2006

# Representation properties of definite lattices in function fields

Jean Edouard Bureau
*Louisiana State University and Agricultural and Mechanical College*

# REPRESENTATION PROPERTIES OF DEFINITE LATTICES IN FUNCTION FIELDS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Jean Edouard Bureau
Maîtrise de Mathématiques, Université Paris VII, 2002
M.S. in Mathematics, Louisiana State University, 2005
December, 2006

Monsieur Fourier avait l'opinion que le but principal des mathématiques était l'utilité publique et l'explication des phénomènes naturels. Un philosophe tel que lui aurait dû savoir que le but unique de la Science, c'est l'honneur de l'esprit humain et que, sous ce titre, une question de nombres vaut bien une question de système du monde.

Karl-Gustav Jacobi (1804-1851)

# Acknowledgments

This work would not have been possible without the help of many people. First, I would like to thank my adviser Jorge Morales for his support and advice. His trust in my work has given me a lot of autonomy. His knowledge and patience were crucial to overcome difficulties in the course of my studies. I would also like to thank Robert Perlis for many helpful discussions and all the committee members Jerome Hoffman, Brendan Owens and Padmanabhan Sundar.

This dissertation would not have been possible without the support of my family, especially of my parents, of my grandparents and of my sisters. They had faith in me and it is a pleasure to express them my gratitude. Finally I would like to thank Sandra Smith for her kindness and her patience; she was a great help during the writing of this dissertation.

# Table of Contents

# Abstract

This work is made of two different parts. The first contains results concerning isospectral quadratic forms, and the second is about regular quadratic forms.

Two quadratic forms are said to be isospectral if they have the same representation numbers. In this work, we consider binary and ternary definite integral quadratic form defined over the polynomial ring $\mathbb{F}[t]$, where $\mathbb{F}$ is a finite field of odd characteristic. We prove that the class of such a form is determined by its representation numbers. Equivalently, we prove that there is no nonequivalent definite $\mathbb{F}[t]$-lattices of rank 2 or 3 having the same theta series.

A quadratic form is said to be regular (resp. spinor-regular) if it represents any element represented by its genus (resp. by its spinor genus). A form is said to be universal if it represents any integral element. We prove that regular and spinor-regular definite $\mathbb{F}[t]$-lattices must have class number one and we give a characterization of definite universal $\mathbb{F}[t]$-lattices.

# Chapter 1

# Introduction

It has been a long-standing question to determine whether an integral definite $\mathbb{Z}$-lattice of a given rank is determined by its theta series (i.e. its representation numbers). This question was recently answered for all ranks. In 1979 Watson (Cf. [28], [29]) proved that definite binary $\mathbb{Z}$-lattices are determined up to integral equivalence by their very first primitive representations. The case of ternary lattices over $\mathbb{Z}$ had to wait until 1997 to be solved by Schiemann ([26]) by means of extensive computations. These computations together with the theory of modular forms enabled him to prove that definite ternary $\mathbb{Z}$-lattices are indeed determined by their representation numbers. For higher ranks, counterexamples have been found. In [17], Kitaoka found a counter example of rank 8 and in [25], Schiemann found counterexamples of rank 4. Since then, these results have been extended by Conway and Sloane to a infinite family of isospectral lattices of rank 4 (i.e. lattices with the same representation numbers).

In this dissertation we are interested in analogous representation properties for $\mathbb{F}_r[t]$-lattices. In this case one has two considerable advantages: a reduction process and the fact that 2 is invertible! A set of invariants called the successive minima can be defined. First, we prove that the sequence of successive minima and the determinant of a binary quadratic form is essentially determined by its representation set (cf. Lemma 2.1.1 and Theorem 2.1.1). One could then argue

using a functions field version of the Tchebotareff density theorem to conclude that two binary forms having the same representation sets are equivalent. Here, nevertheless, we do not use this approach that would not allow to consider just restricted representation sets. Rather, we use counting arguments and we translate the fact that two binary forms have the same restricted representation sets into the language of varieties defined over finite fields; then the Riemann Hypothesis enables to conclude that the forms must be equivalent (Theorem 2.1.2). Theorem 2.1.2 could be stated by saying that, within the binary forms having the same discriminant, the very first representations determine the class of the form. By very first, we mean the representations up to the largest successive minimum. In the ternary case nevertheless, one cannot expect such a strong result as shown in section 2.2.

Since representation sets are not sufficient to determine a ternary lattice up to equivalence we need to consider a stronger property. Instead of just searching for the elements that are represented, we also look for how many times they are represented. The question is then to know if these representations together with their multiplicities will be enough to characterize a lattice; we start with a pair isospectral lattices, that is lattices having the same theta series, and we want to decide if they are equivalent or not.

One possible approach to prove that isospectral quadratic forms are equivalent would be to see the theta series of a quadratic form as a modular form. Nevertheless, the theory of modular forms over function fields in its present form does not seem adapted to handle the isospectral problem.

Another possible approach would be purely algebraic. We could break the genus of a quadratic form into spinor genera and use the strong approximation for the spin group to check that within a single spinor genera there are no nonequivalent isospectral quadratic forms. We would then use the theory of spinor

exceptional integer started by Kneser to conclude that isospectral quadratic forms must live in a single spinor genera. This approach nevertheless does not work, as pointed out by John Hsia, since spinor exceptional integers do not allow to separate spinor genera.

We took a third approach. First, by using some arguments similar to the one used by Kitaoka and Conway in the case of $\mathbb{Z}$-lattices, we prove that the genus of a ternary quadratic form is determined by its representation numbers (cf. Proposition 3.2.1). Then by using a Poisson formula and generalizing an argument due to Rück and Rosson, we prove that dual lattices inherit isospectrality properties (cf. Theorem 3.1.1); if two lattices are isospectral, so are their dual. This result has a very important consequence for us: isospectral ternary lattices will contain isometric copies of a binary lattice (cf. Lemma 4.1.1). Finally we prove that isospectral ternary lattices must be equivalent. To this aim, we have to translate isospectrality properties of $\mathbb{F}_r[t]$-lattices into the language of systems of quadratic forms defined over finite fields. We use a characterization of systems with the same representation numbers using a Fourier inversion. That together with some counting arguments enables to conclude.

The question concerning equivalence of isospectral definite ternary lattice that is answered in this thesis was brought up to our attention by Eva Bayer-Fluckiger. Also, as noted by Juan-Marcos Cerviño, an effective result could allow to create an algorithm to determine endomorphism rings of super-singular Drinfeld modules.

A lattice is said to be universal if it represents any integer. The study of universal $\mathbb{Z}$-lattices started with Ramanujan and culminated by the celebrated Conway-Schneeberger 15-theorem. This theorem asserts that a definite classically integral $\mathbb{Z}$-lattice is universal if and only if it represents the integers $1, 2 \cdots, 15$.

Another interesting property of a lattice is regularity. This notion was introduced by Dickson at the beginning of the $20^{\text{th}}$ century in order to characterise lattices representing any integer not excluded by congruences; if the sum of four squares is one of the most famous universal forms, the sum of three squares is certainly the archetypical regular form. Regular definite $\mathbb{Z}$-lattices were then extensively studied by Watson in his unpublished thesis (early 50's), in which he proved that only finitely classes could be regular.

In a recent paper Chan and Daniels undertook the study of regular definite $\mathbb{F}_r[t]$-lattices (cf. [5]). To that aim, they used the methods developed by Watson in order to prove, among other things, that there were only finitely many classes of regular definite $\mathbb{F}_r[t]$-lattices (for a fixed $r$). When a lattice is regular one can apply a certain transformation to the lattice, called the $\lambda$-transformation, which will not change the regularity. By applying several times this $\lambda$-transformation, one ends up with a regular lattice whose discriminant is squarefree. As proved in [5], there are very few lattices satisfying these two properties simultaneously.

We consider the regular lattices of squarefree discriminants and apply a (local) inverse of the $\lambda$-transformation. By proving that after a few steps all the lattices obtained are not regular, we can conclude that regular ternary lattices have class number one. That also enables us to write a list of all the definite ternary $\mathbb{F}_r[t]$-lattices having class number one. Using this list, some counting arguments and the theory of spinor exceptional integers we are able to conclude that spinor-regular ternary lattices also have class number one.

In the last chapter, we prove a conjecture of Gerstein which is a function field equivalent of the 15-theorem. It says that a definite $\mathbb{F}_r[t]$-lattice is universal if and only if it represents $1, \delta, t, \delta t$ where $\delta$ is a nonsquare in $\mathbb{F}_r$. To prove this result, we follow the approach started by Gerstein. First we notice that universal lattices must be quaternary and we make a list of candidates. For each

of these candidates, we find a ternary sublattice that is known to represent *a lot* of polynomials. We finally show that the polynomials that are not represented by the ternary sublattice must be represented by the quaternary lattice. This conjecture was independentely proved by Chan and Daniels ([5]), by Kim, Wang and Xu ([16]) and by the author.

We use these results on universal lattices together with the $\lambda$-transformation to prove that a quaternary lattice is regular if and only if it is universal. That implies in particular that a quaternary regular lattice must have class number one.

## 1.1 Basic Definitions and Terminology

Let $I$ be a unitary ring in a field $k$ of characteristic not 2. We allow the possibility $I = k$. Let $B$ be a symmetric $n \times n$ matrix with coefficient in $k$. The associated quadratic form on $I^n$ is

$$q(x) = {}^t x\, B\, x$$

We say that $q$ is *I-integral* (or simply *integral*) if it takes values in $I$. This is equivalent to $2B$ being a matrix with coefficients in $I$.

The *symmetric bilinear form* of $q$ is defined by

$$b(x, y) = q(x + y) - q(x) - q(y)$$

and is related to $B$ by

$$b(x, y) = 2x^t\, B\, y.$$

The discriminant of $q$ is defined by $\mathrm{disc}(q) = (-1)^{\frac{n(n-1)}{2}} \det B$. We say that $q$ is *nondegenerate* if $\mathrm{disc}(q) \neq 0$.

Let $R$ be a ring satisfying $I \subset R \subset k$. Two quadratic forms $q$ and $q'$ are said to be *R-equivalent* if there exists $U \in GL_n(R)$ such that $q(Ux) = q'(x)$. We shall

denote this equivalence by $q \cong_R q'$ or when no ambiguity is possible simply by $q \cong q'$.

A *quadratic space* over $k$ is a finite dimensional $k$-vector space $U$ together with quadratic form $q$. Let $W$ be a quadratic $k$-space and let $I$ be a subring of $k$. For our purposes, an $I$-lattice in $W$ is a free $I$-module included in $W$ and whose rank is $dim_k(W)$. There is a well known correspondence between lattices in the previous sense and quadratic forms. Let us briefly explain how they are related. Let $q = \sum_{i \leq j \leq n} a_{ij} x_i x_j$, for $a_{ij} \in I$, be an integral quadratic form. In an usual fashion, one associates to $q$ a matrix, called the Gram matrix and defined to be $M_q = (m_{ij}) = (\partial^2 f / \partial x_i \partial x_j)$. Let $W$ be the $k$-vector space spanned by vectors $e_1, \cdots, e_n$ equipped with the symmetric bilinear form $B$ for which $B(e_i, e_j) = m_{ij}$ and the corresponding quadratic form $Q(v) = B(v, v)$. Then $L = Ie_1 \oplus \cdots \oplus Ie_n$ is the lattice associated to $q$. Because of this correspondance, it is convenient to allow ourselves to oscillate freely between the language of lattices and the one of quadratic forms.

In this work, we are concerned with integral quadratic forms defined over $\mathbb{F}_r[t]$, where $\mathbb{F}_r$ is a finite field with an odd number, $r$, of elements. Let $A = \mathbb{F}_r[t]$ and let $K = \mathbb{F}_r(t)$ stand for the fraction field of $A$. A prime of $A$ is an ideal of the form $\mathfrak{p} = (\pi)$, where $\pi$ is irreducible. There is clearly a one-to-one correspondence between prime and monic irreducible polynomials. By abuse of language, prime will stand for an ideal as well as for a monic irreducible polynomial. For any prime $\mathfrak{p}$, one can, as commonly done, consider the $\mathfrak{p}$-adic completion of $\mathbb{F}_r[t]$ that we shall denote by $A_{\mathfrak{p}}$.

For $f/g \in \mathbb{F}_r(t)$, the discrete valuation corresponding to $\infty$ is the degree function

$$v_\infty = \partial(f/g) = \partial(f) - \partial(g) \quad \text{and} \quad v_\infty(0) = \partial(0) = -\infty$$

so that one can define an absolute value $|f|_\infty = r^{-v_\infty(f)}$. The discrete valuation

ring in $\mathbb{F}_r(t)_\infty = \mathbb{F}_r\left(\left(\frac{1}{t}\right)\right)$ is

$$\mathcal{O}_\infty = \{x \in \mathbb{F}_r(x)_\infty : |x|_\infty \leq 1\} = \mathbb{F}_r\left[\left[\frac{1}{t}\right]\right]$$

and this ring has a unique maximal ideal $\mathfrak{P}_\infty$ defined by

$$\mathfrak{P}_\infty = \{x \in \mathbb{F}_r(x)_\infty : |x|_\infty < 1\}.$$

There is a well known canonical decomposition for quadratic forms defined over non dyadic local fields. If $q$ is such a form then

$$q \cong_{A_\mathfrak{p}} \langle a_1\pi^{\alpha_1}, \cdots, a_n\pi^{\alpha_n}\rangle = a_1\pi^{\alpha_1}x_1^2 + \cdots + a_n\pi^{\alpha_n}x_n^2$$

where $a_i \in A_\mathfrak{p}^\times$ and $\alpha_1 \leq \cdots \leq \alpha_n$. A block

$$\langle b_1\pi^\alpha, b_2\pi^\alpha, \cdots, b_j\pi^\alpha\rangle = \pi^\alpha\langle b_1, \cdots, b_j\rangle$$

is called a *Jordan block*.

Let $W$ be a quadratic space over $k = \mathbb{F}_r(t)$ and let $L$ is a $\mathbb{F}_r[t]$-lattice in it. We say that $L$ is *definite* provided the completion $W_\infty = W \otimes k_\infty$ is anisotropic (i.e. does not represent 0 non trivially). One should notice that, in this case, the Hasse principle (cf. [4], p 75) implies that the rank of a definite $\mathbb{F}_r[t]$-lattice is at most 4.

Recall that two lattices $L$ and $L'$ are said to be in the same *genus* if $L_\mathfrak{p} \cong L'_\mathfrak{p}$ for all primes $\mathfrak{p}$ and if $W_\infty \cong W'_\infty$. The discriminant of a lattice is an invariant of the genus. It is a standard fact that the genus of a $\mathbb{F}_r[t]$-lattice $L$ contains finitely many $\mathbb{F}_r[t]$-equivalence classes. The number of these classes is called the *class number* of $L$.

Let $(L, q)$ be a definite quadratic lattice in a quadratic $\mathbb{F}_r(t)$-space $W$. The *representation set* $V(L)$ and the *restricted representation sets* $V_n(L)$ of $L$ are defined as follows:

$$V(L) = \{q(h) \,:\, h \in L\} \quad \text{and} \quad V_n(L) = \{q(h) \,:\, h \in L, \quad \partial(q(h)) \leq n\}\,.$$

For $f \in \mathbb{F}_r[t]$, one defines the *representation numbers* of $f$ by $L$ as follows:

$$R(L, f) = \#\{\xi \in L : q(\xi) = f\} \tag{1.1}$$

Since we deal with definite lattices, it is clear that the set on the right hand side of (1.1) is finite for any $f$; hence, $R(L, f)$ is well defined. The relation between representation sets and representation numbers is given by the following equality

$$V(L) = \{f \in L : R(L, f) > 0\}.$$

## 1.2 The Work of Gerstein

Because of the nonarchimedean behavior of the degree function it is possible to develop a very effective reduction theory for those definite $\mathbb{F}_r[t]$-lattices. We recall here the principal reductions results obtained by Gerstein in [11]. Using the same notation as Gerstein, we let $\partial(\cdot)$ denote the degree function.

**Definition.** A symmetric matrix $A = [a_{ij}] \in \mathcal{M}(\mathbb{F}_r(t))$ is said to be reduced provided

1. A has dominant diagonal (i.e. $\partial(a_{ii}) > \partial(a_{ij})$ for all $j \neq i$); and
2. $\partial(a_{11}) \leq \cdots \leq \partial(a_{nn})$.

A basis $(e_1, \cdots, e_n)$ for a $\mathbb{F}_r[t]$-lattice $L$ is said to be a reduced basis for $L$, if the associated Gram matrix $[B(e_i, e_j)]$ is reduced. ■

**Theorem 1.2.1 (Djoković, [9])** *Every anisotropic $\mathbb{F}_r[t]$-lattice has a reduced basis.*

**Lemma 1.2.1** *Let $V$ be a quadratic $\mathbb{F}_r(t)$-space and suppose that $V \cong A = (a_{ij}) \in M_n(\mathbb{F}_r[t])$, where $A$ has dominant diagonal. For each $i$, suppose that $a_{ii}$ has leading coefficient $\lambda_i$ and degree $\nu_i$. Then*

$$V_\infty \cong \langle a_{11}, \cdots, a_{nn} \rangle \cong \langle \lambda_1 t^{\nu_1}, \cdots, \lambda_n t^{\nu_n} \rangle.$$

**Theorem 1.2.2 (Gerstein, [11])** *Suppose $L$ is an $\mathbb{F}_r[t]$-lattice on the definite quadratic $K$-space $W$, and that its matrix is given in a reduced basis $(e_1, \cdots, e_n)$ by $A = [a_{ij}]$.*

1. *Let $0 \neq w = \sum_{i=1}^n \alpha_i e_i \in L$. Then the leading term of the polynomial $Q(w)$ is the leading term of $\sum_{i=1}^n \alpha_i^2 a_{ii}$ and*

$$\partial(Q(w)) = \max_i \{\partial(\alpha_i^2 a_{ii})\}.$$

2. *The degree sequence $\{\partial(a_{11}), \cdots, \partial(a_{nn})\}$ is an invariant of $L$.*

The invariant sequence $\{\partial(a_{11}), \cdots, \partial(a_{nn})\}$ will be referred as the sequence of *successive minima*; it will be denoted by $\{\mu_i\}_{i=1}^n$.

**Lemma 1.2.2** *If $\{v_1, \cdots, v_n\}$ is a reduced basis for the $\mathbb{F}_r[t]$-lattice $L$, then the reversed dual basis $\{v_1^\#, \cdots, v_n^\#\}$ is a reduced basis for the dual lattice $L^\#$; in particular for $2 \leq i \leq n$ the inequality $\partial Q(v_i^\#) \leq \partial Q(v_{i-1}^\#)$ holds. Moreover,*

$$\partial Q(v_i^\#) < \partial Q(v_{i-1}^\#) \quad \Leftrightarrow \quad \partial Q(v_i) > \partial Q(v_{i-1}).$$

**Theorem 1.2.3 (Gerstein, [11])** *Let $L$ and $M$ be $\mathbb{F}_r[t]$-lattices on a definite quadratic $\mathbb{F}_r(t)$-space $V$ of dimension $n$ and suppose that $L$ and $M$ have respective Gram matrices $A, C \in M_n(\mathbb{F}_r[t])$. Suppose further that $A, C$ are reduced. Then*

$$L \cong M \quad \Leftrightarrow \quad C = {}^tT\, A\, T \ \text{ for some } \ T \in GL_n(\mathbb{F}_r).$$

*Moreover, if for* $1 \leq i \leq m$ *the successive minimum* $\mu_i$ *occurs with multiplicity* $n_i$*, then* $T$ *has the form*

$$\begin{pmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_m \end{pmatrix} \quad \textit{with } B_i \in GL_{n_i}(\mathbb{F}_r).$$

## 1.3 List of the Main Results

For the convenience of the reader, we now write a list of the main results obtained in this dissertation. Also, in order to demonstrate the relevance of our results, we remind their counterpart over $\mathbb{Z}$.

**1. Representations sets, the binary case:**

- **Theorem (Watson, [28])** Suppose that $L$ and $L'$ are definite binary $\mathbb{Z}$-lattices and suppose $V(L) = V(L')$. Then either $L \cong L'$ or $(L, L') \cong m \cdot (x^2 + xy + y^2, x^2 + 3y^2)$ for some interger $m$.

- **Theorem 2.1.2** Suppose that $L$ and $L'$ are definite binary $\mathbb{F}_r[t]$-lattices and suppose that $V(L) = V(L')$. Then $L \cong L'$.

  Moreover if $L$ and $L'$ have the same discriminant, $V(L)$ and $V(L')$ can be replaced by $V_{\mu_2}(L)$ and $V_{\mu_2}(L')$.

**2. Representations sets, the ternary case:**

- **Theorem (Hsia, [13])** There are some nonequivalent definite ternary $\mathbb{Z}$-lattices having the same representation sets. An example is

  1. $L \cong x^2 + xy + y^2 + 9z^2$
  2. $L' \cong x^2 + 3(y^2 + yz + z^2)$

- **Theorem (Section 2.2)** There are some nonequivalent definite ternary $\mathbb{F}_5[t]$-lattices having the same representation sets. An example is

  1. $L \cong \langle 1, 3t+1, t+4 \rangle$
  2. $L' \cong \langle 1, 3t+1, t \rangle$

**3. Representations numbers:**

- **Theorem (Schiemann, [26])** Let $L$ and $L'$ be definite ternary $\mathbb{Z}$-lattices having the same representations numbers. Then $L \cong L'$.

- **Theorem 4.2.1** Let $(L, Q)$ and $(L', Q')$ be definite ternary $\mathbb{F}_r[t]$-lattices having the same representations numbers. Then $L \cong L'$.

**4. Regular ternary lattices:**

- **Theorem (Jagy-Kaplansky-Schiemann, [15])** There are at most 913 ternary regular $\mathbb{Z}$-lattices; 22 of them are not proved to be regular.

- **Theorem (Chan-Daniels, [5])** For $r$ fixed, there are finitely many classes of definite regular $\mathbb{F}_r[t]$-lattices.

- **Theorem 5.3.1** Let $L$ be a definite regular ternary $\mathbb{F}_r[t]$-lattice. Then, $L$ is regular if and only if $L$ has class number one.

- **Lemma 5.2.8** Suppose $r \neq 3$, then the definite regular ternary $\mathbb{F}_r[t]$-lattices are:

  1. the lattices $L$, with $\partial(\mathrm{disc}(L)) \leq 2$
  2. the lattices $L$ with $\partial(\mathrm{disc}(L)) = 3$ such that
     - $\mathrm{disc}(L) = \mathfrak{p}^3$ and $L_{\mathfrak{p}} = \langle \epsilon, \eta\mathfrak{p}, \rho\mathfrak{p}^2 \rangle$
     - $\mathrm{disc}(L) = \mathfrak{p}^2\mathfrak{q}$ and $L_{\mathfrak{p}} = \langle \epsilon, \eta\mathfrak{p}, \rho\mathfrak{p} \rangle$, $L_{\mathfrak{q}} = \langle \epsilon', \eta', \rho'\mathfrak{q} \rangle$

3. the lattices $L$ with $\partial(\mathrm{disc}(L)) = 4$ such that $L_{\mathfrak{p}} \cong \langle \epsilon, \mathfrak{p}, -\epsilon\mathfrak{p} \rangle$, for some quadratic prime $\mathfrak{p}$, and some $\epsilon \notin A_{\mathfrak{p}}^{\times 2}$.

**5. Spinor regular ternary lattices:**

- **Theorem (Hsia, Earnest, Hung, Chan; [6], [13])** There are finitely many equivalence classes of definite spinor-regular $\mathbb{Z}$-lattices.

- **Theorem 5.4.1** A definite $\mathbb{F}_r[t]$-lattice is spinor regular if and only if it is regular.

**6. Regular quaternary and universal lattices:**

- **Theorem (Earnest, [10])** There are infinitely many equivalence classes of definite regular quaternary $\mathbb{Z}$-lattices.

- **Theorem 6.1.1, Corollary 6.2.1 & Lemma 6.2.4** Let $L$ be a definite quaternary $\mathbb{F}_r[t]$-lattice. The following assertions are equivalent:

  1. $L$ is regular;
  2. $L$ is universal;
  3. $L$ has class number one;
  4. $L$ represents all of $\{1, -\delta, t, -\delta t\}$, for some $\delta \notin \mathbb{F}_r^{\times 2}$.

# Chapter 2

# Representation Sets

## 2.1 The Binary Case

In [28], Watson proved that all the classes of binary $\mathbb{Z}$-lattices, with two exceptions, are determined by their representation sets. Here, we prove that the representation sets determine the discriminant of a definite binary $\mathbb{F}_r[t]$-lattice and that among the binary lattices with a given discriminant, the very first representations determine the equivalence class of the lattice.

**Lemma 2.1.1** *Let $(L, q)$ and $(L', q')$ be definite $\mathbb{F}_r[t]$-lattices of rank 2. If $V(L) = V(L')$, then there are reduced basis in which the diagonal entries of the Gram matrices of $L$ and $L'$ have same degree and same leading coefficients.*

**Remark.** We can reformulate the previous lemma as follows. Let $A, A'$ be reduced Gram matrices of $L$ and $L'$. If $V(L) = V(L')$, then there exists $U \in GL_2(\mathcal{O}_\infty)$ such that $A' =^t UAU$. ■

**Proof.** Suppose $q = [a_{ij}]$ and $q' = [a'_{ij}]$ are both reduced and for $i = 1, 2, 3$, let $\mu_i$ and $\mu'_i$ be the successive minima. Since $a_{11}$ is represented by $q$, it must be represented by $q'$. Since $q$ is reduced, it is clear that no polynomials of degree smaller than $\partial(a_{11}) = \mu_1$ is represented by $q$ and hence by $q'$. In particular $q'$ represents $a_{11}$ primitively. Thus, we can suppose that $a'_{11} = a_{11}$. When applying a transformation to $q'$, in order to get $a'_{11} = a_{11}$ one could end up with a new form which is not reduced. In this case, one applies the reduction algorithm of [9]. The output will be a reduced form in which $a_{11}$ has not changed.

If $\mu_2 \neq \mu'_2$, there is no loss of generality in supposing $\mu_2 < \mu'_2$. There are two possible scenarios:

1. If $\mu_2 \not\equiv \mu_1 \mod 2$ then it is clear that

$$a_{22} \notin V_{\mu_2}(q') = \{a_{11}h^2 \mid \partial(a_{11}h^2) \leq \mu_2\},$$

   since any element of the previous set has degree of the same parity as $\mu_1$.

2. If $\mu_2 \equiv \mu_1 \mod 2$, let $k = (\mu_2 - \mu_1)/2$. For any $\alpha, \beta \in \mathbb{F}_r^\times$ collect $t$ in $q(\alpha t^k, \beta)$ to get

$$q(\alpha t^k, \beta) = Q_0(\alpha, \beta)t^{\mu_2} + P(t)$$

   where $\partial(P) < \mu_2$ and $Q_0$ is a binary quadratic form defined over $\mathbb{F}_r$. Since $L$ is definite, it follows that $Q_0$ is anisotropic; hence, $Q_0$ is non degenerate and therefore is universal. Choose $\alpha, \beta$ such that $Q_0(\alpha, \beta)$ is not in the same square class as the leading coefficient of $a_{11}$. Then $q(\alpha t^k, \beta)$ cannot be represented by $q'$.

Thus, we have $\mu_2 = \mu'_2$. Now it is clear that the leading coefficients of $a_{22}$ and $a'_{22}$ must belong to the same square class of $\mathbb{F}_r$. It follows directly from Gerstein's result in case (1) above. In case (2), it follows from the fact that the binary form $Q_0$ is anisotropic. ■

One will notice that the proof for ternary lattices is essentially the same. Indeed the definiteness of the form implies that the three successive minima cannot have the same parity. Remember that any quadratic space of dimension at least 3 defined over a finite field is isotropic.

It is clear that the equality of the representation sets is not modified by scaling. Hence, we can suppose that the binary forms are primitive.

**Theorem 2.1.1** *Let $L, L'$ be two primitive lattices of respective discriminant $d, d'$. If $V(L) = V(L')$ then $d' = d \mod \mathbb{F}_r^{\times 2}$.*

**Proof.** In view of Lemma 2.1.1, we just need to establish that $d$ and $d'$ have the same prime divisors. More precisely, let $\mathfrak{p} \in \mathbb{F}_r[t]$ be a prime (i.e. a monic irreducible element of $A$). We prove that

$$V(L') \subset V(L) \Rightarrow v_{\mathfrak{p}}(d) \leq v_{\mathfrak{p}}(d') \tag{2.1}$$

where $v_{\mathfrak{p}}(\cdot)$ denotes the $\mathfrak{p}$-adic valuation. In the following, we suppose that $\mathfrak{p} = (p)$ and that $L$ and $L'$ have Gram matrices respectively given by

$$q = \begin{pmatrix} a & b \\ b & c \end{pmatrix} = (a, 2b, c) \quad \text{and} \quad q' = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = (a', 2b', c').$$

**Case 1**: Suppose that $v_{\mathfrak{p}}(d') \equiv 1 \mod 2$, and write $d' = p^n v$ where $v$ and $p$ are coprime. Since the set of primitive forms of a given determinant is a group under Gaussian composition (cf. [21]), it follows that

$$q' = (p^n, 0, -d') \cdot (a'', 2b'', c'').$$

The first form above represents $p^n$ and the second represents $v \in \mathbb{F}_r[t]$ coprime to $p$; hence, $q'$ represents $p^n v$.

In $q$, one can clearly assume that $p$ does not divide $a$. Since $V(L') \subset V(L)$ it follows that $p^n v$ is represented by $L$; we have $rp^n = af^2 + 2bfg + cg^2$ for some $f, g \in \mathbb{F}_r[t]$. Therefore,

$$avp^n = a^2f^2 + 2abfg + acg^2 = (af + bg)^2 - dg^2.$$

If $d$ was divisible by $p^j$ where $j > n$, it would follows that $(af + bg)^2$ is divisible at least by $p^n$ and thus, as $n$ is odd, $(af + bg)^2$ would be divisible by $p^{n+1}$. The contradiction is clear.

**Case 2**: Suppose that $v_{\mathfrak{p}}(d') = 2k \equiv 0 \mod 2$ and $\left(\frac{a}{\mathfrak{p}}\right) = -1$. There is no loss of generality in supposing that $a$ and $a'$ are both coprime to $p$.

Since $p^{2k} | b'^2 - a'c'$ one can find $b''$ satisfying $b''p^k \equiv b' \mod a'$. Let $a'' = a'$ and $c'' = \frac{b''^2 p^{2k} - D}{a'' p^{2k}}$. We get a form

$$(a'', b''p^k, c''p^{2k}) \cong (a', b', c').$$

Consider the form $(a'', b'', c'')$ of discriminant $\frac{d'}{p^{2k}} = D'$. As $D'$ and $p$ are coprime, it follows that the reduction of the form $(a'', b'', c'')$ modulo $\mathfrak{p}$ may be seen as a nonsingular quadratic form over a finite field. It must be universal, and thus represents both quadratic residues and quadratic nonresidues. Let $U$ be such a quadratic residue. There are $f', g' \in \mathbb{F}_r[t]$ with

$$U = a''f'^2 + b''f'g' + c''g'^2.$$

Multiply the previous line by $p^{2k}$, let $f = f'X^k$ and $g = g'$ to obtain

$$Up^{2k} = a''f^2 + b''p^k fg + c''p^{2k}g^2.$$

We see that the polynomial $Up^{2k}$ is represented by $(a'', b''p^k, c''p^{2k})$ which is equivalent to $(a', b', c') = q'$. As $V(L') \subset V(L)$, $Up^{2k}$ is represented by $q$. Therefore, there are $f, g \in \mathbb{F}_r[t]$ with

$$Up^{2k} = af^2 + 2bfg + cg^2.$$

Multiply the previous by $a$ to get

$$aUp^{2k} = a^2f^2 + 2abfg + acg^2 = (af + bg)^2 - dg^2.$$

Suppose that $p^j$ divides $d$ for some $j > 2k$ then $\left(\frac{aU}{P}\right) = 1$ which contradicts $\left(\frac{a}{P}\right) = -1$ and $\left(\frac{U}{P}\right) = 1$.

**Case 3**: If $v_{\mathfrak{p}}(d') \equiv 0 \mod 2$ and $\left(\frac{a}{p}\right) = 1$, we proceed exactly as in the previous case, taking for $U$ a quadratic non residue instead of a quadratic residue. ■

Although it is elementary, we should make an extensive use of the following result.

**Lemma 2.1.2 ([1], V.1)** *Let $a \neq 0$ be an element of $\mathbb{F}_r$ and let $\delta \in \mathbb{F}_r$ be a nonsquare. Define*

1. $n_1 = \#\{(\alpha, \beta) \in \mathbb{F}_r^2 \mid \alpha^2 - \delta\beta^2 = a\}$;
2. $n_2 = \#\{(\alpha, \beta) \in \mathbb{F}_r^2 \mid \alpha^2 - \beta^2 = a\}$
3. $N = \#\{(\alpha^2, \beta^2) \in \mathbb{F}_r^2 \mid \alpha^2 - \delta\beta^2 = -\delta\}$.

*Then $n_1 = r + 1$, $n_2 = r - 1$ and $N < r$.*

**Theorem 2.1.2** *Let $(L, q)$ and $(L', q')$ be two binary definite positive binary lattices with same successive minima $\mu_1, \mu_2$ and same discriminant $D$. If $V_{\mu_2}(L) = V_{\mu_2}(L')$ then $L$ and $L'$ are integrally equivalent.*

**Proof.** In the following we let $q = (a, 2b, c)$ and $q' = (a', 2b', c')$. There is no loss of generality in making the following assumptions: $a = a'$ has leading coefficient 1 and $c, c'$ have same leading coefficients $-\delta$ for some nonsquare $\delta \in \mathbb{F}_r$. We shall treat three cases separately:

**Case 1**: $\mu_1 \not\equiv \mu_2 \mod 2$. Since $c'$ is represented by $q$, and since $q$ is definite we can find $f \in A$ and $\beta \in \mathbb{F}_r$ such that

$$c' = af^2 + 2bf\beta + c\beta^2.$$

The assumption on successive minima implies that $\beta = \pm 1$ and by changing $b'$ into $-b'$ if need be, we can suppose that $\beta = 1$. Make $M = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} \in GL_2(A)$ act on $f$ to get

$$q \cong q'' = \begin{pmatrix} a & b'' \\ b'' & c' \end{pmatrix}$$

for some $b'' \in \mathbb{F}_r[t]$. Since $\det(M) = 1$ we have $\operatorname{disc}(q) = \operatorname{disc}(q'')$ and thus we have $\operatorname{disc}(q'') = \operatorname{disc}(q')$; thus,

$$ac' - b''^2 = ac' - b'^2$$

which leads to $b'' = \pm b'$.

**Case 2**: $\mu_1 \equiv \mu_2 \mod 2$, but $\mu_1 \neq \mu_2$. Since $q$ and $q'$ have the same discriminant, we can suppose that $q = (a, 2b, c)$ and $q' = (a, 2b', c + \Omega)$ where $\Omega = \frac{b'^2 - b^2}{a}$. We have $\partial(\Omega) < \max\{\partial(b), \partial(b')\} < \partial(a)$. For $u \in \mathbb{F}_r$, consider the equation

$$ah^2 + 2bh\beta + c\beta^2 = c + \Omega + 2b'u + au^2 \tag{2.2}$$

where $h = h_k x^k \cdots + h_0 \in \mathbb{F}_r[t]$ and $\beta \in \mathbb{F}_r$.

