin{aligned} m_0^2 &\geq m_1^1 + 15 \\ &= m_0^1 + m_1^1 - (m_0^1 - 15) \\ &\geq 7 \cdot 2^3 + 15 - 32 \\ &= 39 \end{aligned} \tag{4.15}$$

and for this form we can obtain nontrivial solution.

- $29 \leq m_0 \leq 30$. We use the (1)-secondary variables to obtain $s_1, s_2 \geq 1$. We contract the variables at level zero to $n = 14$ primary variables at higher levels. Using the same reasoning as above we can assume $n_1 \geq 13$. So we create the equivalent form $\mathscr{F}^1$ satisfying

$$\begin{aligned} m_0^1 &\geq m_1 + 13 \\ &= m_0 + m_1 - (m_0 - 13) \\ &\geq 6 \cdot 2^3 + 1 + 13 - 30 \\ &= 32 \end{aligned} \tag{4.16}$$

  and we can find non trivial solution for this form.

- $25 \leq m_0 \leq 28$.

  We use the (1)-secondary variables to obtain $s_1, s_2 \geq 1$. We contract the variables at level zero to $n = 12$ primary variables at higher levels. Using the same reasoning as above we can assume $n_1 \geq 9$. So we create the equivalent form $\mathscr{F}^1$ satisfying

$$\begin{aligned} m_0^1 &\geq m_1 + 9 \\ &= m_0 + m_1 - (m_0 - 9) \\ &\geq 6 \cdot 2^3 + 1 + 9 - 28 \\ &= 30 \end{aligned} \tag{4.17}$$

  and we can find non trivial solution for this form.

- $d = 3 \cdot 2^2$.

Now we have to create a (4)-primary. As usual, we divide in cases according to m_0.

  - $m_0 \geq 8 \cdot 2^2 - 1$. This case is just Lemma 3 part I applied recursively.
  - $23 \leq m_0 \leq 30$.

    We use part I of Lemma 3.1 recursively to obtain $p_3 \geq 2$. If we have $m_3 \geq 1$ we are done since we can contract the (3)-primary variables with one (3)-secondary to get a (4)-primary. So, assume $m_3 = 0$. This implies that

$$\begin{aligned} m_0 + \cdots + m_3 &\geq 12 \cdot 2^2 + 1 \\ \Rightarrow m_1 + m_2 &\geq 12 \cdot 2^2 + 1 - 30 \\ &= 19 \end{aligned}$$

    and with these variables we can create a (3)-secondary.
  - $21 \leq m_0 \leq 22$. Now we have $m_1 \geq 3$. We use the variables at level zero to get $p_1 \geq 10$. These variables with one (1)-secondary give us $p_2 \geq 5$ which implies $p_3 \geq 2$. If $m_3 \geq 1$ we are done since we can contract it with the two (3)-primary to one (4)-primary. Assuming $m_3 = 0$ we get $m_1 + m_2 \geq 27$ and we can create a (3)-secondary.
  - $17 \leq m_0 \leq 20$.

    We have $m_1 \geq 5$. we'll analyse two cases.

    First we suppose that at least three of the (1)-secondary variables have the same zeroterm. Then we apply part III of Lemma 3.1 and stay with $s_1, s_2 \geq 1$. Applying Part I of Lemma 3.1 to the variables at level zero we get $p_1 \geq 8$. With these (1)-primary and one (1)-secondary we get $p_2 \geq 4$. And with these four (2)-primary and one (2)-secondary we get $p_3 \geq 2$. If $m_3 \geq 1$ we are done. If not, we have $m_1 + m_2 \geq 29$ and we can create a (3)-secondary.

    Now we analyse the case where at most two of the five (1)-secondary have the same zeroterm. In this case, we necessarily have two pairs of (1)-secondary with distinct zeroterms. Each of these pairs, together with one (1)-primary give us a (2)-primary. With the six remaining (1)-primary and one (1)-secondary we get three more (2)-primary. So, we have $p_2 \geq 5$. Applying part I of Lemma 3.1 to these variables we obtain $p_3 \geq 2$. If $m_3 \geq 1$ we are done. If not, we do as we did above and create a (3)-secondary.

– $15 \leq m_0 \leq 16$.

Since $m_1 \geq 9$, part III of Lemma 3.1 give us $s_1, s_2 \geq 1$. We apply part I of Lemma 3.1 to the variables at level zero and obtain $n = 7$ new variabels at higher levels. As usual we denote by n_i the number of these variables that are at level i so we have

$$n = 7 = n_1 + n_2 + n_3.$$

We assert that if $n_2+n_3 \geq 4$ we can create a (4)-primary. Indeed, assuming the worst case $n_2 \geq 4$, we use these four (2)-primary and one (2)-secondary to get $p_3 \geq 2$. If $m_3 \geq 1$ we are done. If not we have $m_1+m_2 \geq 31$ and we can create a (3)-secondary. So we can assume $n_1 \geq 4$. In fact, putting some thought we can easily see that if $4 \leq n_1 \leq 6$, then we can contract the (1)-primary to get $n_2 + n_3 \geq 4$. So we assume $n_1 \geq 7$. Then we create the equivalent form $\mathscr{F}^1$ satisfying

$$\begin{aligned} m_0^1 &\geq m_1 + 7 \\ &= m_0 + m_1 - (m_0 - 7) \\ &\geq 6 \cdot 2^2 + 1 + 7 - 16 \\ &= 16 \end{aligned} \tag{4.18}$$

and $m_0^1 + \cdots + m_i^1 \geq (i+2)3 \cdot 2^2 - 8$. It is sufficient to find nontrivial solution to $\mathscr{F}^1$. We only have to analyse the case $m_0^1 = 16$. Proceeding exactly as we just did, we get a second equivalent form $\mathscr{F}^2$ satisfying

$$\begin{aligned} m_0^2 &\geq m_1^1 + 7 \\ &= m_0^1 + m_1^1 - (m_0^1 - 7) \\ &\geq 28 + 7 - 16 \\ &= 19 \end{aligned} \tag{4.19}$$

and for this form we can obtain a non trivial solution.

