Astérisque

GUNTHER VOGEL
ULRICH GÖRTZ
TORSTEN WEDHORN
VOLKER MEUSERS
EVA VIEHMANN
KONSTANTIN ZIEGLER
STEFAN WEWERS
INKEN VOLLAARD
IRENE I. BOUW
MICHAEL RAPOPORT

Argos seminar on intersections of modular correspondences

Astérisque, tome 312 (2007)

<http://www.numdam.org/item?id=AST_2007__312__R1_0>

ASTERISQUE 312

ARGOS SEMINAR ON INTERSECTIONS OF MODULAR CORRESPONDENCES

Société Mathématique de France 2007
Publié avec le concours du Centre National de la Recherche Scientifique

2000 ***Mathematics Subject Classification.*** **—** 11G18, 11E08, 11F03, 11F30, 11F32, 11G15, 11G18, 14B12, 14G35, 14K07, 14K22, 14L05.

Key words and phrases. **—** Modular correspondences, endomorphisms of formal groups, quadratic forms over the ring of p-adic integers, Siegel-Eisenstein series.

ARGOS SEMINAR ON INTERSECTIONS OF MODULAR CORRESPONDENCES

Abstract. — This volume contains the written account of the Bonn seminar on arithmetic geometry 2003/2004. It gives a coherent exposition of the theory of intersections of modular correspondences. The focus of the seminar is the formula for the intersection number of arithmetic modular correspondences due to Gross and Keating. Other topics treated are Hurwitz's theorem on the intersection of modular correspondences over the field of complex numbers, and the relation of the arithmetic intersection numbers to Fourier coefficients of Siegel-Eisenstein series.

Also included is background material on one-dimensional formal groups and their endomorphisms, and on quadratic forms over the ring of p-adic integers.

Résumé **(Séminaire ARGOS sur les intersections de correspondances modulaires)**

Ce volume consiste des exposés faits dans le cadre du séminaire de géométrie arithmétique de Bonn en 2003/2004. Il donne une exposition systématique de la théorie des intersections de correspondances modulaires. Le but principal est la formule de Gross-Keating du nombre d'intersection de correspondances modulaires arithmétiques. Autres sujets traités sont le théorème de Hurwitz sur l'intersection de correspondances modulaires sur le corps des nombres complexes, et la relation des nombres d'intersection arithmétiques aux coefficients de Fourier des séries de Siegel-Eisenstein.

On a aussi inclus des rappels sur les groupes formels à un paramètre et leurs endomorphismes, et sur les formes quadratiques sur l'anneau des entiers p-adiques.

CONTENTS

1. FOREWORD

1. Motivation and main results

This book is based on the notes for the ΑΡΓΟΣ[1] seminar of the winter semester 2003/2004 at the University of Bonn. Its aim was to go through the paper *On the intersection of modular correspondences* by Gross and Keating [**GK**], and understand it thoroughly. This subject was chosen for three reasons. First of all, it was felt that the mathematics contained in this paper (and the papers on which Gross and Keating base their article) is extremely interesting, and has become even more important recently, due to the use that S. Kudla and others have made of these results. Secondly, thanks to the elementary methods employed in the proofs of the main theorems, the seminar provided a rapid access, even to a novice in the field, to a deep and sophisticated topic in arithmetic algebraic geometry. Thirdly, it was felt from the start that the literature on the subject was not easy to penetrate and that therefore the effort made by all speakers to master this material should not be lost, and that a written account of the seminar should be made available.

The origin of the topics treated in the seminar goes back to the 19^{th} century. Let $j = j(\tau)$ be the elliptic modular function on the upper half plane. For $m \geq 1$ let $\varphi_m(j, j') \in \mathbb{Z}[j, j']$ be the classical *modular polynomial,* defined by

$$\varphi_m(j(\tau), j(\tau')) = \prod_{\substack{A \in \mathrm{M}_2(\mathbb{Z}) \\ \det(A)=m \\ \bmod SL_2(\mathbb{Z})}} (j(\tau) - j(A\tau')) \quad . \tag{1.1}$$

Kronecker and Hurwitz established a number of important properties of these polynomials, as for instance their factorization into irreducible factors. They also proved degree formulas like

$$\deg\ f_m = \sum_{dd'=m} \max(d, d') \quad , \tag{1.2}$$

where $f_m(j) = \varphi_m(j, j)$, for m not a square.

---

[1] Acronym for **Ar**ithmetische **G**eometrie **O**ber**s**eminar.