As $u$ runs over $\mathbb{F}_r$, we can suppose that the right hand side takes $r$ distinct values. Indeed, if $c + \Omega + 2b'u + au^2 = c + \Omega + 2b's + as^2$ for some $u, s \in \mathbb{F}_r$, the equality of the dominant coefficients implies that $s^2 = u^2$ and if $u = -s$. Thus one gets $-2b'u = 2b'u$, that is $b' = 0$, in which case the equality of discriminant suffices to conclude for the equivalence. Now the equality of the dominant coefficients in (2.2) can be written as

$$h_k^2 - \delta\beta^2 = -\delta.$$

By Lemma 2.1.2, there are less than $r$ pairs $(h_k^2, \beta^2)$ satisfying the equation above. Thus one pair $(h_k^2, \beta^2)$ must appear for two different values of the right hand side. So, there are $u, s, \beta \in \mathbb{F}_r$ and $h, g \in \mathbb{F}_r[t]$ such that

$$ah^2 \pm 2bh\beta + c\beta^2 = c + \Omega + 2b'u + au^2$$

$$ag^2 \pm 2bg\beta + c\beta^2 = c + \Omega + 2b's + as^2 \tag{2.3}$$

By subtracting these equalities, we get

$$a(h^2 - g^2) + 2b\beta(\pm h \pm g) = 2b'(r - s) + a(r^2 - s^2).$$

It follows that $h, g$ are both in $\mathbb{F}_r$. By going back to (2.3) we see that $\beta^2 = 1$ and then that $g^2 = s^2$. That finally implies that

$$\pm 2bs = \Omega + 2b's \quad \Leftrightarrow 2s(b' \pm b) = \frac{b^2 - b'^2}{a}$$

by canceling either $b' + b$ or $b' - b$ from both side of the last equation we obtain a contradiction (since $\partial(a) > \partial(b)$) unless $b^2 = b'^2$. The equality of the discriminants suffices now to conclude.

**Case 3**: $\mu_1 = \mu_2$. Suppose $q = (a, 2b, c)$ and $q' = (a, 2b', c')$ with

$$\begin{aligned}
a &= x^n + \cdots + a_0 \\
c &= -\delta x^n + c_{n-1}x^{n-1} + \cdots + c_0 \\
c' &= -\delta x^n + c'_{n-1}x^{n-1} + \cdots + c'_0 \\
b &= b_k x^k + \cdots + b_0 \\
b' &= b'_m x^m + \cdots + b'_0
\end{aligned}$$

Since the two forms have the same discriminant, we see that $\partial(c - c') < \max\{\partial(b), \partial(b')\}$. Then, a short computation shows that the forms are equivalent if $b_k = \pm b'_k$. Indeed, in this case, by applying a transformation on $q'$, one can

suppose that $b_k = b'_k$. Then the equality of the discriminants allows to conclude that $c$ and $c'$ must coincide at least up to $2\partial(b)-\partial(a)-1$. Also, the equality of the discriminants implies that $2b_kb_{k-1} = 2b_kb'_{k-1}$ and thus we see that $b_{k-1} = b'_{k-1}$. By continuing this process one proves that $b_j = b'_j$ and $c_j = c'_j$ for all $j$.

Since the forms have the same representation sets, to any pair $(\rho, \sigma) \in \mathbb{F}_r^2$, corresponds a pair $(\alpha, \beta) \in \mathbb{F}_r^2$ such that

$$q(\alpha, \beta) = q'(\sigma, \rho) \tag{2.4}$$

The two sides of this equation are polynomials, and since these polynomials are equal, we see that the coefficients of $t^{\partial(a)}$ and $t^k$, where $k = \max\{\partial(b), \partial(b')\}$, must be the same on both sides of (2.4). We finally get equations of two quadrics

$$\begin{cases} \alpha^2 - \delta\beta^2 = \sigma^2 - \delta\rho^2 \\ a_k\alpha^2 + 2b_k\alpha\beta + c_k\beta^2 = a_k\sigma^2 + 2b'_k\sigma\rho + c_k\beta^2 \end{cases}.$$

We count the number of points on the intersection of these quadrics. For any pair $(\rho, \sigma) \in \mathbb{F}_r^2$, one can find $(\alpha, \beta) \in \mathbb{F}_r^2$ satisfying the system. But if $(\alpha, \beta)$ satisfies the system, so does $(-\alpha, -\beta)$, and therefore we see that we get at least $2r + 2$ projective rational points on this intersection. If the curve $E$, defined by these equation was smooth, it would be an elliptic curve. The Riemann hypothesis would apply and would lead to

$$|\#E(\mathbb{F}_r) - (r + 1)| \leq 2\sqrt{r}.$$

A short computation tells that the curve above is singular if and only if

$$\delta^4(b_k - b'_k)^4(b_k + b'_k)^4 \left((a_k\delta + c_k)^2 - 4\delta b'^2_k\right) \left((a_k\delta^2 + c_k)^2 - 4\delta b_k^2\right) = 0.$$

As $\delta$ is not a square, this is equivalent to $b_k = \pm b'_k$. ■

## 2.2 The Ternary Case

Here is an example showing that one cannot expect, in the ternary case, a result as strong as the one that could be proved for binary lattices. In general, the representation sets (without multiplicities) will not be enough to determine the integral class of a definite ternary $\mathbb{F}_r[t]$-lattice.

**Lemma 2.2.1** *Let $L$ and $L'$ be lattices in the same genus with $\partial(\mathrm{disc}(L)) \leq 2$ then $L \cong L'$.*

**Proof.** A proof of this fact may be found in [5]. For an elementary proof, the reader is referred to Corollary 3.5.1 ■

Consider the $\mathbb{F}_5[t]$-lattices $L$ and $L'$ defined by

$$L = \langle 1, 3t+1, t+4 \rangle ; \quad L' = \langle 1, 3t+1, t \rangle$$

of respective discriminants $d = 3t^2 + 2t + 4$ and $d' = 3t^2 + t$.

Since $d$ and $d'$ have degree two, Lemma 2.2.1 tells that a polynomial is represented by $L$ (or by $L'$) if and only if it is represented everywhere locally.

Let $\left(\text{-}\right)$ denote the Legendre symbol. Note that

$$\left(\frac{-(3t+1)}{t+4}\right) = \left(\frac{-1}{t+4}\right) = 1$$
$$\left(\frac{-(3t+1)}{t}\right) = \left(\frac{1}{t}\right) = 1$$
$$\left(\frac{-(t+4)}{3t+1}\right) = \left(\frac{2}{3t+1}\right) = -1$$
$$\left(\frac{-t}{3t+1}\right) = \left(\frac{3}{3t+1}\right) = -1$$

The following observations follow easily:

- $W_\infty \cong W'_\infty$ since both are equivalent to $\langle 1, t, 3t \rangle$

- At $3t+1$ we have $L_{(3t+1)} \cong \langle 1; -2; -2(t+4)(3t+1) \rangle$ and we have $L'_{(3t+1)} \cong \langle 1; -2; -2t(3t+1) \rangle$

- anywhere else the lattices are isotropic and hence universal.

Since $\left(\frac{t+4}{3t+1}\right) = \left(\frac{t}{3t+1}\right)$, these lattices represent the same polynomials locally everywhere. Thus, they represent the same polynomials globally.

This is an example of nonequivalent lattices having the same representation sets. One will notice that these lattices are not even in the same genus as they have different discriminants.

# Chapter 3

# Technical Results

## 3.1 Dual Lattices of Isospectral Lattices

Remember that

1. $A = \mathbb{F}_r[t]$ and let $K = \mathbb{F}_r(t)$
2. $|f|_\infty = r^{-v_\infty(f)}$ (the discrete valuation corresponding to $\infty$ is the degree function)
3. $K_\infty = \mathbb{F}_r\left(\left(\frac{1}{t}\right)\right)$
4. $\mathcal{O}_\infty = \{x \in \mathbb{F}_r(t)_\infty : |x|_\infty \leq 1\} = \mathbb{F}_r\left[\left[\frac{1}{t}\right]\right]$
5. $\mathfrak{P}_\infty = \{x \in \mathbb{F}_r(t)_\infty : |x|_\infty < 1\}$.

If $(L, q)$ is a lattice and if $B$ is the bilinear form defined by

$$B(x, y) = q(x + y) - q(x) - q(y)$$

we define the dual of $L$ to be

$$L^\# = \{h \in \mathbb{F}_r[t] : B(h, L) \subset \mathbb{F}_r[t]\}.$$

In general $L^{\#}$ is not integral, but that can be *corrected* by considering another lattice called the adjoint of $L$, denoted by $\overline{L}$ and defined by $\overline{L} = \mathrm{disc}(L)L^{\#}$. It is standard that the Gram matrix of the dual of a lattice is the inverse of the Gram matrix of the lattice.

As seen in Lemma 1.2.2, a nice property satisfied by a definite $\mathbb{F}_r[t]$-lattice, is that the *dualization* will change the configuration of successive minima. Hence, it is very useful to check that if two ternary lattices are isospectral then so are their dual.

To define theta series, we use the ideas of Rück [24] and of Rosson [23]. We reffer to their papers for details of some computations.

Since $SL_2(\mathcal{O}_\infty)$ is a maximal compact subgroup of $SL_2(K_\infty)$, it is natural to make $\mathfrak{H} = SL_2(K_\infty)/SL_2(\mathcal{O}_\infty)$ play the role of the Poincaré half-plane. A complete set of coset representatives for $\mathfrak{H}$ is the set

$$\left\{ \begin{pmatrix} y & xy^{-1} \\ 0 & y^{-1} \end{pmatrix} : y = t^m, m \in \mathbb{Z}, x \in t^{2m+1}A \right\}.$$

Let $x = \sum_{i=-\infty}^{n} x_i t^i \in K_\infty$. We define a character of $K_\infty$ by

$$e\{x\} = exp\left(\frac{2i\pi Tr(x_1)}{p}\right)$$

where $Tr$ stands for the trace of $\mathbb{F}_r$ to its prime subfield. Let $\Phi$ denote the characteristic function of $\mathcal{O}_\infty$. For $z = \begin{pmatrix} y & xy^{-1} \\ 0 & y^{-1} \end{pmatrix} \in \mathfrak{H}$ and for a lattice $L$, we define the theta series of $L$ by

$$\begin{aligned} \theta_L(z) &= \sum_{v \in tL} \Phi\left(y^2 Q(v)\right)\ e\{xQ(v)\} \\ &= \sum_{w \in L} \Phi(t^2 y^2 Q(w))\, e\{t^2 x q(w)\} \end{aligned}$$

We see that the theta series determine the representation numbers and conversely. Indeed, for $y = t^m$, we have

$$\theta_L(z) = \sum_{v_\infty(a) \geq -2m-2} R(L,a)\, e\{xt^2 a\} \tag{3.1}$$

Let $\lambda$ be an additive Haar measure on $V_\infty$. We identify $V_\infty$ with its dual and define the Fourier transform on $V_\infty$ by

$$\hat{f}(y) = \int_{V_\infty} f(v)e\{-B(v,y)\}d\lambda(v).$$

**Lemma 3.1.1** *Let $(L,Q)$ be lattice in a quadratic space $V$ defined over $K$. Let $z = \begin{pmatrix} y & xy^{-1} \\ 0 & y^{-1} \end{pmatrix} \in K_\infty$. Define $\varphi_z(v) = \Phi(t^2y^2Q(v))e(t^2xQ(v))$. Then*

$$\widehat{\varphi_z}(w) = I_z \cdot \varphi_{S\cdot z}(w) \tag{3.2}$$

*Where $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $I_z$ depends only on $z$ and on the class of $W_\infty$.*

**Proof.** Let $G, H \in K_\infty$ be such that $v_\infty(G) = g > h = v_\infty(H)$. Consider $\varphi(v) = \Phi(GQ(v))e(HQ(v))$.

**Step 1**: We prove that $\hat{\varphi}(w) = 0$ whenever $v_\infty(Q(w)) \leq 2h - g - 1$. Since the measure is additive on $K_\infty$, for any $z \in K_\infty$, we have

$$\begin{aligned}\hat{\varphi}(w) &= \int_{V_\infty} \Phi(GQ(v+z))\, e(HQ(v+z))\, e(-B(v+z,w))dv \\ &= e\{-B(z,w)\} \int_{V_\infty} \Phi(GQ(v+z))\, e(HQ(v+z))\, e(-B(v,w))dv\end{aligned}$$

For $z = \frac{t}{Q(w)}Q(w)$ we see that $B(z,w) = 2t \neq 0$ and $e\{-B(z,w)\} = e\{2t\} \neq 1$. Also, by using the that $v_\infty(Q(w)) \leq 2h - g - 1$, one checks that

$$\Phi(Q(z+v)G) = \Phi(Q(v)G) \quad \text{and} \quad e\{HQ(v+z)\} = e\{HQ(v)\}.$$

Therefore, we see that

$$\hat{\varphi}(w) = e\{-B(z,w)\}\hat{\varphi}(w)$$

which enables to conclude.

**Step 2**: Let us suppose that and that $v_\infty(Q(w)) \geq 2h - g$ and that $g > h$. We have

$$\begin{aligned}\hat{\varphi}(w) &= \int_{V_\infty} \Phi(Q(v)G)\, e\{HQ(v)\}\, e\{-B(v,w)\}dv \\ &= e\left\{-\frac{1}{H}Q(w)\right\} \int_{V_\infty} \Phi(Q(v)G)\, e\left\{HQ\left(v - \frac{w}{H}\right)\right\} dv\end{aligned}$$

By letting $u = v - \frac{1}{H}w$ we see that $\Phi(Q(v)G) = \Phi(Q(u)G)$ and consequently that

$$\hat{\varphi}(w) = e\left\{-\frac{1}{H}Q(w)\right\} \int_{V_\infty} \Phi(Q(u)G)\, e\left\{HQ\left(u\right)\right\} du.$$

We finally get

$$\hat{\varphi}(w) = I_z \cdot e\left\{-\frac{1}{H}Q(w)\right\} \tag{3.3}$$

$$\left(\text{where} \quad I_z = \int_{V_\infty} \Phi(Q(u)G)\, e\left\{HQ\left(u\right)\right\} du\right).$$

The condition $v_\infty(Q(w)) \geq 2h-g$ implies that $\Phi\left(Q(w)\frac{G}{H^2}\right)$ is 1 whenever $\hat{\varphi}(w) \neq 0$. Hence, (3.3) becomes

$$\hat{\varphi}(w) = I_z \cdot e\left\{-\frac{1}{H}Q(w)\right\} \cdot \Phi\left(Q(w)\frac{G}{H^2}\right).$$

Now replace $H$ by $xt^2$ and $G$ by $y^2t^2$ in order to get (3.2).

**Step 3**: One could explicitly compute $I_z$, but it is not necessary for our purposes. We just need to check that $I_z$ depends only on the class of $Q$ over $K_\infty$. To that aim, we need to check that the right hand side of

$$I_z = \int_{V_\infty} \Phi(Q(u)y^2)\, e\left\{xQ\left(u\right)\right\} du \tag{3.4}$$

does not depend on the representative of $Q$. The connoisseur will here recognize $I_z$, which is essentially the invariant $\gamma(xQ)$ defined by Weil in [30]. It therefore only depends on the Witt class of $xQ$. ■

**Proposition 3.1.1** *Let $L$ and $L'$ be ternary definite lattices. If $L$ and $L'$ have the same representation numbers then so do their dual $L^{\#}$ and $L'^{\#}$.*

**Proof.** In view equation (3.1), it is enough to prove that

$$\theta_L = \theta_{L'} \Rightarrow \theta_{L^{\#}} = \theta_{L'^{\#}}.$$

To this aim, we just use Poisson:

$$\sum_{w \in L} \varphi_z(w) = c \sum_{w \in L^{\#}} \widehat{\varphi_z}(w) = c\, I_z \sum_{w \in L^{\#}} \varphi_{S \cdot z}(w)$$

$$\sum_{w \in L'} \varphi_z(w) = c \sum_{w \in L'^{\#}} \widehat{\varphi_z}(w) = c\, I'_z \sum_{w \in L'^{\#}} \varphi_{S \cdot z}(w)$$

where $c$ is a volume depending only on the measure. By Lemma 2.1.1 and by the last step in the proof of Lemma 3.1.1, we have $I_z = I'_z \neq 0$; hence,

$$\sum_{w \in L'^{\#}} \varphi_z(w) = \sum_{w \in L^{\#}} \varphi_z(w).$$

■

## 3.2 Discriminants of Isospectral Lattices

In this subsection we use the terminology of Conway, who calls a property *audible* when it is determined by the theta series. Let $\mathfrak{p}$ be a prime ideal of $A$. Let $\chi_{\mathfrak{p}} : K_{\mathfrak{p}}/A_{\mathfrak{p}} \to \mathbb{C}^{\times}$ be the canonical character.

**Definition.** Let $V$ be a quadratic $K$-space and let $(L, Q)$ be a lattice in it. Let $E_m = E_m(L, Q) = \{x \in L : \partial(Q(x)) \leq m\}$. We define

$$\mu(L, Q, \chi_{\mathfrak{p}}) = \lim_{m \to \infty} \frac{1}{\#E_m} \sum_{x \in E_m} \chi_{\mathfrak{p}}(Q(x)).$$

■

**Lemma 3.2.1** *As defined above, $\mu(L, Q, \chi_{\mathfrak{p}})$ is audible and depends only on $L_{\mathfrak{p}}$.*

**Proof.** The first assertion is rather clear once one has noticed that

$$\begin{aligned}\mu(L, Q, \chi_{\mathfrak{p}}) &= \lim_{m\to\infty} \frac{1}{\#E_m} \sum_{x\in E_m} \chi_{\mathfrak{p}}(Q(x)) \\ &= \lim_{m\to\infty} \left( \sum_{\partial(a)\leq m} R(L,a) \right)^{-1} \sum_{\partial(a)\leq m} R(L,a)\chi_{\mathfrak{p}}(Q(x))\end{aligned}$$

We prove the second assertion. Let $m$ be an integer sufficiently large so that $E_m$ surjects onto $L/L\cap L^{\#}$. For such an integer, we have

$$\frac{1}{\#E_m} \sum_{x\in E_m} \chi_{\mathfrak{p}}(Q(x)) = \frac{1}{[L : L\cap L^{\#}]} \sum_{x\in L/L^{\#}\cap L} \chi_{\mathfrak{p}}(Q(x)).$$

Also notice that

$$L/L\cap L^{\#} = L_{\mathfrak{p}}/L_{\mathfrak{p}}\cap L_{\mathfrak{p}}^{\#} \times M$$

where $M$ is of $\mathfrak{p}'$-torsion for some $\mathfrak{p}'$ coprime to $\mathfrak{p}$. Since the $M$ is of $\mathfrak{p}'$-torsion it does not contribute to the sum and therefore

$$\mu(L, Q, \chi_{\mathfrak{p}}) = \lim_{m\to\infty} \frac{1}{\left[L_{\mathfrak{p}} : L_{\mathfrak{p}}\cap L_{\mathfrak{p}}^{\#}\right]} \sum_{x\in L_{\mathfrak{p}}/L_{\mathfrak{p}}\cap L_{\mathfrak{p}}^{\#}} \chi_{\mathfrak{p}}(Q(x)).$$

■

Althought the methods we use would allow us to prove that isospectral lattices lie in a single genus, we confine ourselves to proving:

**Proposition 3.2.1** *Let $(L, Q)$ and $(L', Q')$ be isospectral definite ternary $\mathbb{F}_r[t]$-lattices, then* $\operatorname{disc}(L) = \operatorname{disc}(L') \mod \mathbb{F}_r^2$.

**Proof.** Let $L, L'$ be isospectral lattices of discriminant $D, D'$. In view of Lemma 2.1.1 and of the note following it, it is enough to prove that for any prime ideal $\mathfrak{p}$, $v_{\mathfrak{p}}(D) = v_{\mathfrak{p}}(D')$ where $v_{\mathfrak{p}}(\cdot)$ stands for the $\mathfrak{p}$-adic valuation.

Let $(M,q) \subset V_{\mathfrak{p}}$ be a modular local lattice, so that $M^{\#} = \pi^{-v}M$ for some integer $v$ and some $\pi$ generating $\mathfrak{p}$. If $q$ is multiplied by $\pi^{-\alpha}$ for some integer $\alpha$, we see that

$$M^{\#}_{\pi^{-\alpha}q} = \pi^{\alpha-v}M.$$

In particular, we have

$$\mu(M,\pi^{-\alpha}q,\chi_{\mathfrak{p}}) = \frac{1}{[M:(\pi^{\alpha-v}M)\cap M]} \sum_{x\in M/(\pi^{\alpha-v}M)\cap M} \chi_p(\pi^{-\alpha}q(x))$$

$$= \begin{cases} 1 & \text{if } \alpha \leq v \\ \frac{1}{[M:(\pi^{\alpha-v}M)\cap M]}\ \gamma_p(\pi^{\alpha}q) & \text{otherwise} \end{cases}$$

where, for a lattice $R$, $\gamma(R)$ is defined by Weil in [30] by

$$\gamma(R) = \frac{1}{[R^{\#}:R]} \sum_{x\in R^{\#}/R} \chi(x)$$

and is proved to satisfy $|\gamma(R)| = 1$. Finally, if $N$ stands for the norm, we have, for the modular case

$$|\mu(M,\pi^{-\alpha}q,\chi_{\mathfrak{p}})| = N(\mathfrak{p})^{-\frac{1}{2}\max\{0,\alpha-v\}}.$$

Consider now a global ternary lattice $(L,Q)$ and suppose that $L_{\mathfrak{p}} = \oplus_{i=1}^{n}\pi^{v_i}M_i$, where $v_1 < \cdots < v_n$. The *average* function $\mu$ is multiplicative and therefore

$$|\mu(L,\pi^{-\alpha}Q,\chi_{\mathfrak{p}})| = N(\mathfrak{p})^{-\frac{1}{2}\sum_{i=1}^{n}\max\{0,\alpha-v_i\}\ \mathrm{rk}(M_i)} \tag{3.5}$$

In particular, in computing the left hand side of this equation for $\alpha = 1,2,\cdots$, one can recover $v_i$ and the rank of $M_i$. To conclude one needs to notice that by Lemma 3.2.1, the left hand side of (3.5) is audible and that $v_{\mathfrak{p}}(D) = \sum v_i\,\mathrm{rk}(M_i)$.

■

**Corollary 3.2.1** *Let $L$ and $L'$ be definite ternary $\mathbb{F}_r[t]$-lattices. If $L$ and $L'$ are isospectral, so are their adjoints.*

**Proof.** Clear from Propositions 3.1.1 and 3.2.1. ■

## 3.3 Lattices with Prime Discriminants

The result of the two previous subsection are easily established by different arguments when the discriminant of the quadratic form is prime. In this case also, the representations sets will be enough to prove the results of the previous section.

**Theorem 3.3.1 ([22], 104:4)** *Let $f, g$ be two integral forms in the same spinor genus and in $n \geq 3$ variables. Suppose that they are isotropic over $V_{\mathfrak{p}}$ for some prime $\mathfrak{p}$. Then they are properly equivalent over $A^{[\mathfrak{p}]} = \{a : |a|_{\mathfrak{l}} \leq 1 \ \ \forall \mathfrak{l} \neq \mathfrak{p}\}$.*

**Corollary 3.3.1** *Let $(L, q)$ be a ternary lattice of squarefree discriminant $D$ and suppose that $L_{\mathfrak{p}}$ is isotropic for some prime $\mathfrak{p}$. Suppose further that $\mathfrak{p} = (\pi)$ and that $L$ represents $c$ locally everywhere. Then $L$ primitively represents $\pi^{2m}c$ for some $m \in \mathbb{N}$.*

**Proof.** It is well known that when a lattice has a squarefree discriminant then the notions of spinor genus and of genus coincide. Let $L = L^1, L^2, \cdots, L^n$ be all the classes in $\mathcal{G} = \mathcal{G}en(L)$ and suppose $c$ is represented locally everywhere by $L$. It follows that $c$ is represented globally by some $L^i \in \mathcal{G}$. Let $\mathfrak{p}$ be the prime such that $L_{\mathfrak{p}}$ is isotropic. Since $(L, q)$ and $(L^i, q^i)$ are in the same spinor genus, there is a matrix $M \in SL_3(A^{[\mathfrak{p}]})$ such that

$$q(Mx) = q^i(x).$$

Now take the smallest $m$ such that $\pi^m M \in A$, then

$$\pi^{2m} c = q^i(\pi^m x) = q(\pi^m M x)$$

and we see that $\pi^{2m} c$ is primitively represented by $q$. ■

**Proposition 3.3.1** *Let $(L, q)$ and $(L', q')$ be two definite ternary lattices of irreducible discriminant $d$ and $d'$. Suppose $L$ and $L'$ have the same representations sets. Then $d = d'$.*

**Proof.** Since the class of a lattice with discriminant of degree $\leq 1$ is determined by the discriminant, we can assume that $\partial d \geq 2$. Note that since $d$ is irreducible, then $L_d$ is anisotropic. Indeed, for all $\mathfrak{p}$ such that $(\mathfrak{p}, d) = 1$, $L_\mathfrak{p}$ is unimodular and so is isotropic. Since $W_\infty$ is anisotropic (i.e. $L$ is definite), reciprocity implies that $L_d$ is anisotropic.

Suppose that $d \neq d'$. It follows that $L'_d = L' \otimes A_d$ is unimodular and thus is totally determined by its discriminant. In other words,

$$L'_d \cong \langle 1, -1, -d' \rangle .$$

Since $L_d$ is anisotropic and it must be of the form

$$L_d \cong \langle 1, -\delta, -\delta d \rangle$$

where $\delta \in A$ is not a square modulo $d$. Let us consider the set $E$ of polynomials which are not represented by $L_d$. Let $a(x) = \alpha_0 + \cdots + \alpha_n x^n$ be a polynomial and write is as:

$$a = a_0 + a_1 d + \cdots + a_k d^k.$$

If $a_0 \neq 0$ then $a$ is a unit at $d$ and therefore is represented by $L_d$ (which, by the way, represents all the $d$-adic units).

Suppose that $a_0 = 0$ and let $k = \nu_d(a)$. Then $a$ is not represented locally at $d$ if and only if the quadratic space

$$\langle 1, -\delta, -\delta d, -a \rangle_d \cong \left\langle 1, -\delta, -\delta d, -a_k d^k \right\rangle_d$$

is anisotropic at $d$. That means

- $k \equiv 1 \mod 2$; and
- $-a_k \not\equiv \delta \mod (A_d^2)$

Hence, any polynomials of the form $s(x)d^{2v+1}$, with $\partial s < \partial d$ is not represented locally by $L$ as long as $s(x)$ is not in the same square class as $\delta$. Since it is not represented locally, such a polynomial will obviously not be represented globally. Choose $s \in A$ such that

- $(s, r) = 1$
- $s \not\equiv \delta \mod (A_d^2)$
- the polynomial $sd$ is represented by $L'_\infty$.

Such a choice is always possible. Indeed, $L'_\infty$ must be equivalent to one of the following: $\langle 1, -\delta, x \rangle$, $\langle 1, -\delta, \delta x \rangle$, $\langle 1, x, -\delta x \rangle$ or $\langle \delta, -\delta x, x \rangle$. We see that $L'_\infty$ necessarily represents all the polynomials with a degree of given parity and we just need to choose $s$ such that $ds$ has this given parity.

By the choice of $s$, $sd$ is represented by $L'$ locally everywhere. Indeed, it is clearly represented at $\infty$. At all the finite place, $l$, with $(l, d') = 1$), $L_l$ is unimodular and thus universal. Finally at $d'$, the polynomial $sd$ is a unit. Since moreover $L'_\mathfrak{p}$ is unimodular, it must be isotropic and therefore, using Corollary 3.3.1 we get that $s\pi^{2u+1}$ is represented globally by $L'$, for some integer $u$, which contradicts the fact that $L$ and $L'$ have the same representation sets. ■

**Proposition 3.3.2** *Let $L$ and $L'$ be two definite ternary lattices having the same representation sets and let $d$ be their primitive discriminant. Then the adjoint lattices $\overline{L} = dL^{\#}$ and $\overline{L'} = dL'^{\#}$ have the same representation sets.*

**Proof.** Consider the forms $q$ and $q'$ associated to $L$ and $L'$ and their Gram matrices $Q$ and $Q'$. We are going to prove that an element $a \in A$ is represented by $\overline{q}$ if and only if $ad$ is represented by $q$. In matrix notation we have

$$\overline{Q} = dQ^{-1}$$

and so $a \in A$ is represented by $\overline{q}$ if and only if the matrix equation

$$^tX\overline{Q}X = a \quad \Leftrightarrow \quad d\,^tXQ^{-1}X = a$$

is solvable for some $X \in A^3$. Consider $Y = dQ^{-1}X$. Since the matrix $dQ^{-1}$ has coefficients in $A$, it follows that $Y \in A^3$. But since $Q, Q^{-1}$ and $\overline{Q}$ are symmetric, the vector $Y$ satisfies:

$$^tYQY = d^2\ {}^tX\ {}^t(Q^{-1})QQ^{-1}X = d\ {}^tX(d\ Q^{-1})X = da.$$

Conversely suppose that $^tYQY = da$ for some $Y \in A^3$ and consider $X = d^{-1}QY$. Since $Q$ is primitive, the vector $X$ is not *a priori* integral (i.e in $A^3$). At $d$, the matrix $Q$ is the matrix of a form

$$q \cong \langle 1, -\delta, \delta d\rangle$$

where $\delta \in A$ is a nonsquare modulo $d$. Since

$$q(y_1, y_2, y_3) = da \quad \Leftrightarrow \quad y_1^2 - \delta y_2^2 - \delta d y_3^2 = da$$

modulo $d$ we have $y_1^2 - \delta y_2^2 \equiv 0$ which implies that $y_1 \equiv y_2 \equiv 0$. That finally implies that $d$ must divide $QY$ and so $X = d^{-1}QY \in A^3$. Thus

$$^tX(dQ^{-1})X = d^{-1}\ {}^tY\ {}^tQQ^{-1}QY = a.$$

■

## 3.4 From Lattices to Systems

### 3.4.1 Systems Defined over Finite Fields

Here we state some properties of systems of quadratic forms defined over the finite field $\mathbb{F}_r$. We also explain how to get such a system from a definite $\mathbb{F}_r[t]$-lattice.

Let $\mathcal{S}$ be the $\mathbb{F}_r$-vector space consisting of $s$-tuples of quadratic forms in the variables $x_1, \cdots, x_v$:

$$\mathcal{S} = \{(q_1, \cdots, q_s) \ : \ q_i = q_i(x_1, \cdots, x_v)\}$$

and let $W = \mathbb{F}_r^v$ (seen as a $\mathbb{F}_r$ vector space). Let $G$ be the group of permutations of elements in $W$, so that $\#G = r^v!$.

For $S = (q_1, \cdots, q_s) \in \mathcal{S}$ and $g \in G$, it is rather clear that the map

$$(g, S) \longmapsto g \cdot S = (q_1 \circ g, \cdots, q_s \circ g)$$

defines an action of $G$ on $\mathcal{S}$. One says that $S, S' \in \mathcal{S}$ are equivalent (and we write $S \cong S'$) if $S = g \cdot S'$ for some $g \in G$.

For $S \in \mathcal{S}$, and for $\alpha = (\alpha_i) \in \mathbb{F}_r^s$ one defines the *representation numbers* of $\alpha$ by $S$ by

$$R(S, \alpha) = \#\{(\xi) \in \mathbb{F}_r^v \mid \forall i = 1, \cdots, s \ \ Q_i(\xi) = \alpha_i\}.$$

Suppose that $r = p^s$ for some $s \in \mathbb{N}$ and let $Tr$ stands for $Tr_{\mathbb{F}_r/\mathbb{F}_p}$. We define a character of $\mathbb{F}_r$ by $\psi(\beta) = \exp\left(\frac{2i\pi \ Tr(\beta)}{p}\right)$ and for any polynomial $f \in \mathbb{F}_r[x_1, \cdots, x_t]$ we let

$$M(f) = \sum_{\xi \in \mathbb{F}_r^t} \psi(f(\xi)).$$

**Theorem 3.4.1 (Carlitz, [3])** *Let $S$ and $S'$ be in $\mathcal{S}$, then the following are equivalent*

1. $S \cong S'$;

2. $R(S, \alpha) = R(S', \alpha)$ *for all* $\alpha \in \mathbb{F}_r^s$;

3. *for all* $\gamma \in \mathbb{F}_r^s$,

$$M(\gamma_1 q_1 + \cdots + \gamma_s q_s) = M(\gamma_1 q'_1 + \cdots + \gamma_s q'_s).$$

**Proof.** (1) $\Rightarrow$ (2) is clear.

Suppose that $R(S, \alpha) = R(S', \alpha)$ for all $\alpha \in \mathbb{F}_r^s$. For $\alpha \in \mathbb{F}_r^s$ take any bijection of sets from $S^{-1}(\{\alpha\})$ to $S'^{-1}(\{\alpha\})$ (that is always possible as $\#S^{-1}(\{\alpha\}) = \#S'^{-1}(\{\alpha\})$). Now, as $\alpha$ runs over $\mathbb{F}_r^s$ the sets $S^{-1}(\{\alpha\})$ (resp. $S'^{-1}(\{\alpha\})$) form a partition of $\mathbb{F}_r^v$ and therefore one can *paste* the bijection obtained in order to get a permutation of $\mathbb{F}_r^v$. That proves (2) $\Rightarrow$ (1)

In order to prove (2) $\Leftrightarrow$ (3), we just need to express the $R(S, \alpha)$ is term of the $M(\gamma_1 Q_1 + \cdots + \gamma_s Q_s)$ and conversely. This is made by the equalities:

$$R(S, \alpha) = r^{-s} \sum_{\beta \in \mathbb{F}_r^s} \psi(-\alpha_1\beta_1 - \cdots - \alpha_s\beta_s) M(\beta_1 Q_1 + \cdots + \beta_s Q_s)$$

$$M(\gamma_1 Q_1 + \cdots + \gamma_s Q_s) = \sum_{\alpha \in \mathbb{F}_r^s} \psi(\alpha_1\gamma_1 + \cdots + \alpha_s\gamma_s) R(S, \alpha).$$

■

### 3.4.2 Creation of the Systems

Let us explain how to get a system from a definite ternary $\mathbb{F}_r[t]$-lattice. Let $(L, q)$ be a ternary lattice with successive minima $\mu_1, \mu_2, \mu_3$. Let $l$ be a positive integer, and let $E_l(L) = E_l$ be the subspace of the $\mathbb{F}_r$-vector space $\mathbb{F}_r[t]$, defined by

$$E_l(L) = \{x \in L : \partial(q(x)) \leq l\}.$$

If $x$ is in $E_l$, collecting $t$ in $q(x)$ leads to

$$q(x) = Q_0(x)t^l + Q_1(x)t^{l-1} + \cdots + Q_l(x) \tag{3.6}$$

where $Q_0, \cdots, Q_l$ are quadratic forms over $\mathbb{F}_r$. The system obtained above will be denoted by $C_L^l$. It is clear that a polynomial $f = f_0t^l + \cdots + f_{l-1}t + f_l$ is represented by the quadratic form $Q$ (defined over $\mathbb{F}_r[t]$) if and only if the system

$$(Q_0(\xi), \cdots, Q_l(\xi)) = (f_0, \cdots, f_l)$$

is solvable for some $\xi \in \mathbb{F}_r^{k_1+k_2+k_3+3}$. Thus, two $\mathbb{F}_r[t]$-lattices have the same representation numbers of polynomials with degree up to $l$ if and only if their associated systems $C_L^l$ and $C_{L'}^l$ have the same representation numbers.

Let us now reformulate Theorem 3.4.1 in a way more convenient to us. To that aim, we shall need the following result.