– $13 \leq m_0 \leq 14$. We use the (1)-secondary variables to obtain $s_1, s_2 \geq 1$. We contract the variables at level zero to $n = 16$ primary variables at higher levels. Using the same reasoning as above we can assume $n_1 \geq 6$. So we create the equivalent form $\mathscr{F}^1$ satisfying

$$\begin{aligned} m_0^1 &\geq m_1 + 6 \\ &= m_0 + m_1 - (m_0 - 6) \\ &\geq 6 \cdot 2^2 + 1 + 6 - 14 \\ &= 17 \end{aligned} \tag{4.20}$$

and we can find non trivial solution for this form.

- $d = 3 \cdot 2$

In the second part of this work, we show that $\Gamma(6, \mathbb{Q}_2(\sqrt{5})) \leq 29$. In particular, Artin's conjecture holds. But for completeness we give here a more elementary proof that avoids some information of the sixth powers in $O_{\mathbb{Q}_2(\sqrt{5}))}$.

Here we have to construct a (3)-primary. Again we divide in cases according to m_0.

– $m_0 \geq 15$. In This case we just apply part I of Lemma 3.1 successively.

– $11 \leq m_0 \leq 14$.

Here we analyse two cases. First we assume $m_2 \geq 1$. Then we use the variables at level zero to create five (1)-primary and use these five (1)-primary to get $p_2 \geq 2$. And with one (2)-secondary and two (2)-primary we get a (3)-primary. Now assume $m_2 = 0$. This implies that $m_1 \geq 5$. If we have at least three of these (1)-secondary variables having the same zeroterm we use Part III of Lemma 3.1 and create a (2)-secondary and proceed as before. So we assume that at most two of these five (1)-secondary have same zeroterm. In this case we can construct two pairs of (1)-secondary with distinct zeroterms. Like before, we construct five (1)-primary. Each of the two pairs of (1)-secondary together with one (1)-primary give us a (2)-primary. With the three remaining (1)-primary we get a third (2)-primary. Finally, with three (2)-primary, we can get a (3)-primary.

– $9 \leq m_0 \leq 10$.

Here we have $m_1 \geq 3$. With the variables at level zero we can create four (1)-primary. These four together with one (1)-secondary give us $p_2 \geq 2$. If $m_2 \geq 1$ we are done. If not, we must have $m_1 \geq 9$ and by Part III of Lemma 3.1 we can create a (2)-secondary.

– $7 \leq m_0 \leq 8$.

Now we have $m_1 \geq 5$. We use the variables at level zero to create n = 3 new variables at higher levels. As usual we denote by n_i the number of these variables that are at level i so we have

$$3 = n_1 + n_2.$$

Suppose $n_2 \geq 2$. If $m_2 \geq 1$, then we can contract these three variables to a (3)-primary. If $m_2 = 0$ we must have $m_1 \geq 11$ and we can create a (2)-secondary. So we can assume $n_1 \geq 2$. We again appeal to the equivalent form $\mathscr{F}^1$ satisfying

$$\begin{aligned} m_0^1 &\geq m_1 + 2 \\ &= m_0 + m_1 - (m_0 - 2) \\ &\geq 7 \end{aligned} \tag{4.21}$$

and

$$\begin{aligned} m_0^1 + m_1^1 &\geq 14 \\ m_0^1 + m_1^1 + m_2^1 &\geq 20 \\ m_0^1 + m_1^1 + m_2^1 + m_4^1 &\geq 26 \end{aligned} \tag{4.22}$$

and it is sufficient to find non trivial solution for $\mathscr{F}^1$. We can assume $7 \leq m_0^1 \leq 8$. And repeating the arguments just used, we obtain a second equivalent form $\mathscr{F}^2$ satisfying

$$
\begin{aligned}
m_0^2 &\geq 8 \\
m_0^2 + m_1^2 &\geq 15 \\
m_0^2 + m_1^2 + m_2^2 &\geq 21
\end{aligned} \tag{4.23}
$$

and it is sufficient to find non trivial zero for $\mathscr{F}^2$. We can assume $m_0^2 = 8$. Repeating the same argument we get a third equivalent form $\mathscr{F}^3$ satisfying

$$
\begin{aligned}
m_0^3 &\geq 9 \\
m_0^3 + m_1^3 &\geq 16
\end{aligned} \tag{4.24}
$$

and for this form we can find non trivial solution.

- $d = 3$.

This is the easiest case. We only have to produce a (1)-primary. But since $m_0 \geq 3$ we use Lemma 3.1 and get it. This completes the proof of the theorem.

□

Chapter 5

Additive forms of degree 6

In this chapter we prove Theorem 2. We restate it here.

Theorem 2. *Let $K = \mathbb{Q}_2(\sqrt{5})$ be the only unramified quadratic extension of $\mathbb{Q}_2$. Then $\Gamma(6, K) \leq 29$.*

We give the proof of this theorem in the first section of this chapter. In the second section we present a lower bound for $\Gamma(6, K)$ that was found by Knapp.

5.1 Upper bound for $\Gamma(6, \mathbb{Q}_2(\sqrt{5}))$

Proof of Theorem 2. Let $\mathscr{F}$ be a diagonal form with coefficients in K in 29 variables and with degree 6 . We assume $\mathscr{F}$ normalized. Remember (Lemma 2.3) that this implies

$$\begin{aligned}
&m_0 \geq 5\\
&m_0 + m_1 \geq 10\\
&m_0 + m_1 + m_2 \geq 15\\
&m_0 + m_1 + m_2 + m_3 \geq 20\\
&m_0 + m_1 + m_2 + m_3 + m_4 \geq 25\\
&m_0 + m_1 + m_2 + m_3 + m_4 + m_5 = 29.
\end{aligned} \tag{5.1}$$

We want to find non-trivial zero for $\mathscr{F}$. By Hensel's Lemma, it is sufficient to construct a (3)-primary variable. We again divide our proof in cases, according to the value of m_0. But first, we make some observations.