From the point of view of the seminar, the interest in these results lies in the fact that they can be interpreted as giving intersection numbers on the complex surface $S_{\mathbb{C}} = \operatorname{Spec} \mathbb{C}[j, j']$. Let $T_{m,\mathbb{C}} \subseteq S_{\mathbb{C}}$ be the divisor defined by $\varphi_m = 0$. Then (1.2) can be interpreted as the intersection formula

$$(T_{m,\mathbb{C}} \cdot T_{1,\mathbb{C}}) = \sum_{dd'=m} \max(d, d') \quad , \tag{1.3}$$

if m is not a square. Here $(T_{m_1,\mathbb{C}} \cdot T_{m_2,\mathbb{C}})$ is defined by

$$(T_{m_1,\mathbb{C}} \cdot T_{m_2,\mathbb{C}}) = \dim_{\mathbb{C}} \mathbb{C}[j, j']/(\varphi_{m_1}, \varphi_{m_2}) \quad . \tag{1.4}$$

More generally, Hurwitz showed that the divisors $T_{m_1,\mathbb{C}}$ and $T_{m_2,\mathbb{C}}$ intersect properly on $S_{\mathbb{C}}$ if and only if $m_1 m_2$ is not a perfect square and gave an explicit expression for the intersection number $(T_{m_1,\mathbb{C}} \cdot T_{m_2,\mathbb{C}})$. This in turn leads to the famous class number relations of Kronecker and Hurwitz.

Gross and Keating took up this classical subject by adding an arithmetic dimension to it. Instead of usual intersection numbers they consider arithmetic intersection numbers. Let $S = \operatorname{Spec} \mathbb{Z}[j, j']$, which we consider as an arithmetic threefold. Let T_m be the arithmetic divisor defined by $\varphi_m = 0$. The arithmetic intersection number is defined for any triple of positive integers m_1, m_2, m_3 by

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3}) = \log \#\ \mathbb{Z}[j, j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3}) \quad . \tag{1.5}$$

Gross and Keating derive a criterion for when this number is finite and give in this case an explicit expression for it (see below). This result is the main focus of the present book. Let us state it from the point of view adopted in these notes. Let $\mathcal{M}$ be the moduli space of elliptic curves over $\operatorname{Spec} \mathbb{Z}$ (since we impose no level structure, $\mathcal{M}$ is not a scheme, but a Deligne-Mumford stack). Put $\mathcal{S} = \mathcal{M} \times_{\operatorname{Spec} \mathbb{Z}} \mathcal{M}$. For a positive integer m, let $\mathcal{T}_m$ be the moduli space of isogenies of elliptic curves $E \to E'$ of degree m. Then $\mathcal{T}_m$ maps by a finite unramified morphism to $\mathcal{M} \times \mathcal{M}$. From this point of view, the intersection number above should be interpreted as

$$\sum_p \log(p) \cdot \sum_{x \in \mathcal{X}(\overline{\mathbb{F}}_p)} \frac{1}{\#\mathrm{Aut}(x)} \lg\, \widehat{\mathcal{O}}_{\mathcal{X},x},$$

where we denote by $\mathcal{X}$ the triple fiber product of $\mathcal{T}_{m_1}$, $\mathcal{T}_{m_2}$, and $\mathcal{T}_{m_3}$ over $\mathcal{M} \times \mathcal{M}$. Here the weighting factor $\frac{1}{\#\mathrm{Aut}(x)}$ is due to the fact that $\mathcal{X}$ is a stack.

We now state the main results contained in this volume.

We denote by $S_{\mathbb{C}}$ resp. by $T_{m,\mathbb{C}}$ the base change of S resp. T_m to $\operatorname{Spec} \mathbb{C}$. The first result is Hurwitz's theorem.

Theorem 1.1. — *The cycles $T_{m_1,\mathbb{C}}$ and $T_{m_2,\mathbb{C}}$ intersect properly on $S_{\mathbb{C}}$ if and only if the integer $m = m_1 m_2$ is not a perfect square. In this case, the intersection $T_{m_1,\mathbb{C}} \times_{S_{\mathbb{C}}} T_{m_2,\mathbb{C}}$ lies over the locus in $S_{\mathbb{C}}$ corresponding to pairs (E, E') of elliptic curves with complex multiplication by orders in the imaginary-quadratic field $\mathbb{Q}(\sqrt{-m})$ of discriminant $\geq -4m$. The intersection number is equal to*

$$(T_{m_1,\mathbb{C}} \cdot T_{m_2,\mathbb{C}}) = \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4m}} \sum_{d \mid gcd(m_1, m_2, t)} d \cdot H\left(\frac{4m - t^2}{d^2}\right) \quad . \quad \square$$

Here $H(n)$ denotes the Hurwitz class number (the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of positive definite binary quadratic forms over $\mathbb{Z}$ with determinant n).