**Lemma 3.4.1** *Let $Q \in \mathbb{F}_r[x_0, \cdots, x_s]$ be a nonsingular quadratic form, then*

$$\sum_{\xi \in \mathbb{F}_r^{s+1}} \psi(Q(\xi)) = \chi(det(Q))C^{s+1}$$

*where $\chi$ is the quadratic character of $\mathbb{F}_r$ and $C = \sum_{\alpha \in \mathbb{F}_r} \psi(\alpha^2)$ so that $|C| = r^{\frac{1}{2}}$.*

**Remark.** If $Q \in \mathbb{F}_r[x_0, \cdots, x_s]$ is singular, then it is well known that the form $Q(x_0, \cdots, x_s)$ is equivalent to a nonsingular quadratic form $Q'(y_0, \cdots, y_u)$ for some $u < s$. In this case one should have

$$\sum_{\xi \in \mathbb{F}_r^t} \psi(Q(\xi)) = r^{s-u} \sum_{\xi \in \mathbb{F}_r^{u+1}} \psi(Q'(\xi)).$$

■

If we consider Theorem 3.4.1 and Lemma 3.4.1 together, we obtain a very useful necessary condition to check if two systems of quadratic forms have the

same representation numbers. Indeed, let $\{Q_0, \cdots, Q_l\}$ and $\{Q'_0, \cdots, Q'_l\}$ be systems of quadratic forms defined over $\mathbb{F}_r$. Theorem 3.4.1 tells that they have the same representation numbers if and only if for any $\gamma_1, \cdots, \gamma_s \in \mathbb{F}_r$ one has

$$M\left(\sum_{i=1}^{s} \gamma_i Q_i\right) = M\left(\sum_{i=1}^{s} \gamma_i Q'_i\right)$$

and Lemma 3.4.1 enables to evaluate these sums. So, for any $\gamma_1, \cdots, \gamma_s \in \mathbb{F}_r$, we must have,

$$\chi \det\left(\sum_{i=1}^{s} \gamma_i Q_i\right) = \chi \det\left(\sum_{i=1}^{s} \gamma_i Q_i\right) \tag{3.7}$$

Some homogeneous polynomials representing only squares were studied in general by Dickson, who calls them *definite*. Here, we give a short proof of the following result:

**Lemma 3.4.2** *Let $F = (a, b, c)$ and $G = (a', b', c')$ be two binary quadratic forms defined over $\mathbb{F}_r$ and let $\chi$ be the quadratic character of $\mathbb{F}_r$. If $\chi \circ F = \chi \circ G$ then there is $\lambda \in \mathbb{F}_r$ such that*

$$F = \lambda^2 G.$$

**Proof.** Remember that $\chi(0) = 0$. Therefore, it is clear that if one of $F$ and $G$ is isotropic in $\mathbb{F}_r$ so is the other. By applying the same transformation to $F$ and $G$, one can suppose that $a \neq 0$. That implies in particular that $a' \neq 0$ as $0 \neq \chi(F(1,0)) = \chi(G(1,0))$. Using the same argument one sees easily that $c$ and $c'$ are simultaneously 0 or $\neq 0$. If $c = 0$ and $c' = 0$ then the result is clear.

Suppose that $c \neq 0$, $c' \neq 0$ and that both forms are isotropic. The dehomogeneized polynomials $F(x, 1)$ and $G(x, 1)$ have the same roots in $\mathbb{F}_r$ and therefore $G(x, 1)$ must be a scalar multiple of $F(x, 1)$. The scalar involved is necessarily a square in $\mathbb{F}_r$, say $\lambda^2$ and it is clear that $F = \lambda^2 G$.

Suppose now that both $F$ and $G$ are anisotropic (and therefore nonsingular). Consider the curve $E : z^2 = F(x, 1)G(x, 1)$. If $f(x) = F(x, 1)$ and $g(x) = G(x, 1)$

have common zeros in a quadratic extension of $\mathbb{F}_r$, then the result follows easily. If not, the polynomials $f$ and $g$ are relatively prime and

$$E : z^2 = f(x)g(x) \tag{3.8}$$

defines an elliptic curve. The leading coefficient of $f(x)g(x)$ is $F(0,1)G(0,1)$ and therefore is a square. Hence, in the smooth model of $E$, there are two points at $\infty$. Let $N_a$ be the number of affine solution of (3.8). Then by Riemmann Hypothesis,

$$N_a + 2 \leq r + 1 + 2\sqrt{r}.$$

On the other hand, since $f(x)g(x)$ is always a square, there are $2r$ affine solutions to (3.8); hence $N_a = 2r$. This is impossible fo $r \geq 3$.

Finally, $f$ and $g$ are not coprime and the lemma follows easily.

■

### 3.4.3 Explicit Computation of the Systems

Let $L$ be a ternary lattice with successive minimum $\mu_1 = n, \mu_2 = m$ and $\mu_3 = l$. For simplicity, suppose that $n \equiv l \mod 2$ and define

$$k_1 = \left[\frac{l-n}{2}\right] \quad \text{and} \quad k_2 = \left[\frac{l-m}{2}\right]$$

where $[\cdot]$ denotes the maximum of the integral part and 0. Consider the representation set (with multiplicity) of $L$ and intersect the set found with the set of polynomials of degree at most $l$. Since the $L$ is definite, Theorem 1.2.2 implies that the intersection obtained is exactly

$$\{q(h,g,s) \mid \partial(h) \leq k_1, \quad \partial(g) \leq k_2 \text{ and } s \in \mathbb{F}_r\}.$$

Let $E_l$ be the subspace of the $\mathbb{F}_r$-vector space $\mathbb{F}_r[t]$ defined by

$$E_l = \{(h,g,s) \in \mathbb{F}_r[t] : \partial(h) \leq k_1, \quad \partial(g) \leq k_2 \text{ and } s \in \mathbb{F}_r\}.$$

For any $(h, g, s) \in E_l$ with

$$h = h_{k_1} t^{k_1} + \cdots + h_0$$

$$g = g_{k_2} t^{k_2} + \cdots + g_0$$

$$s = s_{k_3} t^{k_3} + \cdots + s_0$$

let $\widetilde{X} = (h_{k_1}, \cdots, h_0, g_{k_2}, \cdots, g_0, s_{k_3}, \cdots, s_0)$. If $(h, g, s)$ is in $E_l$, collecting $t$ in $q(h, g, s)$ leads to

$$q(h, g, m) = Q_0(\widetilde{X}) t^l + Q_1(\widetilde{X}) t^{l-1} + \cdots + Q_l(\widetilde{X}) \tag{3.9}$$

where $Q_0, \cdots, Q_l$ are quadratic forms over $\mathbb{F}_r$.

Suppose that

$$q = \begin{pmatrix} a & b & e \\ b & c & f \\ e & f & d \end{pmatrix}$$

where

$$a = t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$$

$$b = b_{n-1} t^{n-1} + \cdots + b_1 t + b_0, \quad \text{where } b_{n-1}, b_{n-2}, \cdots \text{ are possibly } 0$$

$$c = c_m t^m + c_{m-1} t^{m-1} + \cdots + c_1 t + c_0$$

$$d = -\delta t^l + d_{l-1} t^{l-1} + \cdots + d_0$$

$$e = e_{n-1} t^{n-1} + \cdots + e_1 t + e_0$$

$$f = f_{m-1} t^{m-1} + \cdots + f_1 t + f_0$$

We can find the shape of the matrix $Q_j$ in the variables $\widetilde{X}$. We have

$$Q_0 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & -\delta \end{pmatrix}$$

and more generally, by taking for convention that for a polynomial $s$, we have $s_i = 0$ whenever $i > \partial(s)$, we get:

$$Q_j = \begin{pmatrix} a_{n-j} & \cdots & a_{n-j+k_1} & b_u & \cdots & b_{u+k_2+1} & e_v \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-j+k_1} & \cdots & a_{n-j+2k_1} & b_{u+k_1} & \cdots & b_{u+k_2+k_1} & e_{v+k_1} \\ b_u & \cdots & b_{u+k_1} & c_{m-j} & \cdots & c_{m-j+k_2} & f_w \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{u+k_2+1} & \cdots & b_{u+k_2+k_1} & c_{m-j+k_2} & \cdots & c_{m-j+2k_2} & f_{w+k_2} \\ e_v & \cdots & e_{v+k_1} & f_w & \cdots & f_{w+k_2} & d_{l-j} \end{pmatrix}.$$

In particular, we can write the Gram matrix of the quadratic form with coefficients in $\mathbb{F}_r[x_0, x_1, \cdots, x_l]$ given by $F = \sum_{i=0}^{l} x_i Q_i$. We get

$$F = \begin{pmatrix} a_{(0)} & \cdots & a_{(k_1-1)} & b_{(\rho)} & \cdots & b_{(\rho+k_2)} & e_{(\sigma)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{(k_1-1)} & \cdots & a_{(2k_1)} & b_{(\rho+k_1)} & \cdots & b_{(\rho+k_2+k_1)} & e_{(\sigma+k_1)} \\ b_{(\rho)} & \cdots & b_{(\rho+k_1)} & c_{(1)} & \cdots & c_{(k_2)} & f_{(\tau)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{(\rho+k_2)} & \cdots & b_{(\rho+k_2+k_1)} & c_{(k_2)} & \cdots & c_{(2k_2+1)} & f_{(\tau+k_2)} \\ e_{(\sigma)} & \cdots & e_{(\sigma+k_1)} & f_{(\tau)} & \cdots & f_{(\tau+k_2)} & d_{(0)} \end{pmatrix} \tag{3.10}$$

where $\rho = \mu_3 - \partial(b) - k_1 - k_2$, $\sigma = \mu_3 - \partial(e) - k_1$, $\tau = \mu_3 - \partial(f) - k_2$ and, for a polynomial $g(x) = g_s t^s + g_{s-1} t^{s-1} + \cdots + g_0$ we define

$$g_{(j)} = \begin{cases} g_s x_j + g_{s-1} x_{j+1} + \cdots + g_0 x_{j+s} & \text{if } \ j \leq s \\ 0 & \text{if } \ j > s \end{cases}.$$

For example if $g(t) = g_2 t^2 + g_1 t + g_0$ then $g_{(3)} = g_2 x_3 + g_1 x_4 + g_0 x_5$.

## 3.5 Classification of Binary Pencils

A *pencil of quadratic forms* over a finite field, $\mathbb{F}_r$, is a finite dimensional $\mathbb{F}_r$-vector space of quadratic forms. The dimension of a pencil $\mathcal{P}$ is the dimension of the $\mathbb{F}_r$-vector space $\mathcal{P}$. The rank of a pencil $\mathcal{P}$ is the maximal rank of an element of $\mathcal{P}$. A pencil of rank 2 is called a binary pencil.

Let $\mathcal{P}$ and $\mathcal{P}'$ be pencils of ranks $k = k'$. These are said to be *equivalent* if there exists an invertible transformation $\varphi \in GL_k(\mathbb{F}_r)$ such that $\mathcal{P} \circ \varphi = \mathcal{P}'$.

The goal of this section is to apply the previous results to binary pencils in order to find some invariants.

**Proposition 3.5.1** *Let $\{Q_i\}_{i=1}^n$ and $\{Q'_i\}_{i=1}^n$ be sets of binary quadratic forms defined over $\mathbb{F}_r$ each of which contains at least one form that is anisotropic. Suppose that*

$$Q_i = \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix} \quad \text{and} \quad Q'_i = \begin{pmatrix} a'_i & b'_i \\ b'_i & c'_i \end{pmatrix}.$$

*Then, there exist $\phi \in GL_2(\mathbb{F}_r)$ such that for all $i$, $Q_i \circ \phi = Q'_i$ if and only if the following conditions hold:*

1. *the following equality holds in $\mathbb{F}_r[x_1, \cdots, x_n]$:*

$$\det\left(\sum_{i=1}^n x_i Q_i\right) = \det\left(\sum_{i=1}^n x_i Q'_i\right)$$

2. *for any $(x_1, \cdots, x_n) \in \mathbb{F}_r^n$ such that $\sum_{i=1}^n x_i Q_i$ is degenerate, the sets*

$$\left\{\chi\left(\sum_{i=1}^n x_i a_i\right), \chi\left(\sum_{i=1}^n x_i c_i\right)\right\} \quad \text{and} \quad \left\{\chi\left(\sum_{i=1}^n x_i a'_i\right), \chi\left(\sum_{i=1}^n x_i c'_i\right)\right\}$$

*are equal.*

**Proof.** We can suppose without loss of generality that $Q_1 = Q'_1 = \begin{pmatrix} 1 & 0 \\ 0 & -\delta \end{pmatrix}$. We see that $q = \sum_{i=1}^n Q_i t^{n-i-1}$ and $q' = \sum_{i=1}^n Q'_i t^{n-i-1}$ are some binary definite quadratic forms defined over $\mathbb{F}_r[t]$, with $\mu_1 = \mu_2 = n - 1$. By construction $\{Q_i\}$ and $\{Q'_i\}$ are their systems.

Conditions (1) and (2) in the proposition may be translated as the fact that for all $x_1, \cdots, x_n \in \mathbb{F}_r^n$,

$$M\left(\sum x_i Q_i\right) = M\left(\sum x_i Q'_i\right).$$

So by Theorem 3.4.1, we see that (1) and (2) are satisfied if and only if $q$ and $q'$ have the same representation numbers for polynomials of degree at most $n-1$. One will also notice that the pencils $\mathcal{P}$ and $\mathcal{P}'$ are equivalent if and only if $q$ and $q'$ are integrally equivalent.

Now, it is clear that two equivalent $\mathbb{F}_r[t]$-lattices have the same representation numbers. Hence, to conclude we just need to prove that binary forms having the same minima structure as $q$ and $q'$ and having the same representation numbers for polynomials of degree smaller than $n-1$ are equivalent.

We write $q = (a, 2b, c)$ and $q' = (a', 2b', c')$. Since $q$ and $q'$ are supposed to have the same representation numbers, there is no loss of generality in making the following assumptions: $a = a'$ is monic and the leading coefficients of $c$ and $c'$ are the same, say $-\delta$. With this assumption,

$$Q_i = (a_i, b_i, c_i) \quad \text{and} \quad Q'_i = (a_i, b'_i, c'_i).$$

Now, Theorem 3.4.1 tells that for all $x_1, x_2 \in \mathbb{F}_r$ and for all $i, j = 1, \cdots, \mu_2$ one must have

$$M(x_1 Q_i + x_2 Q_j) = M(x_1 Q'_i + x_2 Q'_j).$$

These are just Gauss sums and Lemma 3.4.1 enables us to evaluate them. In particular, for $i = 1$, we see that for all $x_1, x_2 \in \mathbb{F}_r$ and for all $j = 2, \cdots, \mu_2$ we must have

$$\chi(\det(x_1 q_1 + x_2 q_j)) = \chi(\det(x_1 q_1 + x_2 q'_j)).$$

But,

$$\det(x_1 q_1 + x_2 q_j) = -\delta x_1^2 + (-\delta a_k + c_k) x_1 x_2 + (a_k c_k - b_k^2) x_2^2.$$

Lemma 3.4.2 now implies that

$$(-\delta a_k + c_k) = (-\delta a_k + c'_k) \ \text{ and } \ (a_k c_k - b_k^2) = (a_k c'_k - b'^2_k).$$

So for all $k = 1, \cdots, \mu_2$, we have $c_k = c'_k$ and $b_k^2 = b'^2_k$. Thus $c = c'$ and for all $k$, $b_k = \pm b'_k$. Suppose that there are $i, j$ such that $b_i = b'_i$ and $b_j = -b'_j$ so

that $q_i = q_i' = (a_i, b_i, c_i)$ and $q_j = (a_j, b_j, c_j) \neq (a_j, -b_j, c_j) = q_j'$ and apply the reasoning above to the pair of quadratic forms $(q_i, q_j)$. Again we should get for all $x_1, x_2$,

$$\chi(\det(x_1 Q_i + x_2 Q_j)) = \chi(\det(x_1 Q_i + x_2 Q_j'))$$

which would lead, again by the corollary to Lemma 3.4.2, to

$$a_i c_j + a_j c_i - 2b_i b_j = a_i c_j + a_j c_i + 2b_i b_j \quad \text{(i.e. } b_i b_j = 0\text{)}.$$

■

**Corollary 3.5.1** *Let $q$ be a definite binary form over $\mathbb{F}_r[t]$. Suppose that $\mu_1(q) = \mu_2(q) = 1$, then $q$ has class number one.*

**Proof.** Let $q$ and $q'$ be binary forms with $\mu_1 = \mu_2 = 1$ and suppose that $q$ and $q'$ are in the same genus. The discriminant is an invariant of the genus; hence $\text{disc}(q) = \text{disc}(q')$. Since $\partial(\text{disc}(q)) = 2$, we see that condition (1) of Proposition 3.5.1 is satisfied. If $\text{disc}(q)$ is irreducible, then condition (2) is also satisfied and we are done. Suppose therefore that $\text{disc}(q) = -\delta \mathfrak{p}_1 \mathfrak{p}_2$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are some linear primes (i.e. monic linear polynomials). Suppose also that $\mathfrak{p}_i(t) = t - \alpha_i$, for $i = 1, 2$. We can suppose without loss of generality that $q = Q_0 t + Q_1$ (resp. $q' = Q_0 t + Q_1'$) where

$$Q_0 = (1, -\delta), \quad Q_1 = (a, 2b, c) \quad \text{and} \quad Q_1' = (a', 2b', c').$$

One will notice first that at least one of $t + a$ or $-\delta t + c$ and one of $t + a'$, $-\delta t + c'$ is coprime to $\mathfrak{p}_1$. Since $q$ and $q'$ are in the same genus, we get:

$$\left(\frac{t+a}{\mathfrak{p}_1}\right) = \left(\frac{t+a'}{\mathfrak{p}_1}\right) \quad \text{(i.e. } \chi(\alpha_1 + a) = \chi(\alpha_1 + a'))\,.$$

■

# Chapter 4

# Isospectral Quadratic Forms

## 4.1 Preliminaries

**Definition.** Let $L$ be a definite $\mathbb{F}_r[t]$-lattice with reduced basis $(e_1, \cdots, e_n)$. For $k \leq n$, a $k \times k$-section of $L$ is denoted $L^{k\times k}$ and is defined to be the lattice spanned by $(e_1, \cdots, e_k)$. ■

**Lemma 4.1.1** *Let $(L, Q)$ and $(L', Q')$ be two isospectral definite ternary $\mathbb{F}_r[t]$-lattices with successive minima $\mu_1, \mu_2, \mu_3$. If $\mu_2 \neq \mu_3$, $L^{2\times 2}$ and $L'^{2\times 2}$ are isometric.*

**Proof.** If $L$ is a ternary lattice with successive minima $(\mu_1, \mu_2, \mu_3)$, $\overline{L}$ will stand for its adjoint and $(\nu_1, \nu_2, \nu_3)$ for the successive minima of $\overline{L}$.

Since $L$ and $L'$ are isospectral, so are $\overline{L}$ and $\overline{L'}$ (Corollary 3.2.1). Since $\mu_2 < \mu_3$, we see that $\nu_1 < \nu_2$. In particular the minimal representation of $\overline{L}$ and $\overline{L'}$ are unique up to multiplication by a square of $\mathbb{F}_r^\times$. By isospectrality, these representations must be equal (up to multiplication by a square in $\mathbb{F}_r^\times$).

It is easy to see that the minimal representation of $\overline{L}$ (resp. $\overline{L'}$) is $\mathrm{disc}(L^{2\times 2})$ (resp. $\mathrm{disc}(L'^{2\times 2})$). Thus we see that $L^{2\times 2}$ and $L'^{2\times 2}$ have essentially the same discriminant.

Now, as $\mu_2 < \mu_3$, it is clear that $V_{\mu_2}(L^{2\times 2}) = V_{\mu_2}(L'^{2\times 2})$. One these facts noticed, Theorem 2.1.2 enables to conclude. ■

Let $L$ be a definite ternary lattice. Remember that $k_1 = \frac{\mu_3-\mu_1}{2}$ and $k_2 = \frac{\mu_3-\mu_2-1}{2}$. Let $l = \mu_3$ and let $(h, g, \xi) \in E_l$. We use here the explicit computation of the system made in section 3.4.3. Consider an integer $N$ such that $N \geq k_1 + 1$ and define

$$\mathcal{Q}(x_1, \cdots, x_N) = \sum_{i=0}^{N} x_i Q_i$$

where $\{Q_i\}_{i=0}^{l}$ is the system associated to $L$. As computed before (cf. equation (3.10)), the matrix of $\mathcal{Q}(x_1, \cdots, x_n)$ is the following

$$\begin{pmatrix} a_{(0)} & \cdots & a_{(k_1-1)} & b_{(\rho)} & \cdots & b_{(\rho+k_2)} & e_{(\sigma)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{(k_1-1)} & \cdots & a_{(2k_1)} & b_{(\rho+k_1)} & \cdots & b_{(\rho+k_2+k_1)} & e_{(\sigma+k_1)} \\ b_{(\rho)} & \cdots & b_{(\rho+k_1)} & c_{(1)} & \cdots & c_{(k_2)} & f_{(\tau)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{(\rho+k_2)} & \cdots & b_{(\rho+k_2+k_1)} & c_{(k_2)} & \cdots & c_{(2k_2+1)} & f_{(\tau+k_2)} \\ e_{(\sigma)} & \cdots & e_{(\sigma+k_1)} & f_{(\tau)} & \cdots & f_{(\tau+k_2)} & d_{(0)} \end{pmatrix} \tag{4.1}$$

where $\rho = \mu_3 - \partial(b) - k_1 - k_2$, $\sigma = \mu_3 - \partial(e) - k_1$ and $\tau = \mu_3 - \partial(f) - k_2$.

Suppose that for a polynomial $p$ we have $p_{(j)} = 0$ whenever $j > N$ and consider the form $\widetilde{\mathcal{Q}} = \mathcal{Q}|_{E_{l-1}}$. It is easy to see that the Gram matrix of $\widetilde{\mathcal{Q}}$ is just the Gram matrix of $\mathcal{Q}$ from which the first and last rows and columns have be removed. For the sake of clarity we write $\widetilde{\mathcal{Q}}$ as a block matrix:

$$\begin{pmatrix} A_0 & A_1 & B_0 & B_1 \\ {}^tA_1 & A_2 & B_2 & B_3 \\ {}^tB_0 & {}^tB_2 & C_0 & C_1 \\ {}^tB_1 & {}^tB_3 & {}^tC_1 & C_2 \end{pmatrix} \tag{4.2}$$

which can be replaced by the equivalent matrix obtained by permutation:

$$\begin{pmatrix} A_0 & B_0 & A_1 & B_1 \\ {}^tB_0 & C_0 & {}^tB_2 & {}^tC_1 \\ {}^tA_1 & B_2 & A_2 & B_3 \\ {}^tB_1 & C_1 & {}^tB_3 & C_2 \end{pmatrix} \tag{4.3}$$

Let $s_1 = \min\{0, 2k_1 - N\}$, $s_2 = \min\{0, 2k_2 - N\}$, $\rho_1 = k_1 - \varphi_1 - 1$ and $\rho_2 = k_2 - \varphi_2$. With this notation we see that $A_0$ is a matrix of dimension $\rho_1 \times \rho_1$ and $C_0$ is a matrix of dimension $\rho_2 \times \rho_2$. We have

$$A_0 = \begin{pmatrix} a_{(2)} & \cdots & a_{(\rho_1)} \\ \vdots & \ddots & \vdots \\ a^{(\rho_1)} & \cdots & a^{(2\rho_1)} \end{pmatrix}, \quad C_0 = \begin{pmatrix} c_{(1)} & \cdots & c_{(\rho_2+1)} \\ \vdots & \ddots & \vdots \\ c_{(\rho_2+1)} & \cdots & c_{(2\rho_2+1)} \end{pmatrix}.$$

$A_1$ is a matrix of dimension $(\rho_1) \times (2k_1 - s_1)$ and $C_1$ is a matrix of dimension $(\rho_2) \times (2k_2 - s_2)$. We have

$$A_1 = \begin{pmatrix} a_{(\rho_1+1)} & \cdots & a_{(k_1+1)} \\ \vdots & \ddots & \vdots \\ a_{(2\rho_1+1)} & \cdots & a_{(N-1)} \end{pmatrix}, \quad C_1 = \begin{pmatrix} c_{(\rho_2+2)} & \cdots & c_{(k_2)} \\ \vdots & \ddots & \vdots \\ c_{(2\rho_2+1)} & \cdots & c_{(N-1)} \end{pmatrix}.$$

$A_2$ is a matrix of dimension $(2k_1 - s_1) \times (2k_1 - s_1)$ and if $N \leq 2k_1$, it looks like

$$A_2 = \begin{pmatrix} a_{(2\rho_1+2)} & \cdots & a_{(N-1)} & 1 \\ \vdots & \iddots & \iddots & 0 \\ a_{(N-1)} & 1 & \iddots & \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

$C_2$ is a matrix of dimension $(2k_2 - s_2) \times (2k_2 - s_2)$ and if $N \leq 2k_2$, it looks like

$$C_2 = \begin{pmatrix} c_{(2\rho_2+3)} & \cdots & c_{(N-1)} & 1 \\ \vdots & \iddots & \iddots & 0 \\ c_{(N-1)} & 1 & \iddots & \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

Now $B_0$, $B_1$, $B_2$ and $B_3$ are some matrix of dimension respectively $\rho_1 \times \rho_2$, $\rho_1 \times (2k_2 - s_2)$, $(2k_1 - s_1) \times \rho_2$ and $(2k_1 - s_1) \times (2k_2 - s_2)$. If the matrix exists (depending on the dimension), the smallest subscript appearing

1. in $B_0$ is $n + 1 = \mu_3 - \partial(b) - k_1 - k_2 + 1$;

2. in $B_1$ is $n+1+N-k_2$;

3. in $B_2$ is $n+1+N-k_1$; and

4. in $B_3$ is $n+1+2N-k_1-k_2$.

Note that one can always recover all the coefficients from the coefficient with the smallest subscript which necessarily appears on the top left corner of the matrix.

**Lemma 4.1.2** *The quadratic form whose Gram matrix is given by*

$$M = \begin{pmatrix} A_2 & B_3 \\ {}^tB_3 & C_2 \end{pmatrix}$$

*is non degenerate. More precisely one has* $\det(M) = 1$.

**Proof.** It is clear that the statement can only be considered when $N \leq 2k_1$. We first prove that the last row and column of $B_3$ is identically 0. To that aim, remember that $b_j = 0$ whenever $j > N$. Also by symmetry and since $B_3$ has more rows than it has columns we just need to prove that the last column of $B_3$ is identically 0. The smallest subscript on this column is the one appearing on the top of the column and is

$$\begin{aligned}(n+1+2N-k_1-k_2)+s_2 &\geq (n+2N-k_1-k_2)+2k_2-N \\ &= n+1+N-k_1+k_2 \\ &= \mu_3-\partial(b)-k_1-k_2+N-k_1+k_2 \\ &= \mu_3-2k_1-\partial(b)+N \\ &= \mu_1-\partial(b)+N > N\end{aligned}$$

In particular, we can expand $\det M$ through the first row of $M$ and the last column of $A_2$, through the first column of $M$ and le the last row of $A_2$, through the first row of $C_2$ and the last column of $M$ and finally through the last row of

$M$ and the first column of $C_2$. After these expansions we obtain a new matrix having the very same shape as $M$ and we can conclude by induction. ■

**Lemma 4.1.3** *Consider the matrix* $M_1 = \begin{pmatrix} A_1 & B_1 \end{pmatrix}$. *On a given row of* $M_1$, *the smallest subscript is strictly bigger than subscript of the coefficient on the diagonal of* $A_0$ *which is on the same row.*

**Proof.** It is clear that the subscript of any coefficients on a row of $A_1$ is strictly bigger than the subscript of the diagonal coefficient in $A_0$ on the same line. Let us prove that for $B_1$. Remember that $B_1$ has $N - k_1$ rows and choose $j$ such that $0 \leq j \leq N - k_1$. We have

$$\begin{aligned} N - k_1 < N - k_2 + (n-1) &\Rightarrow j + 2 < N - k_2 + n + 1 \\ &\Rightarrow 2(j+1) < n + N - k_2 + j + 1 \end{aligned}$$

On the last inequality the left hand side is the subscript of the coefficient on the diagonal and on the $j^{th}$ row. The one on the right hand side is the smallest subscript on in $j^{th}$ row of $B_1$. ■

**Lemma 4.1.4** *Consider the matrix* $M_2 = \begin{pmatrix} {}^tB_2 & {}^tC_1 \end{pmatrix}$. *On a given row of* $M_2$, *the smallest subscript is strictly bigger than subscript of the coefficient on the diagonal of* $C_0$ *which is on the same row. Equivalently let*

$${}^tM_2 = \begin{pmatrix} B_2 \\ C_1 \end{pmatrix}.$$

*On a given column of* ${}^tM_2$, *the smallest subscript is strictly bigger than subscript of the coefficient on the diagonal of* $C_0$ *which is on the same column.*

**Proof.** It is clear that the subscript of any coefficients on a column of $C_1$ is strictly bigger than the subscript of the diagonal coefficient in $C_0$ on the same column. Let us prove that for $B_2$. Remember that $B_2$ has $N - k_2$ columns and choose $j$ such that $0 \leq j \leq N - k_2$. We have

$$\begin{aligned} N - k_2 < N - k_2 + n \Rightarrow j &< N - k_2 + n \\ \Rightarrow 1 + 2j &< N - k_2 + n + j + 1 \end{aligned}$$

On the last inequality the left hand side is the subscript of the coefficient on the diagonal and on the $j^{th}$ column. The one on the right hand side is the smallest subscript on in $j^{th}$ column of $B_2$. ■

Let $\Omega_0 = \begin{pmatrix} A_0 & B_0 \\ {}^tB_0 & C_0 \end{pmatrix}$, $\Omega_1 = \begin{pmatrix} A_1 & B_1 \\ {}^tB_2 & {}^tC_1 \end{pmatrix}$ and as above let $M = \begin{pmatrix} A_2 & B_3 \\ {}^tB_3 & C_2 \end{pmatrix}$. By Lemma 4.1.2, we know that $M$ is not degenerate and hence, there exist a transformation $\varphi$ such that ${}^t\varphi M \varphi$ is diagonal. Let us apply

$$\Phi = \begin{pmatrix} Id & 0 \\ 0 & \varphi \end{pmatrix}$$

to the form $\Delta = \begin{pmatrix} \Omega_0 & \Omega_1 \\ {}^t\Omega_1 & M \end{pmatrix}$, in order to get

$${}^t\Phi \begin{pmatrix} \Omega_0 & \Omega_1 \\ {}^t\Omega_1 & M \end{pmatrix} \Phi = \begin{pmatrix} \Omega_0 & \Omega_1\varphi \\ {}^t(\Omega_1\varphi) & {}^t\varphi M \varphi \end{pmatrix}.$$

One will notice that $\Omega_1\varphi$ is a matrix that is obtained by replacing a given coefficient by a linear combination of coefficients on the same line.

Now, we complete the squares in ${}^t\varphi M \varphi$. That has for effect to *integrate* the nonzero coefficients of $\Omega_1\varphi$ in the diagonal of ${}^t\varphi M \varphi$. We nevertheless have to remove the parasite terms that this process will create in the matrix $\Omega_0$. That leaves us with

$$\begin{pmatrix} \Omega - \Omega_0' & 0 \\ 0 & {}^t\varphi M \varphi \end{pmatrix}$$

where $\Omega_0'$ *corrects* the squares and the mixed products in $\Omega_0$. Note that the coefficient on the $i^{th}$ row and $j^{th}$ column of $\Omega_0'$ is a linear combination of the

products of terms appearing on the $i^{th}$ and $j^{th}$ rows of $\Omega_1\varphi$. In particular Lemma 4.1.2 and 4.1.3 implies that for any $i, j$ the subscript in $(\Omega_0 - \Omega_0')_{ij}$ is strictly bigger than the smallest subscript in $\{(\Omega_0 - \Omega_0')_{ii}, (\Omega_0 - \Omega_0')_{jj}\}$.

Let $W = \Omega_0 - \Omega_0' = (\omega^{ij})$ and suppose $dim(W) = s$. If need be, we can permute the vectors of the basis in which $W$ is written to make sure that the subscripts on its diagonal appear by increasing order. Let us explain this change of basis in more details. Suppose that $k_i$ is the smallest subscript appearing in $\omega^{ii}$, that is $\omega^{ii}$ is written either $a_{(k_i)}+$bigger subscripts or $c_{(k_i)}+$bigger subscripts. After the change of basis, we will have

$$k_1 \leq k_2 \leq \cdots \leq k_s.$$

Now, $k_s$ is the largest subscript on the diagonal of $W$. Choose $x_{k_s}$ such that $w^{ss} \neq 0$ and complete the squares. It has for effect to subtract on the diagonal of $W$ some coefficients of the same row and to the right of this diagonal. In particular the quantity subtracted will always have a strictly bigger subscript than the one on the diagonal. Choose $x_{k_{s-1}}$ such that $w^{(s-1)(s-1)} \neq 0$ and complete the squares. Continue this process until $W$ is diagonal. We have proved:

**Theorem 4.1.1** *There are some non degenerate forms in the pencil*

$$\{\widetilde{Q_1}, \cdots, \widetilde{Q_N}\}.$$

*Furthermore let* $s = \max\{2\rho_2 + 3, 2\rho_2 + 1\}$. *To get a non degenerate form of the type*

$$x_1\widetilde{Q_1} + \cdots + x_N\widetilde{Q_N}$$

*one can choose freely* $x_s, \cdots, x_N$. *Also one has* $r-1$ *choices for* $x_{s-1}, \cdots, x_1$*; the possible choices for* $x_m$ *depend on the choices made for* $x_n$, $n > m$.

## 4.2 The Ternary Case

### 4.2.1 Statement of the Theorem

We are now in position of stating the principal theorem of this paper and we shall prove it in the next subsections.

**Theorem 4.2.1** *Let $(L, Q)$ and $(L', Q')$ be two definite ternary $\mathbb{F}_r[t]$-lattices. If $L$ and $L'$ are isospectral, they are integrally equivalent.*

Since $L$ and $L'$ are isospectral, their sequences of successive minima are equal, say it is $(\mu_1, \mu_2, \mu_3)$ (cf. Lemma 2.1.1). Also, we shall suppose that $\mathrm{disc}(L) = \mathrm{disc}(L')$ (not only $\mathrm{disc}(L) = \mathrm{disc}(L') \mod \mathbb{F}_r^{\times 2}$).

By Corollary 3.2.1, we can consider $\overline{L}$ (resp. $\overline{L'}$) instead of $L$ (resp. $L'$). In particular, there is no loss of generality in supposing that successive minima have one of the following configurations:

1. $\mu_1 \equiv \mu_2 \mod 2$; hence $\mu_1 \not\equiv \mu_3 \mod 2$ and $\mu_2 \not\equiv \mu_3 \mod 2$; or
2. $\mu_1 \equiv \mu_3 \mod 2$; hence $\mu_1 \not\equiv \mu_2 \mod 2$ and $\mu_2 \not\equiv \mu_3 \mod 2$;

In both of these cases, we see that $\mu_2 \neq \mu_3$. Thus, Lemma 4.1.1 applies and we shall suppose in the following that $L$ and $L'$ have isometric $2 \times 2$ sections. In other words, we shall suppose that $Q$ and $Q'$ are given by the following reduced Gram matrices

$$Q = \begin{pmatrix} a & b & e \\ b & c & f \\ e & f & d \end{pmatrix}; \quad Q' = \begin{pmatrix} a & b & e' \\ b & c & f' \\ e' & f' & d' \end{pmatrix} \tag{4.4}$$

where $\partial(c) < \partial(d) = \partial(d')$. For the sake of clarity, we shall break the proof in two parts. We first prove the theorem when $\mu_1 \equiv \mu_3 \mod 2$ and then we prove it when $\mu_1 \equiv \mu_2 \mod 2$.

### 4.2.2 Proof of Theorem 4.2.1 when $\mu_1 \equiv \mu_3 \mod 2$

We use the notations introduced in the previous subsection. Also, we suppose that $r \neq 3$. We are going to prove that the Gram matrices $Q$ and $Q'$ of $L$ and $L'$ must be equal. Lemma 4.1.1 already tells us that the $2 \times 2$ submatrix on the top left corner are equal. We now use the systems defined above to show that the three remaining coefficients must also be equal. Let $d, e, f$ and $d', e', f'$ be these coefficients (as in (4.4)) and suppose that $e = e_s t^s + \cdots + e_0, e' = e'_s t^s + \cdots + e'_0$. We prove that

1. By working with the $2 \times 2$ sections of the adjoints, we prove that
   - $\partial(f - f') < \partial(e - e')$
   - $\partial(d - d') < \partial(e - e')$.
2. By working with systems of quadratic forms defined over $\mathbb{F}_r$, we prove that
   - $[\forall i \in \{k, \cdots, s\},\ e_i = e'_i] \ \Rightarrow \ e_{k-1} = e'_{k-1}$
   - $Q$ and $Q'$ are isospectral $\Rightarrow \ e_s = e'_s$.

**Lemma 4.2.1** *Suppose that $\partial(e) = s$ and let $N$ be an integer such that $N > \mu_3 - s - k_1$. Let $u = \mu_3 - N$ and suppose that $e_i = e'_i$ for all $i$ such that $u < i \leq s$. Suppose further that $\partial(f - f') + k_2 < u + k_1$ and $\partial(d - d') < u + k_1$. If $Q$ and $Q'$ are isospectral then $e_u = e'_u$.*

**Proof.** First we see that the first coefficient of $e$ appears in $Q_{\mu_3 - \partial(e) - k_1}$. Since the form is reduced we know that $\partial(e) < \partial(a)$. Using this fact it is easily proved that $\mu_3 - \partial(e) - k_1 > k_1$.