1 - Again we emphasize that when contracting primary variables, we'll assume the worst case scenario, that is, the jump in the level being of exactly one unit (unless stated otherwise). It is easy to see that, if we can obtain a (3)-primary under this assumption, then we would also be able to do the same if the jumps were higher.

2 - Lemma 3.1 is again our basic tool when contracting variables. So, in order to avoid a massive use of the same quotation, whenever we say that a set of variables can be contracted to a new variable of higher level, and no reference is given, keep in mind that Lemma 3.1 is being used.

So, lets have some fun.

- **Case** $m_0 \geq 15$**.**

  This is easy. Just apply Lemma 3.1 repeatedly and get $p_3 \geq 1$.

- **Case** $13 \leq m_0 \leq 14$**.**

  If $m_2 \geq 1$, then using Lemma 3.1 repeatedly we get $p_2 \geq 2$. Two (2)-primary and one (1)-secondary give us one (3)-primary. Now, if $m_2 = 0$, then we'll have $m_1 \geq 1$ (see (5.1)). Applying Lemma 3.1 to the variables at level zero we obtain six (1)-primary. These six (1)-primary and one (1)-secondary give us three (2)-primary. We contract these three to one (3)-primary.

- **Case** $11 \leq m_0 \leq 12$**.**

  If $m_2 \geq 1$ we proceed as we did above. Suppose $m_2 = 0$. This implies $m_1 \geq 3$. If the three (1)-secondary have all the same zeroterm, then part (c) of Lemma 3.1 says that we can create a (2)-secondary and then proceed as in case $m_2 \geq 1$. So we suppose that not all (1)-secondary have the same zeroterm. We'll try to create sets containing three variables at level zero all having distinct zeroterms. The maximum number of these sets that we can form will be denoted by I_3. By Corollary 3.5 we can assume $I_3 = 0$. So, we'll have only two zeroterms represented by the variables at level zero. Let them be a and b. We assume the worst case $m_0 = 11$ and analyse the possibilities.

Possibility I - $11a$ (meaning we have eleven elements with zeroterm a) - In this case we use Corollary 3.9 repeatedly to create two (2)-primary having zeroterm a (see the observation following Corollary 3.9). And then we contract these two variables to a (3)-primary.

Possibility II - $10a, 1b$ **-** If one of the (1)-secondary have zeroterm a we proceed as above. If not, we have the other two zero terms (b and c) represented. So we use Corollary 3.9 to create a (1)-primary having zeroterm a. This (1)-primary and the (1)-secondary having zeroterms b and c can be contracted to a (2)-primary. We remain with 8 variables at level zero having zeroterm a. We contract these eight to four (1)-primary. These four together with the (1)-secondary that was left behind can be contracted to two more (2)-primary. Three (2)-primary give us one (3)-primary.

Possibility III - $9a, 2b$ **-** Same reasoning as Possibility II.

Possibility IV - $8a, 3b$ **-** We know that one of the (1)-secondary must have zeroterm a or b. Without loss of generality we assume it is a. We use Corollary 3.9 to create a (1)-primary having zeroterm a. This (1)-primary and the (1)-secondary with zeroterm a can be contracted to a (2)-primary. With the remaining variables at level zero we create four (1)-primary. These four and one (1)-secondary give us two more (2)-primary. Three (2)-primary give us one (3)-primary.

Possibility V - $7a, 4b$ **-** Same reasoning as Possibility IV.

Possibility VI - $6a, 5b$ **-** Same reasoning as Possibility IV.

- **Case** $m_0 = 10$**.** Here we can assume $m_2 \geq 1$. Indeed, suppose $m_2 = 0$. Then we would have $m_1 \geq 5$. If three of the (1)-secondary have the same zeroterm, then part (c) of Lemma 3.1 says that we can contract two of them to a (2)-secondary. So, assume this does not happen. Then we would have all three zeroterms appearing. We choose three (1)-secondary having all distinct zeroterms. By Lemma 3.3 either we can contract these three to a (4)-secondary (which would solve our problem by Hensel's Lemma) or to a (2)-secondary. So, we assume $m_2 \geq 1$.

Suppose first that $I_3 \geq 2$. Then we can select three variables having the same zeroterm and use two of them to create a (1)-primary. We can do this in such a way that after the contraction we still have $I_3 \geq 2$. Then Corollary 3.4 give us one (3)-primary.

Now we assume $I_3 = 1$. We would have three variables having distinct zeroterms a, b and c and the others all having zeroterms a or b (Without loss of generality). We have the following possibilities.

Possibility I - $1a, 1b, 1c, 7a$ **-** If the zeroterm of the (2)-secondary if different from a we apply Corollary 3.7 and get a (2)-primary having this same zeroterm. We then contract these two variables to a (3)-primary. So we assume the zeroterm of the (2)-secondary being a. With seven variables at level zero having zeroterm a we create one (2)-primary with zeroterm a (Corollary 3.9). Then we contract the (2)-secondary and the (2)-primary to a (3)-primary.

Possibility II - $1a, 1b, 1c, 6a, 1b$ **-** Same thing we did in possibility I.

Possibility III - $1a, 1b, 1c, 5a, 2b$ **-** We can use Corollary 3.9 to create one (1)-primary having zeroterm a and one (1)-primary having zeroterm b. Then we have $I_3 = 1$ and there are two variables at level 1 having distinct zeroterms. We are done by Corollary 3.5.

Possibility IV - $1a, 1b, 1c, 4a, 3b$ **-** Same thing we did in possibility III.

It remains the case $I_3 = 0$. Now we'll have just two types of zeroterms being represented by the variables at level zero. We assume these types being a and b. We'll have the following possibilities.