The second result is the theorem of Gross and Keating.

Theorem 1.2. — *The cycles T_{m_1}, T_{m_2} and T_{m_2} intersect properly on S if and only if there is no positive definite binary quadratic form over $\mathbb{Z}$ which represents the three integers m_1, m_2, m_3. In this case the intersection $T_{m_1} \times_S T_{m_2} \times_S T_{m_3}$ lies over the locus in S corresponding to pairs (E, E') of elliptic curves which are supersingular in some characteristic p with $p < 4m_1m_2m_3$. The arithmetic intersection number is equal to*

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3}) = \sum_{p<4m_1m_2m_3} n(p) \log p \quad ,$$

where

$$n(p) = \frac{1}{2} \cdot \sum_{Q} \Big(\prod_{\substack{\ell \mid \Delta, \\ \ell \neq p}} \beta_\ell(Q) \Big) \cdot \alpha_p(Q) \quad . \quad \square$$

Here the sum is the taken over all positive definite integral ternary quadratic forms Q with diagonal (m_1, m_2, m_3) which are isotropic over $\mathbb{Q}_\ell$ for all $\ell \neq p$. Furthermore $\Delta = \frac{1}{2} \det Q$ and $\beta_\ell(Q)$ is a normalized representation density of Q by the $\mathbb{Z}_\ell$-lattice $\mathrm{M}_2(\mathbb{Z}_\ell)$ with its norm form. Finally, $\alpha_p(Q)$ is the length of a certain local deformation space. Namely, one considers the universal deformation space of a triple of isogenies of formal groups of dimension 1 and height 2 over $\overline{\mathbb{F}}_p$. Here the passage from a global problem involving elliptic curves to a local problem on formal groups is provided by the Serre-Tate theorem. In [**GK**], Gross and Keating give completely explicit expressions for the factors $\beta_\ell(Q)$ and $\alpha_p(Q)$, comp. Chapters 5 and 13. They express these quantities in terms of new invariants of ternary quadratic forms over $\mathbb{Z}_p$ which are defined by them for this purpose (the Gross-Keating invariant in $(\mathbb{Z}_{\geq 0})^3$ and the Gross-Keating epsilon factor in $\{\pm 1\}$). This is especially striking in the cases when $\ell = 2$ resp. $p = 2$, in the other cases these invariants can be expressed in terms of classical quantities.

The invariant $\alpha_p(Q)$ is probably the most interesting ingredient in the formula above, and we now give a precise definition.

Let G be a formal group of dimension 1 and height 2 over $\bar{\mathbb{F}}_p$. Let $W = W(\bar{\mathbb{F}}_p)$ be the ring of Witt vectors. The universal deformation of the pairs (G, G) is then (Γ, Γ') over the formal scheme $\hat{\mathcal{S}} = \mathrm{Spf}\ W[[t, t']]$. If now $f_1, f_2, f_3 : G \to G$ are three endomorphisms $\neq 0$, we let $I_i \subset W[[t, t']]$ for $i = 1, 2, 3$ be the minimum ideal such that f_i lifts to a homomorphism $\tilde{f}_i : \Gamma \to \Gamma'$ (mod I_i). Then I_i defines a divisor $\hat{\mathcal{T}}_i$ on $\hat{\mathcal{S}}$. Consider

$$(\hat{\mathcal{T}}_1 \cdot \hat{\mathcal{T}}_2 \cdot \hat{\mathcal{T}}_3) = \mathrm{length}_W\ W[[t, t']]/(I_1 + I_2 + I_3) \quad . \tag{1.6}$$

On $\mathrm{End}(G)$ we have the usual quadratic form Nm with values in $\mathbb{Z}_p$ (the norm form, after identifying $\mathrm{End}(G)$ with the maximal order in the quaternion division algebra over $\mathbb{Q}_p$). It turns out that (1.6) only depends on the quadratic form $Q(f_1, f_2, f_3)$:

$(x, y, z) \mapsto \mathrm{Nm}(xf_1 + yf_2 + zf_3)$, and even only on its $\mathrm{GL}_3(\mathbb{Z}_p)$-equivalence class. We then set

$$\alpha_p(Q) = (\hat{\mathcal{T}}_1 \cdot \hat{\mathcal{T}}_2 \cdot \hat{\mathcal{T}}_3) \quad , \tag{1.7}$$

for any triple f_1, f_2, f_3 with $Q(f_1, f_2, f_3) = Q$. The formula for $\alpha_p(Q)$ in terms of the Gross-Keating invariant $(a_1, a_2, a_3) \in (\mathbb{Z}_{\geq 0})^3$ with $a_1 \leq a_2 \leq a_3$ is as follows. We note that for $p \neq 2$, in which case Q can be diagonalized, the integers a_1, a_2, a_3 are simply the p-adic valuations of the diagonal entries.

$$\begin{aligned}\alpha_p(Q) &= \sum_{i=0}^{a_1-1} (i+1)(a_1+a_2+a_3-3i)p^i + \sum_{i=a_1}^{(a_1+a_2-2)/2} (a_1+1)(2a_1+a_2+a_3-4i)p^i \\ &\quad + \frac{a_1+1}{2}(a_3-a_2+1)p^{(a_1+a_2)/2}, \text{ if } a_1 \equiv a_2 \pmod 2\end{aligned}$$

$$\begin{aligned}\alpha_p(Q) &= \sum_{i=0}^{a_1-1} (i+1)(a_1+a_2+a_3-3i)p^i + \sum_{i=a_1}^{(a_1+a_2-1)/2} (a_1+1)(2a_1+a_2+a_3-4i)p^i, \\ &\quad \text{if } a_1 \not\equiv a_2 \pmod 2\end{aligned}$$

The above results are the main focus of these notes. In the last chapter we reformulate Theorem 1.2 as a relation between the arithmetic intersection numbers and the Fourier coefficients of special values of derivatives of Siegel Eisenstein series, along the lines sketched in the introduction to [**GK**]. The idea that this can be done is attributed there to S. Kudla and D. Zagier; in the intervening years Kudla and others have gone a long way towards proving such relations in much greater generality [**Ku2, Ku3**]. Let

$$E(\tau, s) = \sum \det(\mathbf{c}\tau + \mathbf{d})^{-2} \cdot \frac{\det(y)^{\frac{s}{2}}}{|\det(\mathbf{c}\tau + \mathbf{d})|^s} \tag{1.8}$$

be the classical Siegel Eisenstein series of genus 3 and weight 2 for the full modular group. Here $\tau = x + iy \in \mathfrak{H}_3$ and $s \in \mathbb{C}$ is a complex parameter with large real part, and the sum is over representatives $\left(\gamma = \begin{smallmatrix} * & * \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$ of the left cosets of the Siegel parabolic in $\mathrm{Sp}_3(\mathbb{Z})$. Then $E(\tau, s)$ has a meromorphic continuation to the entire s-plane and vanishes at $s = 0$. The derivative $E'(\tau, 0) = \frac{\partial E}{\partial s}(\tau, 0)$ is a non-holomorphic modular form of weight 2 for $\mathrm{Sp}_3(\mathbb{Z})$ and has a Fourier expansion

$$E'(\tau, 0) = \sum_{T \in \mathrm{Sym}_3(\mathbb{Z})^\vee} c'(T, y) \cdot q^T \quad , \tag{1.9}$$

where $q^T = \exp(2\pi i \ \mathrm{tr}(T\tau))$, for any half-integral matrix T. It turns out that for positive-definite T the coefficient $c'(T, y) \equiv c'(T)$ is independent of $y = \mathrm{Im}(\tau)$.

Theorem 1.3. — *Let m_1, m_2, m_3 be a triple of positive integers such that there is no positive definite binary quadratic form over $\mathbb{Z}$ which represents m_1, m_2 and m_3. There*

exists a constant κ *independent of* m_1, m_2, m_3 *such that*

$$(\mathcal{T}_{m_1} \cdot \mathcal{T}_{m_2} \cdot \mathcal{T}_{m_3}) = \kappa \cdot \sum_{\substack{T \in \mathrm{Sym}_3(\mathbb{Z})^\vee_{>0} \\ \mathrm{diag}(T)=(m_1,m_2,m_3)}} c'(T) \quad . \quad \square$$

It should be pointed out that the left hand side in Theorem 1.3 also breaks into geometrically defined terms indexed by quadratic forms T and that the identity above holds termwise.

2. Content of this book

We now explain what is to be found in this book and what is not. In Chapter 2, G. Vogel gives a review of classical results on modular polynomials. It is followed by the brief Chapter 3 by U. Görtz, where a certain sum of representation numbers is computed. In Chapter 4, U. Görtz proves the first part of Theorem 1.2, which states under which conditions the three divisors intersect in dimension 0, and it is explained how the formula for the intersection number follows from the results of the later chapters. T. Wedhorn then investigates in Chapter 5 the quadratic space obtained as the space of homomorphisms between two supersingular elliptic curves with the degree form.