Now, consider forms in the pencil generated by $\{Q_0, \cdots, Q_N\}$. It is easy to see that the Gram matrix of forms

$$\mathcal{Q}(x_0, \cdots, x_N) = \sum_{i=0}^{N} x_i Q_i, \quad \text{and} \quad \mathcal{Q}'(x_0, \cdots, x_N) = \sum_{i=0}^{N-1} x_i Q_i + x_n Q'_N$$

may be written as a block matrices

$$\mathcal{Q} = \begin{pmatrix} a^0 & e^\rho & \widetilde{A_0} & \widetilde{B_0} & \widetilde{A_1} & \widetilde{B_1} \\ e^\rho & d^0 & {}^tE_0 & {}^tF_0 & {}^tE_1 & {}^tF_1 \\ {}^t\widetilde{A_0} & E_0 & A_0 & B_0 & A_1 & B_1 \\ {}^t\widetilde{B_0} & F_0 & {}^tB_0 & C_0 & {}^tB_2 & {}^tC_1 \\ {}^t\widetilde{A_1} & E_1 & {}^tA_1 & B_2 & A_2 & B_3 \\ {}^t\widetilde{B_1} & F_1 & {}^tB_1 & C_1 & {}^tB_3 & C_2 \end{pmatrix} \text{and} \mathcal{Q}' = \begin{pmatrix} a^0 & e'^\rho & \widetilde{A_0} & \widetilde{B_0} & \widetilde{A_1} & \widetilde{B_1} \\ e'^\rho & d^0 & {}^tE_0 & {}^tF_0 & {}^tE_1 & {}^tF_1 \\ {}^t\widetilde{A_0} & E_0 & A_0 & B_0 & A_1 & B_1 \\ {}^t\widetilde{B_0} & F_0 & {}^tB_0 & C_0 & {}^tB_2 & {}^tC_1 \\ {}^t\widetilde{A_1} & E_1 & {}^tA_1 & B_2 & A_2 & B_3 \\ {}^t\widetilde{B_1} & F_1 & {}^tB_1 & C_1 & {}^tB_3 & C_2 \end{pmatrix}$$

where $A_0, A_1, A_2, B_0, B_1, B_2, C_0, C_1, C_2$ are the same as defined previously and

1. $\widetilde{A_0} = [a_{(1)}, \cdots, a_{(N-k_1+1)}]$
2. $\widetilde{A_1} = [a_{(N-k_1+2)}, \cdots, a_{(k_1)}]$
3. $\widetilde{B_0} = [b_{(n)}, \cdots, b_{(n+N-k_2)}]$
4. $\widetilde{B_1} = [b_{(n+N-k_2+1)}, \cdots, b_{(n+k_2+1)}]$
5. ${}^tE_0 = [e_{(\rho+1)}, \cdots, e_{(\rho+1+N-k_1)}]$, with $\rho = \mu_3 - \partial(e) - k_1$
6. ${}^tE_1 = [e_{(\rho+N-k_1+2)}, \cdots, e_{(\rho+k_1+2)}]$
7. ${}^tF_0 = [f_{(\eta)}, \cdots, f_{(\eta+N-k_2)}]$, with $\eta = \mu_3 - \partial(f) - k_2$
8. ${}^tF_1 = [f_{(\eta+N-k_2+1)}, \cdots, f_{(\eta+k_2+1)}]$
9. $e^\rho = e_s x_\rho + e_{s-1} x_{\rho+1} + \cdots + e_{u-1} x_{N-1} + e_u x_N$
10. $e'^\rho = e_s x_\rho + e_{s-1} x_{\rho+1} + \cdots + e_{u-1} x_{N-1} + e'_u x_N$

Let us *complete the squares* as we did to prove Theorem 4.1.1. When completing the squares in $\begin{pmatrix} A_2 & B_3 \\ {}^tB_3 & C_2 \end{pmatrix}$ we will have to *correct* on one hand the form

$\begin{pmatrix} A_0 & B_0 \\ {}^tB_0 & C_0 \end{pmatrix}$ (that is exactly what we did to prove Theorem 4.1.1). On the other hand we also have to *correct* the form $\begin{pmatrix} a_{(0)} & e_{(\rho)} \\ e_{(\rho)} & d_{(0)} \end{pmatrix}$. We will subtract in this form some squares and mixed products that come from the product of coefficients in $\begin{pmatrix} \widetilde{A_1} & \widetilde{B_1} \end{pmatrix}$ times coefficients in $\begin{pmatrix} {}^tE_1 & {}^tF_1 \end{pmatrix}$.

Remember that the smallest subscript in $\begin{pmatrix} \widetilde{A_1} & \widetilde{B_1} \end{pmatrix}$ is $N - k_1 + 2 = \sigma_1$ and the one in $\begin{pmatrix} {}^tE_1 & {}^tF_1 \end{pmatrix}$ is $\min\{\rho + N - k_1 + 2, \eta + N - k_2 + 1\} = \sigma_2$. Let $\sigma = \min\{\sigma_1, \sigma_2\}$. We see that when we complete the square in $\begin{pmatrix} A_2 & B_3 \\ {}^tB_3 & C_2 \end{pmatrix}$ the binary form $\begin{pmatrix} a_{(0)} & e_{(\rho)} \\ e_{(\rho)} & d_{(0)} \end{pmatrix}$ becomes

$$\begin{pmatrix} a_{(0)} - \zeta_0(x_\sigma, \cdots, x_N) & e_{(\rho)} - \zeta_1(x_\sigma, \cdots, x_N) \\ e_{(\rho)} - \zeta_1(x_\sigma, \cdots, x_N) & d_{(0)} - \zeta_2(x_\sigma, \cdots, x_N) \end{pmatrix}$$

and the binary form $\begin{pmatrix} a_{(0)} & e'_{(\rho)} \\ e'_{(\rho)} & d_{(0)} \end{pmatrix}$ becomes

$$\begin{pmatrix} a_{(0)} - \zeta_0 & e'_{(\rho)} - \zeta_1 \\ e'_{(\rho)} - \zeta_1 & d_{(0)} - \zeta_2 \end{pmatrix}$$

where $\zeta_0, \zeta_1, \zeta_2$ all depend on $x_\sigma, \cdots, x_N$.

Now we complete the squares in $\begin{pmatrix} A_0 & B_0 \\ {}^tB_0 & C_0 \end{pmatrix} - \Omega'_0$ as we did in the proof of Theorem 4.1.1 (i.e. by starting with the biggest subscript on the diagonal) with the exception that we stop the process when we reach a subscript 2 on the diagonal. When completing the squares in that fashion we see that $\mathcal{Q}$ becomes

$$\begin{pmatrix} a_{(0)} - \zeta_0 & e_{(\rho)} - \zeta_\rho & b_{(n)} & a_{(1)} & \\ e_{(\rho)} - \zeta_\rho & d_{(0)} - \zeta'_0 & f_{(\eta)} & e_{(\rho+1)} & 0 \\ b_{(n)} & f_{(\eta)} & c_{(1)} - \zeta_1 & b_{(j)} - \zeta'_1 & \\ a_{(1)} & e_{(\rho+1)} & b_{(j)} - \zeta'_1 & a_{(2)} - \zeta_2 & \\ & 0 & & & D \end{pmatrix}$$

where $j = \mu_1 - \partial(b) - k_2 + N + 1$ and $\mathcal{Q}'$ becomes

$$\begin{pmatrix} a_{(0)} - \zeta_0 & e'_{(\rho)} - \zeta_\rho & b_{(n)} & a_{(1)} & \\ e'_{(\rho)} - \zeta_\rho & d_{(0)} - \zeta'_0 & f_{(\eta)} & e_{(\rho+1)} & 0 \\ b_{(n)} & f_{(\eta)} & c_{(1)} - \zeta_1 & b_{(j)} - \zeta'_1 & \\ a_{(1)} & e_{(\rho+1)} & b_{(j)} - \zeta'_1 & a_{(2)} - \zeta_2 & \\ & 0 & & & D \end{pmatrix}$$

where $\zeta_i$ and $\zeta_i'$ depend on $x_{i+1}, \cdots, x_N$ and $D$ is a diagonal matrix. Let $P$ and $P'$ be the $4 \times 4$ sections of $\mathcal{Q}(x_0, \cdots, x_N)$ and $\mathcal{Q}'(x_0, \cdots, x_N)$ and let $v = k_1 + k_2 + 3$. Since the quadratic forms $Q$ and $Q'$ are isospectral, Theorem 3.4.1 tells that for any $x_1, \cdots, x_N$

$$\sum_{X \in \mathbb{F}_r^4, Y \in \mathbb{F}_r^{v-4}} ({}^tXPX + {}^tYDY) = \sum_{X \in \mathbb{F}_r^4, Y \in \mathbb{F}_r^{v-4}} ({}^tXP'X + {}^tYDY)$$

but Gauss sums are multiplicative on orthogonal complements, and therefore we have

$$\sum_{X \in \mathbb{F}_r^4} ({}^tXPX) \sum_{Y \in \mathbb{F}_r^{v-4}} ({}^tYDY) = \sum_{X \in \mathbb{F}_r^4} ({}^tXP'X) \sum_{Y \in \mathbb{F}_r^{v-4}} ({}^tYDY).$$

By Lemma 3.4.1 we know that $\sum_{Y \in \mathbb{F}_r^{v-4}} ({}^tYDY) \neq 0$ and we finally get

$$\sum_{X \in \mathbb{F}_r^4} ({}^tXPX) = \sum_{X \in \mathbb{F}_r^4} ({}^tXP'X).$$

In particular Lemma 3.4.1 implies that for any $x_0, \cdots, x_N$

$$\chi(\det P) = \chi(\det P')$$

where $\chi$ stands for the quadratic character of $\mathbb{F}_r$. Once $x_1, \cdots, x_N$ are chosen, $\det P$ and $\det P'$ may be seen as polynomials in $x_0$. It is clear that the degree of these polynomials cannot exceed 2; hence, we can apply Lemma 3.4.2. By computing these determinants and by letting:

1. $A_0 = a_{(0)} - \zeta_0$
2. $E = e_{(\rho)} - \zeta_\rho$
3. $E' = e'_{(\rho)} - \zeta_\rho$
4. $b = b_{(n)}$
5. $A_1 = a_{(1)}$

6. $f = f_{(\eta)}$

7. $B = b_{(j)} - \zeta_1'$

8. $A_2 = a_{(2)} - \zeta_2$

9. $C_1 = c_{(1)} - \zeta_1$

we end up with

$$(A_2C_1-B^2)\left(E^2-E'^2\right)(B^2-A_2C_1)+(E-E')\,(2fbA_2+2eA_1C_1-2fA_1B-2ebB) = 0$$

which rewrites as

$$(A_2C_1-B^2)(E-E')\left\{(E+E')(B^2-A_2C_1) +(2fbA_2+2eA_1C_1-2fA_1B-2ebB)\right\}=0.$$

We let $x_N = 1$, we choose $x_{\rho+1}, \cdots, x_{N-1}$ so that $e_{\rho+1} \neq 0$. Note that this choice is always possible as $N > \mu_1 - s - k_1$. Choose $x_3, \cdots, x_\rho$ freely but so that completing the squares is possible. Now we still have a totally free choice on $x_1$ and $x_2$; hence, we choose them so that

$$(A_2C_1-B^2)\left((E+E')(B^2-A_2C_1)+(2fbA_2+2eA_1C_1-2fA_1B-2ebB)\right)\neq 0 \tag{4.5}$$

That is always possible as the right hand side of (4.5) may be seen as a polynomial of degree 3 in $x_1$ which is clearly not identically 0. That finally enables to conclude that

$$E - E' = 0 \quad (\text{i.e. } e_u = e'_u).$$

■

**Lemma 4.2.2** *Let $e = e_s t^s + \cdots + e_0$ so that $\partial(e) = s$. Suppose that $\partial(f) + k_2 > \partial(e) + k_1$ and that $\partial(b) + k_1 + k_2 > \partial(e) + k_1$. Suppose further that $\partial(f - f') + k_2 < \partial(e) + k_1$. Suppose finally that $Q$ and $Q'$ are isospectral, then $e_s = e'_s$.*

**Proof.** In order to prove this result we start exactly as in the previous proof (of Lemma 4.2.1). We let $N = \mu_3 - \partial(e) - k_1$. The very same argument allows to conclude that $(A_2C_1 - B^2) \det P = (A_2C_1 - B^2) \det P'$ for the same $P$ and $P'$ as in Lemma 4.2.1. Again we end up with the equation

$$(A_2C_1 - B^2)(E - E') \big\{ (E + E')(B^2 - A_2C_1) + (2fbA_2 + 2eA_1C_1 - 2fA_1B - 2ebB) \big\} = 0.$$

Note that in this case we have $N = \mu_3 - \partial(e) - k_1$ and hence, in this equation, contrary to the previous case, we have $e = 0$. Thus

$$(A_2C_1 - B^2)(E - E') \big\{ (E + E')(B^2 - A_2C_1) + 2f(bA_2 - A_1B) \big\} = 0.$$

Let $x_N = 1$ and let $\tau = \min\{n, \eta\}$. Choose $x_\tau, \cdots, x_{N-1}$ so that $f_{(\eta)} \neq 0$ and $b_{(n)} \neq 0$. Then choose $x_1, x_2$ so that

$$(A_2C_1 - B^2) \big\{ (E + E')(B^2 - A_2C_1) + 2f(bA_2 - A_1B) \big\} \neq 0 \qquad (4.6)$$

To this aim, choose $x_2$ so that $A_2 \neq 0$. If $E = -E'$, equation (4.6) becomes

$$(A_2C_1 - B^2) \left( 2f(bA_2 - A_1B) \right).$$

It is linear in $x_1$ if $B = 0$ and quadratic in $x_1$ if $B \neq 0$. In both cases it is not identically 0. If $E \neq -E'$, suppose further that $x_2$ was chosen so that $(E + E')A_2 \neq 2fB$. Then equation (4.6) becomes

$$(A_2C_1 - B^2) \big\{ (E + E')(B^2 - A_2C_1) + 2f(bA_2 - A_1B) \big\}.$$

It is quadratic in $x_1$ and clearly not identically 0. Finally, we see that $(E - E') = 0$ (i.e. $e_s = e'_s$). ■

**Lemma 4.2.3** *Let $e = e_s t^s + \cdots + e_0$, let $f = f_u t^u + \cdots + f_0$, let $b = b_v t^v + \cdots + b_0 \neq 0$. Let also $N = \mu_3 - v - k_1 - k_2$ and $M = \mu_3 - s - k_1$. Suppose that $u \geq v + k_1$, that $v + k_2 < s$ and that $\partial(d - d') < v + k_1 + k_2$ . Suppose further that $\partial(f - f') < v + k_1$. If $Q$ and $Q'$ are isospectral then $e_s = e'_s$.*

**Proof.** For the sake of clarity, let us explain the conditions on the degrees that are in the hypothesis of this lemma. First, recall that from the quadratic forms $Q$ and $Q'$ we have created systems $Q_0, \cdots, Q_l$. The number $N$ defined above is the smallest index $i$ such that a coefficient of $b$ appears in $Q_i$ and the number $M$ is the smallest index $i$ such that a coefficient of $e$ appears in $Q_i$. Suppose that the first coefficient of $f$ to appear in the system appears in some form $Q_j$. The fact $u \geq v + k_1$, just translates by $j \leq N$. The fact $\partial(f - f') < v + k_1$ translates in term of systems by saying that the coefficients of $f$ and of $f'$ in the forms $Q_0, \cdots, Q_{N-1}$ and $Q'_0, \cdots, Q'_{N-1}$ are the same.

By Theorem 4.1.1, we know that $x_1, \cdots, x_{M-1}$ can be chosen in order to make $\widetilde{\mathcal{Q}}(x_1, \cdots, x_{M-1}, 1)$ and $\widetilde{\mathcal{Q}'}(x_1, \cdots, x_{M-1}, 1)$ nondegenerate. For this choice we can complete the squares and see that

$$\begin{pmatrix} a_0 - \zeta_0 & e_s & \\ e_s & c_0\zeta'_0 & \\ & & D \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a_0 - \zeta_0 & e'_s & \\ e'_s & c_0\zeta'_0 & \\ & & D \end{pmatrix}$$

where $D$ is a diagonal matrix, are isospectral. Let $q$ (resp. $q'$) be the $2 \times 2$-sections of the forms above. It is well known that Gauss sums are multiplicative on orthogonal summand and therefore, as we did in the proof of Lemma 4.2.1 we conclude that

$$\sum_{\xi \in \mathbb{F}_r^2} \varphi(q(\xi)) = \sum_{\xi \in \mathbb{F}_r^2} \varphi(q(\xi)).$$

Lemma 3.4.1 allows us to compute these sums and to see that for any choice of $x_0$

$$\chi(\mathrm{disc}(q)) = \chi(\mathrm{disc}(q')).$$

But $\mathrm{disc}(q)$ and $\mathrm{disc}(q')$ are quadratic in $x_0$ and have the same leading coefficients. By applying Lemma 3.4.2, we can conclude that $e_s^2 = e_s'^2$ (i.e. $e_s = \pm e_s'$). If $e_s = e_s'$ we are done. Suppose therefore that $e_s = -e_s'$. Replace the form

$$Q' = \begin{pmatrix} a & b & e' \\ b & c & f' \\ e' & f' & d' \end{pmatrix}$$

by the equivalent form

$$Q'' = \begin{pmatrix} a & b'' & e'' \\ b'' & c & f' \\ e'' & f' & d' \end{pmatrix} = \begin{pmatrix} a & -b & -e' \\ -b & c & f' \\ -e' & f' & d' \end{pmatrix}.$$

It is clear that $Q$ and $Q''$ are isospectral and that we now have $e_s'' = e_s$. Also, since no coefficient of $b$ appears on the forms $Q_i'$ for $i < N$, we can use Lemma 4.2.1 to conclude that $Q_i = Q_i''$ for any $i$ with $0 \leq i < N$.

What happens in $Q_N$? To know that, we apply the same reasoning as in the proof of Lemma 4.2.1. With the notations we used above, we can conclude that $\chi \det P = \chi \det P'$, that is

$$\chi \det \begin{pmatrix} A_0 & E & b_v & a_{(1)} \\ E & C_0 & f_{(\eta)} & e_{(\rho+1)} \\ b_v & f_{(\eta)} & C_1 & B \\ a_{(1)} & e_{(\rho+1)} & B & A_2 \end{pmatrix} = \chi \det \begin{pmatrix} A_0 & E' & -b_v & a_{(1)} \\ E' & C_0 & f_{(\eta)} & e_{(\rho+1)} \\ -b_v & f_{(\eta)} & C_1 & B \\ a_{(1)} & e_{(\rho+1)} & B & A_2 \end{pmatrix} \tag{4.7}$$

for any set of variables $x_3, \cdots, x_N$ so that $\widetilde{\mathcal{Q}}$ is non degenerate. First choose $x_2, \cdots, x_{\rho+1}, \cdots, x_{N-1}$ so that $e_{(\rho+1)} \neq 0$ and $A_2 \neq 0$. Equation (4.7) implies that

$$(A_2C_1 - B^2)\left\{(E'^2 - E^2)(C_1A_2 - B^2) + 2(E' + E)(f_{(\eta)}b_vA_2 - e_{(\rho+1)}bB) + \right.$$

$$\left. 2(E' - E)(f_{(\eta)}A_1B - e_{(\rho+1)}A_1C_1)\right\} = -4b_ve_{(\rho+1)}A_1f_{(\eta)}(A_2C_1 - B^2)$$

If $E \neq E'$ this equality cannot hold for all $x_1$. Indeed, the left hand side may be seen as a polynomial of degree 3 in $x_1$ which is nonzero as it leading coefficient is $-A_2e_{\rho+1} \neq 0$. The right hand side is at most quadratic in $x_1$.

Thus, $E = E'$ and equation (4.7) becomes

$$(A_2C_1 - B^2)\left\{2E^2(C_1A_2 - B^2) + 4E(f_{(\eta)}b_vA_2 - e_{(\rho+1)}bB) + 4b_ve_{(\rho+1)}A_1f_{(\eta)}\right\} = 0 \tag{4.8}$$

Choose $x_2, x_3, \cdots, x_\rho$ so that the diagonalization argument work and so that $f_{(\eta)} \neq 0$, $e_{(\rho+1)} \neq 0$, $A_2 \neq 0$ and $2E^2A_2 \neq -4b_vf_{(\eta)}e_{(\rho+1)}$. The left hand side is a non-identically-zero polynomial of degree 2 in $x_1$; it cannot take only zero values on $\mathbb{F}_r$. This is a contradiction with the hypothesis $e_s = -e'_s$; that proves the lemma. ■

**Lemma 4.2.4** *Let*

$$Q = \begin{pmatrix} a & b & e \\ b & c & f \\ e & f & d \end{pmatrix}$$

*be a reduced quadratic form with successive minima* $(\mu_1, \mu_2, \mu_3)$ *and let*

$$\overline{Q} = \begin{pmatrix} \overline{a} & \overline{b} & \overline{e} \\ \overline{b} & \overline{c} & \overline{f} \\ \overline{e} & \overline{f} & \overline{d} \end{pmatrix}$$

*be its adjoint. Suppose that* $\partial(f) < \partial(b) + k_1$, *then* $\partial(\overline{f}) \geq \partial(\overline{b}) + \overline{k_1}$.

**Proof.** It is easy to see that $\overline{k_1} = \frac{\mu_3 - \mu_1}{2}$. We want to prove that

$$\partial(bd - fe) \geq \partial(af - be) + \frac{\mu_3 - \mu_1}{2}.$$

To this aim, we first prove that $\partial(bd - fe) = \partial(b) + \partial(d)$. If this is not the case, then we must have

$$\partial(b) + \partial(d) \leq \partial(f) + \partial(e).$$

By using the assumption on $\partial(f)$, this inequality leads to

$$\partial(b) + \partial(d) \leq \partial(b) + k_1 + \partial(e) \Leftrightarrow \partial(d) \leq \partial(e) + k_1.$$

This is clearly absurd. Now, it is easy to see that $\partial(d) + \partial(b) \geq \partial(b) + \partial(e) + k_1$. Also

$$\begin{aligned} \partial(d) + \partial(b) \geq \partial(a) + \partial(f) + k_1 &\Leftrightarrow \mu_3 + \partial(b) \geq \mu_1 + \partial(f) + \frac{\mu_3 - \mu_1}{2} \\ &\Leftrightarrow \partial(b) + \frac{\mu_3 - \mu_1}{2} \geq \partial(f) \\ &\Leftrightarrow \partial(b) + k_1 \geq \partial(f) \end{aligned}$$

■

Remember that for a ternary lattice $L$ with successive minima $(\mu_1, \mu_2, \mu_3)$, we denote its adjoint by $\overline{L}$ and by $(\nu_1, \nu_2\nu_3)$ the successive minima of $\overline{L}$. It is clear that when $\mu_1 \equiv \mu_3 \mod 2$ we have $\nu_1 \equiv \nu_3 \mod 2$.

Suppose that $(L, Q)$ and $(L', Q')$ are isospectral ternary lattices with $\mu_1 \equiv \mu_3 \mod 2$ and suppose that Gram matrices of $Q$ and $Q'$ in some reduced basis are respectively given by

$$Q = \begin{pmatrix} a & b & e \\ b & c & f \\ e & f & d \end{pmatrix} \quad \text{and} \quad Q' = \begin{pmatrix} a & b & e' \\ b & c & f' \\ e' & f' & d' \end{pmatrix} \tag{4.9}$$

There is no loss of generality in assuming that the leading coefficient of $a$ and of $c$ is 1 and that the one of $d$ and $d'$ is $-\delta$ for a given nonsquare $\delta \in \mathbb{F}_r$.

We know that $Q$ and $Q'$ are isospectral and therefore we see (Theorem 3.1.1) that $\overline{Q}$ and $\overline{Q'}$ are isospectral. By using the fact that $\mu_1 \equiv \mu_3 \mod 2$, an easy computation will show that $\nu_1 \equiv \nu_3 \mod 2$. Hence Lemma 4.1.1 applies and enables to conclude that $\overline{Q}$ and $\overline{Q'}$ contain isomorphic binary quadratic forms;

let $\overline{q}$ and $\overline{q'}$ be these forms. It is easy to see that

$$\overline{q} = \begin{pmatrix} ac - b^2 & af - be \\ af - be & ad - e^2 \end{pmatrix} \cong \begin{pmatrix} ac' - b'^2 & af' - b'e' \\ af' - b'e' & ad' - e'^2 \end{pmatrix} = \overline{q'}.$$

So we have $ad - e^2 = ad' - e'^2$ and $af - be = \pm(af' - be')$. By changing $e'$ and $f'$ into $-e'$ and $-f'$ if need be, we can suppose that

$$d - d' = \frac{e^2 - e'^2}{a} \quad \text{and} \quad f - f' = \frac{b(e - e')}{a}.$$

Remember that the forms $Q$ and $Q'$ were reduced and so one gets

1. $\partial(d - d') < \partial(e - e')$;
2. $\partial(f - f') < \partial(e - e')$;
3. $\partial(f - f') < \partial(b)$.

Lemma 4.2.1,4.2.2, 4.2.3 and 4.2.4 allow to conclude that $e = e'$, thus that $f = f'$ and $d = d'$.

### 4.2.3 Proof of Theorem 4.2.1 when $\mu_1 \equiv \mu_2 \mod 2$

Let us define $q$ (resp. $q'$) to be reduced Gram matrix of the quadratic form on $L^{2\times 2}$ (resp. $L'^{2\times 2}$).

**Lemma 4.2.5** *Suppose that $L \cong Q$ and $L' \cong Q'$ where $Q, Q'$ are as in equation (4.9). There are reduced basis of $L$ and $L'$ such that $q = q'$ and $d = d'$.*

**Proof.** Since $d'$ is represented by $Q'$, it must be represented by $Q$, thus

$$d' = Q(h, g, k) \tag{4.10}$$

for some $h, g, k \in \mathbb{F}_r[t]$. Definiteness and the condition on the successive minima in fact implies that $k \in \mathbb{F}_r$ and comparing the leading coefficients in (4.10) enables

to see that $k = \pm 1$ (remember that $W_\infty = W'_\infty$). It is clear that we do not lose any generality by assuming $k = 1$. Now, consider the action of the transformation

$$M = \begin{pmatrix} 1 & 0 & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} \in SL_2(\mathbb{F}_r[t])$$

on $Q$. We get a new matrix, $Q''$ with determinant satisfying $\det(Q'') = \det(Q) = \det(Q')$. This matrix nevertheless is not *a priori* reduced. We write it:

$$Q'' = {}^tM\, Q\, M = \begin{pmatrix} a & b & ah + bg + e \\ * & c & bh + cg + f \\ * & * & d' \end{pmatrix}.$$

We are going to prove that $\det(Q'') = \det(Q')$ is not possible unless $Q''$ is reduced. We have

$$\begin{aligned} d' \det(q) - q(-bh + cg + f, ah + bg + e) &= \operatorname{disc}(Q'') \\ &= \operatorname{disc}(Q') \\ &= d' \det(q) - q(-f', e') \end{aligned}$$

and so we see that

$$q(-bh + cg + f, ah + bg + e) = q(-f', e') \tag{4.11}$$

Suppose first that $g = 0$ and suppose that $\partial(ah) \geq \partial(c)$. In particular, we have $\partial(ah) > \partial(e)$. Therefore, in (4.11), definiteness implies that

$$\partial(q(-bh + f, ah + e)) \geq \partial(ca^2h^2).$$

Now on the right hand side of (4.11), we have

$$\partial(q(-f', e')) = \max\{\partial(af'^2), \partial(ce'^2)\}.$$

But is is clear that $\partial(ca^2h^2) > \partial(ce'^2)$ and $\partial(ca^2h^2) \geq \partial(c^2ah) > \partial(af'^2)$. This is a contradiction; hence $\partial(ah) \geq \partial(c)$ is not possible.

Suppose that $\partial(ah) < \partial(c)$. Clearly this assumption implies that $\partial(a) < \partial(c)$. Choose $r \in \mathbb{F}_r$ such that the leading coefficient of $1 + 2hr$ is not a square (which is possible unless $h = 0$, in which case we are done). Then $a + 2(ah + e)r + d'r^2$ is represented by $Q''$ and therefore must be represented by $Q'$. So we can find $k, l, m \in \mathbb{F}_r[t]$ such that

$$\begin{aligned} a + 2(ah + e)r + d'r^2 \\ = ak^2 + cl^2 + d'm^2 + 2bkl + 2e'km + 2f'lm. \end{aligned}$$

Conditions one degree and leading coefficients tell that in fact $m \in \mathbb{F}_r$ and $m^2 = r^2$. Thus

$$a + 2(ah + e)r = ak^2 + cl^2 + 2b'kl \pm 2e'kr \pm 2f'lm.$$

Under the assumption we have made, the degree of the right hand side is strictly bigger than the one of the left hand side unless $l = 0$. Thus

$$\begin{aligned} a + 2(ah + e)r = ak^2 \pm 2e'kr \\ \Leftrightarrow a(1 + 2hr) + 2er = ak^2 \pm 2e'kr. \end{aligned}$$

This is a contradiction and therefore we have $h = 0$.

Suppose that $g \neq 0$. If $\partial(cg) = \partial(bh)$, we see that $\partial(ah) > \partial(cg)$. Thus in equation (4.11), we have

$$\partial(q(-(bh + cg + f), (ah + bg + e))) \geq \partial(ca^2h^2) > \partial(c^2ah).$$

Now on the right hand side of (4.11), we have

$$\partial(q(-f', e')) = \max\{\partial(af'^2), \partial(ce'^2)\}.$$

But is is clear that $\partial(ca^2h^2) > \partial(ce'^2)$ and $\partial(c^2ah) > \partial(af'^2)$. That is not possible; hence $\partial(cg) \neq \partial(bh)$.

Now, in equation (4.11), we have

$$\partial(q(-(bh + cg + f), (ah + bg + e))) \geq \partial(ac^2g^2).$$

But here again, we have $\partial(ac^2g^2) > \partial(ce'^2)$ and $\partial(ac^2g^2) > \partial(af'^2)$. The contradiction is clear; hence $g \neq 0$ is not possible. ■

We are now ready to conclude when $\partial(a) \neq \partial(c)$. Indeed, since $a + 2e + d'$ is represented by $Q''$ and thus must be represented by $Q'$. So we can find $k, l, m \in \mathbb{F}_r[t]$ such that

$$a + 2e + d' = ak^2 + cl^2 + d'm^2 + 2bkl + 2e'km + 2f'lm.$$

Here again, definiteness implies $m = \pm 1$ and $l = 0$. Thus

$$a + 2e = ak^2 \pm 2e'k.$$

From there, one sees that $k = \pm 1$ and that finally $e' = \pm e$. So far we know that all the coefficients are equal but maybe $f$ and $f'$, but we know that the discriminants are equal.

When $\partial(a) = \partial(c)$ (i.e. $\mu_1 = \mu_2$), we have some more work to do. In this case, indeed, the binary form $q$ could possibly have some non trivial automorphism (cf Theorem 1.2.3).

So far we have two forms $Q$ and $Q'$ having the same representation numbers and reduced Gram matrices

$$Q = \begin{pmatrix} a & b & e \\ b & c & f \\ e & f & d \end{pmatrix}; \quad Q' = \begin{pmatrix} a & b & e' \\ b & c & f' \\ e' & f' & d \end{pmatrix}.$$

If both $e$ and $e'$ (resp. $f$ and $f'$) are 0, then the equality of discriminants is enough to conclude. Suppose thus it is not the case and let $\alpha, \beta, \mu$ be any elements in $\mathbb{F}_r$. It is clear that

$$Q(\alpha, \beta, \mu) = a\alpha^2 + 2b\alpha\beta + c\beta^2 + 2e\alpha\mu + 2f\beta\mu + d\mu^2$$

is represented by $Q'$. Thus, we can find $h, g, k$, all in $\mathbb{F}_r[t]$, such that

$$\begin{aligned} a\alpha^2 + 2b\alpha\beta + c\beta^2 + 2e\alpha\mu + 2f\beta\mu + d\mu^2 \\ = ah^2 + 2bhg + cg^2 + 2e'hk + 2f'gk + dk^2. \end{aligned}$$

Since $Q'$ is definite it follows that in fact $k \in \mathbb{F}_r$. The only leading term on the left hand side comes from $d\mu^2$ and on the right hand side comes from $dk^2$ (remember that $\partial(d)$ does not have same parity as $\partial(a)$, nor $\partial(c)$). From this observation follows easily that $k = \pm\mu$ and by replacing $e, f, e', f'$ by their negative when need be, we can suppose that $k = \mu$. The equation given above becomes:

$$a\alpha^2 + 2b\alpha\beta + c\beta^2 + 2e\alpha\mu + 2f\beta\mu = ah^2 + 2bhg + cg^2 + 2e'h\mu + 2f'g\mu.$$

Since the forms are definite and since the degree of the left hand side is exactly $\partial(a)$, it follows that in fact $h$ and $g$ are both in $\mathbb{F}_r$. In particular, we can assert that for all pairs $(\alpha, \beta) \in \mathbb{F}_r^2$, and all $\mu \in \mathbb{F}_r$, there exists a pair $(\sigma, \rho) \in \mathbb{F}_r^3$ such that

$$\begin{aligned} a\alpha^2 + 2b\alpha\beta + c\beta^2 + 2e\alpha\mu + 2f\beta\mu \\ = a\sigma^2 + 2b\sigma\rho + c\rho^2 + 2e'\sigma\mu + 2f'\rho\mu \end{aligned} \tag{4.12}$$

It is clear that the leading coefficient of the left hand side is $\alpha^2 - \delta\beta^2$ and does not depend on $\mu$. On the right hand side it is given by $\sigma^2 - \delta\rho^2$ and does not depend on $\mu$ neither.

Let us suppose to start that $b \neq 0$. In the equation (4.12), let $\alpha = 1$ and $\beta = 0$ in order to get

$$a + 2e\mu = a\sigma^2 + 2b\sigma\rho + c\rho^2 + 2e'\sigma\mu + 2f'\rho\mu \tag{4.13}$$

and let $\mu$ run over $\mathbb{F}_r$. Assuming that $e \neq 0$, we get $r = \#\mathbb{F}_r$ distinct values for the left hand side. On the right hand side we must also have $r$ pairs $(\sigma, \rho)$ satisfying the equation above. If one of these pairs is $(\pm 1, 0)$ we are able to conclude that $e = e'$. If not, using Lemma 2.1.2, we see that there will be exactly $r - 1$ possible pairs $(\sigma, \rho)$ satisfying $\sigma^2 - \delta\rho^2 = 1$. One of these pairs must appear in 4.13 for at least two distinct values of $\mu$. In other words, we have :

$$\begin{cases} a + 2e\mu = a\sigma^2 + 2b\sigma\rho + c\rho^2 + 2e'\sigma\mu + 2f'\rho\mu \\ \\ a + 2e\mu' = a\sigma^2 + 2b\sigma\rho + c\rho^2 + 2e'\sigma\mu' + 2f'\rho\mu' \end{cases}.$$

By subtracting these equations we get $e = e'\sigma + f'\rho$, and substituting in equation 4.13 tells us that

$$a = a\sigma^2 + 2b\sigma\rho + c\rho^2 \tag{4.14}$$

Let $b_k$ be the leading coefficient of $b$ and let us write the equation we have obtained in terms of the coefficients of $a, b, c$. We have :

$$\sigma^2 - \delta\rho^2 = 1 \quad \text{and} \quad a_k\sigma^2 + 2b_k\sigma\rho + c_k\rho^2 = a_k.$$

Some easy computations allow to find exact values for $\sigma$ and $\rho$. Indeed, as long as $\rho \neq \pm 1$ (i.e. the automorphism is non trivial), after substituting the first equation into the second and letting $\Omega = \delta a_k + c_k$ one gets

$$\rho = \pm\frac{2b}{\sqrt{\Omega^2 - 4\delta b_k^2}} \quad \text{and} \quad \sigma = \pm\frac{\Omega}{\sqrt{\Omega^2 - 4\delta b_k^2}}.$$

Also by substituting back into 4.14 and by remembering that $b \neq 0$, one sees that the solutions above have not the same *sign* (i.e. $\rho = \frac{2b}{\sqrt{\Omega^2-4\delta b_k^2}}$ if and only if $\sigma = -\frac{\Omega}{\sqrt{\Omega^2-4\delta b_k^2}}$).