Possibility I - $11a$ **-** If the zeroterm of the (2)-secondary is different from a we are done by Corollary 3.7. Assume it is a. Then we apply Corollary 3.9 repeatedly and get a (2)-primary with zeroterm a. We contract this (2)-primary and the (2)-secondary to a (3)-primary.

The same reasoning used in Possibility I can be applied to all possibilities that have at least seven variables with zeroterm a. So we skip these cases.

Possibility II - $6a, 5b$ **-** Here we can use Corollary 3.9 to create four (1)-primary, two of them having zeroterm a and the other two having zeroterm b. Each pair of these can be contracted to a (2)-primary. Then, two (2)-primary and one (2)-secondary give us one (3)-primary.

- **Case** $m_0 = 9$**.** We have $m_1 \geq 1$ and again we can assume $m_2 \geq 1$.

  If $I_3 \geq 2$, then we are done by Corollary 3.4. Suppose $I_3 = 1$. We analyse all the possibilities separately.

  Possibility I - $1a, 1b, 1c, 6a$ **-** If the (2)-secondary has zeroterm different from a then we apply Corollary 3.7 and we are done. If it is a, then Corollary 3.9 applied repeatedly give us a (2)-primary with zeroterm a, and we contract it with the (2)-secondary to a (3)-primary.

  Possibility II - $1a, 1b, 1c, 5a, 1b$ **-** Again we can assume the (2)-secondary having zeroterm a. If the zeroterm of the (1)-secondary is also a, then we use Corollary 3.9 to create a (2)-primary with zeroterm a and we are done. If not, then we use Corollary 3.9 to create a (1)-primary with zeroterm a. Then, $I_3 = 1$ and we have two variables at level 1 with distinct zeroterms and we are done by Corollary 3.5.

  Possibility III - $1a, 1b, 1c, 4a, 2b$ **-** Same thing we did in Possibility II.

  Possibility IV - $1a, 1b, 1c, 3a, 3b$ **-** We use Corollary 3.9 to create one (1)-primary with zeroterm a and another with zeroterm b. Then Corollary 3.5 give us a (3)-primary.

  Now we analyse the case $I_3 = 0$. We'll have just two types of zeroterms being represented by the variables at level zero. We assume these types being a and b. It is easy to see, that it will always be possible to form four pairs of variables at level zero such that the variables of each pair have the same zeroterm. Each of these pairs can be contracted to a (1)-primary. Four (1)-primary and one (1)-secondary give us two (2)-primary. Two (2)-primary and one (2)-secondary give us a (3)-primary.

- **Caso** $m_0 = 8$**.** Now we have $m_1 \geq 2$ and again we can assume $m_2 \geq 1$.

If $I_3 = 2$ then we are done by Corollary 3.4. Assume $I_3 = 1$. By Corollary 3.5 we can assume the two (1)-secondary variables having the same zeroterm. We analyse the possibilities.

Possibility I - $1a, 1b, 1c, 5a$ **-** By Corollary 3.7 we can assume the (2)-secondary having zeroterm a. If the (1)-secondary variables have zeroterm a, then we use Corollary 3.9 to create a (2)-primary with zeroterm $a$and then contract it with one (2)-secondary obtaining a (3)-primary. If not, then we use the same lemma to create a (1)-primary having zeroterm a. So we stay with $I_3 = 1$ and two variables at level 1 having distinct zeroterms. Then we are done by Corollary 3.5.

Possibility II - $1a, 1b, 1c, 4a, 1b$ **-** Same thing we did in Possibility I.

Possibility III - $1a, 1b, 1c, 3a, 2b$ **-** Here we can use Lemma 3.9 to create one (1)-primary with zeroterm a and one (1)-primary with zeroterm b. Then we are done by Corollary 3.5.

Now we assume $I_3 = 0$. The possibilities are:

Possibility I - $8a$ **-** If the zeroterm of the (2)-secondary is different from a we are done by Corollary 3.7. Assume it is a. Then we apply Corollary 3.9 repeatedly and get a (2)-primary with zeroterm a. We contract this (2)-primary and the (2)-secondary to a (3)-primary.

Possibility II - $7a, 1b$ **-** Same thing we did in possibility I.

possibility III - $6a, 2b$ **-** We contract three pairs of variables having zeroterm a to three three (1)-primary and the pair of variables with zeroterm b to a fourth (1)-primary. With four (1)-primary and one (1)-secondary we get two (2)-primary. Two (2)-primary and one (2)-secondary give us one (3)-primary.

Before we start the next case we make an observation.

Observation. Suppose we have two variables at level zero with same zeroterm a and same oneterm. Then we can contract them to a variable T at level 1 having zeroterm a and we have a choice of two possible oneterms for T.

Indeed, Consider the two variables with their respective coefficients

$$(a + 2b + 2^2c_1)x^6, \quad (a + 2b + 2^2c_2)y^6.$$

Contracting them we get a new variable T with cofficient $2a + 4(b + c_1 + c_2 + \delta_a)$. So we have two possibilities for the oneterm of T according to $\delta_a = 0$ or $\delta_a = a$.

Possibility IV - $5a, 3b$ - Again we can assume the zeroterm of the (2)-secondary being a (Corollary 3.7).

Suppose one of the (1)-secondary having zeroterm a. Then we use Corollary 3.9 to create a (2)-primary with zeroterm a and we are done. Now suppose one of the (1)-secondary having zeroterm b. Then we use Corollary 3.9 to create one (1)-primary with zeroterm b and contract it with the (1)-secondary with zeroterm b to a (2)-primary. Then we use Corollary 3.9 to create two (1)-primary with zeroterm a. We contract these two to a second (2)-primary. Two (2)-primary and one (2)-secondary give us one (3)-primary. Remains to be analysed the case where the two (1)-secondary variables have zeroterm c. If they also have the same oneterm, then we would be able to contract them to a (2)-secondary having zeroterm c (Corollary 3.9) and then we would be done by Corollary 3.7. So we assume they have distinct oneterms. We use Corollary 3.9 to create two (1)-primary variables having zeroterm a and one (1)-primary having zeroterm b. If the two (1)-primary having zeroterm a also have the same oneterm, then we can contract them to a (2)-primary with zeroterm a (Corollary 3.9), and we are done, since we can contract it with the (2)-secondary to a (3)-primary. So, the critical situation is: We have two (1)-primary having zeroterm a and distinct oneterms, one (1)-primary with zeroterm b and two (2)-secondary with zeroterm c and distinct oneterms. The coefficients of these variables mod8 are represented bellow:

$$2a + 2^2\gamma_1, \; 2a + 2^2\gamma_2, \; 2b + 2^2\beta, \; 2c + 2^2\lambda_1, \; 2c + 2^2\lambda_2$$

where $\lambda_1 \neq \lambda_2$ and $\gamma_1 \neq \gamma_2$.