Next we come to the local theory. We have made an effort to give all the necessary background on formal groups, their deformations and the deformations of their endomorphisms. Chapter 6 by V. Meusers gives a summary of Lubin-Tate theory for formal groups, cf. [**LT1**]. In Chapter 7, E. Viehmann and K. Ziegler give the construction of the formal moduli space of formal groups, and more generally, formal A-modules, following Drinfeld [**D**]. Chapter 8 by S. Wewers is devoted to Gross' theory of canonical and quasi-canonical lifts, cf. [**G**], and in Chapter 9 V. Meuser explains an analogous theory in the split case, expanding on a remark in [**G**].

Since we will be interested in lifting isogenies of elliptic curves rather than just the curves themselves, we need to understand how endomorphisms of formal groups can be lifted. This was analyzed in much detail by Keating, see [**K2**] (which is based on Keating's unpublished Harvard thesis [**K1**]). This theory is presented here in Chapter 10 by E. Viehmann and Chapter 11 by I. Vollaard. Another ingredient we need is the theory of quadratic forms over $\mathbb{Z}_\ell$, including the delicate case $\ell = 2$ treated in section 4 of [**GK**], comp. also the account of Yang [**Y1**]. This is dealt with in Chapter 12 by I. Bouw. We come back to the theory of quadratic forms, namely to the computation of certain representation densities, in T. Wedhorn's Chapter 15, where, however, we have merely quoted from Kitaoka [**Ki**] and Katsurada [**Ka**] the facts that we use.

We then come to the investigation of the invariants $\alpha_p(Q)$, and to the proof of the explicit formula for them. Here the case $p = 2$ causes additional complications. We provide two different proofs of the formula in that case – one which relies on laborious explicit computations (Chapter 13, by M. Rapoport), and another one which is more conceptual (Chapter 14, by S. Wewers). We feel that both are enlightening in their own way.

Whereas we have provided a lot of background information on the ingredients of the results in [**GK**], with Theorem 1.3 we were less ambitious, contenting ourselves with references to the appropriate papers (mostly of Kudla) to calculate the Fourier coefficients of $E'(\tau, 0)$, see Chapter 16 by M. Rapoport et T. Wedhorn.

3. Perspective

We believe that Gross' theory of canonical and quasi-canonical liftings is going to have even more applications than have been found so far. We hope that our book can serve as a basis of future research. At the end of this introduction there is a list of references of which we are aware, where this theory is used. The theory was invented originally by Gross in connection with the proof of the Gross-Zagier formula. We note that in B. Conrad's recent account of the geometric ingredients of this proof [**Co**] the theory of quasi-canonical liftings is explicitly excluded; therefore our notes may also be viewed as a complement to Conrad's exposition. Also, Chapter III of [**KRY**] is based on the present notes (in loc. cit., only the intersection numbers $(\mathcal{T}_1 \cdot \mathcal{T}_{m_2} \cdot \mathcal{T}_{m_3})$ are needed).

The main ingredient of the proof of Theorem 1.2 is the determination of the quantity $\alpha_p(Q)$. This may be viewed as a special case of the following general problem. Let G and G' be two p-divisible groups over $\bar{\mathbb{F}}_p$. The universal deformation of (G, G') is then (Γ, Γ') over the formal spectrum of a power series ring R over W. Let $f : G \to G'$ be an isogeny. The problem is to determine the minimal ideal I in R such that f lifts to an isogeny $\tilde{f} : \Gamma \to \Gamma'$ (mod I). Related to this question is the following problem: Let I be the minimal ideal such that a given set of isogenies $f_1, \ldots, f_r : G \to G'$ lifts to a set of isogenies $\tilde{f}_1, \ldots, \tilde{f}_r : \Gamma \to \Gamma'$ (mod I). The problem is to determine when I is of finite colength in R, and if so, to determine this colength explicitly.

To the sophisticated reader, it may seem curious that old-fashioned power series methods are used here to solve these problems in the case of p-divisible formal groups of dimension 1 and height 2. It is natural to ask whether more recent methods, like Grothendieck-Messing lifting theory, Cartier theory, or the theory of displays can be used to solve this problem. Indeed, as Zink [**Z**] has shown, the theory of displays can be used in some instances to prove results in this direction. However, so far these methods have not succeeded in obtaining the full statement. In view of the fact that the cases of finite colength in [**KR1, KR2**] all reduce to the Gross-Keating problem, it is conceivable that the special case of the general problem studied here is the only one where a reasonable uniform answer exists. This might also explain the relative failure of the more generally applicable methods.