Instead of letting $\alpha = 1$ and $\beta = 0$, we let $\alpha = 0$, $\beta = 1$ and then we get an equation of the form:

$$c + 2f\mu = a\epsilon^2 + 2b\epsilon\xi + c\xi^2 + 2e'\epsilon\mu + 2f'\xi\mu$$

and doing exactly the same work we obtain two similar equalities:

$$f = e'\epsilon + f'\xi \quad \text{and} \quad c = a\epsilon^2 + 2b\epsilon\xi + c\xi^2$$

and computations on the coefficients give:

$$\xi = \pm\frac{\Omega}{\sqrt{\Omega^2 - 4\delta b_k^2}} \quad \text{and} \quad \epsilon = \pm\frac{2\delta b}{\sqrt{\Omega^2 - 4\delta b_k^2}}$$

and again a $+$ for $\xi$ correspond to a $-$ for $\rho$. In particular, we see that the following transformation

$$M = \begin{pmatrix} \sigma & \epsilon & 0 \\ \rho & \xi & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

has discriminant $\pm 1$. Let it act on $Q'$ in order to get

$$Q' \cong Q'' = \begin{pmatrix} a & B & e \\ B & c & f \\ e & f & d \end{pmatrix}.$$

Since $det(M)^2 = 1$, it follows that $Q''$ and $Q$ have the same discriminant which allows to conclude about $B$.

We still need to treat the case when $b = 0$. It is clear that if $a$ has only two representations then using arguments as above, we are done. Suppose that $a$ is represented more than trivially. By converting $a = a\alpha^2 + c\beta^2$ coefficient wise, we see that $1 = \alpha^2 - \delta\beta^2$, and that for all $k < \partial(a)$, $a_k = a_k\alpha^2 + c_k\beta^2$. By substituting one sees easily that one must have $c = -\delta a$. By going back to equation of the same type as 4.13, we see that for any $\mu \in \mathbb{F}_r$ the equations

$$\begin{cases} a + 2e\mu = a(\sigma^2 - \delta\rho^2) + 2e'\sigma\mu + 2f'\rho\mu \\ c + 2f\mu = a(\epsilon^2 - \delta\eta^2) + 2e'\epsilon\mu + 2f'\eta\mu \end{cases}$$

must be solvable. But considerations on leading coefficients prove that $\sigma^2 - \delta\rho^2 = 1$ and $\epsilon^2 - \delta\eta^2 = -\delta$, which leaves us with

- $e = e'\sigma + f'\rho$, where $\sigma^2 - \delta\rho^2 = 1$;
- $f = e'\epsilon + f'\eta$, where $\epsilon^2 - \delta\eta^2 = -\delta$.

On the other hand we have

$$a + c + 2e\mu + 2f\mu = a(\omega^2 - \delta\nu^2) + 2e'\omega\mu + 2f'\nu\mu$$

and from this we get

$$e + f = e'\omega + f'\nu \quad \text{where} \quad \omega^2 - \delta\nu^2 = 1 - \delta.$$

Equating everything, we see that if the family $(e, f)$ is free, we have $w = \sigma + \epsilon$ and $\nu = \rho + \eta$. The relation $\omega^2 - \delta\nu^2$ translates into

$$(\sigma + \epsilon)^2 - \delta(\rho + \eta)^2 = 1 - \delta \quad (\text{i.e.} \quad \sigma\rho = \delta\rho\eta)$$

and therefore we see that $\begin{pmatrix} \sigma & \epsilon \\ \rho & \eta \end{pmatrix}$ is an automorphism of $q$ which allows to conclude.

When $(e, f)$ and $(e', f')$ are both linearly dependent we see that $f, e', f'$ are all $\mathbb{F}_r$-multiples of $e$, say $f = ue$, $e' = se$ and $f' = te$. The equality of the discriminants of $Q$ and $Q'$ implies that

$$t^2 - \delta s^2 = u^2 - \delta.$$

For a fixed $u$ there are exactly $r + 1$ pairs $(t, s)$ such that $t^2 - \delta s^2 = u^2 - \delta$. Now there are $r + 1$ pairs of $(\alpha, \beta)$ such that $\alpha^2 - \delta\beta^2 = 1$ and each of these pairs can be extended to the following automorph of $q$:

$$\begin{pmatrix} \alpha & \delta\beta \\ \beta & \alpha \end{pmatrix}.$$

In particular there are $r+1$ automorphs of $q$, each of which has a different action on $e$ and $f$ since

$$\alpha t + \beta s = \alpha t' + \beta s' \quad \text{and} \quad \delta\beta t + \alpha s = \delta\beta t' + \alpha s'$$

clearly implies that $(t, s) = (t', s')$. It follows that under the action of the previous automorphs each pair $(t, s)$ with $t^2 - \delta s^2 = u^2 - \delta$ will be reached and allows to conclude that the forms are equivalent.

# Chapter 5

# Regular Ternary Lattices

## 5.1 Preliminaries

### 5.1.1 Generalities on Spinor Genera

Let $(V, q)$ be a quadratic space over $k$. There is an application $\theta$, from $O^+(V)$ to $k^\times/(k^\times)^2$, defined by the following way. Let $\phi \in O^+(V)$ and write $\phi$ as a product of symmetries (Cf. [4], Lemma 4.3 p20) $\phi = \tau(v_1)\cdots\tau(v_n)$ then we define

$$\theta(\phi) = q(v_1)\cdots q(v_n) \mod (k^\times)^2.$$

This is well defined (cf. [18], p 29 ). We shall denote by $O'(V)$ the kernel of this application.

For some aesthetic concerns, in this section the language of adèles will be used. We review now the principal notations and definitions. Let $\Omega$ be the set of all the places of $k$. We let $J_k$ be the full group of idèles; namely

$$J_k = \{(j_\mathfrak{p}) \mid j_\mathfrak{p} \in k_\mathfrak{p}^\times \ \ \forall \mathfrak{p} \in \Omega \text{ and } j_\mathfrak{p} \in A_\mathfrak{p}^\times \text{ for almost all } \mathfrak{p}\}.$$

There is a natural injection $k \hookrightarrow J_k$, that send $a \in k$ to $(a)_\mathfrak{p} \in J_k$. We define the group a principal ideles $P_k$ to be image in $J_k$ of this natural mapping.

Let $V$ be a regular quadratic space on $k$ and let $L$ be a lattice in $V$. We define the group of split rotations $J_V$ to be the adelization of $O^+(V)$. In other words it is

$$J_V = \{(\Sigma_\mathfrak{p})_\mathfrak{p} \mid \Sigma_\mathfrak{p} \in O^+(V_\mathfrak{p}) \ \forall \mathfrak{p} \in \Omega, \text{ and } \Sigma_\mathfrak{p} L_\mathfrak{p} = L_\mathfrak{p} \text{ for almost all } \mathfrak{p}\}.$$

This definition clearly does not depend on the choice of the lattice $L$, for if $M$ is another lattice then $M_\mathfrak{p} = L_\mathfrak{p}$ almost everywhere. Now consider the set of split rotation which have the property that for all $\mathfrak{p} \in \Omega$,

$$\Sigma_\mathfrak{p} \in O'(V_\mathfrak{p}).$$

This subset is in fact a subgroup that we shall denote $J'_V$. Since $J'_V$ contains the commutator subgroup of $J_V$, it follows that $J'_V$ is normal in $J_V$. Note also that the quotient $J_V/J'_V$ is abelian. Let $L$ be a lattice then, $J_L$ is the subgroup of $J_V$ of those split rotations such that $\Sigma_\mathfrak{p} \in O^+(L_\mathfrak{p})$ for all $\mathfrak{p} \in \Omega$.

As we did with the idele group, we can inject $O^+(V)$ into $J_V$, by sending $\sigma \in O^+(V)$ to $(\sigma_\mathfrak{p})_\mathfrak{p}$, where $\sigma_\mathfrak{p}$ just denote the localization of $\sigma$ at $\mathfrak{p}$. We say that a split rotation is principal, if it belongs to the image of the previous injection. Let $D = \theta(O^+(V))$, then $D$ is a subgroup of $k^\times$. We shall denote $P_D$ the subgroup of principal ideles image of $D$ by the injection defined before. Note that the spinor norm $\theta$ extends to $J_V$ by just putting $\theta(\Sigma)_\mathfrak{p} = \theta(\Sigma_\mathfrak{p})$.

Let us translate the notion of genus and that of spinor genus in this adelic language. Let $L$ and $M$ be two lattices, then $L$ and $M$ are in the same genus if and only if there exists $\Sigma \in J_V$ such that

$$M = \Sigma L.$$

Similarly, we say that $L$ and $M$ are in the same spinor genus if and only if there is $\sigma \in O(V)$ and $\Sigma \in J'_V$ such that

$$M = \sigma \Sigma L.$$

**Lemma 5.1.1** *Let $\mathfrak{p}$ be a prime in $A$ and let $a \in A_{\mathfrak{p}}^{\times}$. Then $a = x^2$ for some $x \in k_p$ if and only if $a \equiv y^2 \mod \mathfrak{p}$ for some $y \in A$.*

**Lemma 5.1.2** *Let $s$ be a formal Laurent series in $\frac{1}{t}$ and write*

$$s = \sum_{n=-\infty}^{u} a_n t^n.$$

*Then $s \in \left(\mathbb{F}_r\left[\left[\frac{1}{t}\right]\right]\right)^2$ if and only if $a_u \in (\mathbb{F}_r)^2$ and $u \equiv 0 \mod 2$.*

**Corollary 5.1.1** *Let $\mathfrak{p}$ be a prime in $A$ and suppose that $\mathfrak{p} = (p)$. We have $k_{\mathfrak{p}}^{\times}/(k_{\mathfrak{p}}^{\times})^2 \cong 1, \epsilon, p, \epsilon p$, where $\epsilon$ is any fixed nonsquare of $A_{\mathfrak{p}}^{\times}$.*

**Proof.** The field $A/\mathfrak{p}$ may be seen as a finite field with $r^{\partial \mathfrak{p}}$ elements. In particular $(A/\mathfrak{p})^{\times}$ is a cyclic group of even order. Let $x \in k_{\mathfrak{p}}^{\times}$ and write $x = p^n y$, where $y \in A_{\mathfrak{p}}^{\times}$. We have $y = a^2 \mod \mathfrak{p}$ or $y = \epsilon a^2 \mod \mathfrak{p}$ for some $a \in A$ and we conclude using the previous lemma.

Also note that the corollary is valid at $\infty$ by replacing the set $\{1, \epsilon, p, \epsilon p\}$, by the set $\{1, \epsilon, t, \epsilon t\}$ where $t$ is the indeterminate and $\epsilon$ is a nonsquare in $\mathbb{F}_r$. ■

**Proposition 5.1.1** *Let $V$ be a ternary quadratic space over $k$, let $V_{\mathfrak{p}} = V \otimes k_{\mathfrak{p}}$ and let $O^+(V_{\mathfrak{p}})$ be the group of proper automorphisms of $V_{\mathfrak{p}}$. Then*

$$\theta(O^+(V_{\mathfrak{p}})) = k_{\mathfrak{p}}^{\times} \mod k_{\mathfrak{p}}^{\times 2}.$$

**Proof.** It is well known that a regular ternary form defined over a local field $k_p$ represents all, but possibly one, cosets of $k_p^{\times}$ modulo $(k_{\mathfrak{p}}^{\times})^2$ (Cf [4] Lemma 2.6 p60).

Let $w \in k_{\mathfrak{p}}^{\times}$. By Lemma 5.1.1, we know that $k_{\mathfrak{p}}^{\times}/(k_{\mathfrak{p}}^{\times})^2$ has order 4 and therefore, we can suppose that there are $u, v \in k_{\mathfrak{p}}^{\times}$, not in the same square class as

$w$ such that $uv = w$. There are $a, b \in k_{\mathfrak{p}}^{\times}$ such that $q(a) = u$ and $q(b) = v$ and finally $\theta(\tau(a)\tau(b)) = w \mod (k_{\mathfrak{p}}^{\times})^2$. ■

**Proposition 5.1.2** *Let $(V, q)$ be a ternary space over $k$, then*

$$\theta(O^+(V)) = k^{\times}/(k^{\times})^2.$$

**Proof.** By the Hasse principle, we know that $e \in k^{\times}$ is represented globally by $q$ if and only if it is represented locally everywhere by $q$. Moreover $q$ is universal almost everywhere and therefore there may be an (at most) finite set $P$, of primes $\mathfrak{p}$, such that the elements of a single coset $e_{\mathfrak{p}} \mod k_{\mathfrak{p}}^{\times 2}$ are omitted. Let $w \in k^{\times}$ and choose $u, v \in k^{\times}$ such that

1. $w = uv$;
2. $u \not\equiv e_{\mathfrak{p}} \mod k_{\mathfrak{p}}^{\times 2}$ and $v \not\equiv e_{\mathfrak{p}} \mod k_{\mathfrak{p}}^{\times 2}$;

Note that the second condition above was proved to be possible in the finite case (Cf. 5.1.1) and works also in the infinite case as in the function field case $k_{\infty}^{\times}/(k_{\infty}^{\times})^2$ is also isomorphic to the Klein group.

By Hasse principle there are $a, b \in V$ such that $q(a) = u$ and $q(b) = v$ and finally $\theta(\tau(a)\tau(b)) = w \mod k_{\mathfrak{p}}^{\times 2}$ ■

The following result is now well known. A proof can be found in [18].

**Theorem 5.1.1** *Let $V$ be a ternary quadratic space over $k$, let $L$ be a lattice in $V$ and let $spn^+$ be the number of proper spinor genera in $\mathcal{G}en(L)$. Then*

$$spn^+ = [J_k : P_D\theta(J_L)].$$

**Theorem 5.1.2 (Kneser, [19])** *Let $V$ be a ternary quadratic space over $k$ and $(L, q)$ be a ternary quadratic lattice in $V$. Let $\mathfrak{p}$ be a prime and suppose that $\mathfrak{p} = (\pi)$. Suppose further that*

$$L_{\mathfrak{p}} = \pi^{\alpha_1} L_1 + \cdots + \pi^{\alpha_n} L_n.$$

*Let $m_i$ be the set of all the $f \in k_{\mathfrak{p}}^{\times}$ represented by $\pi^{\alpha_i} L_i$ such that $v_{\mathfrak{p}}(f) \leq \alpha_i$. Let $\mathfrak{m}(L_{\mathfrak{p}})$ be the set of the those elements which can be written as a product of an even number of elements in $\cup m_i$. Then*

$$\theta(O^+(L_{\mathfrak{p}})) = \mathfrak{m}(L_p)\ (k_p^{\times})^2.$$

**Corollary 5.1.2** *Let $L$ be a lattice. If the Jordan decomposition of $L_{\mathfrak{p}}$ contains a $\mathfrak{p}$-modular component of rank at least 2, then*

$$\theta(O^+(L_{\mathfrak{p}})) \supset A_{\mathfrak{p}}^{\times} \mod k_{\mathfrak{p}}^{\times 2}.$$

**Proof.** This corollary follows easily from Theorem 5.1.2, by noticing that if $L_i$ has rank at least 2, then $L_i$ represents $A_{\mathfrak{p}}^{\times}$.

■

**Corollary 5.1.3** *Let $L$ be a lattice and suppose that*

$$L \cong \langle a_1 \mathfrak{p}^{\alpha_1}, a_2 \mathfrak{p}^{\alpha_2}, a_3 \mathfrak{p}^{\alpha_3} \rangle.$$

*Suppose that $\alpha_i \equiv \alpha_j \mod 2$ for some $i \neq j$, and that then $a_i a_j \notin \mod A_{\mathfrak{p}}^{\times 2}$. Then $\theta(O^+(L_{\mathfrak{p}})) \supset A_{\mathfrak{p}}^{\times}$.*

**Proof.** There is no loss of generality in supposing that $a_i = 1$ and $a_j = \delta \notin A_{\mathfrak{p}}^{\times 2}$. Let $m$ and $n$ be integers with the same parity. Then $m_i = \{r^2 \mathfrak{p}^m : r \in A_{\mathfrak{p}}^{\times}\}$ and

$m_j = \{\delta s^2 \mathfrak{p}^n : s \in A_\mathfrak{p}^\times\}$. It is clear that $\mathfrak{m}(L_\mathfrak{p}) \supset A_\mathfrak{p}^\times \mod k_\mathfrak{p}^{\times 2}$. ■

**Definition.** Let $\Omega$ be the set of all the places of $k$ and let $V$ be a ternary quadratic space and let $(L, q)$ be an integral lattice of discriminant $d$ in $V$. Let $c \in A$, $x \in L$ such that $q(x) = c$ and let $N_c$ stand for the subgroup of $J_k$ defined by

$$N_c = \{j_\mathfrak{p} \in J_k \mid (j_\mathfrak{p}; -cd)_\mathfrak{p} = 1 \ \ \forall \mathfrak{p} \in \Omega\}$$

where $(\ ,\ )_\mathfrak{p}$ denote the Hilbert symbol.

Define also

$$\theta(L_\mathfrak{p}, c) = \{\theta(\sigma) \subset k_p^\times \mid \sigma \in O^+(V_\mathfrak{p}) \text{ and } c \in \sigma(L_\mathfrak{p})\}.$$

■

The proofs of the following results are normally presented for $\mathbb{Z}$-lattices in some quadratic $\mathbb{Q}$-spaces. They use some local and group-theoretic arguments that are valid with no change in the function field case.

**Theorem 5.1.3 (Kneser, Hsia, Shulze-Pillot,[18])** *Suppose that $V$ is a regular quadratic space over $k$. Let $L$ be a lattice in $V$ and let $c \in A$ be represented by $L$. Then $c$ is either represented by all the spinor genera in $\mathcal{G}en(L)$ or exactly by half of these genera. The latter case occurs if and only if the following three conditions hold:*

1. $-cd \notin k^{\times 2}$
2. $\theta(J_L) \subset N_c$
3. $\theta(L_\mathfrak{p}, c) = (N_c)_\mathfrak{p}$

*Moreover two lattice $S, T$ in the same genus as $L$ lie in the same $c$-half-genus (i.e. both represent $c$ or both fail to do so) if and only if $T = \Sigma T$ for some $\Sigma \in J_V$ with $\theta(\Sigma) \in P_{k^\times} \cdot N_c \cdot \theta(J_L)$.*

**Definition.** Let $L$ be a ternary lattice of discriminant $d$, and let $c \in A$ be such that $-cd \notin (k^\times)^2$. Let $E$ be the quadratic extension $k[\sqrt{-cd}]/k$ and let $\mathfrak{p}$ be a prime in $E$ above $p$. ■

**Theorem 5.1.4 (Schulze-Pillot, [27])** *Let $p$ be a non dyadic prime and $c \in A$ with $-cd \notin (k^\times)^2$.*

1. *Suppose that $E_\mathfrak{p}/k_p$ is unramified. Then $\theta(O^+(L_p)) \subset (N_c)_p$ exactly when*

$$L_p \cong \langle a_1, a_2 p^{2r}, a_3 p^{2s} \rangle \qquad (a_i \in A_p^\times, 0 \leq r \leq s)$$

   *and in this case $\theta(L_p, c) \neq (N_c)_p$ if and only if*

   (a) *$-a_1 a_2 \in (k_p^\times)^2$ and $c \in p^{2r+1}$*

   (b) *$-a_1 a_2 \notin (k_p^\times)^2$ and $c \in p^{2s+1}$*

2. *Suppose that $E_\mathfrak{p}/k_p$ is ramified. Then from $\theta(O^+(L_p)) \subset (N_c)_p$ follows that*

$$L_p \cong \langle a_1, a_2 p^r, a_3 p^s \rangle \qquad (a_i \in A_p^\times, 0 < r < s)$$

   *and therefore $\theta(L_p, c) \neq (N_c)_p$ if and only if*

   (a) *$r$ is even and $c \in p^r$*

   (b) *$r$ is odd and $c \in p^s$*

*In particular we see that $v_\mathfrak{p}(c) \leq v_\mathfrak{p}(d)$ for all $\mathfrak{p} \neq \infty$ satisfying $-cd \notin (k_p^\times)^2$.*

### 5.1.2 The Work of Watson, Earnest and Chan-Daniels

We introduce the $\lambda$-transformation defined by Watson in his unpublished thesis. Let $L$ be a ternary lattice. For a prime $\mathfrak{p}$ consider $\Lambda_{\mathfrak{p}}(L) = \{x \in L : \forall z \in L, Q(x) + B(x,z) \equiv 0 \mod \mathfrak{p}\}$. It is clear that $\mathfrak{p}L \subset \Lambda_{\mathfrak{p}}(L) \subset L$. By suitably scaling the form on $\Lambda_{\mathfrak{p}}(L)$, one obtains a primitive lattice, which we call $\lambda_{\mathfrak{p}}(L)$. Note that one can also define this transformation locally. For the properties of this transformation, we refer to [6]. It is proved that

1. $\lambda_{\mathfrak{p}}(L)_{\mathfrak{p}} = \lambda_{\mathfrak{p}}(L_{\mathfrak{p}})$
2. $\lambda_{\mathfrak{p}}(L)_{\mathfrak{q}} = \epsilon L_{\mathfrak{q}}$ for some $\epsilon \in A_{\mathfrak{q}}^{\times}$
3. The transformations defined above do not increase the class number and preserve regularity.

**Lemma 5.1.3 (Lemma 2.7,[6])** *Let $L$ be an integral lattice and suppose $L_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}^{\beta}, c\mathfrak{p}^{\gamma}\rangle$. Then*

$$\lambda_{\mathfrak{p}}(L)_{\mathfrak{p}} = \begin{cases} \langle a, b, c\mathfrak{p}^{\gamma-2}\rangle & \text{if } \beta = 0 \text{ and } \gamma \geq 2 \\ \langle b, a\mathfrak{p}, c\mathfrak{p}^{\gamma-1}\rangle & \text{if } \beta = 1 \\ \langle a, b\mathfrak{p}^{\beta-2}, c\mathfrak{p}^{\gamma-2}\rangle & \text{if } \beta \geq 2 \end{cases}.$$

If a prime is such that $v_{\mathfrak{p}}(\mathrm{disc}(L)) \geq 2$, one applies $\lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}}$ to $L$, for a suitable $k_{\mathfrak{p}} \in \mathbb{N}$, and ends up with a lattice whose discriminant satisfies $v_{\mathfrak{p}}(\mathrm{disc}(L)) \leq 1$. Thus by applying these transformations for all the primes with $v_{\mathfrak{p}}(\mathrm{disc}(L)) \geq 2$, we find a lattice with a squarefree discriminant. If the original lattice is regular, so is the new lattice.

**Definition.** A definite ternary $\mathbb{F}_r[t]$-lattice $L$ is said to be special if

1. $L_{\mathfrak{p}}$ has a unimodular component of rank 2 for every $\mathfrak{p}$;

2. $v_{\mathfrak{p}}(\mathrm{disc}(L)) \leq 2$ for every $\mathfrak{p}$ with $\partial(\mathfrak{p}) \leq 2$.

■

One will notice that lattice with squarefree discriminants are special. From the definition above follows that if a lattice $L$ is special, then it represents all of $A_{\mathfrak{p}}^{\times}$ for any prime $\mathfrak{p}$ and hence $\mathcal{G}en(L)$ represents an element in $\mathbb{F}_r$. That implies in particular that, when $L$ is regular, $\mu_1(L)$ must be 0.

**Theorem 5.1.5 (Chan-Daniels, [5])** *Suppose that $L$ is a definite, regular, special ternary $\mathbb{F}_r[t]$-lattice. Then*

$$(\mu_1, \mu_2, \mu_3) = \begin{cases} (0,0,1) \\ (0,1,1) \\ (0,0,3) \end{cases}.$$

*Consequently $\partial(\mathrm{disc}(L)) \leq 3$. Also, the last case above can occur only if $r = 3$.*

## 5.2 Technical Lemmata

**Lemma 5.2.1 (V.1, [3])** *Let $a \neq 0$ be an element of $\mathbb{F}_r$ and let $\delta \in \mathbb{F}_r$ be a nonsquare. Then*

- $\#\{(x,y) \in \mathbb{F}_r^2 : x^2 - \delta y^2 = a\} = r + 1$
- $\#\{(x,y) \in \mathbb{F}_r^2 : x^2 - y^2 = a\} = r - 1$

**Lemma 5.2.2** *Suppose that $(L, q)$ is a binary definite lattices and suppose that $q = (1, 0, a)$ where $\partial(a) = 2$. We let $N = 2n$ be an even integer and let $V_N'(L) \subset$*

*$V_N(L)$ be the set of monic polynomials in $V_N(L)$. Then*

$$\#V'_N(L) \leq \frac{r(r^{2n}-1)}{4(r-1)} + \frac{r(r^n-1)}{2(r-1)} + 2.$$

**Proof.** Definiteness implies that $q$ represents only polynomials with even degrees. Let $E_{2k}$ be the set of polynomials of degree $2k$ represented by $q$.

We first find $\#E_{2k}$. We need to choose two polynomials, $f$ and $g$, of respective degree $k$ and $k-1$ and need to make sure that the leading coefficient of $q(f,g)$ is 1. To achieve that, we have $(r+1)r^k r^{k-1}$ choices. Among these we need to notice that except when $g=0$, 4 pairs will rise to the same value of $q(f,g)$. When $g=0$, only two pairs will give a given value $q(f,g)$. Also, notice that the only polynomial of degree $< 2$ represented by $q$ is 1 and it comes from $q(\pm 1, 0)$. Hence

$$\#E_{2k} \leq \begin{cases} \frac{1}{4}((r+1)r^k r^{k-1} - 2r^k) + r^k & \text{if} \quad k \neq 0 \\ 2 & \text{if} \quad k = 0 \end{cases}.$$

The result is obtained by summing these values. ■

**Lemma 5.2.3** *Let $\mathfrak{p}$ be a prime and let $\epsilon \in \{-1, 1\}$ and let $N_\epsilon$ be the number of linear primes $\mathfrak{l} \neq \mathfrak{p}$ with $\left(\frac{\mathfrak{l}}{\mathfrak{p}}\right) = \epsilon$.*

1. *If $\mathfrak{p}$ is linear, $N_\epsilon = \frac{r-1}{2}$;*
2. *If $\mathfrak{p}$ is quadratic,*
   - $N_{-1} = \frac{r+1}{2}$;
   - $N_{+1} = \frac{r-1}{2}$;

*In particular, if $\partial(\mathfrak{p}) \leq 2$, there are linear polynomials whose leading coefficients are in arbitrary square classes of $\mathbb{F}_r$, which are squares or nonsquares in $A_\mathfrak{p}^\times$.*

**Proof.** Let $\mathfrak{p} = t - a$, then $\left(\frac{t+\omega}{\mathfrak{p}}\right) = \left(\frac{a+\omega}{\mathfrak{p}}\right) = \chi(a+w)$. The possibility $a+w=0$ is to be excluded since $\mathfrak{l} \neq \mathfrak{p}$.

Suppose that $\mathfrak{p} = t^2 + bt + c$ where $b^2 - 4c = \delta\xi^2$ and let $\mathfrak{l} = t - \omega$. By reciprocity we have

$$\left(\frac{t-\omega}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{p}}{t-w}\right) = \chi(\mathfrak{p}(\omega)).$$

The result follows easily from Lemma 5.2.1 by noticing that $\mathfrak{p}(\omega) = (\omega + b/2)^2 - 4\delta\xi^2$. ■

**Lemma 5.2.4** *Let $(L, q)$ be a reduced binary lattice and suppose $q = (a, 2b, c)$. Suppose further that $\mathrm{disc}(L) = D$ and that $\mu_1(L) = \mu_2(L) = 1$. Let $N$ be the number of linear polynomials represented by $L$ (i.e. $N = \#V_1(L)$). Then*

1. *$N = \frac{(r-1)^2}{2}$ if $D$ is irreducible;*
2. *$N = \frac{(r+1)^2}{4} - 1$ if $D$ has two disctinct prime divisors; and*
3. *$N = r - 1$ if $D$ is divisible by a square.*

**Proof.** By [5], Lemma 3.7, we know that $h(L) = 1$, where $h(\cdot)$ denotes the class number. Since $L$ is definite, we can suppose that $D = -\delta D'$ where $D'$ is monic.

We first suppose that $D' = \mathfrak{p}$ where $\mathfrak{p}$ is a quadratic prime. Since $\partial(\mathfrak{p}) = 2$, we see that $\mathbb{F}_r^\times \subset A_\mathfrak{p}^{\times 2}$. In particular, for any non zero constant $\alpha$ we have $\left(\frac{\alpha l}{D}\right) = \left(\frac{l}{D}\right)$. Let $\mathfrak{l} = t - \omega$ be a prime, and suppose that $\mathfrak{p} = t^2 + bt + c$ where $b^2 - 4c = \delta\xi^2$ for some nonsquare $\delta$. The quadratic reciprocity tells that

$$\left(\frac{l}{-\delta\mathfrak{p}}\right) = \chi(-\delta)\left(\frac{-\delta\mathfrak{p}}{l}\right) = \left(\frac{\mathfrak{p}}{l}\right) = \chi(\mathfrak{p}(\omega)).$$

Let $\omega \in \mathbb{F}_r^\times$, $\mathfrak{p}(\omega)$ is a square if and only if there is $\rho \in \mathbb{F}_r^\times$ such that $(\omega + \frac{b}{2})^2 - \frac{1}{4}\delta\xi^2 = \rho^2$. The number of such $\omega$ is therefore $\frac{r-1}{2}$. Putting everything together, we get $N = \frac{(r-1)^2}{2}$.

Let us now suppose that $D' = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 \neq \mathfrak{p}_2$ are both linear primes. It is easily proved that $L$ must be decomposable. Let us suppose for instance that $q \cong (\mathfrak{p}_1, 0, -\delta\mathfrak{p}_2)$. Any linear polynomial represented is of the form $\alpha^2\mathfrak{p}_1 - \delta\beta^2\mathfrak{p}_2$. Clearly the pairs $(\alpha, \beta)$ and $(-\alpha, -\beta)$ will lead to the same linear polynomials. Let us prove that no pair $(\alpha, \beta)$, $(\gamma, \eta)$ with $\eta^2 \neq \beta^2$ can lead to the same linear polynomial. Suppose to that aim that

$$\alpha^2\mathfrak{p}_1 - \delta\beta^2\mathfrak{p}_2 = \gamma^2\mathfrak{p}_1 - \delta\eta^2\mathfrak{p}_2 \tag{5.1}$$

The equality of the leading coefficients writes as $\alpha^2 - \delta\beta^2 = \gamma^2 - \delta\eta^2$ and substituting these values in (5.1), one gets $\delta(\beta^2 - \eta^2)(\mathfrak{p}_1 - \mathfrak{p}_2) = 0$. The claim follows since $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Now, we see easily that $N = \frac{(r+1)^2}{4} - 1$.

We finally suppose that $D' = \mathfrak{p}^2$. As proved by Chan, we have $q \cong (\mathfrak{p}, 0, -\delta\mathfrak{p})$. A short computation proves that the automorphs of $q$ are in correspondance with the pairs $(\alpha, \beta) \in \mathbb{F}_r^\times \times \mathbb{F}_r^\times$ such that $\alpha^2 - \delta\beta^2 = 1$. But the number of such pairs is $r + 1$ and we get $N = \frac{r^2-1}{r+1}$. ■

**Lemma 5.2.5** *Let $\mathfrak{p} = t - a$ and $\mathfrak{l} = t - b$ be two distinct linear primes and let $\epsilon_1, \epsilon_2 \in \{\pm 1\}$. Define $N_{\epsilon_1,\epsilon_2}$ to be the number of linear polynomials, $l$, satisfying $\left(\frac{l}{\mathfrak{p}}\right) = \epsilon_1$ and $\left(\frac{l}{\mathfrak{l}}\right) = \epsilon_2$. Then*

1. $N_{1,1} = \begin{cases} \frac{(r-1)(r-5)}{4} & \text{if} \quad \chi(b-a) = \chi(-1) = 1 \\ \frac{(r-1)^2}{4} & \text{if} \quad \chi(b-a) = -1; \chi(-1) = 1 \\ \frac{(r-1)(r-3)}{4} & \text{if} \quad \chi(-1) = -1 \end{cases}$

2. $N_{1,-1} = \begin{cases} \frac{(r-1)(r-3)}{4} & \text{if} \quad \chi(b-a) = \chi(-\delta) = 1 \\ \frac{(r-1)(r+1)}{4} & \text{if} \quad \chi(b-a) = -1; \chi(-\delta) = 1 \\ \frac{(r-1)(r-1)}{4} & \text{if} \quad \chi(-\delta) = -1 \end{cases}$

3. $N_{-1,-1} = \begin{cases} \frac{(r-1)(r+1)}{4} & \text{if} \quad \chi(b-a) = \chi(-\delta) = 1 \\ \frac{(r-1)(r-3)}{4} & \text{if} \quad \chi(b-a) = -1; \chi(-\delta) = 1 \\ \frac{(r-1)(r-1)}{4} & \text{if} \quad \chi(-\delta) = -1 \end{cases}$

**Proof.** Since $\partial(\mathfrak{p}) = 1$, we see that $A_{\mathfrak{p}}^{\times 2} \cap \mathbb{F}_r^{\times} = \mathbb{F}_r^{\times 2}$. It is therefore enough to compute $N$ for monic polynomials and then to multiply the number found by $\frac{r-1}{2}$. Let $\mathfrak{g} = t + \xi$ be a linear prime, we have $\left(\frac{\mathfrak{g}}{\mathfrak{p}}\right) = \chi(a+\xi)$ and $\left(\frac{\mathfrak{g}}{\mathfrak{l}}\right) = \chi(b+\xi)$.