Keep in mind that, by the observation we did above, we can choose the oneterm γ_1 between two options. Indeed, in the five variables with same zeroterm from which we selected two in order to contract them to the new (1)-secondary with zeroterm a and ondeterm γ_1, at least two of them had the same oneterm (pigeonhole principle).

We have four possible ways to contract three variables with distinct zeroterms between the five above. The possible results are

1	$2^2(1+\alpha+\gamma_1+\beta+\lambda_1)$
2	$2^2(1+\alpha+\gamma_1+\beta+\lambda_2)$
3	$2^2(1+\alpha+\gamma_2+\beta+\lambda_1)$
4	$2^2(1+\alpha+\gamma_2+\beta+\lambda_2)$

If at least three zeroterms are represented by these four possibilities, we are done. Indeed, if one of them is zero we have a (3)-primary. If not, we choose the contraction that give us a (2)-primary having zeroterm a and then contract the new variable with the (2)-secondary to a (3)-primary. Note that the first three ways to contract the variables will not be all different if, and only if,

$$\gamma_1 + \lambda_2 = \lambda_1 + \gamma_2.$$

If this is the case, we just choose the second option for γ_1 (guaranteed by the observation above) and proceed as before.

Possibility V - $4a, 4b$ **-** Same thing we did in Possibility III.

Before we start the next case, we make a little pause in order to highlight the following fact: We are halfway through the demonstration and we already have a partial result. That is, we already know that:

Partial Result. If $\mathscr{F}$ is an additive form of degree 6, with coefficients in O_K and satisfy

$$m_0 \geq 8$$
$$m_0 + m_1 \geq 10$$
$$m_0 + m_1 + m_2 \geq 15$$

then we can find nontrivial zero for $\mathscr{F}$.

Our strategy to attack the next case is to obtain an equivalent form satisfying these hypothesis.

- **Case $m_0 = 7$.** Here we have $m_1 \geq 3$ and again we can assume $m_2 \geq 1$.

  If $I_3 \geq 2$ we are done by Corollary 3.4. Assume $I_3 = 1$. By Corollary 3.5 we can assume the (1)-secondary variables having the same zeroterm. We analyse the possibilities.

  Possibility I - $1a, 1b, 1c, 4a$ **-** If the (1)-secondary variables have zeroterm distinct from a we use Corollary 3.9 to create a (1)-primary with zeroterm a and we are done by Corollary 3.5. If it is a, then we use the same lemma to create a (1)-primary with zeroterm a and contract it with one (1)-secondary to a (2)-primary. We contract two variables at level zero with zeroterm a to a (1)-primary and still have $I_3 = 1$, which give us a second. Two (1)-primary and one (1)-secondary give us a second (2)-primary. Two (2)-primary and one (2)-secondary give us one (3)-primary.

  Possibility II - $1a, 1b, 1c, 3a, 1b$ **-** If the (1)-secondary variables have zeroterm distinct from a we use Corollary 3.9 to create a (1)-primary with zeroterm a and we are done by Corollary 3.5. If it is a, then we use the same lemma to create a (1)-primary with zeroterm a and contract it with one (1)-secondary to a (2)-primary. With two pairs of variables at level zero having the same zeroterm we obtain two (1)-primary. These two (1)-primary and one (1)-secondary give us a second (2)-primary. Two (2)-primary and one (2)-secondary give us one (3)-primary.

  Possibility III - $1a, 1b, 1c, 2a, 2b$ **-** We use Corollary 3.9 to create two (1)-primary with distinct zeroterms (a and b). Then we are done by Corollary 3.5.

  Remains the case $I_3 = 0$. Remember that, since our form is normalized we have

$$m_0 = 7$$
$$m_0 + m_1 \geq 10$$
$$m_0 + m_1 + m_2 \geq 15$$
$$m_0 + m_1 + m_2 + m_3 \geq 20$$
$$m_0 + m_1 + m_2 + m_3 + m_4 \geq 25$$
$$m_0 + m_1 + m_2 + m_3 + m_4 + m_5 = 29.$$

With six of the seven variables at level zero we can obtain three new variables at higher levels. It is easy to see that if at least one of these variables has level higher than 1, then we can create a (3)-primary. So we assume all variables at level 1.

Next we use Lemma 2.3 and consider the change of variables

$$\mathscr{F}^1 = \frac{1}{2}\mathscr{F}(2x_1, \cdots, 2x_{m_0}, x_{m_0+1}, \cdots, x_{29}).$$

This give us an equivalent form $\mathscr{F}^1$. We denote by m_i^1 the number of variables of the form $\mathscr{F}^1$ that are at level i . Then we have

$$m_0^1 \geq m_1 + 3 \geq 6$$

$$m_0^1 + m_1^1 \geq m_1 + 3 + m_2 = m_0 + m_1 + m_2 - (m_0 - 3) \geq 11$$

and analogously

$$\begin{aligned}
&m_0^1 + m_1^1 + m_2^1 \geq 16 \\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 \geq 21 \\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 + m_4^1 \geq 25 \\
&m_5^1 = 1 \text{ (since we only used six variables at level 0)}
\end{aligned}$$

And it is sufficient to find nontrivial solution for $\mathscr{F}^1$. If $m_0^1 \geq 8$ we appeal to our partial result and we are done. If $m_0^1 = 7$, repeating the same argument twice, we find an equivalent form $\mathscr{F}^3$ satisfying the hypothesis of our partial result. So we only have to analyse the case $m_0^1 = 6$. We use the six variables at level zero in contractions in order to produce two variables at higher levels. If one of them has level higher than 2 we have nothing to do. Same thing goes if the two of them have level 2. So we have to analyse two possibilities.