4. Acknowledgements

We thank all participants of the seminar for their interest and their pertinent questions, especially Ch. Kaiser and E. Lau. We also thank S. Kudla for his encouragement, for his many explanations and for his thorough reading of Chapter 16.

References

[Co] B. Conrad – Gross-Zagier revisited, in [**DZ**], with an appendix by W. R. Mann, p. 67–164.

[D] V. G. Drinfel'd – Elliptic modules, *Math. USSR Sbornik* **23** (1974), p. 561–592.

[DZ] H. Darmon & S.-W. Zhang (eds.) – *Heegner points and Rankin L-series*, Math. Sci. Res. Inst. Publ., vol. 49, 2004, papers from the Workshop on Special Values of Rankin L-Series held in Berkeley, CA, December 2001.

[G] B. H. Gross – On canonical and quasi-canonical liftings, *Invent. Math.* **84** (1986), p. 321–326.

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Invent. Math.* **112** (1993), p. 225–245.

[Ka] H. Katsurada – An explicit formula for Siegel series, *Amer. J. Math.* **121** (1999), p. 415–452.

[K1] K. Keating – Lifting endomorphisms of formal groups, Ph.D. Thesis, Harvard, 1987.

[K2] ———, Lifting endomorphisms of formal A-modules, *Compos. Math.* **67** (1988), p. 211–239.

[Ki] Y. Kitaoka – *Arithmetic of quadratic forms*, Cambridge University Press, 1993.

[Ku2] S. Kudla – Derivatives of Eisenstein series and generating functions for arithmetic cycles, Astérisque, vol. 276, Soc. Math. France, Paris, 2002, séminaire Bourbaki, vol. 1999/200, p. 341–368.

[Ku3] ———, Derivatives of Eisenstein series and arithmetic geometry, in *Proceedings of the International Congress of Mathematicians (Beijing, 2002), vol. II*, Higher Ed. Press, Beijing, 2002, p. 173–183.

[KR1] S. Kudla & M. Rapoport – Arithmetic Hirzebruch Zagier cycles, *J. Reine Angew. Math.* **515** (1999), p. 155–244.

[KR2] ———, Cycles on Siegel 3-folds and derivatives of Eisenstein series, *Ann. Sci. École Norm. Sup.* **33** (2000), p. 695–756.

[KRY] S. Kudla, M. Rapoport & T. Yang – Modular forms and special cycles on Shimura curves, to appear.

[LT1] J. Lubin & J. Tate – Formal complex multiplication in local fields, *Ann. Math.* **81** (1965), p. 380–387.

[Y1] T. Yang – Local densities of 2-adic quadratic forms, *J. Number Theory* **108** (2004), p. 287–345.

[Z] T. Zink – The display of a formal p-divisible group, in *Cohomologies p-adiques et applications arithmétiques (I)*, Astérisque, vol. 278, 2002, p. 127–248.

Additional references on quasi-canonical lifts

[DG] O. Demchenko & A. Gurevich – p-adic period map for the moduli space of deformations of a formal group, *J. Algebra* **288** (2005), no. 445–462.

[Fa] L. Fargues – Application de Hodge-Tate duale d'un groupe de Lubin-Tate, immeuble de Bruhat-Tits du groupe lineaire et filtrations de ramification, url-math.NT/0604252, to appear in *Duke Math. J.*

[Fu1] Y. Fujiwara – On divisibilities of special values of real analytic Eisenstein series, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **35** (1988), p. 393–410.

[Fu2] ———, On Galois actions on p-power torsion points of some one-dimensional formal groups over $F_p[\![t]\!]$, *J. Algebra* **113** (1988), p. 491–510.

[GH1] M. Hopkins & B. Gross – The rigid analytic period mapping, Lubin-Tate space, and stable homotopy theory, *Bull. Amer. Math. Soc. (N.S.)* **30** (1994), p. 76–86.

[GH2] ———, Equivariant vector bundles on the Lubin-Tate moduli space, in *Topology and representation theory (Evanston, IL, 1992)*, Contemp. Math., vol. 158, Amer. Math. Soc., 1994, p. 23–88.

[K3] K. Keating – Galois characters associated to formal A-modules, *Compositio Math.* **67** (1988), p. 241–269.