We first compute $N_{1,1}$, which is exactly $\frac{r-1}{2}$ times the number of $\xi$ such that $a + \xi = \eta^2$ and $b + \xi = \rho^2$ for some $\eta, \rho \in \mathbb{F}_r^{\times}$. So, we see that

$$N_{1,1} = \frac{r-1}{2} \cdot \frac{1}{2} \cdot \#\{(\eta, \rho) : \rho \neq 0\,, \eta \neq 0, \text{ and } \rho^2 - \eta^2 = b - a\}.$$

We now compute $N_{1,-1}$, which is exactly $\frac{r-1}{2}$ times the number of $\xi$ such that $a + \xi = \eta^2$ and $b + \xi = \delta\rho^2$ for some $\eta, \rho \in \mathbb{F}_r^{\times}$. So, we see that

$$N_{1,-1} = \frac{r-1}{2} \cdot \frac{1}{2} \cdot \#\{(\eta, \rho) : \rho \neq 0\,, \eta \neq 0, \text{ and } \rho^2 - \delta\eta^2 = b - a\}.$$

Finally to compute $N_{-1,-1}$, one notices that it is exactly $\frac{r-1}{2}$ times the number of $\xi$ such that $a + \xi = \delta\eta^2$ and $b + \xi = \delta\rho^2$ for some $\eta, \rho \in \mathbb{F}_r^{\times}$. So, we see that

$$N_{1,-1} = \frac{r-1}{2} \cdot \frac{1}{2} \cdot \#\{(\eta, \rho) : \rho \neq 0\,, \eta \neq 0, \text{ and } \rho^2 - \eta^2 = \frac{b-a}{\delta}\}.$$

In the three cases we can conclude with Lemma 5.2.1. ■

**Lemma 5.2.6** *Let $p$ and $p'$ be two quadratic monic irreducible polynomials. Suppose that for all $\alpha \in \mathbb{F}_r$, we have $\chi(p(\alpha)) = \chi(p'(\alpha))$, then $p = p'$.*

**Proof.** If $p(t) = t^2 + bt + c$ then $\chi(p(\alpha/\beta)) = \chi(\alpha^2 + b\alpha\beta + c\beta^2)$. The result then follows from Lemma 3.4.2. ■

**Lemma 5.2.7** *Let $L$ and $L'$ be binary lattices whose Gram matrix can be written in reduced basis as*

$$q = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \quad \text{and} \quad q' = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}.$$

*Suppose further that $L$ and $L'$ have the same sequence of successive minima, say $\mu_1, \mu_2$. Suppose finally that $\mu_1 \not\equiv \mu_2 \mod 2$. If $V_{\mu_2}(L) = V_{\mu_2}(L')$ then $L$ and $L'$ are isometric.*

*In particular, if $a, a'$ have same leading coefficients and so do $c, c'$, we have $(a, 2b, c) = (a', 2b', c')$.*

**Proof.** There is no loss of generality in assuming that $a = a'$ and that $c, c'$ have the same leading coefficients.

Since $c'$ is represented by $q$, and since $q$ is definite we we can find $f \in A$ and $\beta \in \mathbb{F}_r$ such that

$$c' = af^2 + 2bf\beta + c\beta^2.$$

Note that the assumption on successive minima implies that $\beta \neq 0$. Make $M = \begin{pmatrix} 1 & f \\ 0 & \beta \end{pmatrix} \in GL_2(A)$ act on $f'$ to get

$$q' \cong \begin{pmatrix} a & af + b'\beta \\ af + b'\beta & q(f, \beta) \end{pmatrix}.$$

One has to be careful because as written above the form $q'$ is not *a priori* reduced. Nevertheless, the work above tells that

$$\partial(af + b'\beta) < \partial c.$$

So $q = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ and $q' = \begin{pmatrix} a & af + b'\beta \\ af + b'\beta & c \end{pmatrix}$ have same representations up to $\partial c$. If $f \neq 0$ choose $r \in \mathbb{F}_r$ such that the leading coefficient of $1 + rf$, say $\xi$, is not a square $\in \mathbb{F}_r$ . The polynomial $a + r(af + b'\beta) + cr^2$ is represented by $q'$ and so is also represented by $q$. So we have $\epsilon, \gamma = \gamma_n x^n + \cdots + \gamma_1 x + \gamma_0 \in A$ with

$$a + r(a\beta + b'f) + cr^2 = a\gamma^2 + c\epsilon^2 + \gamma\epsilon b.$$

Degree implies that in fact $\epsilon \in \mathbb{F}_r$ and considerations on the leading coefficients of the expression above imply $\epsilon^2 = r^2$. Thus,

$$a + r(af + b'\beta) = a\gamma^2 \pm r\gamma b$$

which leads to

$$a(1 + rf) + rb'\beta = a\gamma^2 \pm \gamma b.$$

But $\partial b$ and $\partial b'$ are both $< \partial a$. So we see that $a_n \xi = a_n \gamma_n^2$ which is a contradiction. So $f = 0$ and the Gram matrix of $L'$ may be written in some reduced basis

$$q' = \begin{pmatrix} a & b' \\ b' & c \end{pmatrix}.$$

Now $a + b + c$ is represented by $q$ and so must be represented by $q'$. We find $g, \beta \in A$ with

$$a + b + c = ag^2 + b'\beta g + c\beta^2.$$

Considerations on the degree and the leading coefficients of both sides give that in fact $\beta \in \mathbb{F}_r$ and $\beta^2 = 1$. Thus

$$a + b = ag^2 \pm b'g.$$

Since $\partial(b'g) < \partial(ag^2)$ it clearly follows that $g \in \mathbb{F}_r$ and equality of leading coefficient tells that in fact $g^2 = 1$. This finally leads to $b = \pm b'$. ■

**Lemma 5.2.8** *Ternary lattices with the following properties have class number one:*

1. *lattices of discriminant $D$ with $\partial D \leq 2$;*

2. *lattices of discriminant $D$ with $\partial D = 3$ such that*

   (a) *$D = -\delta\mathfrak{p}^3$ and $L_\mathfrak{p} \cong \langle \epsilon, \eta\mathfrak{p}, \rho\mathfrak{p}^2 \rangle$*

*(b)* $D = -\delta\mathfrak{p}^2\mathfrak{q}$, $L_\mathfrak{p} \cong \langle \epsilon, \eta\mathfrak{p}, \rho\mathfrak{p}\rangle$ *and* $L_\mathfrak{q} \cong \langle \epsilon', \eta', \rho'\mathfrak{q}\rangle$.

3. *lattices of discriminant* $D$ *with* $\partial D = 4$ *such that* $L_\mathfrak{p} \cong \langle \epsilon, \mathfrak{p}, -\epsilon\mathfrak{p}\rangle$, *for some quadratic prime,* $\mathfrak{p}$ *and some* $\epsilon \notin A_\mathfrak{p}^{\times 2}$.

**Proof.** (1) is proved in [5].

Let $L$ be a lattice as in 2.$(a)$ or 2.$(b)$. We see that $W_\infty \cong \langle 1, -\delta, t\rangle$. Since $\partial(\mathfrak{p}) = 1$, we can suppose that $\epsilon, \eta, \rho \in \mathbb{F}_r^\times$. The configuration for the successive minima of a lattice in the genus of $L$ is $(0, 0, 3)$ or $(0, 1, 2)$. But, locally $L$ represents only one square class of $\mathbb{F}_r^\times$; hence the sequence of minima of any lattice in $\mathcal{G}en(L)$ is $(0, 1, 2)$. Let $(L', q')$ be a lattice in $\mathcal{G}en(L)$ and write the Gram matrix of $q'$ and $q$ in reduced basis,

$$q' \cong \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & c' & f' \\ 0 & f' & g' \end{pmatrix}; \quad q \cong \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & c & f \\ 0 & f & g \end{pmatrix}$$

where $\partial(c') = 1$, $\partial(f') \leq 0$ and $\partial(g') = 2$. Also, note that the assumption on $W_\infty$ implies that $c'$ is monic.

We now count the number, $N$, of linear polynomials represented by $L'^{2\times 2}$. A linear polynomial is represented by $L'^{2\times 2}$ if it is of the form $\epsilon\alpha^2 + c_i\beta^2$ and therefore there are exactly $\frac{r^2-1}{2}$ of them. On the other hand a monic linear polynomial is locally represented by $L'$ if it is a square in $A_\mathfrak{p}^\times$ or a square multiple of $\mathfrak{p}$ in one case and in the other case, if it is a square in $A_\mathfrak{p}^\times$ or a square multiple of $\mathfrak{q}$. That tells that there is at most $\frac{r^2-1}{1}$ linear polynomials represented locally. Now, a linear prime represented globally is clearly represented locally and it follows that $L^{2\times 2}$ and $L'^{2\times 2}$ represent the same linear prime. Lemma 5.2.7 applies and tells that $L^{2\times 2} \cong L'^{2\times 2}$ and in particular that $c = c'$. Since $L$ and $L'$ must have the same discriminant it follows that $cg - f^2 = cg' - f'^2$ (i.e. $c(g - g') = f^2 - f'^2$). As $\partial(f) = \partial(f') = 0$ the previous equality is impossible unless $g = g'$ and $f = \pm f'$.

Let $\mathcal{G}$ be a genus as in 3. above. Let $L$ be a lattice in it. Since $\mathcal{G}$ does not represent any constant, and since $\partial(\mathrm{disc}(L)) = 4$, the only possible configuration for successive minima of $L$ is $(1, 1, 2)$. Suppose a Gram matrix for $L$ written in a reduced basis is

$$M = \begin{pmatrix} a & b & e \\ b & c & f \\ e & f & g \end{pmatrix}$$

where $\partial a = \partial c = 1$ and $\partial g = 2$. Let $q$ be the binary form on $L^{2\times 2}$. Since $L_{\mathfrak{p}} \cong \langle \epsilon, \mathfrak{p}, -\epsilon\mathfrak{p} \rangle$, we see that $\mathfrak{p}$ must divide $\mathrm{disc}\,(M^{2\times 2}) = \mathrm{disc}(q)$. Now, we have

$$\eta\mathfrak{p}^2 = \mathrm{disc}(L) = g \cdot \mathrm{disc}(q) - q(-f, e)$$

and we see that $\mathfrak{p}$ must divide $q(-f, e)$. But $q$ is definite and $\partial(\mathfrak{p}) = 2$. Also, we have $\partial(q(-f, e)) = 1$, except when both $e$ and $f$ are 0. So we see that $L$ is decomposable.

Let $L$, $L'$ be two lattices in $\mathcal{G}$, let $q, q'$ be forms on their $2 \times 2$-sections and let $M$ and $M'$ be their reduced Gram matrices. We have

$$M = \begin{pmatrix} a & b & 0 \\ b & c & 0 \\ 0 & 0 & g \end{pmatrix} \quad , \quad M = \begin{pmatrix} a' & b' & 0 \\ b' & c' & 0 \\ 0 & 0 & g' \end{pmatrix}.$$

Since $L$ and $L'$ are in the same genus, we can suppose that $g = g'$. Then follows easily that $q$ and $q'$ have the same irreducible discriminant (up to multiplication by a square of $\mathbb{F}_r^{\times}$). Since $\mathrm{disc}(q) = \mathrm{disc}(q')$ are irreducible, Corollary 3.5.1 implies that $q \cong q'$. Finally $L \cong L'$.

■

## 5.3 Regular Ternary Lattices

In [5], Chan and Daniels proved that there are finitely many definite regular lattices. Here we prove that any definite regular lattice has class number one and

we make a list of all the lattices having class number one.

**Definition.** Let $L$ be a ternary lattice with discriminant $D$, let $\mathfrak{p}$ be a prime dividing $D$ and let $\lambda = \prod_{\mathfrak{p}|D} \lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}}$. We say that

1. $\mathfrak{p}$ is a good prime for $L$ if $v_{\mathfrak{p}}(\mathrm{disc}(\lambda(L))) = 1$;

2. $\mathfrak{p}$ is a bad prime for $L$ if $v_{\mathfrak{p}}(\mathrm{disc}(\lambda(L))) = 0$.

For a given lattice $L$, we let $G$ and $B$ respectively stand for the sets of good and bad primes. ■

**Lemma 5.3.1** *Let $L$ be a regular ternary $\mathbb{F}_r[t]$-lattice with $r \neq 3$. There are three possibilities:*

1. *$L$ has only one good prime which is linear;*

2. *$L$ has only one good prime which is quadratic;*

3. *$L$ has two linear good primes.*

**Proof.** If $L$ does not have any good prime then $\lambda(L)$ is unimodular (and therefore isotropic) at any finite place. By reciprocity, it cannot be anisotropic at $\infty$; hence this case is to be excluded.

For the other cases, the result follows easily from Theorem 5.1.5 by noticing that the good primes are exactly those primes dividing $\mathrm{disc}(\lambda(L))$. ■

We start by writing what happens if we apply $\lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}-i}$ instead of $\lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}}$ to $L_{\mathfrak{p}}$. For a given prime $\mathfrak{p}$, we have

1. If $\mathfrak{p}$ is good:

$$\begin{array}{ccccc}
\lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}-2}(L)_{\mathfrak{p}} & & \langle b, a\mathfrak{p}, c\mathfrak{p}^2\rangle & & \langle b, a\mathfrak{p}^3, c\mathfrak{p}^3\rangle \\
 & \searrow & & \swarrow & \\
\lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}-1}(L)_{\mathfrak{p}} & & \langle a, b, \mathfrak{p}^3 c\rangle \quad \langle c, a\mathfrak{p}, b\mathfrak{p}\rangle & & \langle a, b\mathfrak{p}^2, c\mathfrak{p}^3\rangle \\
 & \searrow & \downarrow & \swarrow & \\
\lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}}(L)_{\mathfrak{p}} & & \langle a, b, \mathfrak{p}c\rangle & &
\end{array} \tag{5.2}$$

2. If $\mathfrak{p}$ is bad :

$$\begin{array}{ccccc}
\lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}-1}(L)_{\mathfrak{p}} & & \langle a, b\mathfrak{p}^2, c\mathfrak{p}^2\rangle & & \langle a, b, c\mathfrak{p}^2\rangle \\
 & & \searrow & \swarrow & \\
\lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}}(L)_{\mathfrak{p}} & & & \langle a, b, c\rangle & 
\end{array} \tag{5.3}$$

**Theorem 5.3.1** *Let $L$ be a definite ternary $\mathbb{F}_r[t]$-lattice, where $r > 3$. The following assertions are equivalent:*

1. *$L$ is regular;*

2. *$L$ has class number one;*

3. *$L$ is one of the forms in Lemma 5.2.8.*

**Proof.** Let $L$ be a regular lattice of discriminant $D$. First, notice that multiplying all the lattices in a genus by a nonsquare of $\mathbb{F}_r$ will change neither regularity, nor change the class number. In particular, when $\partial(D) \equiv 1 \mod 2$, one can suppose that $W_\infty \cong \langle 1, -\delta, t\rangle$ and when $\partial(D) \equiv 0 \mod 2$, one can suppose that $W_\infty \cong \langle 1, t, -\delta t\rangle$.

**Claim 1.** If $L$ is regular, then $L$ has no bad prime.

**Proof.** Let $\mathfrak{q}$ be a bad prime for $L$ and consider the transformation

$$\Lambda = \lambda_{\mathfrak{q}}^{k_{\mathfrak{q}}-1} \cdot \prod_{\mathfrak{p}|D, \mathfrak{p}\neq\mathfrak{q}\in G} \lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}}.$$

Since $\mathfrak{q}$ is a bad prime for $L$, $\Lambda(L)$ must be regular. Also, the previous tables tell that either $\Lambda(L)_{\mathfrak{q}} \cong \langle a, b, c\mathfrak{q}^2\rangle$ or $\Lambda(L)_{\mathfrak{q}} \cong \langle a, b\mathfrak{q}^2, c\mathfrak{q}^2\rangle$. In both of these cases it is easy to see that $\Lambda(L)_{\mathfrak{q}}$ is isotropic. We have to deal we any possible configuration for the good primes. For the sake of clarity, we split the proof into some cases:
(1) If $\Lambda(L)_{\mathfrak{q}} \cong \langle a, b, c\mathfrak{q}^2\rangle$ we see that at any finite place all the units must be represented. Thus $\Lambda(L)$ must represent either

(i) all of $\mathbb{F}_r$ and one linear prime; or

(ii) one square class of $\mathbb{F}_r$ and two linear primes.

In both cases we see that the sum of the successive minima cannot exceed 2, which is a contradiction. Indeed the tables above show that $\partial(\mathrm{disc}(\Lambda L)) \geq 2\partial(\mathfrak{q})+1 \geq 3$.

(2) Suppose that $\lambda(L)_{\mathfrak{q}} \cong \langle 1, b\mathfrak{q}^2, c\mathfrak{q}^2\rangle$.

(i) Let $\mathfrak{p}$ be the unique good prime for $L$. If $\lambda(L)_{\mathfrak{p}} \cong \langle 1, -\delta, \epsilon\mathfrak{p}\rangle$ with $\partial(\mathfrak{p}) = 1$ then $\lambda(L)_{\infty} \cong \langle 1, -\delta, t\rangle$. Clearly 1 is represented by $\Lambda L$ and thus $\mu_1 = 0$. We claim that $0 < \mu_2 \leq 2$. It is clear that a nonsquare of $\mathbb{F}_r$ cannot be represented at $\mathfrak{q}$. If there is a linear prime coprime to $\mathfrak{p}$ which is a square in $A_{\mathfrak{q}}^{\times}$ (which is the case whenever $\partial(\mathfrak{q}) \leq 2$ as proved in Lemma 5.2.3), then we have $\mu_2 = 1$. If not, all the linear primes but maybe $\mathfrak{p}$ are nonsquare in $A_{\mathfrak{q}}^{\times}$. The product of two distinct nonsquares becomes a square in $A_{\mathfrak{q}}^{\times}$ and is therefore represented by $\Lambda L$. Note that this product cannot be represented by $\langle 1\rangle$ since it is not a square in $A$. If $\mu_2 = 1$, we are done. Indeed, $\Lambda L$ represents any multiple of $\mathfrak{q}^2$. In particular $\mu_3 \leq 2\partial(\mathfrak{q})$ and thus $4\partial(\mathfrak{q}) + 1 = \partial(\mathrm{disc}(\Lambda L)) \leq 2\partial(\mathfrak{q}) + 1$.
We assume, therefore, that $\mu_2 = 2$ and define $A^{(d)} = \{h \in A : \partial(h) \leq d-1\}$. Note that a monic polynomials in $A^{(d)}$ is represented by $\Lambda L$ whenever it is coprime to $\mathfrak{p}$ and is a square in $A_{\mathfrak{q}}^{\times}$. If $N$ is the number of such polynomials, we have

$$N \geq \frac{1}{r-1}\left(\frac{r^d - 1}{2} - (r^{d-1} - 1)\right).$$

On the other hand, remember that the $2 \times 2$-section of $\Lambda L$ is decomposable since $\mu_1 = 0$. In particular Lemma 5.2.2 applies and tells that the number of polynomials represented by this $2 \times 2$ section is

$$N' \leq \frac{r(r^{2\left[\frac{d-1}{2}\right]} - 1)}{4(r-1)} + \frac{r(r^{\left[\frac{d-1}{2}\right]} - 1)}{2(r-1)} + 2.$$

Since $d \geq 3$, we see that $N' < N$. In particular $\mu_3 < \partial(\mathfrak{q})$, which is a contradiction.

(ii) If $\lambda(L)_{\mathfrak{p}} \cong \langle 1, -\eta, \epsilon\mathfrak{p} \rangle$ with $\partial(\mathfrak{p}) = 2$ and $\eta \notin A_{\mathfrak{p}}^{\times 2}$, then $\lambda(L)_{\infty} \cong \langle 1, t, -\delta t \rangle$. Clearly 1 is represented by $\Lambda L$ and thus $\mu_1 = 0$. It is clear that a linear polynomials is represented by $\Lambda L$ if and only if it is represented at $\mathfrak{q}$ (i.e. if it is a square in $A_{\mathfrak{q}}^{\times}$). Suppose that no linear prime is a square in $A_{\mathfrak{q}}^{\times}$. If $\mathfrak{l} \neq \mathfrak{l}'$ are both nonsquares in $A_{\mathfrak{q}}$ their product must be a square, and since it is monic and coprime to $\mathfrak{p}$ it is represented by $\Lambda L$. Since $\mathfrak{l}\mathfrak{l}'$ is not a square in $A$, it cannot be represented by $\langle 1 \rangle$; hence $\mu_2 = 2$ and we get a contradiction since $\Lambda L$ can only have one even successive minimum. We finally conclude that $\mu_1 = 1$. In particular we have

$$\Lambda L^{2\times 2} \cong \begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix}$$

where $\xi = \xi_1 t + \xi_0$ is a linear polynomial. If there is a linear polynomial whose leading coefficient is not in the same square class as $\xi_1$ and which is a square in $A_{\mathfrak{q}}^{\times}$, then we see that $\mu_3 = 1$, which is not possible. In particular, any linear polynomial whose leading coefficient is not in the same square class as $\xi_1$ is a not a square in $A_{\mathfrak{q}}^{\times}$.

The number of monic polynomials of degree 2 represented by $\Lambda L^{2\times 2}$ is $N = r + \frac{r(r-1)}{2}$ and the number of monic polynomials of degree 2 which are not multiple of $\mathfrak{p}$ is $N' = r^2 - 1$. Thus there are monic polynomials of degree 2, which are not multiple of $\mathfrak{p}$ and which are not represented by $\Lambda L^{2\times 2}$. It is clear that these polynomials cannot be square in $A_{\mathfrak{q}}^{\times}$. If $\mathfrak{l}$ is any of them and if $\mathfrak{l}'$ is a linear

polynomial whose leading coefficient is not in the same square class as $\xi_1$, we see that $\mathfrak{l}\mathfrak{l}'$ is a square in $A_{\mathfrak{q}}^{\times}$. It is represented globally. But its leading coefficient is not in the same square class as $\xi_1$ and hence it cannot be represented by $\Lambda L^{2\times 2}$. Finally $\mu_3 = 3$ which contradicts degree conditions.

(iii) Suppose that $L$ has two linear good primes, $\mathfrak{p}$ and $\mathfrak{g}$. Since $\Lambda(L)_{\mathfrak{q}}$ is isotropic, we can, by reciprocity, suppose that $\Lambda(L)_{\mathfrak{g}}$ is isotropic (and hence universal). So, we have $\lambda(L)_{\mathfrak{p}} \cong \langle 1, -\delta, \epsilon_{\mathfrak{p}}\mathfrak{p}\rangle$, $\lambda(L)_{\mathfrak{g}} \cong \langle 1, -1, \epsilon_{\mathfrak{g}}\mathfrak{g}\rangle$ and hence $\lambda(L)_{\infty} \cong \langle 1, t, -\delta t\rangle$. It is clear that 1 is represented by $\Lambda L$; hence $\mu_1 = 0$. If $\mu_2 \neq 1$, we see that any linear polynomial except maybe $\mathfrak{p}$ must be a nonsquare in $A_{\mathfrak{q}}$. We conclude exactly as in the previous case.

(3) Suppose that $\lambda(L)_{\mathfrak{q}} \cong \langle a, b\mathfrak{q}^2, c\mathfrak{q}^2\rangle$ where $a \notin A_{\mathfrak{q}}^{\times 2}$. Suppose further that $\partial(\mathfrak{q}) \equiv 1 \mod 2$. It implies in particular that $\alpha \in \mathbb{F}_r$ is a square in $A_{\mathfrak{q}}^{\times}$ if and only if it is a square in $\mathbb{F}_r$.

(i) If $\lambda(L)_{\mathfrak{p}} \cong \langle 1, -\delta, \epsilon\mathfrak{p}\rangle$ with $\partial(\mathfrak{p}) = 1$ then $\lambda(L)_{\infty} \cong \langle 1, -\delta, t\rangle$ and we can conclude as in 2(i) above. Under the assumptions made on $\partial(\mathfrak{q})$ we see that $\delta \in \mathbb{F}_r$ is represented by $\Lambda L$; hence $\mu_1 = 0$. If there is a linear prime not equal to $\mathfrak{p}$ which is not a square in $A_{\mathfrak{q}}^{\times}$ (which is the case when $\partial(\mathfrak{q}) = 1$), we can conclude that $\mu_2 = 1$. But, we see that any multiple of $\mathfrak{q}^2$ is represented by $\Lambda L$, and that leads to a contradiction since in this case $4\partial(\mathfrak{q}) + 1 = \partial(\mathrm{disc}(\Lambda L)) \leq 2\partial(\mathfrak{q}) + 1$. We suppose that any linear prime $\mathfrak{l} \neq \mathfrak{p}$ is a square in $A_{\mathfrak{q}}^{\times}$. Let $\mathfrak{l} \neq \mathfrak{l}'$ be two such primes. For a nonsquare $\alpha \in \mathbb{F}_r$, $\alpha\mathfrak{l}\mathfrak{l}'$ becomes a nonsquare in $A_{\mathfrak{q}}$, it has degree 2, is in $A_{\mathfrak{p}}^{\times}$: it must be represented by $\lambda L$, but cannot be represented by $\langle 1\rangle$. Therefore we see that $\mu_2 = 2$. We can now use the same argument as in 2.(i) above.

(ii) If $\lambda(L)_{\mathfrak{p}} \cong \langle 1, -\eta, \epsilon\mathfrak{p}\rangle$ with $\partial(\mathfrak{p}) = 2$ and $\eta \notin A_{\mathfrak{p}}^{\times 2}$, then $\lambda(L)_{\infty} \cong \langle 1, t, -\delta t\rangle$. We see that no element of $\mathbb{F}_r^{\times}$ is represented by $\Lambda L$. Furthermore,

$\Lambda(L)_\infty$ and $\Lambda(L)_\mathfrak{p}$ represent all the linear primes. If $\mathfrak{l}$ is a linear prime and $\alpha$ is a nonsquare in $\mathbb{F}_r$ then either $\mathfrak{l}$ or $\alpha\mathfrak{l}$ is represented by $\Lambda(L)_\mathfrak{q}$. Hence $\mu_1 = 1$. Let $\langle\xi\rangle = \Lambda L^{1\times 1}$ and suppose that $\xi = \xi_1 t + \xi_0$. If there is a linear polynomial $g$ which is not a square in $A_\mathfrak{q}^\times$, and whose leading coefficient is not in the same square class as $\xi_1$ then we have $\mu_2 = 1$. That is not possible, since $\Lambda L$ represents $\mathfrak{q}^2$ and thus $\mu_3 \leq 2\partial(\mathfrak{q})$. In this case, we see that $2 + 2\partial(\mathfrak{q}) \geq \partial(D) = 2 + 4\partial(q)$. So, any linear polynomial whose leading coefficient is not in the same square class as $\xi_1$ is a square in $A_\mathfrak{q}^\times$. Let $g$ be one of them. If there is a monic quadratic polynomial, $m$, which is represented by $\Lambda(L)$ then we see that $\mu_2 = 2$. Also, we can choose $m$ so that it is different from $\mathfrak{p}$. It is clear that $m$ is a square in $A_q^\times$ and that it is a unit in $A_\mathfrak{p}$. In particular we see that $gm$ is represented by $\Lambda L$ and cannot be represented by $\xi$. Hence, $\mu_3 = 3$ which is absurd.
Suppose finally that no quadratic polynomials is represented by $\Lambda L$ and consider two distinct linear polynomials, whose leading coefficients are not in the same square class as $\xi_1$; call them $g$ and $g'$. It is clear that $gg'\xi$ is represented by $\Lambda L$ but is not represented by $\xi$. Hence $\mu_2 = 3$. So we must have $4+2\partial(\mathfrak{q}) \geq 2+4\partial(\mathfrak{q})$ which is a contradiction.

(iii) Suppose that $L$ has two linear good primes, $\mathfrak{p}$ and $\mathfrak{g}$. Since $\Lambda(L)_\mathfrak{q}$ is isotropic, we can, by reciprocity, suppose that $\Lambda(L)_\mathfrak{g}$ is isotropic (and hence universal). So, we have $\lambda(L)_\mathfrak{p} \cong \langle 1, -\delta, \epsilon_\mathfrak{p}\mathfrak{p}\rangle$, $\lambda(L)_\mathfrak{g} \cong \langle 1, -1, \epsilon_\mathfrak{g}\mathfrak{g}\rangle$ and hence $\lambda(L)_\infty \cong \langle 1, t, -\delta t\rangle$. Any linear polynomial which is coprime to $\mathfrak{p}$ is represented by both $\lambda(L)_\mathfrak{p}$ and $\lambda(L)_\infty$. Therefore the proof is similar to the proof of the previous case (i.e. 3.(ii)).

(4) Suppose that $\lambda(L)_\mathfrak{q} \cong \langle a, b\mathfrak{q}^2, c\mathfrak{q}^2\rangle$ where $a \notin A_\mathfrak{q}^{\times 2}$. Suppose also that $\partial(\mathfrak{q}) \equiv 0 \mod 2$ so that $\mathbb{F}_r \subset A_\mathfrak{q}^{\times 2}$.

(i) If $\lambda(L)_\mathfrak{p} \cong \langle 1, -\delta, \epsilon\mathfrak{p}\rangle$ with $\partial(\mathfrak{p}) = 1$ then $\lambda(L)_\infty \cong \langle 1, -\delta, t\rangle$. First, notice that no element of $\mathbb{F}_r$ is represented by $\Lambda L$. Also, it is impossible that two distinct

linear primes are represented by $\Lambda L$, since it would not be compatible with the shape of $(\Lambda L)_\infty$. Since a linear prime $\mathfrak{l} \neq \mathfrak{p}$ is represented by $\Lambda L$ if and only it is a nonsquare in $A_\mathfrak{q}$, we see that all the linear primes but maybe two are squares in $A_\mathfrak{q}^\times$.

Let $d = \partial(\mathfrak{q})$ and consider $A^{(d)}$ defined above. In $A^{(d)}$, there are exactly $\frac{q^d-1}{2}$ polynomials which are not squares in $A_\mathfrak{q}^\times$ and there are $A^{d-1} - 1$ multiples of $\mathfrak{p}$. Hence there is a quadratic non residue modulo $\mathfrak{q}$ which is not a multiple of $\mathfrak{p}$. Since $d \equiv 0 \mod 2$, we may further suppose that this quadratic non residue is monic. Let us call it $\mathfrak{g}$, let $\mathfrak{l} \neq \mathfrak{p}$ be a linear prime which is a square in $A_\mathfrak{q}^\times$ and let finally $\delta$ stands, as usual, for a nonsquare in $\mathbb{F}_r$. If $\partial(\mathfrak{g}) \equiv 1 \mod 2$, then $\mathfrak{g}$, $\mathfrak{lg}$ and $\delta\mathfrak{lg}$ are represented by $\Lambda L$; hence we see that $\partial(D) < 3\partial(\mathfrak{q})$ which is absurd. If $\partial(\mathfrak{g}) \equiv 0 \mod 2$, then $\mathfrak{g}$, $\delta\mathfrak{g}$ and $\mathfrak{lg}$ are represented by $\Lambda L$; hence we see that $\partial(D) < 3\partial(\mathfrak{q})$ which is also absurd.

(ii) If $\lambda(L)_\mathfrak{p} \cong \langle 1, -\eta, \epsilon\mathfrak{p}\rangle$ with $\partial(\mathfrak{p}) = 2$ and $\eta \notin A_\mathfrak{p}^{\times 2}$, then $\lambda(L)_\infty \cong \langle 1, t, -\delta t\rangle$. We see that no element of $\mathbb{F}_r^\times$ is represented by $\Lambda L$. If two linear primes are represented by $\Lambda L$ then, $\mu_1 = \mu_2 = 1$ and since $\mu_3 \leq 2\partial(\mathfrak{q})$ we get a contradiction. In particular, we see that there is at most one linear prime represented by $\Lambda L$. But, a linear prime is represented by $\Lambda L$ if and only if it is represented at $\mathfrak{q}$, which means that it is a nonsquare in $A_\mathfrak{q}$. Finally all but maybe one linear primes are squares in $A_\mathfrak{q}^\times$. The proof finishes as the previous one (i.e. 4.(i)).

(iii) Suppose that $L$ has two linear good primes, $\mathfrak{p}$ and $\mathfrak{g}$. Since $\Lambda(L)_\mathfrak{q}$ is isotropic, we can, by reciprocity, suppose that $\Lambda(L)_\mathfrak{g}$ is isotropic (and hence universal). So, we have $\lambda(L)_\mathfrak{p} \cong \langle 1, -\delta, \epsilon_\mathfrak{p}\mathfrak{p}\rangle$, $\lambda(L)_\mathfrak{g} \cong \langle 1, -1, \epsilon_\mathfrak{g}\mathfrak{g}\rangle$ and $\lambda(L)_\infty \cong \langle 1, t, -\delta t\rangle$. If there are two linear primes which are represented by $\Lambda L$ we are done by a similar way as above. Again we see that at most two linear primes (including $\mathfrak{p}$) are not squares in $A_\mathfrak{q}^\times$. Let $\mathfrak{l}$ be one of these (square) linear primes.

Clearly, there is a polynomial of $A^{(d)}$, which is not a square of $A_{\mathfrak{q}}$ and which is not a multiple of $\mathfrak{p}$. Suppose it monic and call it $\mathfrak{g}$. If $\partial(\mathfrak{g}) \equiv 1 \mod 2$, then $\mathfrak{g}$, $\delta\mathfrak{g}$ and $\mathfrak{l}\mathfrak{g}$ are represented by $\Lambda L$; hence we see that $\partial(D) < 3\partial(\mathfrak{q})$ which is absurd. If $\partial(\mathfrak{g}) \equiv 0 \mod 2$, then $\mathfrak{g}$, $\mathfrak{l}\mathfrak{g}$ and $\delta\mathfrak{l}\mathfrak{g}$ are represented by $\Lambda L$; hence we see that $\partial(D) < 3\partial(\mathfrak{q})$ which is absurd. ■

**Claim 2.** If $L$ is regular, then $L$ has class number one.

**Proof.** Let $L$ be a ternary regular lattice and let $D$ be its discriminant. By applying a transformation $\lambda = \prod_{\mathfrak{q}|D} \lambda_{\mathfrak{q}}^{k_{\mathfrak{q}}}$, we obtain a lattice $\lambda(L)$ which is also regular and whose discriminant is squarefree. For a prime $\mathfrak{p}$, define

$$\Lambda = \lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}-1} \cdot \prod_{\mathfrak{q}\neq\mathfrak{p}} \lambda_{\mathfrak{q}}^{k_{\mathfrak{q}}}\,, \quad \Lambda_1 = \lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}-2} \cdot \prod_{\mathfrak{q}\neq\mathfrak{p}} \lambda_{\mathfrak{q}}^{k_{\mathfrak{q}}} \quad \text{and} \quad \Lambda_2 = \lambda_{\mathfrak{p}}^{k_{\mathfrak{p}}-3} \cdot \prod_{\mathfrak{q}\neq\mathfrak{p}} \lambda_{\mathfrak{q}}^{k_{\mathfrak{q}}}.$$

(1) Let us suppose that $L$ has one linear good prime, $\mathfrak{p}$ and suppose that $\lambda(L)_{\mathfrak{p}} \cong \langle 1, -\delta, \epsilon\mathfrak{p}\rangle$. By construction, $\Lambda(L)$ is unimodular everywhere but at $\mathfrak{p}$.

If $\Lambda(L)_{\mathfrak{p}} \cong \langle a, b, c\mathfrak{p}^3\rangle$ then $\Lambda(L)_{\infty} \cong \langle 1, -\delta, t\rangle$. It is clear that $\Lambda L$ represents all $\mathbb{F}_r$; hence $\mu_1 = \mu_2 = 0$. Moreover by Lemma 5.2.3, $\Lambda L$ represents some linear primes; hence $\mu_3 = 1$. This is impossible.

If $\Lambda(L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}^2, c\mathfrak{p}^3\rangle$, we see that $\partial(\mathrm{disc}(\Lambda L))) = 5 \equiv 1 \mod 2$ and we suppose $\Lambda(L)_{\infty} \cong \langle 1, -\delta, t\rangle$. We see that $\Lambda(L)$ represents one square class of $\mathbb{F}_r$; hence $\mu_1 = 0$. Also Lemma 5.2.3 enables to see that $\Lambda L$ represents some linear primes; hence $\mu_2 = 1$. To conclude, we notice that $\Lambda(L)$ represents any multiple of $\mathfrak{p}^2$; hence $\mu_3 = 2$ and we obtain a contradiction.

If $\Lambda(L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}\rangle$, Lemma 5.2.8 tells that $\Lambda L$ has class number 1; hence it is regular. We consider $\Lambda_1 L$. We have either $\Lambda_1(L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}^2\rangle$ or $\Lambda_1(L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}^3, c\mathfrak{p}^3\rangle$. In the former case $\Lambda_1(L)$ has still class number one and we have to consider $\Lambda_2(L)$. In the latter case $\Lambda_1(L)$ cannot be regular. Indeed, we can

suppose that $\Lambda_1(L)_\infty \cong \langle 1, t, -\delta t\rangle$, and so, we see that $\Lambda_1(L)$ represents either one class of $\mathbb{F}_r$ and linear polynomials with arbitrary coefficients (when $a \in A_\mathfrak{p}^{\times 2}$), or some linear polynomials with arbitrary coefficients and some quadratic polynomials (when $a \notin A_\mathfrak{p}^{\times 2}$). Both of these cases implies $\partial(D) \leq 4$ which is impossible.

When we have $\Lambda_1(L)_\mathfrak{p} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}^2\rangle$, table 5.2 show that either $\Lambda_2(L)_\mathfrak{p} \cong \langle a, b\mathfrak{p}^3, c\mathfrak{p}^4\rangle$ or $\Lambda_2(L)_\mathfrak{p} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}^3\rangle$. In the former case we have $\Lambda_2(L)_\infty \cong \langle 1, -\delta, t\rangle$ and so we see that $\Lambda_2(L)$ represents on square class of $\mathbb{F}_r$, some linear primes and some quadratic polynomials with arbitrary leading coefficients; hence $\partial(D) \leq 3$ which is impossible.

Let us finally suppose that $\Lambda_2(L)_\mathfrak{p} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}^3\rangle$ so that $\Lambda_2(L)_\infty \cong \langle 1, t, -\delta t\rangle$. If $a \in A_\mathfrak{p}^{\times 2}$, we see that 1 is represented by $\Lambda_2(L)$, also some linear polynomials with arbitrary leading coefficients are represented ; hence $\partial(D) \leq 3$ which is not possible.

Suppose therefore that $a \notin A_\mathfrak{p}^{\times 2}$. In this case the configuration of successive minima is necessarily $(1, 1, 2)$. Lemma 5.2.4 tells that $\Lambda_2(L)^{2\times 2}$ cannot represent more than $N = \frac{(r-1)^2}{2}$ linear polynomials. Let us count the number, $N'$, of linear polynomials locally represented by $\Lambda_2(L)$. Those are

(i) The linear polynomials which are coprime to $\mathfrak{p}$ and which are not squares in $A_\mathfrak{p}^\times$: there are exactly half the number of polynomials coprime to $\mathfrak{p}$; hence there is exactly $\frac{r(r-1)-(r-1)}{2}$ of them.