Possibilite I - Both variables at level 1.

We proceed as before and obtain an equivalent form $\mathscr{F}^2$ satisfying

$$
\begin{aligned}
&m_0^2 = 7 \\
&m_0^2 + m_1^2 \geq 12 \\
&m_0^2 + m_1^2 + m_2^2 \geq 17 \\
&m_0^2 + m_1^2 + m_2^2 + m_3^2 \geq 21 \\
&m_4^2 = 1
\end{aligned}
$$

and repeating the argument one more time we get another equivalent form $\mathscr{F}^3$ that satisfy the hypothesis of our partial result and we are done.

Possibilite II - One variable at level 1 and one at level 2.

We proceed as before and get an equivalent form $\mathscr{F}^2$ satisfying

$$
\begin{aligned}
&m_0^2 = 6 \\
&m_0^2 + m_1^2 \geq 12 \\
&m_0^2 + m_1^2 + m_2^2 \geq 17 \\
&m_0^2 + m_1^2 + m_2^2 + m_3^2 \geq 21 \\
&m_4^2 = 1
\end{aligned}
$$

and it is sufficient to find nontrivial solution for $\mathscr{F}^2$. If $m_0^2 \geq 8$ we have nothing to do. If $m_0^2 = 7$ then we repeat the same argument and find an equivalent form $\mathscr{F}^3$ satisfying the hypothesis of our partial result. So we suppose $m_0^3 = 6$. We contract these six variables to two new variables at higher levels. Again we only have to analyse two cases. If the two new variables are at level 1, then we repeat the same argument and obtain an equivalent form $\mathscr{F}^3$ satisfying the hypothesis of our partial result and we are done. If one is at level 1 an the other at level 2, we construct an equivalent form $\mathscr{F}^3$ satisfying

$$m_0^3 = 7$$
$$m_0^3 + m_1^3 \geq 13$$
$$m_0^3 + m_1^3 + m_2^3 \geq 17$$
$$m_3^3 = 1$$

and repeating the same argument we find an equivalent form $\mathscr{F}^4$ satisfying

$$m_0^4 = 9$$
$$m_0^4 + m_1^4 \geq 13$$
$$m_2^4 = 1$$

and proceeding as in cases $m_0 \geq 9$ we can obtain a nontrial zero for $\mathscr{F}^4$. We observe that the extra variable at level 2 that remained after so many changes of variables is of primal importance. This justify the separate approach of the cases $I_3 \neq 0$.

- **Case** $m_0 = 6$**.** The strategy here is similar to what was done in Case $m_0 = 7$. Now that we have proved that the theorem is valid for normalized forms satisfying $m_0 \geq 7$ one is tempted to use a second *partial result* as we did above and try to obtain an equivalent form $\mathscr{F}^1$ satisfying $m_0^1 \geq 7$. But there is a little problem in that. Suppose we make one change of variables and get an equivalent form $\mathscr{F}^1$ satisfying $m_0^1 \geq 7$ and then try proceed as in case $m_0 = 7$. We would need more changes of variables that we could perform. So, we have to be more careful here.

  We use four (maybe five) of the six variables at level zero in contractions to get two new variables at higher levels. If one of them is at a level higher than two we are done. Same thing goes if both are at level 2. So we analyse the two possibilities that are left.

  Possibility I - Both variables at level 1.

  We use Lemma 2.3 and consider the change of variables

$$\mathscr{F}^1 = \frac{1}{2}\mathscr{F}(2x_1, \cdots, 2x_{m_0}, x_{t+1}, \cdots, x_{29}).$$

This give us an equivalent form $\mathscr{F}^1$ satisfying

$$
\begin{aligned}
&m_0^1 \geq 6\\
&m_0^1 + m_1^1 \geq 11\\
&m_0^1 + m_1^1 + m_2^1 \geq 16\\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 \geq 21\\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 + m_4^1 \geq 25\\
&m_5^1 \geq 1
\end{aligned}
$$

and it is sufficient to find nontrivial zero for $\mathscr{F}^1$. We already know that if $m_0^1 \geq 8$ we can find it. If $m_0^1 = 7$, we repeat the same process twice and find an equivalent form $\mathscr{F}^3$ for which the hypothesis of our partial result are satisfied and we are done. Suppose $m_0^1 = 6$. We use the variables at level zero to create two new variables of higher levels. Again we only have to analyse two cases. If the two new variables are at level one, we use the same change of variables one more time and obtain an equivalent form $\mathscr{F}^2$ satisfying

$$
\begin{aligned}
&m_0^2 = 7\\
&m_0^2 + m_1^2 \geq 12\\
&m_0^2 + m_1^2 + m_2^2 \geq 17\\
&m_0^2 + m_1^2 + m_2^2 + m_3^2 \geq 21\\
&m_4^2 \geq 1\\
&m_5^2 \geq 1
\end{aligned}
$$

and repeating the process one more time we get an equivalent form $\mathscr{F}^3$ satisfying the hypothesis of our partial result. Now, if one of the new variables is at level 1 and the other at level 2, this process would give us an equivalent form $\mathscr{F}^2$ satisfying

$$\begin{aligned}
&m_0^2 = 6\\
&m_0^2 + m_1^2 \geq 12\\
&m_0^2 + m_1^2 + m_2^2 \geq 17\\
&m_0^2 + m_1^2 + m_2^2 + m_3^2 \geq 21\\
&m_4^2 \geq 1
\end{aligned}$$