[K4] ———, Galois extensions associated to deformations of formal A-modules, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **37** (1990), p. 151–170.

[Ku1] S. Kudla – Central derivatives of Eisenstein series and height pairings, *Ann. of Math.* **146** (1997), p. 545–646.

[LT2] J. Lubin & J. Tate – Formal moduli for one-parameter formal Lie groups, *Bull. Soc. Math. France* **94** (1966), p. 49–60.

[RT] H.-G. Rück & U. Tipp – Heegner points and L-series of automorphic cusp forms of Drinfeld type, *Doc. Math.* **5** (2000), p. 365–444.

[S] T. Scanlon – Local André-Oort conjecture for the universal abelian variety, *Invent. Math.* **163** (2006), no. 1, p. 191–211.

[Ta] L. H. Tatevossian – Canonical liftings of formal modules, in *Number theory (Montreal, 1985)*, CMS Conf. Proc., vol. 7, Amer. Math. Soc., 1987, p. 457–463.

[DYu] J.-D. Yu – Special lifts of ordinary K3 surfaces and applications, math.AG/0611481.

[Yu] J.-K. Yu – On the moduli of quasi-canonical liftings, *Compositio Math.* **96** (1995), p. 293–321.

[Zh1] S.-W. Zhang – Gross-Zagier formula for GL(2), II, in [**DZ**], p. 191–214.

[Zh2] ———, Gross-Zagier formula for GL_2, *Asian J. Math.* **5** (2001), p. 183–290.

[Zh3] ———, Heights of Heegner points on Shimura curves, *Ann. of Math.* **153** (2001), p. 27–147.

NOTATION

We assemble some of the notation which is used more or less systematically throughout the book.

For an integer $m > 0$, we denote by $\varphi_m \in \mathbb{Z}[X, Y]$ the modular polynomial (see [**Vg**]). We write $S = \operatorname{Spec} \mathbb{Z}[X, Y]$, and denote by $T_m \subseteq S$ the divisor associated to φ_m. By $S_{\mathbb{C}}$, $T_{m,\mathbb{C}}$ etc. we denote the base change to $\mathbb{C}$, and by $\mathcal{S}$, $\mathcal{T}_m$ we denote the corresponding Deligne-Mumford stacks (see [**Go2**]).

In [**Me1**], [**VZ**], [**Ww1**], [**Me2**], [**Vi**], [**Vl**] dealing with the local theory, the following situation is considered: K is a field, complete with respect to a discrete valuation v_K, with ring of integers $\mathcal{O}_K$. We denote by $\mathfrak{p}$ the maximal ideal of $\mathcal{O}_K$, and by π a uniformizer. The residue class field $\mathcal{O}_K/\mathfrak{p}$ of K is assumed to be finite, of cardinality q, and k is an extension field of $\mathcal{O}_K/\mathfrak{p}$, in fact in most cases it is an algebraic closure of the residue class field. Furthermore, L is a quadratic extension of K, with ring of integers $\mathcal{O}_L$, and M is the completion of the maximal unramified extension of K (or in some places of L). By D we denote 'the' quaternion division algebra over K. The maximal order of D is denoted by $\mathcal{O}_D$, and $\Pi = \pi_D$ is a uniformizing element. In [**R**], [**Ww2**] the special case where the base field is $\mathbb{Q}_p$ is considered, and the notation is slightly different: there $K/\mathbb{Q}_p$ is a quadratic extension (and L denotes a quadratic space). Also, in [**Wd1**] D denotes a quaternion algebra over $\mathbb{Q}$.

The letters F, G, H, Γ usually denote formal groups (or formal $\mathcal{O}_K$-modules etc.). Often, G denotes the special fiber of a deformation F. Whereas mostly F_r denotes a quasi-canonical lifting of level r (and in particular F_0 denotes the canonical lift), see [**Ww1**], in [**Vi**] and [**Vl**] F_n denotes the base change $F \otimes_{k[\![t]\!]} k[\![t]\!]/t^n$ or $F \otimes_A A/\pi^n$.