(ii) The multiples of $\mathfrak{p}$ of the form $\alpha\mathfrak{p}$ where $\alpha$ and $b$ are in the same square class modulo $\mathfrak{p}$: there are exactly $\frac{r-1}{2}$ of them.

Finally $N' = \frac{r(r-1)}{2}$ and we see that $N' > N$ which is a contradiction.

(2) We now suppose that $L$ has one quadratic good prime, which we call $\mathfrak{p}$. By construction, $\Lambda(L)$ is unimodular everywhere but at $\mathfrak{p}$. Also, by table 5.2, we have

three possibilities for $\Lambda(L)_{\mathfrak{p}}$. For all these possibilities we have $\partial(\mathrm{disc}(\Lambda(L))) \equiv 0 \mod 2$ and therefore we will suppose that $\Lambda(L)_{\infty} \cong \langle 1, t, -\delta t\rangle$. Here, a regular form must represent any element locally represented at $\mathfrak{p}$ and at $\infty$.

If $\Lambda(L)_{\mathfrak{p}} \cong \langle a, b, c\mathfrak{p}^3\rangle$, we see that $\Lambda(L)$ must represent the squares of $\mathbb{F}_r$; hence, $\mu_1 = 0$. Also $\Lambda(L)_{\infty}$ represents all the linear polynomials and so does $\Lambda(L)_{\mathfrak{p}}$, since any linear polynomial is a unit at $\mathfrak{p}$. Thus $\mu_2 = \mu_3 = 1$. Hence $\partial(\mathrm{disc}(\Lambda L)) = 2$, which is a contradiction.

Suppose that $\Lambda(L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}^2, c\mathfrak{p}^3\rangle$. Remember that $\partial(\mathfrak{p}) = 2$, which implies that $\mathbb{F}_r^{\times} \subset A_{\mathfrak{p}}^{\times 2}$. If $a$ is a square in $A_{\mathfrak{p}}$ we see that $\mu_1 = 0$. Also there are some linear polynomials with arbitrary leading coefficients represented by $\Lambda L$; hence $\mu_2 = \mu_3 = 1$. That is a contradiction. If $a$ is not a square in $A_{\mathfrak{p}}$, we see that no constant is represented by $\Lambda L$. Nevertheless we can still conclude that $\mu_1 = \mu_2 = 1$. Also, since $a$ is not a square in $A_{\mathfrak{p}}^{\times}$ and since $\Lambda(L)_{\mathfrak{p}}$ is anisotropic (by reciprocity), we see that $b$ is a square in $A_{\mathfrak{p}}$. It follows that that $\mathfrak{p}^2$ is represented by $\Lambda L$; hence $\mu_2 \leq 4$ which is not possible.

Suppose finally that $\Lambda(L)_{\mathfrak{p}} \cong \langle c, a\mathfrak{p}, b\mathfrak{p}\rangle$. If $c$ is a square modulo $\mathfrak{p}$, we see that 1 is represented by $\Lambda(L)$; hence, $\mu_1 = 0$. Any linear polynomial is represented by $\Lambda(L)_{\infty}$ and some linear polynomials with arbitrary leading coefficients are represented by $L_{\mathfrak{p}}$ (cf. Lemma 5.2.3); hence $\mu_2 = \mu_3 = 1$. That is a contradiction, since $\partial(\mathrm{disc}(\Lambda(L))) = 4$.

If $c$ is not a square $\mod \mathfrak{p}$, then Lemma 5.2.8 tells that $\Lambda(L)$ has class number one; hence it is regular. We have to consider $\Lambda_1(L)$ instead of $\Lambda L$. Suppose that $\Lambda(L) = \langle \epsilon, \mathfrak{p}, -\epsilon\mathfrak{p}$ for some $\epsilon \notin A_{\mathfrak{p}}^{\times 2}$. Then we have to treat the following cases.

Suppose $\Lambda_1(L) \cong \langle a, \epsilon\mathfrak{p}, b\mathfrak{p}^2\rangle$ where $-ab \notin A_{\mathfrak{p}}^{\times}$.

- If $a \in A_{\mathfrak{p}}^{\times 2}$, then 1 is represented by $\Lambda_1 L$; hence $\mu_1(\Lambda_1 L) = 0$. By Lemma 5.2.3, we see that there are some linear polynomials with arbitrary leading coefficients represented by $\Lambda_1 L$; hence $\mu_2(\Lambda_1 L) = \mu_3(\Lambda_1 L) = 1$. This is not

possible.

- If $a \notin A_{\mathfrak{p}}^{\times 2}$, then no constant is represented by $\Lambda_1 L$. Nevertheless, Lemma 5.2.3 still applies and tells that there are some linear polynomials with arbitrary leading coefficients represented by $\Lambda_1 L$; hence $\mu_1(\Lambda_1 L) = \mu_2(\Lambda_1 L) = 1$. There is also some monic quadratic polynomials represented by $(\Lambda_1 L)_{\mathfrak{p}}$ and therefore represented by $\Lambda_1 L$. To exhibit one, consider for example two monic linear polynomials one of which is a square and one of which is not a square in $A_{\mathfrak{p}}^{\times}$. Then their product is a nonsquare in $A_{\mathfrak{p}}^{\times}$. Finally, we see that $\mu_3(\Lambda_1 L) = 2$; that is a contradiction.

Suppose that $\Lambda_1(L) \cong \langle \epsilon, \mathfrak{p}^3, -\epsilon\mathfrak{p}^3 \rangle$. Lemma 5.2.3 tells that there are some linear polynomials with arbitrary leading coefficients represented by $\Lambda_1 L$ and the very same argument as in the previous case will prove that there are quadratic polynomial represented by $\Lambda_1 L$. Hence $\mu_1(\Lambda_1 L) = \mu_2(\Lambda_1 L) = 1$ and $\mu_3(\Lambda_1 L) = 2$; that is not possible.

(3) We now suppose that $L$ has two linear good primes, which we call $\mathfrak{p}$ and $\mathfrak{l}$. By construction, $\Lambda(L)$ is unimodular everywhere but at $\mathfrak{p}$ and at $\mathfrak{l}$. Since $\Lambda L$ is anisotropic at $\infty$, reciprocity implies that it must be isotropic (and therefore universal) at exactly one of $\mathfrak{p}$ or $\mathfrak{l}$.

If $\Lambda(L)_{\mathfrak{p}} \cong \langle a, b, c\mathfrak{p}^3 \rangle$, we see that $\Lambda(L)_{\infty} \cong \langle 1, t, -\delta t \rangle$. It is clear that $\Lambda L$ represents $\mathbb{F}_r^2$; hence $\mu_1 = 0$. Moreover by Lemma 5.2.3, $\Lambda L$ represents some linear polynomials with arbitrary leading coefficients; hence $\mu_2 = \mu_3 = 1$. This is impossible since $\partial D = 4$.

If $\Lambda(L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}^2, c\mathfrak{p}^3 \rangle$, we suppose $\Lambda(L)_{\infty} \cong \langle 1, t, -\delta t \rangle$. If $a$ is a square in $A_{\mathfrak{p}}$, we see that $\Lambda(L)$ represents $\mathbb{F}_r^2$. Also, we see that $\Lambda(L)$ represents some linear polynomials with arbitrary leading coefficients; hence $\mu_1 = 0$ and $\mu_2 = \mu_3 = 1$. That is impossible.

Suppose that $a \notin A_{\mathfrak{p}}^{\times 2}$. We see that $\Lambda(L)$ does not represent any constant and reciprocity implies that $b \in A_{\mathfrak{p}}^{\times 2}$. We can conclude by the same way as above that $\mu_1 = \mu_2 = 1$. It is also easy to remark that $\Lambda(L)$ represents $\mathfrak{p}^2$; hence $\mu_3 = 2$. That is a contradiction.

If $\Lambda(L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}\rangle$ and $\Lambda(L)_{\mathfrak{l}} \cong \langle a', b', c'\mathfrak{l}\rangle$, we suppose that $\Lambda(L)_\infty \cong \langle 1, -\delta, t\rangle$. Lemma 5.2.8 shows that $\Lambda L$ has class number 1, and thus is regular. We consider $\Lambda_1$ and $\Lambda_2$.

(i) If $\Lambda_1(L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}^3, c\mathfrak{p}^3\rangle$ and $\Lambda_1(L)_{\mathfrak{l}} \cong \langle a', b', c'\mathfrak{l}\rangle$, we suppose that $\Lambda_1(L)_\infty \cong \langle 1, -\delta, t\rangle$. Using arguments similar as those we used before, one shows that $\Lambda_1(L)$ represents some constants and some linear polynomials. There are linear polynomials with arbitrary leading coefficients that are squares or nonsquares in $A_{\mathfrak{p}}^{\times}$. It implies that there are some quadratic polynomials with arbitrary leading coefficients represented locally at $\mathfrak{p}$. Those polynomials must be also represented at $\infty$ and thus they must be represented by $\Lambda_1(L)$; this lead again to a contradiction.

(ii) If $\Lambda_1(L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}^2\rangle$ and $\Lambda_1(L)_{\mathfrak{l}} \cong \langle a', b', c'\mathfrak{l}\rangle$, we suppose that $\Lambda_1(L)_\infty \cong \langle 1, t, -\delta t\rangle$. It is clear that if $a \in A_{\mathfrak{p}}^{\times 2}$ then 1 is represented by $\Lambda_1 L$; hence $\mu_1 = 0$. Also, by Lemma 5.2.3, we see that some linear polynomials with arbitrary leading coefficients are represented by $\Lambda_1 L$. That leads to $\mu_2 = \mu_3 = 1$, which is a contradiction.

Suppose thus that $a$ is not a square in $A_{\mathfrak{p}}^{\times}$. In particular we see that $\Lambda_1 L$ does not represent any constant. Nevertheless Lemma 5.2.3 still applies and enable to conclude that $\mu_1 = \mu_2 = 1$. The linear polynomials that are represented locally include:

(a) The linear polynomials coprime to $\mathfrak{p}$ and coprime to $\mathfrak{l}$ which are squares in $A_{\mathfrak{p}}^{\times}$: there are $\frac{r(r-1)-2(r-1)}{2}$ of them.

(b) The multiples of $\mathfrak{p}$ of the shape $\alpha\mathfrak{p}$ where $\alpha$ is in the same square class as $b$: there are $\frac{r-1}{2}$ of them.

(c) If $\left(\frac{c'l}{\mathfrak{p}}\right) = 1$ or if $\Lambda_1(L)_\mathfrak{l}$ is universal, the multiples $\alpha\mathfrak{l}$ where $\alpha$ and $c'$ are in the same square class.

(c)' If $\left(\frac{c'l}{\mathfrak{p}}\right) = 1$ and $\Lambda_1(L)_\mathfrak{l}$ is not universal, no multiple of $\mathfrak{l}$.

In case $(c)$ above, we conclude as in the last paragraph of (1). In case $(c)'$ we conclude as in the last paragraph of (2).

(iii) $\Lambda_1(L)_\mathfrak{p} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}\rangle$ and $\Lambda_1(L)_\mathfrak{l} \cong \langle a', b'\mathfrak{l}, c'\mathfrak{l}\rangle$, we suppose that $\Lambda_1(L)_\infty \cong \langle 1, t, -\delta t\rangle$.

(a) If $\Lambda_1(L)_\mathfrak{p} \cong \langle 1, \mathfrak{p}, -\delta\mathfrak{p}\rangle$ and $\Lambda_1(L)_\mathfrak{l} \cong \langle 1, \mathfrak{l}, -\mathfrak{l}\rangle$ we see that 1 is represented by $\Lambda_1(L)$; hence $\mu_1 = 0$. Also Lemma 5.2.5 enables to see that there are some linear polynomials with arbitrary leading coefficients represented by $\Lambda_1 L$; hence $\mu_2 = \mu_3 = 1$ which is not possible.

(b) If $\Lambda_1(L)_\mathfrak{p} \cong \langle 1, \mathfrak{p}, -\delta\mathfrak{p}\rangle$ and $\Lambda_1(L)_\mathfrak{l} \cong \langle \delta, \mathfrak{l}, -\mathfrak{l}\rangle$ we see that no constant is represented by $\Lambda_1(L)$. Since the discriminant has degree 4 the only possible configuration for the successive minima is $(1, 1, 2)$. The linear polynomials represented by locally by $\Lambda_1(L)$ are the polynomials coprime to $\mathfrak{p}$ and $\mathfrak{l}$, which are square in $A_\mathfrak{p}^\times$ and nonsquares in $A_\mathfrak{l}^\times$, the multiple $\alpha\mathfrak{p}$ of $\mathfrak{p}$ which are not squares in $A_\mathfrak{l}^\times$ and finally the multiple $\beta\mathfrak{l}$ of $\mathfrak{l}$ which are square in $A_\mathfrak{p}^\times$. By Lemma 5.2.5, we see that the number, $N'$, of such polynomials satisfies $N' = N_{1,-1} + (r-1)$ ; that contradicts Lemma 5.2.4.

(c) If $\Lambda_1(L)_\mathfrak{p} \cong \langle \delta, \mathfrak{p}, -\delta\mathfrak{p}\rangle$ and $\Lambda_1(L)_\mathfrak{l} \cong \langle \delta, \mathfrak{l}, -\mathfrak{l}\rangle$, we use the same method as in the previous case.

■

**Claim 3.** The only ternary regular lattices those listed in Lemma 5.2.8.

**Proof.** Clear from the proof of claim 2. ■

■

## 5.4 Spinor Regular Ternary Lattices

**Definition.** A lattice $L$ is said to be spinor regular if it represents any integral element represented by its spinor genus. ■

Let $L$ be a lattice. Since $\mathcal{S}pn(L) \subset \mathcal{G}en(L)$ it follows that any regular lattice is also spinor regular.

Let $L$ be a lattice and $\mathfrak{p}$ be a prime. We say that $L$ behaves well at $\mathfrak{p}$ if either $\mathfrak{p}^2$ does not divide $\mathrm{disc}(L)$ or if $L_\mathfrak{p}$ is split by a hyperbolic space, $\mathbb{H}$. In particular if $L$ behaves well at $\mathfrak{p}$, then $L_\mathfrak{p}$ has a unimodular component of rank 2.

**Lemma 5.4.1** *Let $L$ be a ternary lattices. If $\theta(O^+(L_\mathfrak{p})) \supset A_\mathfrak{p}^\times \mod k_\mathfrak{p}^{\times 2}$ for all $\mathfrak{p} \in \Omega$. Then $\mathcal{S}pn(L) = \mathcal{G}en(L)$.*

**Proof.**

If $\tilde{A} = \prod_\mathfrak{p} A_\mathfrak{p}^\times$, then we have

$$J_k \cong k^\times \cdot \tilde{A} \cdot k_\infty^\times$$

where $k_\infty^\times$ is identified with the elements of $J_k$ with all finite component being 1. Indeed, let $(j_\mathfrak{p}) \in J_k$, then $|j_\mathfrak{p}|_\mathfrak{p} = 1$ for almost all $\mathfrak{p}$. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be the places

at which $|j_{\mathfrak{p}}|_{\mathfrak{p}} \neq 1$ and write in this case $j_{\mathfrak{p}} = \beta_{\mathfrak{p}}^m u_{\mathfrak{p}}$ where $u_{\mathfrak{p}}$ is a $\mathfrak{p}$-adic unit. Then $(j_{\mathfrak{p}})$ can be identified to $\beta_{\mathfrak{p}_1} \cdots \beta_{\mathfrak{p}_n} \prod_{\mathfrak{p}} u_{\mathfrak{p}}$. Hence

$$\begin{aligned} spn^+ &= [J_k : \theta(J_L) P_{k^\times}] \\ &= [k^\times \cdot \tilde{A} \cdot k_\infty^\times : \prod_{\mathfrak{p} \text{ incl } \infty} \theta(O^+(L_{\mathfrak{p}})) \cdot k^\times] \\ &\leq [k^\times \cdot \tilde{A} \cdot k_\infty^\times : \prod_{\mathfrak{p}} A_{\mathfrak{p}}^\times \cdot k_\infty^\times \cdot k^\times] \\ &\leq 1 \end{aligned}$$

■

**Corollary 5.4.1** *Let $L$ be a ternary lattices. Suppose that $L$ behaves well at all primes. Then $\mathcal{S}pn(L) = \mathcal{G}en(L)$.*

**Proof.** Since $L$ behaves well at all primes, it follows that $L_{\mathfrak{p}}$ has a unimodular component of rank 2. The result follows then from the previous lemma together with Corollary 5.1.2. ■

**Proposition 5.4.1 ([6], 3.2 & 3.3)** *Let $L$ be a lattice.*

1. *If $L$ is spinor regular, $\mathfrak{p}^2|\mathrm{disc}(L)$ and $L_{\mathfrak{p}}$ is not split by $\mathbb{H}$ then $\lambda_{\mathfrak{p}}(L)$ is spinor regular.*

2. *If $L$ is regular, $\mathfrak{p}^2|\mathrm{disc}(L)$ and $L_{\mathfrak{p}}$ is split by $\mathbb{H}$ then $\lambda_{\mathfrak{p}}(L)$ is regular.*

**Theorem 5.4.1** *Let $L$ be a definite ternary $\mathbb{F}_r[t]$-lattice. If $L$ is spinor regular, then $L$ is regular. In particular spinor regular lattice have class number* 1.

**Proof.** Let $W$ be the set of primes at which $L$ behaves well and let $W'$ be the sets of primes at which $L$ does not behave well. For $\mathfrak{p} \in W'$, there is $n_{\mathfrak{p}} \in N$ such that $v_{\mathfrak{p}}\left(\text{disc}\left(\lambda_{\mathfrak{p}}^{n_{\mathfrak{p}}}(L)\right)\right) \leq 1$. Consider

$$\Lambda = \prod_{\mathfrak{p} \in W'} \lambda_{\mathfrak{p}}^{n_{\mathfrak{p}}}.$$

By Proposition 5.4.1, $\Lambda(L)$ is spinor regular. Also, $\Lambda(L)$ behaves well at all primes. Indeed, if $\mathfrak{p} \in W$, then $\Lambda(L)_{\mathfrak{p}} = \epsilon L_{\mathfrak{p}}$ for some $\epsilon \in A_{\mathfrak{p}}^{\times}$ and if $\mathfrak{p} \in W'$ then $v_{\mathfrak{p}}(\Lambda L) \leq 1$.

Since $\Lambda L$ behaves well at all primes, Corollary 5.4.1 implies that the genus of $\Lambda L$ contains only one spinor genus. Since $\Lambda L$ is spinor regular, it follows that it is also regular. Since $\Lambda(L)$ is regular, Theorem 5.3.1 and Lemma 5.2.8 tell that it must be equivalent to one of the following:

1. lattices of discriminant $D$ with $\partial D \leq 2$;

2. lattices of discriminant $D$ with $\partial D = 3$ such that

   (a) $D = -\delta\mathfrak{p}^3$ and $L_{\mathfrak{p}} \cong \langle \epsilon, \eta\mathfrak{p}, \rho\mathfrak{p}^2 \rangle$

   (b) $D = -\delta\mathfrak{p}^2\mathfrak{q}$, $L_{\mathfrak{p}} \cong \langle \epsilon, \eta\mathfrak{p}, \rho\mathfrak{p} \rangle$ and $L_{\mathfrak{q}} \cong \langle \epsilon', \eta', \rho'\mathfrak{q} \rangle$.

3. lattices of discriminant $D$ with $\partial D = 4$ such that $L_{\mathfrak{p}} \cong \langle \epsilon, \mathfrak{p}, -\epsilon\mathfrak{p} \rangle$, for some quadratic prime, $\mathfrak{p}$ and some $\epsilon \notin A_{\mathfrak{p}}^{\times 2}$.

Now we use the same argument as is the proof of Theorem 5.3.1. Let $\mathfrak{p} \in W'$ be a prime, instead of applying $\prod_{\mathfrak{q} \in W'} \lambda_{\mathfrak{q}}^{n_{\mathfrak{q}}}$, we apply

$$\Gamma = \lambda_{\mathfrak{p}}^{n_{\mathfrak{p}} - i} \cdot \prod_{\mathfrak{q} \in W', \mathfrak{q} \neq \mathfrak{p}} \lambda_{\mathfrak{q}}^{n_{\mathfrak{q}}}.$$

If $L$ is spinor regular and if $L$ is not one of the lattice listed above, then $\Gamma L$ is also spinor regular. In the proofs of Theorem 5.3.1 we have listed all the possibilities of $\Gamma L$. We just need to prove that none of these possibilities is spinor regular.

To that aim, we use two different arguments. On one hand we compute the number of spinor genera in $\mathcal{G}en(\Gamma L)$. If we find that $\mathcal{S}pn(\Gamma L) = \mathcal{G}en(\Gamma L)$ then we can conclude using Theorem 5.3.1 since, in this case, spinor regularity and regularity are the same notion. On the other hand, if $\mathcal{G}en(\Gamma L)$ contains more than one spinor genus, we prove that $\mathcal{G}en(\Gamma L)$ does not have any spinor exceptions. That implies that any spinor genus represents all the integers represented by $\mathcal{G}en(\Gamma L)$. Hence Theorem 5.3.1 enables again to conclude.

The possibilities for $\Gamma L$ are the following:

I. If $\Gamma L$ has a bad prime then either $(\Gamma L)_{\mathfrak{q}} \cong \langle a, b, c\mathfrak{q}^2 \rangle$ or $(\Gamma L)_{\mathfrak{q}} \cong \langle a, b\mathfrak{q}^2, c\mathfrak{q}^2 \rangle$. Also the three different configurations for good primes are

- $(\Gamma L)_{\mathfrak{p}} \cong \langle u_1, u_2, u_3\mathfrak{p} \rangle$, $\mathfrak{p}$ linear;
- $(\Gamma L)_{\mathfrak{p}} \cong \langle u_1, u_2, u_3\mathfrak{p} \rangle$, $\mathfrak{p}$ quadratic;
- $(\Gamma L)_{\mathfrak{p}} \cong \langle u_1, u_2, u_3\mathfrak{p} \rangle$, $(\Gamma L)_{\mathfrak{l}} \cong \langle u'_1, u'_2, u'_3\mathfrak{l} \rangle$, $\mathfrak{p}$ and $\mathfrak{l}$ linear.

In any configuration, we see that the localizations of $L$ have some modular components of rank at least 2, then Theorem 5.1.1 and corollary 5.1.2 enable to conclude that $\mathcal{S}pn(\Gamma L) = \mathcal{G}en(\Gamma L)$; hence $L$ is regular.

II. If $\Gamma L$ has no bad prime then the possible configurations for good primes are :

| (1). $\mathfrak{p}$ is linear | (2). $\mathfrak{p}$ is quadratic | (3). $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are linear |
|---|---|---|
| (i). $(\Gamma L)_{\mathfrak{p}} \cong \langle a, b, c\mathfrak{p}^3 \rangle$ | (i). $(\Gamma L)_{\mathfrak{p}} \cong \langle a, b, c\mathfrak{p}^3 \rangle$ | (i).$(\Gamma L)_{\mathfrak{p}_1} \cong \langle a_1, b_1, c_1\mathfrak{p}_1^3 \rangle$ $(\Gamma L)_{\mathfrak{p}_2} \cong \langle a_2, b_2, c_2\mathfrak{p}_2 \rangle$ |
| (ii). $(\Gamma L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}^2, c\mathfrak{p}^3 \rangle$ | (ii). $(\Gamma L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}^2, c\mathfrak{p}^3 \rangle$ | (ii).$(\Gamma L)_{\mathfrak{p}_1} \cong \langle a_1, b_1\mathfrak{p}_1^2, c_1\mathfrak{p}_1^3 \rangle$ $(\Gamma L)_{\mathfrak{p}_2} \cong \langle a_2, b_2, c_2\mathfrak{p}_2 \rangle$ |
| (iii). $(\Gamma L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}^2 \rangle$ | (iii). $(\Gamma L)_{\mathfrak{p}} \cong \langle a, \epsilon\mathfrak{p}, c\mathfrak{p}^2 \rangle$ where $\epsilon, -ac \notin A_{\mathfrak{p}}^{\times 2}$ | (iii).$(\Gamma L)_{\mathfrak{p}_1} \cong \langle a_1, b_1\mathfrak{p}_1, c_1\mathfrak{p}_1 \rangle$ $(\Gamma L)_{\mathfrak{p}_2} \cong \langle a_2, b_2, c_2\mathfrak{p}_2 \rangle$ |
| (iv). $(\Gamma L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}^3 \rangle$ | (iv). $(\Gamma L)_{\mathfrak{p}} \cong \langle \epsilon, \mathfrak{p}^3, -\epsilon\mathfrak{p}^3 \rangle$ where $\epsilon \notin A_{\mathfrak{p}}^{\times 2}$ | (iv).$(\Gamma L)_{\mathfrak{p}_1} \cong \langle a_1, b_1\mathfrak{p}_1, c_1\mathfrak{p}_1 \rangle$ $(\Gamma L)_{\mathfrak{p}_2} \cong \langle a_2, b_2\mathfrak{p}_2, c_2\mathfrak{p}_2 \rangle$ |

Whenever all the localizations of $L$ have some modular components of rank at least 2, then Theorem 5.1.1 and corollary 5.1.2 enable to conclude that $\mathcal{S}pn(L) = \mathcal{G}en(L)$ and in particular that $L$ is regular. That solves cases (1).(i), (2).(i), (2).(iv), (3).(i), (3).(iii) and II.(3).(iv).

Suppose that $-1$ is a square in $A_{\mathfrak{p}}^{\times}$ and write $L$ as

$$L \cong \langle a_1 p^{\alpha_1}, a_2\mathfrak{p}^{\alpha_2}, a_3\mathfrak{p}^{\alpha_3} \rangle$$

where $\alpha_1 = 0$. As $\mathfrak{p}$ is a good prime, reciprocity implies that $(\Gamma L)_{\mathfrak{p}}$ is anisotropic. In particular, we see that if $\alpha_i \equiv \alpha_j \mod 2$ for some $i \neq j$, then $a_i a_j = -\delta = \delta \mod A_{\mathfrak{p}}^{\times 2}$, where $\delta$ is a nonsquare in $A_{\mathfrak{p}}^{\times}$. In this case, Corollary 5.1.3 enables to conclude that $\theta(O^+(L_{\mathfrak{p}})) \supset A_{\mathfrak{p}}^{\times}$ and Lemma 5.4.1 implies that $\mathcal{S}pn(\Gamma L) = \mathcal{G}en(\Gamma L)$. That solves case (2).(ii) and (2).(iv).

Now, we have to deal with the cases where possibly $\mathcal{S}pn(\Gamma L) \neq \mathcal{G}en(\Gamma L)$.

**Cases (1).(ii) or (3).(ii)**.

Let $\mathfrak{p}$ be the prime such that $(\Gamma L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}^2, c\mathfrak{p}^3 \rangle$ and let $d = \mathrm{disc}(\Gamma L)$. Let $x \in A$ be a spinor exceptional integer. Since $x$ must be represented by $\mathcal{G}en(\Gamma L)$,

it follows that $v_{\mathfrak{p}}(x) \geq 2$. Moreover one can suppose that the only prime divisor of $x$ is $\mathfrak{p}$ and then, condition (1) of Theorem 5.1.3 enables to tell that $-xd$ is not a square in $k_{\mathfrak{p}}^{\times}$. Condition (2) in Theorem 5.1.3 forces $k_{\mathfrak{p}}^{\times}[\sqrt{-xd}]$ to ramify; hence $v_{\mathfrak{p}}(x) \equiv 0 \mod 2$. We are in case (2) of Theorem 5.1.4, and therefore since $\mathfrak{p}^2|x$ it follows that $x$ cannot be a spinor exception.

**Case (1).(iii)**.

Let $\mathfrak{p}$ be the prime such that $(\Gamma L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}^2 \rangle$ and let $d = \mathrm{disc}(\Gamma L)$. Let $x \in A$ be a spinor exceptional integer. Since $x$ must be represented by $\mathcal{G}en(\Gamma L)$, it follows that $v_{\mathfrak{p}}(x) \geq 1$. Moreover one can suppose that the only prime divisor of $x$ is $\mathfrak{p}$ and then, condition (1) of Theorem 5.1.3 enables to tell that $-xd$ is not a square in $k_{\mathfrak{p}}^{\times}$. Condition (2) in Theorem 5.1.3 forces $k_{\mathfrak{p}}^{\times}[\sqrt{-xd}]$ to ramify; hence $v_{\mathfrak{p}}(x) \equiv 0 \mod 2$. We are in case (2) of Theorem 5.1.4, and therefore since $\mathfrak{p}^2|x$ it follows that $x$ cannot be a spinor exception.

**Case (1).(iv)**.

Let $\mathfrak{p}$ be the prime such that

$$(\Gamma L)_{\mathfrak{p}} \cong \langle a, b\mathfrak{p}, c\mathfrak{p}^3 \rangle$$

and let $d = \mathrm{disc}(\Gamma L)$. Let $x \in A$ be a spinor exceptional integer. Since $x$ must be represented by $\mathcal{G}en(\Gamma L)$, it follows that $v_{\mathfrak{p}}(x) \geq 1$. Moreover one can suppose that the only prime divisor of $x$ is $\mathfrak{p}$ and then, condition (1) of Theorem 5.1.3 enables to tell that $-xd$ is not a square in $k_{\mathfrak{p}}^{\times}$.

If $ab \notin A_{\mathfrak{p}}^{\times 2}$ or $ac \notin A_{\mathfrak{p}}^{\times 2}$, then Theorem 5.1.1 implies that $\theta(O^+(L_{\mathfrak{p}})) = k_{\mathfrak{p}}^{\times} \mod k_{\mathfrak{p}}^{\times 2}$. In particular, condition (2) of Theorem 5.1.3 cannot be satisfied.

Otherwise, condition (2) in Theorem 5.1.3 forces $k_{\mathfrak{p}}^{\times}[\sqrt{-xd}]$ to ramify; hence $v_{\mathfrak{p}}(x) \equiv 1 \mod 2$. We see that $x = \epsilon\mathfrak{p}$ for some $\epsilon \in A_{\mathfrak{p}}^{\times}$ satisfies all the conditions to be a spinor exception. Also, it is clear that any polynomials $f$ coprime to $\mathfrak{p}$ cannot be exceptional. Since $\Gamma L$ is spinor regular, it must represent any element

which is coprime to $\mathfrak{p}$ and which is represented by its genus.

If $\mathcal{S}pn(\Gamma L)$ represents $x$, then the elements represented by $\mathcal{S}pn(\Gamma L)$ and by $\mathcal{G}en(\Gamma L)$ are the same; since $\Gamma L$ is spinor regular, it must be regular and we can conclude.

Suppose that $\mathcal{S}pn(\Gamma L)$ does not represent $x$. By the work above, we can suppose that $-1$ is not a square in $A_{\mathfrak{p}}^{\times}$ and therefore, we can suppose that

$$(\Gamma L)_{\mathfrak{p}} \cong \langle a, \eta\mathfrak{p}, \eta\mathfrak{p}^3 \rangle.$$

Since $\partial(d) \equiv 0 \mod 2$, we will suppose that $(\Gamma L)_{\infty} \cong \langle 1, t, -\delta t \rangle$. If $a \in A_{\mathfrak{p}}^2$, we see that 1 is represented by $\mathcal{G}en(\Gamma L)$, and therefore by $\Gamma L$; hence $\mu_1 = 0$. Then some linear polynomials coprime to $\mathfrak{p}$ and with arbitrary leading coefficients of represented by $\mathcal{G}en(\Gamma L)$, and therefore by $\Gamma L$; hence $\mu_2 = \mu_3 = 1$. That is a contradiction.

If $a \notin A_{\mathfrak{p}}^2$, then the configuration of the successive minima of $\Gamma L$ is necessarily $(1, 1, 2)$. The linear polynomials represented by $\mathcal{S}pn(\Gamma L)$ are precisely those linear polynomials which are coprime to $\mathfrak{p}$ and are not squares in $A_{\mathfrak{p}}^{\times}$. This number is exactly half the number of polynomials coprime to $\mathfrak{p}$; hence

$$N' = \frac{r(r-1) - (r-1)}{2} = \frac{(r-1)^2}{2}.$$

Since $\Gamma L$ is spinor regular, we see that $\Gamma L^{2\times 2}$ must also represent $\frac{(r-1)^2}{2}$ elements. Lemma 5.2.4 applies and tells that $\Gamma L^{2\times 2}$ must have an irreducible discriminant. Let $D = -\delta\mathfrak{q}$ be this discriminant.

Let $f$ be a monic linear polynomial. The previous computations, imply that the following are equivalent:

1. $\left(\frac{f}{\mathfrak{q}}\right) = 1$;
2. $f$ is represented by $\Gamma L^{2\times 2}$;
3. $f$ is represented locally by $\Gamma L$;

4. $f$ is coprime to $\mathfrak{p}$ and $\left(\frac{f}{\mathfrak{p}}\right) = -1$.

Let $f = t - \omega$, then

$$(1) \Leftrightarrow \chi(\mathfrak{q}(\omega)) = 1 \text{ and } (4) \Leftrightarrow \chi(-\mathfrak{p}(w)) = -1.$$

We can suppose that $-1$ is not a square in $\mathbb{F}_r$ and that implies that

$$\chi(\mathfrak{q}(\omega)) \Leftrightarrow \chi(\mathfrak{p}(w)) = 1.$$

This last equivalence is not possible. Indeed, that would mean that the polynomial of degree three, $\mathfrak{q}(t)\mathfrak{p}(t)$ represents only squares and that would contradict Lemma 3.4.2.

■

## 5.5 Indefinite Regular Lattices

In this section we shall prove that the results obtained for definite lattices are not true for indefinite lattices. More precisely, using methods similar to those used by Hsia in [14], we are going to construct an indefinite genus with an arbitrarily large number of classes all of which are regular. Remember that $k = \mathbb{F}_r(t)$ and that $A = \mathcal{O}_k = \mathbb{F}_r[t]$.

Let $\mathbb{F}_r$ be a finite field and suppose that $r \equiv 1 \mod 4$ so that $-1$ is a square in $\mathbb{F}_r$. Choose a prime $\mathfrak{q}$ such that $\partial(\mathfrak{q}) \equiv 1 \mod 2$ and let $\mathfrak{p}_1 \cdots, \mathfrak{p}_r$ be primes such that

$$\left(\frac{\mathfrak{q}}{\mathfrak{p}_i}\right) = 1.$$

Consider the lattice

$$L \cong \langle 1, (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^2, \mathfrak{q}(\mathfrak{p}_1, \cdots, \mathfrak{p}_r)^4 \rangle \tag{5.4}$$

and let $\mathcal{G}$ be its genus. We claim that all the forms in $\mathcal{G}$ are regular.

In the following we let $c \in A$ be a spinor exceptional integer for $\mathcal{G}$ and we suppose that $D = \mathrm{disc}(L)$.

**Lemma 5.5.1** *Let $\mathfrak{l}$ be a prime that does not divide $D$; then $v_{\mathfrak{l}}(c) \equiv 0 \mod 2$. In particular, we can suppose that the only divisors of $c$ are at most those of $D$.*

**Proof.** Since $\mathfrak{l}$ does not divide $D$, we see that $L_{\mathfrak{l}}$ is unimodular and Corollary 5.1.2 implies that $\theta(O^+(L_{\mathfrak{l}})) = A_{\mathfrak{l}}^{\times}$. Since $c$ is a spinor exceptional integer for $\mathcal{G}$, it follows that condition (2) of Theorem 5.1.3 must be satisfied; in other words we must have

(i) $(1, cd)_{\mathfrak{l}} = 1$; and

(ii) $(\epsilon, cd)_{\mathfrak{l}} = 1$ for $\epsilon \notin A_{\mathfrak{l}}^{\times 2}$.

Condition (ii) above clearly forces $v_{\mathfrak{l}}(cD) = v_{\mathfrak{l}}(c)$ to be even.