and we try to find nontrivial solution for $\mathscr{F}^2$. If $m_0^2 \geq 8$ we are done. If $m_0^2 = 7$ we just have to repeat the same argument one more time. So we assume $m_0^2 = 6$. Again we contract the variables at level zero to obtain two new variables and consider the only two problematic cases. If both of the new variables are at level 1 we make the same change of variables one more time to get an equivalent form satisfying the hypothesis of our partial result. If one is at level 1 and the other at level 2, we use the same change of variables and the new equivalent form $\mathscr{F}^3$ will satisfy

$$\begin{aligned}
&m_0^3 = 7\\
&m_0^3 + m_1^3 \geq 13\\
&m_0^3 + m_1^3 + m_2^3 \geq 17\\
&m_3^3 \geq 1
\end{aligned}$$

and we only have to find nontrivial zero for $\mathscr{F}^3$. If $m_0^3 \geq 8$ we have nothing to do. If $m_0^3 = 7$ we use the same change of variables and get an equivalent form $\mathscr{F}^4$ satisfying

$$\begin{aligned}
&m_0^4 = 9\\
&m_0^4 + m_1^4 \geq 13\\
&m_2^4 = 1
\end{aligned}$$

and proceeding as in cases $m_0 \geq 9$ we can find nontrivial zero for $\mathscr{F}^4$.

Possibility II - One variable at level 1 and one at level 2.

Again we appeal to Lemma 2.3 and make the same change of variables to obtain an equivalent form $\mathscr{F}^2$ satisfying

$$\begin{aligned}
&m_0^1 \geq 5\\
&m_0^1 + m_1^1 \geq 11\\
&m_0^1 + m_1^1 + m_2^1 \geq 16\\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 \geq 21\\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 + m_4^1 \geq 25\\
&m_5^1 \geq 1
\end{aligned}$$

and we have to find nontrivial solution for $\mathscr{F}^1$. If $m_0^1 \geq 8$ we are done. If $m_0^1 = 7$ we repeat the same process twice and get an equivalent form satisfying the hypothesis of our partial result. If $m_0^1 = 6$ we use the variables at level zero to create two new variables at higher levels and analyse the two problematic cases. If both of the new variables are at level 1, then we make the same change of variables and obtain an equivalent form $\mathscr{F}^2$ satisfying

$$\begin{aligned}
&m_0^2 = 7\\
&m_0^2 + m_1^2 \geq 12\\
&m_0^2 + m_1^2 + m_2^2 \geq 17\\
&m_0^2 + m_1^2 + m_2^2 + m_3^2 \geq 21\\
&m_4^2 \geq 1
\end{aligned}$$

and repeating the process one more time we get and equivalent form $\mathscr{F}^3$ satisfying the hypothesis of our partial result. Now, if one variable is at level 1 and the other at level 2, the same change of variables lead us to an equivalent form $\mathscr{F}^1$ satisfying

$$\begin{aligned}
&m_0^2 = 6\\
&m_0^2 + m_1^2 \geq 12\\
&m_0^2 + m_1^2 + m_2^2 \geq 17\\
&m_0^2 + m_1^2 + m_2^2 + m_3^2 \geq 21\\
&m_4^2 \geq 1
\end{aligned}$$

and we have to find nontrivial zero for $\mathscr{F}^2$. If $m_0^2 \geq 8$ we are done. If $m_0^2 = 7$ we repeat the process one more time to find an equivalent form satisfying the hypothesis of our partial result. If $m_0^2 = 6$ we contract the variables at level zero and obtain two new variables of higher levels. Again we only have two problematic cases. If both new variables are at level 1 we make the same change of variables and obtain an equivalent form $\mathscr{F}^3$ satisfying the hypothesis of our partial result. If one is at level 1 and the other at level 2, the same change of variables lead us to an equivalent form $\mathscr{F}^3$ satisfying

$$
\begin{aligned}
&m_0^3 \geq 7 \\
&m_0^3 + m_1^3 \geq 13 \\
&m_0^3 + m_1^3 + m_2^3 \geq 17 \\
&m_3^3 \geq 1
\end{aligned}
$$

and we have to find nontrivial solution for $\mathscr{F}^3$. If $m_0^3 \geq 8$ we are done. If $m_0^3 = 7$ we repeat the process and obtain an equivalent form $\mathscr{F}^4$ satisfying

$$
\begin{aligned}
&m_0^4 \geq 9 \\
&m_0^4 + m_1^4 \geq 13 \\
&m_2^4 = 1
\end{aligned}
$$

and proceeding as in cases $m_0 \geq 9$ we are done. We are almost there, remains only the case $m_0^1 = 5$. We contract the variables at level zero and get two new variables. Again we analyse the two problematic cases. If both new variables are at level 1, then we make the same change of variables and obtain an equivalent form $\mathscr{F}^2$ satisfying the hypothesis of our partial result. If one is at level 1 and other at level two, the same change of variables lead us to an equivalent form $\mathscr{F}^2$ satisfying

$$
\begin{aligned}
&m_0^2 = 7 \\
&m_0^2 + m_1^2 \geq 13 \\
&m_0^2 + m_1^2 + m_2^2 \geq 18 \\
&m_0^2 + m_1^2 + m_2^2 + m_3^2 \geq 22
\end{aligned}
$$

and repeating the same process one more time we get an equivalent form $\mathscr{F}^3$ satisfying the hypothesis of our partial result.

- **Case $m_0 = 5$.**

We use the variables at level zero in contractions and get two new variables at higher levels. If one of them is at a level higher than two we are done. Same thing if both are at level 2. So we analyse the last two possibilities.

Possibility I - Both variables at level 1. We make the same change of variables and get an equivalent form $\mathscr{F}^1$ satisfying

$$\begin{aligned}
&m_0^1 \geq 7 \\
&m_0^1 + m_1^1 \geq 12 \\
&m_0^1 + m_1^1 + m_2^1 \geq 17 \\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 \geq 22 \\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 + m_4^1 \geq 26
\end{aligned}$$

and we have to find nontrivial zero for $\mathscr{F}^1$. If $m_0^1 \geq 8$ we are done. If $m_0^1 = 7$ then we repeat the process one more time and get an equivalent form $\mathscr{F}^2$ satisfying the hypothesis of our partial result.

Possibility II - One variable at level 1 and one at level 2. We apply the same change of variables and get an equivalent form $\mathscr{F}^1$ satisfying

$$\begin{aligned}
&m_0^1 \geq 6 \\
&m_0^1 + m_1^1 \geq 12 \\
&m_0^1 + m_1^1 + m_2^1 \geq 17 \\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 \geq 22 \\
&m_0^1 + m_1^1 + m_2^1 + m_3^1 + m_4^1 \geq 26
\end{aligned}$$

and we look for nontrivial zero for $\mathscr{F}^1$. If $m_0 \geq 8$ we are done. If $m_0^1 = 7$ we repeat the process one more time and obtain an equivalent form satisfying the hypothesis of our partial result. So we analyse the case $m_0^1 = 6$. We contract the variables at level zero and get two new variables at higher levels. Again we only have to analyse the two problematic cases. If both new variables are at level 1, the same change of variables give us an equivalent form satisfying the hypothesis of our partial result. If one is at level 1 and the other at level 2, the change of variables give us an equivalent form $\mathscr{F}^2$ satisfying

$$\begin{aligned}&m_0^2 = 7\\&m_0^2 + m_1^2 \geq 13\\&m_0^2 + m_1^2 + m_2^2 \geq 18\\&m_0^2 + m_1^2 + m_2^2 + m_3^2 \geq 22\end{aligned}$$

and it is sufficient to find nontrivial solution for $\mathscr{F}^2$. If $m_0^2 \geq 8$ we are done. If $m_0^2 = 7$ we repeat the process one more time and get an equivalent form satisfying the hypothesis of our partial result. This completes the proof.

□

5.2 Lower bound for $\Gamma(6, \mathbb{Q}_2(\sqrt{5}))$

Here we present a diagonal form in 18 variables and of degree 6 having no non-trivial zeros in K. This example was found by Knapp. For $x = (x_1, x_2, x_3)$ we set $\mathscr{F}(x) = x_1^6 + x_2^6 + x_3^6$. Let

$$\mathscr{G} = \mathscr{F}(x) + 2\alpha\mathscr{F}(y) + 2^2(1+\alpha)\mathscr{F}(z) + 2^3\mathscr{F}(u) + 2^4\alpha\mathscr{F}(v) + 2^5(1+\alpha)\mathscr{F}(w).$$

We will show that $\mathscr{G}$ does not admit non-trivial zero. Suppose we have $\mathscr{G} = 0$. Then, in particular we would have $\mathscr{G} \equiv 0(\mathrm{mod}2)$. Consequently, $\mathscr{F}(x) \equiv 0(\mathrm{mod}2)$. Since the only sixth powers modulo 4 are 0 and 1, we would have two possibilities. Either $x_1, x_2, x_3 \equiv 0(\mathrm{mod}2)$ or exactly two of them are not $0(\mathrm{mod}2)$. If the latter case occurs, then, since $\mathscr{G} \equiv 0(\mathrm{mod}4)$, we would have $2(1 + \alpha\mathscr{F}(y)) \equiv 0(\mathrm{mod}4)$, and so $1 + \alpha\mathscr{F}(y) \equiv 0(\mathrm{mod}2)$. But this is a contradiction since $\mathscr{F}(y) \equiv 0, 1(\mathrm{mod}2)$. We conclude that $x_1, x_2, x_3 \equiv 0(\mathrm{mod}2)$. The same reasoning used above shows us that all the variables of $\mathscr{G}$ must be 0 (mod2). This implies that all of them are divisible by any power of 2. We conclude that this solution is trivial and then we have $\Gamma(6, K) \geq 19$.

Bibliography

[1] Yismaw Alemu, *On zeros of diagonal forms over $\mathfrak{p}$-adic fields*, Acta Arith. **48** (1987), no. 3, 261-273. MR921089

[2] James Ax and Simon Kochen, *Diophantine problems over local fields*, I, Amer. J. Math. **87** (1965), 605-630. MR0184930

[3] B. J. Birch, *Diagonal equations over $\mathfrak{p}$-adic fields*, Acta Arith. **9** (1964), 291-300. MR0167456

[4] D. Brink, H. Godinho, and P.H.A. Rodrigues, *Simultaneous diagonal equations over p-adic fields*, Acta Arith. **132** (2008), no. 4, 393-399. MR2413361

[5] J. W. S. Cassels, *Local fields*, London Math. Soc. Student Texts **3**, Cambridge: Cambridge University Press, (1986)

[6] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. Ser. A **274** (1963), 443-460. MR0153655

[7] M. Knapp, *Solubility of additive sextic forms over ramified quadratic extensions of* $\mathbb{Q}_2$, Manuscript in preparation (2016)

[8] Serge Lang, *On quasi algebraic closure*,ProQuest LLC, Ann Arbor, MI (1951). Thesis (Ph.D.) - Princenton University. MR2938192

[9] Serge Lang, *On quasi algebraic closure*, Ann. of Math. (2) **55** (1952), 373-390. MR0046338

[10] Miranda Moore, *Solvability of diagonal equations over p-adic fields* (2017). Thesis (Ph.D.) - Princenton University.

[11] J. E. Olson, *A combinatorial problem on finite abelian groups, I and II*, J. Number Theory **1** (1969), 8-10 and 195-199

[12] Christopher M. Skinner, *Solvability of $\mathfrak{p}$-adic diagonal equations (again)*, Acta Arith. **124** (2006), no. 1, 73-77. MR2262141

[13] Luis A. Sordo Vieira, *On p-adic fields and p-groups* (2017). Thesis (Ph.D.) - University of Kentucky.

[14] Guy Terjanian, *Un contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris Sér. A-B **262** (1966), A612. MR0197450