Now it is clear that if conditions (1),(2) and (3) of Theorem 5.1.3 are satisfied for $c = c'\mathfrak{l}^2$, they also be satisfied for $c'$. Finally since $\mathfrak{l}$ does not divide $D$ we see that $c$ is represented by $\mathcal{G}$ if and only if $c'$ is represented by $\mathcal{G}$. ■

**Lemma 5.5.2** *If $\mathfrak{q}$ is defined as in equation (5.4) then $v_{\mathfrak{q}}(c) \equiv 1 \mod 2$.*

**Proof.** Since $L_{\mathfrak{q}}$ contains a unimodular component of rank 2 we must have $\theta(O^+(L_{\mathfrak{q}})) \supset A_{\mathfrak{q}}^{\times}$. In particular condition (2) of Theorem 5.1.3 imply that

(i) $(1, cD)_{\mathfrak{q}} = 1$; and

(ii) $(\epsilon, cD)_{\mathfrak{q}} = 1$ for $\epsilon \notin A_{\mathfrak{q}}^{\times 2}$.

Condition (ii) above clearly forces $v_{\mathfrak{q}}(cD) = 1 + v_{\mathfrak{q}}(c)$ to be even. ■

**Lemma 5.5.3** *If $\mathfrak{p}_i$ is defined as in equation (5.4) then $v_{\mathfrak{p}_i}(c) \equiv 0 \mod 2$.*

**Proof.** Since $L_{\mathfrak{p}_i} \cong \langle 1, \mathfrak{p}_i^2, \mathfrak{p}_i^4 \rangle$ the computations of the spinor norm made above tell that $\theta\left(O^+(L_{\mathfrak{p}_i})\right) = A_{\mathfrak{p}_i}^{\times 2}$. In particular condition (2) of Theorem 5.1.3 is automatically satisfied.

If $\mathfrak{p}_i$ does not divide $c$, then we are done. If $v_{\mathfrak{p}_i}(c) > 0$, then since $L_{\mathfrak{p}_i} \cong \langle 1, \mathfrak{p}_i^2, \mathfrak{p}_i^4 \rangle$ we see that $v_{\mathfrak{p}_i}(c) \geq 2$. Suppose that $v_{\mathfrak{p}_i}(c) \equiv 1 \mod 2$ and let $E_{\mathfrak{p}_i}$ be the extension $k_{\mathfrak{p}_i}\left[\sqrt{cD}\right]/k_{\mathfrak{p}_i}$. Since $v_{\mathfrak{p}_i}(c) \equiv 1 \mod 2$ we see that $E_{\mathfrak{p}_i}$ is quadratic and ramified. But $c \in \mathfrak{p}^2$ and therefore condition (3) of Theorem 5.1.3 cannot be satisfied. ■

**Theorem 5.5.1** *Let $L$ be the lattice defined in equation 5.4. All the classes of $\mathcal{G}en(L) = \mathcal{G}$ are regular.*

**Proof.**

We prove first that $\mathcal{G}$ has no spinor exception. From lemmas 5.5.1, 5.5.2 and 5.5.3, we see that for any prime $\mathfrak{p}$,

$$v_{\mathfrak{p}}(cD) \equiv 0 \mod 2.$$

Since $c$ is suppose to be a spinor exception, condition (1) of Theorem 5.1.3 implies that

$$c = \delta \mathfrak{q}^{2\alpha+1} \mathfrak{u}^2$$

where $\delta$ is a nonsquare of $\mathbb{F}_r$ and $\mathfrak{u}$ is a product of primes (i.e. of monic irreducible polynomials). Note that this equality rewrites as

$$cD = \delta \mathfrak{u}'^2.$$

Let $E_{\mathfrak{q}}$ be the extension $k_{\mathfrak{q}}\left[\sqrt{\delta \mathfrak{u}'^2}\right]/k_{\mathfrak{q}}$. Since $\delta$ is not a square and since $\mathfrak{q}$ was chosen of odd degree, $E_{\mathfrak{q}}$ is quadratic. Also, since $v_{\mathfrak{q}}(\delta \mathfrak{u}'^2) \equiv 0 \mod 2$, we see that $E_{\mathfrak{q}}$ is unramified. The fact that $c$ cannot be spinor exceptional follows from condition (3) of Theorem 5.1.3 and from Theorem 5.1.4 by noticing that $v_{\mathfrak{q}}(c) \geq 1$.

Since $\mathcal{G}$ has no spinor exception, it follows that any spinor genera of $\mathcal{G}$ represent all of $\mathcal{G}$. But $\mathcal{G}$ is indefinite and the strong approximation for the spin group (cf. [22], 104:4) implies that classes and spinor genera coincide: all the classes of $\mathcal{G}$ represent all of $\mathcal{G}$. ■

**Corollary 5.5.1** *There are some genera with arbitrary large class numbers, in which all the forms are regular.*

**Proof.** Let $S$ be the set of primes dividing $D$. Let $spn^+$ (resp. $cls^+$) be the number of proper spinor genera (resp. classes) in $\mathcal{G}en(L) = \mathcal{G}$.

By Theorem 5.1.1, we have $spn^+ = [J_k : P_D\theta(J_L)]$. Now, if we let $\tilde{A} = \prod_{\mathfrak{p}} A_{\mathfrak{p}}^{\times}$, we obtain

$$spn^+ = [J_k : \theta(J_L)P_{k^\times}]$$

$$= [k^\times \cdot \tilde{A} \cdot k_\infty^\times : \prod_{\mathfrak{p} \text{ incl } \infty} \theta(O^+(L_{\mathfrak{p}})) \cdot k^\times]$$

$$= \# \frac{k^\times \cdot \prod_{\mathfrak{p}\in S} A_{\mathfrak{p}} \cdot \prod_{\mathfrak{p}\notin S} A_{\mathfrak{p}} \cdot k_\infty^\times}{k^\times \cdot \prod_{\mathfrak{p}\in S} \theta(O^+(L_p)) \cdot \prod_{\mathfrak{p}\notin S} \theta(O^+(L_p)) \cdot k_\infty^\times}$$

$$= \#\frac{k^\times \cdot \prod_{\mathfrak{p}\in S} A_\mathfrak{p} \cdot \prod_{\mathfrak{p}\notin S} A_\mathfrak{p} \cdot k_\infty^\times}{k^\times \cdot \prod_{\mathfrak{p}\in S} \theta(O^+(L_p)) \cdot \prod_{\mathfrak{p}\notin S} A_\mathfrak{p} \cdot k_\infty^\times}$$

$$= \#\frac{\prod_{\mathfrak{p}\in S} A_\mathfrak{p}}{\prod_{\mathfrak{p}\in S} \theta(O^+(L_p))}$$

$$= \prod_{\mathfrak{p}\in S, \mathfrak{p}\neq\mathfrak{q}} 2$$

$$= 2^r$$

By choosing $r$ suitably, the class number of $\mathcal{G}$ can be made arbitrarily large. ■

# Chapter 6

# Regular Quaternary Lattices

## 6.1 Universal Lattices

In [12], Gerstein formulated a function field version of the Conway-Schneeberger 15-theorem. He called this conjecture the 4-conjecture. It says that if $L$ is a definite $\mathbb{F}_r[t]$-lattice then $L$ is universal (i.e. represent all of $\mathbb{F}_r[t]$) if and only if $L$ represents the four elements $1, \delta, t, \delta t$ for any given nonsquare $\delta \in \mathbb{F}_r$. One will notice that the necessity of the condition above is clear. One will also notice that a universal definite lattice is necessarily quaternary and has the following shape:

$$L \cong \langle 1, -\delta \rangle \perp \begin{pmatrix} \alpha t + \beta & \gamma \\ \gamma & -\delta\alpha t + \eta \end{pmatrix}.$$

By considering a lattice which is isometric to $L$ instead of $L$ itself, one sees easily that the four conjecture will be established as long as one can prove the universality of

$$L \cong \langle 1, -\delta \rangle \perp \begin{pmatrix} t & \epsilon \\ \epsilon & -\delta t + \alpha \end{pmatrix}$$

for any $\alpha \in \mathbb{F}_r$, $\epsilon = 0, 1$.

**Proposition 6.1.1 (Gerstein)** *If $L \cong \langle 1, -\delta, t, -\delta t \rangle$, then $L$ is universal.*

**Sketch of proof.** We let $V$ be the underlying quadratic space. By Hasse principle $V$ is universal. Hence for every $f \in \mathbb{F}_r[t]$, there is a $\mathbb{F}_r[t]$-maximal lattice on $V$ that represents $f$. It is well known that $\mathbb{F}_r[t]$-maximal lattices constitute a single genus. One then just need to prove that $L$ is $\mathbb{F}_r[t]$-maximal and has class number one. ■

**Proposition 6.1.2 (Gerstein)** *Suppose $J \cong \langle 1, -\delta, t\rangle$ and let $f \in \mathbb{F}_r[t]$. Then $f$ is represented by $J$ if and only if neither the highest degree term nor the lowest degree term of $f$ has odd degree and a nonsquare coefficient.*

**Sketch of proof.** It is clear that $J$ is $\mathbb{F}_r[t]$-maximal and that $J$ is alone in its genus (since $\partial(\mathrm{disc}(J)) = 1$). Therefore $f$ is represented by $J$ if and only if $f$ is represented by $J$ locally everywhere. This is equivalent to the space $W \cong \langle 1, -\delta, t, \rangle$ being isotropic. It is clear that $J_{\mathfrak{p}}$ is unimodular and therefore isotropic for all $\mathfrak{p} \notin \{t, \infty\}$.

Suppose that $f(t) = f_s t^s + f_{s-1}t^{s-1} + \cdots + f_j t^j$ where $f_j f_s \neq 0$. Then

$$\langle f\rangle_t \cong \langle f_j t^j\rangle_t \quad \text{and} \quad \langle f\rangle_\infty \cong \langle f_s t^s\rangle_\infty.$$

Also note that $W$ is isotropic if and only if $\langle f\rangle_t \ncong \langle \delta t\rangle_t$ and $\langle f\rangle_\infty \ncong \langle \delta t\rangle_{infty}$. The result follows easily. ■

The following result was independentely proved by Chan and Daniels ([5]), by Kim, Wang and Xu ([16]) and by the author.

**Theorem 6.1.1** *The Four conjecture is true.*

**Proof.** In the following $\delta$ stands for a nonsquare in $\mathbb{F}_r$. We want to show that the lattice

$$\langle 1, -\delta \rangle \perp \begin{bmatrix} x & \epsilon \\ \epsilon & -\delta x + \alpha \end{bmatrix}$$

where $\epsilon = 0, 1$ and $\alpha \in \mathbb{F}_r$ is universal. Let $L = \langle 1, -\delta, x \rangle$. We know that the $k[t]$-lattice $L$ represents any element of $k[t]$ whose neither the highest degree term, nor the lowest degree term have odd degrees and nonsquare coefficients.

**Case1:** $\epsilon = 0$**.**

We know that any polynomial of the form $a_n t^n + \cdots + a_l t^l$ where both of $a_n t^n$ and $a_l t^l$ have even degree or square coefficients is represented by $L$. It is *a fortiori* by $\langle 1, -\delta, x, -\delta x + \alpha \rangle$.

Let $f = a_n t^n + \cdots + a_l t^l$ be an element that may be not represented. In particular one of $a_n t^n$ or $a_l t^l$ has odd degree and nonsquare coefficient. We also know that the lattice $\langle 1, -\delta, x, -\delta x \rangle$ is universal and thus we assume that $\alpha \neq 0$.

Suppose $\partial f \geq 5$. By counting the number of elements of the form $a_n + \delta b^2$ when $b$ ranges over $\mathbb{F}_r$ we see that there is necessarily an element $b$ in $k$ such that $a_n + \delta b^2$ is a square in $\mathbb{F}_r$. Fix such an element $b$. As $char(k) \neq 2$, $b \neq 0$ and $\delta \neq 0$, one can choose $c \in k$ such that

$$a_{n-1} - (\alpha b - 2\delta b c) \neq 0.$$

Since $\alpha \neq 0$, one can choose $r \in k^\times$ such that $a_0 - \alpha r^2 \neq 0$ (where $a_0 = 0$ if $l \geq 1$). Then

$$f(t) - (-\delta t + \alpha) \left( b t^{\frac{n-1}{2}} + c t^{\frac{n-1}{2}-1} + r \right)^2$$

is represented by $L$. Indeed, the lowest degree term of this polynomial is $0 \neq a_0 - \alpha r^2$ and is therefore of degree 0. The highest degree coefficient of this polynomial is $a_n + \delta b^2$ as long as $a_n + \delta b^2 \neq 0$ and therefore has a square coefficient.

If now $a_n + \delta b^2 = 0$, the highest degree term is $0 \neq (a_{n-1} - (\alpha b - 2\delta bc)t^{n-1}$ and is therefore of even degree. So there are $f_1, f_2, f_3 \in k[t]$ such that

$$f = f_1^2 - \delta f_2^2 + t f_3^2 + (-\delta t + \alpha)\left(bt^{\frac{n-1}{2}} + ct^{\frac{n-1}{2}-1} + r\right)^2.$$

Which shows that $\langle 1, -\delta, x, -\delta x + \alpha\rangle$ represents any polynomial of degree $\geq 5$. If $n < 5$ then $\frac{n-1}{2} \leq 2$ and so the previous argument cannot apply. Nevertheless:

If $\partial f = 4$ or $\partial f = 2$ then the same method as above applies taking (with the same notation) $b = c = 0$ and $r$ chosen as above.

If $\partial f = 3$ the same method as above applies. Let $f(t) = a_3t^3 + \cdots + a_0$, $a_3 \neq 0$. One can choose $s$ such that $a_3 - \delta s^2$ is a square in $k$. If $s \neq 0$ one can choose $v \in k$ such that both of $-2\delta sv + \alpha s^2$ and $\alpha v^2$ are nonzero elements. Finally $f - (-\delta t + \alpha)(st + v)^2$ is represented by $L$ and we conclude as previously.

Finally, it is clear that any linear polynomial if represented. polynomial

**Case 2:** $\epsilon = 1$**.**

Let $f = a_nt^n + \cdots + a_lt^l$, where

1. either $l = 1 \mod 2$ and $a_l \notin \mathbb{F}_r^{\times 2}$;
2. or $m = 1 \mod 2$ and $a_m \notin \mathbb{F}_r^{\times 2}$.

As that the polynomial of degree $\leq 1$ are represented by

$$\langle 1, -\delta\rangle \perp \begin{pmatrix} x & 1 \\ 1 & -\delta x + \alpha \end{pmatrix}$$

we may assume that $n \geq 2$.

Assume first $\partial f \geq 9$. Choose $b \in k$ such that $a_n + \delta b^2$ is a square in $k$. As in the previous case, one can choose $c \in k$ such that $a_{n-1} + 2\delta bc - b^2\alpha \neq 0$. Choose $r \in k$ such that $a_1 - r^2$ (where $a_1$ is possibly 0) is a square in $k$. If $a_0 \neq 0$ or if $a_1$ is a square in $k$ then the lowest degree term has even degree or square coefficient.

If $a_0 = 0$ and if $a_1$ is not a square, then $r \neq 0$. One can therefore choose $d \in k$ such that $a_2 - 2rd - \alpha r^2 \neq 0$. Expand

$$f - (-\delta t^3 + \alpha t^2 + t)(bt^{\frac{n-3}{2}} + ct^{\frac{n-3}{2}-1} + dt + r)^2$$

to see that

$$(a_n + \delta b^2)t^n + (a_{n-1} + 2\delta bc - b^2\alpha)t^{n-1} + \cdots + (a_2 - 2rd - \alpha r^2)t^2 + (a_1 - r^2)t + a_0$$

is represented by $\langle 1, -\delta, t\rangle$. Thus, there are polynomials $f_1, f_2, f_3$ such that

$$f = f_1^2 - \delta f_2^2 + t f_3^2 + (-\delta t^3 + \alpha t^2 + t)h^2$$

where $h = (bt^{\frac{n-3}{2}} + ct^{\frac{n-3}{2}-1} + dt + r)$.

Let $F_1 = f_1$, $F_2 = f_2$, $F_3 = f_3 - h(t)$ and $F_4 = th(t)$. We have

$$f(t) = F_1^2 - \delta F_2^2 + tF_3^2 + 2F_3F_4 + (-\delta t + \alpha)F_4^2$$

and so $f$ is represented by $\langle 1, -\delta\rangle \perp \begin{pmatrix} x & 1 \\ 1 & -\delta x + \alpha \end{pmatrix}$

The previous argument fails when the elements $b, c, d, r$ of $k$ may not be chosen freely (i.e. $\frac{n-3}{2} \leq 2$). Nevertheless, if $\partial f \geq 4$ and $\partial f = 0 \mod 2$ then the previous argument applies with $b = c = 0$ and $d, r$ chosen as above.

If $\partial f = 2, 3$ then a direct computation shows that $f$ is indeed represented by $L$. If $\partial f = 5$ and $a_0 \neq 0$ then the same method as above may be applied. Indeed, modifying the polynomial $f$ by a factor of $(-\delta t^3 + \alpha t^2 + t)$ will not change the constant term of $f$. One might also assume that the leading coefficient $a_5$ is not a square. If not, modifying the polynomial $f$ by a factor $(-\delta t^3 + \alpha t^2 + t)r^2$ will not change the leading coefficient. If finally $a_1 = 0$ then $f(t) = t^2(a_5 t^3 + \cdots)$ and so by the previous case is represented by the lattice. Now, as $a_5$ is not a square, it follows that there is $b \in \mathbb{F}_q$ so that $a_5 + \delta b^2$ is a nonzero square in $\mathbb{F}_r$. Suppose $a_1 \neq 0$. If $a_1$ is a square, then take $b$ as above and $r = 0$. If $a_1$ is not a square, choose $b$ as above and $r$ such that $a_1 - r^2$ is a nonzero square. In both case

$$f(t) - (-\delta t^3 + \alpha t^2 + t)(bt + r)^2$$

is represented by $L$.

If $\partial f = 7$ (if need be) take $v \in k$ such that $a_{n-1} + 2\delta bv - b^2\alpha v \neq 0$ and $a_2 - 2rv - \alpha r^2 \neq 0$. Then the same argument as in the case $\partial f \geq 9$ applies. ■

**Corollary 6.1.1** *Any definite $\mathbb{F}_r[t]$-lattice is universal if and only if it has rank 4 and its discriminant has degree 2.*

**Proof.** Clear from above. ■

**Corollary 6.1.2** *Any universal definite $\mathbb{F}_r[t]$-lattice has class number one.*

**Proof.** Clear from Theorem 6.1.1 and Lemma 2.2.1. ■

## 6.2 Regular Quaternary Quadratic Forms

**Lemma 6.2.1 ([5], 4.4)** *Let $L$ be a regular quaternary lattice. Suppose that $\mathfrak{p}$ is a finite place for which the unimodular Jordan component of $L_\mathfrak{p}$ is not isotropic. Then, there exists a regular lattice $L'$ such that either the unimodular Jordan component of $L'_\mathfrak{p}$ is isotropic or $L'_\mathfrak{p}$ is the unique anisotropic $A_\mathfrak{p}$-maximal lattice, and for each $\mathfrak{q} \neq \mathfrak{p}$, $L'_\mathfrak{q} \cong \epsilon L_\mathfrak{q}$ for some $\epsilon \in A_q^\times$.*

**Sketch of Proof.** Apply the $\lambda_\mathfrak{p}$-transformation to $L$ in order to get $L'$. Also one needs to prove that if $L$ is regular then so if $\lambda_\mathfrak{p}(L)$. For this proof, we refer to ([7], 2.7). ■

**Definition.** Let $\mathfrak{p}$ be a prime, let $L$ and $L'$ be lattices defined as Lemma 6.2.1.

1. $\mathfrak{p}$ is a good prime for $L$ if $L'_{\mathfrak{p}}$ is the unique anisotropic $A_{\mathfrak{p}}$-maximal lattice;

2. $\mathfrak{p}$ is a bad prime for $L$ if the unimodular Jordan component of $L'_{\mathfrak{p}}$ is isotropic.

■

**Lemma 6.2.2** *Let $L$ be a regular quaternary lattice. Then, $L$ has at most one good primes and its degree is* 1.

**Proof.** Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be good primes for $L$. By the definition of a good prime, we see that there exist a regular lattice $L'$ such that

1. $L'_{\mathfrak{p}_i} \cong \langle 1, -\eta_i, \mathfrak{p}_i, -\eta_i\mathfrak{p}_i \rangle$ where $\eta_i \notin A_{\mathfrak{p}_i}^{\times 2}$.

2. $L'_{\mathfrak{q}}$ has an isotropic unimodular Jordan component for $\mathfrak{q} \neq \mathfrak{p}_i$ , $i = 1, \cdots, n$.

Since $L'_{\mathfrak{q}}$ has an isotropic unimodular Jordan component we see that $L'_{\mathfrak{q}}$ is universal. Also, since $L'$ is definite, it is clear that $W_\infty$ is universal. Finally, $L_{\mathfrak{p}_i}$ is clearly universal for all $i = 1, \cdots, n$. Since $L'$ is regular, we see that it must be universal. We can conclude with Corollary 6.1.1. ■

**Lemma 6.2.3** *Let $L$ be a definite quaternary lattice. If $L$ has a good prime, then $L$ has no bad prime.*

**Proof.** By Lemma 6.2.2, we know that the good prime has degree 1; call it $\mathfrak{p}$. Suppose that $L$ has a bad prime, say $\mathfrak{q}$.

By applying some $\lambda_{\mathfrak{l}}$-transformations, we can suppose that for $\mathfrak{l} \neq \mathfrak{p}, \mathfrak{q}$, $L_{\mathfrak{l}}$ is unimodular. Since $L'$ is universal, we know that $\partial(\mathrm{disc}(L')) \leq 2$; hence $L'_{\mathfrak{q}}$ is

unimodular. Suppose that $\lambda_{\mathfrak{q}}^{n}(L)_{\mathfrak{q}} = L'_{\mathfrak{q}}$. Clearly neither $L_{\mathfrak{q}}$ nor any $\lambda_{\mathfrak{q}}^{m}(L)_{\mathfrak{q}}$ for $m < n$ can have a unimodular isotropic component (otherwise the lattice would be universal). Let $L''$ be a lattice with $L''_{\mathfrak{q}} = \lambda_{\mathfrak{q}}^{n-1}(L)_{\mathfrak{q}}$, $L''_{\mathfrak{p}} = \epsilon L'_{\mathfrak{p}}$ ($\epsilon \in A_{\mathfrak{p}}^{\times}$) and $L''_{\mathfrak{l}}$ is unimodular for $\mathfrak{l} \neq \mathfrak{p}, \mathfrak{q}$. Since $L$ is regular, we can suppose that so is $L''$.

We start by proving that $L''_{\mathfrak{q}}$ cannot have a unimodular component of rank 2. Indeed, it is clear that $L''_{\mathfrak{p}}$ is universal. Since $L''$ is regular, we see that an element of $A$ is represented by $L''$ if and only if it is represented by $L''_{\mathfrak{q}}$. If $L''_{\mathfrak{q}}$ has a unimodular component of rank 2, then all of $A_{\mathfrak{q}}^{\times}$ is represented by $L''_{\mathfrak{q}}$. In particular $1, \delta, \mathfrak{p}$ and $\delta\mathfrak{p}$ must be represented by $L''$; hence $L''$ is universal and thus $\partial(\mathrm{disc}(L'')) = 2$. This is not possible.

That leaves us with one possibility for $L''_{\mathfrak{q}}$; that is $L''_{\mathfrak{q}} \cong \langle a, b\mathfrak{q}^2, c\mathfrak{q}^2, d\mathfrak{q}^2 \rangle$ for some $a, b, c, d \in A_{\mathfrak{q}}^{\times}$. In particular, we see that one square class of $\mathbb{F}_r$ is represented by $L''_{\mathfrak{q}}$; hence $\mu_1(L'') = 0$. By ([5],4.2) we can further suppose that $\partial(\mathfrak{q}) \leq 2$ and therefore Lemma 5.2.3 tells that there are some linear polynomials with arbitrary coefficients represented by $L''_{\mathfrak{q}}$. Those polynomials must be represented by $L''$; hence $\mu_2 = \mu_3 = 1$. By Lemma 5.2.3, we can choose two linear polynomials, $f, g \in A$ satisfying the following conditions. The leading coefficient of $fg$ is not in the same square class as $L''^{1\times 1}$ and we have

$$\left(\frac{fg}{\mathfrak{q}}\right) = \left(\frac{a}{\mathfrak{q}}\right).$$

Now, we see that $fg$ is represented by $L''_{\mathfrak{q}}$ and therefore by $L''$. By the assumption above, it cannot be represented by $L''^{1\times 1}$; hence $\mu_4 = 2$. That is a contradiction.

■

**Corollary 6.2.1** *Let $L$ be a quaternary regular lattice and suppose that $L$ has some good primes. Then, $L$ is regular if and only if $L$ is universal.*

**Lemma 6.2.4** *Let $L$ be a quaternary lattice. Suppose that $L$ has no good primes. Then, $L$ is regular if and only if $L$ is universal.*

**Proof.** The sufficiency in the lemma is clear. We prove here the necessity. Let $\mathfrak{q}_1, \cdots, \mathfrak{q}_n$ be the prime dividing $\mathrm{disc}(L)$. All of them are good primes, which means that for any $i = 1, \cdots, n$, the localizations $L'_{\mathfrak{q}_i}$ all have an isotropic unimodular component. We see that $L'_{\mathfrak{q}_i}$ is universal for all $i$ and since $L'$ is regular, we conclude that $L'$ is universal. But then Corollary 6.1.1 implies that $\partial(\mathrm{disc}(L')) = 2$. Then $\mathfrak{q}_1$ and (possibly) $\mathfrak{q}_2$ be primes dividing $\mathrm{disc}(L)$. The sum of the degrees of these primes must be 2.

Let $\mathfrak{q} \neq \mathfrak{q}_1, \mathfrak{q}_2$ be a prime dividing $\mathrm{disc}(L)$ and suppose that $\lambda^n_{\mathfrak{q}}(L)_{\mathfrak{q}} = L'_{\mathfrak{q}}$. Clearly neither $L_{\mathfrak{q}}$ nor any $\lambda^m_{\mathfrak{q}}(L)_{\mathfrak{q}}$ for $m < n$ can have a unimodular isotropic component (otherwise the lattice would be universal). Let $L''$ be a lattice with

1. $L''_{\mathfrak{q}} = \lambda^{n-1}_{\mathfrak{q}}(L)_{\mathfrak{q}}$;
2. $L''_{\mathfrak{q}_1} = \epsilon_1 L'_{\mathfrak{p}_1}$, with $\epsilon_1 \in A^{\times}_{\mathfrak{q}_1}$;
3. $L''_{\mathfrak{q}_2} = \epsilon_2 L'_{\mathfrak{p}_2}$, with $\epsilon_2 \in A^{\times}_{\mathfrak{q}_2}$;
4. $L''_{\mathfrak{l}}$ is unimodular for $\mathfrak{l} \notin \{\mathfrak{q}, \mathfrak{q}_1, \mathfrak{q}_2\}$.

Note that since $L$ is regular, we can suppose that so is $L''$. Again, we prove that $L''_{\mathfrak{q}}$ cannot have a unimodular component of rank 2. Indeed, it is clear that $L''_{\mathfrak{q}_i}$ is universal for $i = 1, 2$. Since $L''$ is regular, we see that an element of $A$ is represented by $L''$ if and only if it is represented by $L''_{\mathfrak{q}}$. If $L''_{\mathfrak{q}}$ has a unimodular component of rank 2, then all of $A^{\times}_{\mathfrak{q}}$ is represented by $L''_{\mathfrak{q}}$. In particular $1, \delta, \mathfrak{q}_1$ and $\delta\mathfrak{q}_1$ must be represented by $L''$; hence $L''$ is universal and thus $\partial(\mathrm{disc}(L'')) = 2$. This is not possible.

That leaves us with one possibility for $L''_{\mathfrak{q}}$; that is $L''_{\mathfrak{q}} \cong \langle a, b\mathfrak{q}^2, c\mathfrak{q}^2, d\mathfrak{q}^2 \rangle$ for some $a, b, c, d \in A^{\times}_{\mathfrak{q}}$. In particular, we see that one square class of $\mathbb{F}_r$ is represented

by $L''_{\mathfrak{q}}$; hence $\mu_1(L'') = 0$. By ([5],4.2) we can further suppose that $\partial(\mathfrak{q}) \leq 2$ and therefore Lemma 5.2.3 tells that there are some linear polynomials with arbitrary coefficients represented by $L''_{\mathfrak{q}}$. Those polynomials must be represented by $L''$; hence $\mu_2 = \mu_3 = 1$. By Lemma 5.2.3, we can choose two linear polynomials, $f, g \in A$ satisfying the following conditions. The leading coefficient of $fg$ is not in the same square class as $L''^{1\times 1}$ and we have

$$\left(\frac{fg}{\mathfrak{q}}\right) = \left(\frac{a}{\mathfrak{q}}\right).$$

Now, we see that $fg$ is represented by $L''_{\mathfrak{q}}$ and therefore by $L''$. By the assumption above, it cannot be represented by $L''^{1\times 1}$; hence $\mu_4 = 2$. That is a contradiction.

Finally we see that if $L$ is regular then $L = L'$ and we can conclude that $L$ is universal. ■

The results on regular put together leads to

**Theorem 6.2.1** *Let $L$ be a definite $\mathbb{F}_r[t]$-lattice. Then $L$ is regular if and only if $L$ has class number one.*

One will notice the contrast with the case over $\mathbb{Z}$ where there are infinitely many quaternary regular classes (cf. [10]).

# Chapter 7

# Open Questions

## 7.1 Isospectral Indefinite Lattices

All the results presented in the first four sections of this work are valid for definite $\mathbb{F}_r[t]$-lattice where $\mathbb{F}_r$ has odd characteristic. One could wonder if these results, especially those on isospectrality are still valid if the lattice we consider is not definite.

Let $L$ be an indefinite $\mathbb{F}_r[t]$-lattice. The representations numbers, as defined in the definite case

$$R(L,a) = \#\{x \in L : q(x) = a\} \tag{7.1}$$

do not make sense anymore, as the set on the right hand side of (7.1) is infinite. There are then two possibilities. One is to replace these representations numbers by some densities; although this kind of work has been done for $\mathbb{Z}$-lattices, it seems to be hard to use it in our case. Another possibility is to follow the approach of M. Car (cf. [2]) and to add some restrictive degree conditions in the set on the right hand side of (7.1). In this case, we would get

$$R(L,a) = \#\left\{x = (x_1, \cdots, x_n) \in L : q(x) = a \text{ and } \partial(x_i) \leq \frac{\partial(a)}{2} + 1\right\}.$$

All the arguments made with the systems would still work; but all the results using definiteness of the forms (e.g. Proposition 3.1.1, Proposition 3.2.1...) would not work anymore.

## 7.2 Isospectral Quaternary Lattices

The work above seems to suggest that representation numbers and more generally representation sets determine a lattice quite a lot. More precisely the representation sets seem to determine $\mathbb{F}_r[t]$-lattices much more than they determine $\mathbb{Z}$-lattices. For example there are some regular definite $\mathbb{Z}$ lattices having class number greater than one (cf. [13]). That is why, it seems reasonable to believe that representations numbers will determine the equivalence class of a quaternary definite lattice. As of today, we have not been able to solve this problem. A possible approach would be the same as the one we used in the ternary case.

## 7.3 Even Characteristic

All the work above made in this dissertation applies for a finite field of odd characteristic. One could wonder what happens in characteristic 2. This case seems to be considerably harder to solve. One would maybe like to develop first a reduction theory à la Gerstein. Also, one should note that the arguments on systems and more generally the formulas given by Carlitz (cf. 3.4.1) fails in even characteristic.

# Bibliography


[1] M. Car, Sommes de carrés dans $F_q[X]$, Dissertationes Math. 215 (1983).

[2] M. Car, Quadratic forms on $F_q[T]$. J. Number Theory 61 (1996), no. 1.

[3] L. Carlitz, Invariant theory of systems of equations, J. D'analyse Mathématique, Vol 3 (1954), p 382–413.

[4] J. W. S. Cassels, Rational quadratic forms, London Mathematical Society Monographs, 13 Academic Press, London-New York, 1978.

[5] W. K. Chan, J. Daniels, Definite regular quadratic forms over $\mathbb{F}_r[T]$, Proc. Amer. Math. Soc. 133 (2005), no. 11.

[6] W. K. Chan and A. G. Earnest, Discriminant bounds for spinor regular ternary quadratic lattices, J. London Math. Soc. (2) 69 (2004), no. 3, 545–561.

[7] W. K. Chan, A. G. Earnest, B. -K. Oh, Regularity properties of positive definite integral quadratic forms. Algebraic and arithmetic theory of quadratic forms, 59–71, Contemp. Math., 344 (2004).

[8] J. H. Conway and N. J. Sloane, Four-dimensional lattices with the same theta series, Internat. Math. Res. Notices , no. 4 (1992), 93–96.

[9] D.Z. Djoković, Hermitian matrices over polynomial rings, J. Algebra 43 (1976), 359-374.

[10] A.G. Earnest, An application of character sum inequalities to quadratic forms, Number theory, 155–158, CMS Conf. Proc., 15, Amer. Math. Soc., Providence, RI, 1995.

[11] L. Gerstein, Definite quadratic form over $\mathbb{F}_r[x]$, Journal of Algebra, v. 268 (2002), p 252-263.

[12] L. Gerstein, On representation by quadratic $\mathbb{F}_q[x]$-lattices. Algebraic and arithmetic theory of quadratic forms, 129–134, Contemp. Math., 344, Amer. Math. Soc., Providence, RI, 2004.

[13] J. S. Hsia, Regular positive ternary quadratic forms. Mathematika 28 (1981), no. 2.

[14] J. S. Hsia, On primitive spinor exceptional representations. J. Number Theory 26 (1987), no. 1

[15] W. Jagy, I. Kaplansky, A. Schiemann, There are 913 regular ternary forms, Mathematika 44 (1997), no. 2.

[16] M.-H. Kim, Y. Wang and F. Xu, Universal quadratic forms over $\mathbb{F}_q[T]$, preprint, 2004.

[17] Y. Kitaoka, Positive definite quadratic forms with the same representation numbers, Arch. Math. 28 (1977), no. 5, 495–497.

[18] Y. Kitaoka, Arithmetic of quadratic forms. Cambridge Tracts in Mathematics, 106. Cambridge University Press, Cambridge, 1993.

[19] M. Kneser, Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Vernderlichen, Arch. Math. 7 (1956).

[20] M. Kneser, Darstellungsmasse indefiniter quadratischer Formen. Math. Z. 77 (1961).

[21] M. Kneser, Composition of binary quadratic forms. J. Number Theory 15 (1982), no. 3, 406–413.

[22] O. T. O'Meara, Introduction to quadratic forms, Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[23] H. Rosson, Theta series of quaternion algebras over function fields, J. Number Theory 94 (2002), no. 1, 49–79.

[24] H. G. Rück, Theta series of imaginary quadratic function fields, Manuscripta Math. 88 (1995), no. 3, 387–407.

[25] A. Schiemann, Ein Beispiel positiv definiter quadratischer Formen der Dimension 4 mit gleichen Darstellungszahlen, Arch. Math. (Basel) 54 (1990), no. 4, 372–375.

[26] A. Schiemann, Ternary positive definite quadratic forms are determined by their theta series, Math. Ann. 308 (1997), no. 3, 507–517.

[27] R. Schulze-Pillot, Darstellung durch Spinorgeschlechter ternrer quadratischer Formen. J. Number Theory 12 (1980), no. 4.

[28] G. L. Watson, Determination of a binary quadratic form by its values at integer points, Mathematika 26 (1979), no. 1, 72–75.

[29] G. L. Watson, Aknowledgement: *Determination of a binary quadratic form by its values at integer points*, Mathematika 27 (1980), no. 2, 188 (1981).

[30] A. Weil, Sur certains groupes d'opérateurs unitaires, Acta Math. 111 (1964), 143–211.

# Vita

Jean E. Bureau was born on July 7th, 1980 in Paris, France. As an undergraduate he studied in *Université Denis Diderot* (Paris VII) and in the International University of Leeds (U.K.). In June 2001, he obtained a *Licence de Mathématiques* (*supra cum laude*) and in June 2002 he obtained a *Maîtrise de Mathématiques* (*sume cum laude*). In August 2002 he came to Louisiana State University to pursue graduate studies in mathematics where he earned a Master of Science in mathematics in December 2005. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in December 2006.