If R is a ring, and (L, Q) is a quadratic space over R, *i.e.*, a free R-module L with a quadratic form Q, we associate to it the bilinear form $(x, y) = Q(x+y) - Q(x) - Q(y)$ and—after fixing a basis $\psi_1, \ldots, \psi_n$—the matrix $B = B(\boldsymbol{\psi}) = ((\psi_i, \psi_j))_{i,j}$ (in [**B**]) or the matrix $T = (\frac{1}{2}(\psi_i, \psi_j))_{i,j}$ (in [**R**], [**Wd2**]). If Q' is another quadratic form, on R^m, say, then we denote by $R_L(Q')$ the representation number of Q' in L, *i.e.*, the number of isometries from (R^m, Q') to (L, Q); see [**Vg**], [**Go2**] and in particular [**Wd2**]. To a ternary quadratic form over $\mathbb{Z}_\ell$ we attach its Gross-Keating invariants a_1, a_2, a_3 and ϵ, see [**B**]. Finally, the numbers $\alpha_p(Q) \in \mathbb{Z}$, $\beta_\ell(Q) \in \mathbb{Z}$ which appear in the statement of the main theorem are defined in [**R**] and [**Wd2**], respectively.

References

[B] I. I. Bouw – Invariants of ternary quadratic forms, this volume, p. 113–137.

[Go2] U. Görtz – Arithmetic intersection numbers, this volume, p. 15–24.

[Me1] V. Meusers – Lubin–Tate formal groups, this volume, p. 49–55.

[Me2] V. Meusers – Canonical and quasi-canonical liftings in the split case, this volume, p. 87–98.

[R] M. Rapoport – Deformations of isogenies of formal groups, this volume, p. 139–169.

[Vg] G. Vogel – Modular polynomials, this volume, p. 1–7.

[Vi] E. Viehmann – Lifting endomorphisms of formal $\mathcal{O}_K$-modules, this volume, p. 99–104.

[VZ] E. Viehmann & K. Ziegler – *Formal moduli of formal $\mathcal{O}_K$-modules*, this volume, p. 57–66.

[Vl] I. Vollaard – Endomorphisms of quasi-canonical lifts, this volume, p. 105–112.

[Wd1] T. Wedhorn – The genus of the endomorphisms of a supersingular elliptic curve, this volume, p. 25–47.

[Wd2] T. Wedhorn – Calculation of representation densities, this volume, p. 179–190

[Ww1] S. Wewers – Canonical and quasi-canonical liftings, this volume, p. 67–86.

[Ww2] S. Wewers – An alternative approach using ideal bases, this volume, p. 171–177.

Astérisque
312, 2007, p. 1–7

2. MODULAR POLYNOMIALS

by

Gunther Vogel

Abstract. — We introduce the classical modular polynomials and calculate (modulo the determination of a certain sum of representation numbers) the intersection number of two divisors defined by modular polynomials (Hurwitz's theorem).

***Résumé* (Polynômes modulaires).** — On introduit les polynômes modulaires classiques et détermine (modulo le calcul d'une certaine somme de nombres de représentations) le nombre d'intersection de deux diviseurs définis par des polynômes modulaires (théorème de Hurwitz).

We introduce modular polynomials and prove some elementary properties. This is classical and well-known, see e.g. [**L**, §5]. In the second part, we compute the intersection numbers of the divisors defined by two modular polynomials in the 2-dimensional complex plane. This computation, due to Gross and Keating ([**GK**]), re-proves the class number relations of Kronecker (Corollary 2.2).

We only consider elliptic curves over $\mathbb{C}$.

1. Modular Polynomials

Let $m \in \mathbb{N}$. Consider the elliptic curve $E = \mathbb{C}/\Gamma$ with $\Gamma = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{H}$.

Theorem 1.1 **([L, §5.3,5.1]).** — *There are canonical bijections between the following sets:*

(i) *isomorphism classes of isogenies $f\colon E_1 \to E$ of degree m (as group schemes over E),*
(ii) *subgroups $\Gamma_1 \subseteq \Gamma$ of index m,*

2000 ***Mathematics Subject Classification.*** — 11F32, 11F03, 11G15.
Key words and phrases. — Modular polynomials, representation number of a quadratic form, class number relations.

(iii) $\mathrm{SL}_2(\mathbb{Z})\backslash\{A \in M_2(\mathbb{Z}) \mid \det A = m\}$, *and*
(iv) $\left\{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \,\middle|\, ad = m,\ a \geq 1 \text{ and } 0 \leq b < d\right\}$.
All of these sets have $\sigma_1(m) = \sum_{d|m} d$ *elements.*

Proof
(i)→(ii): Set $\Gamma_1 := f_*\pi_1(E_1)$. (ii)→(i): Set $E_1 := \mathbb{C}/\Gamma_1$.
(ii)↔(iii): Choose a basis $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ \tau \end{smallmatrix}\right)$ of Γ_1 with $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$.
(iii)↔(iv): Left multiplication by matrices from $\mathrm{SL}_2(\mathbb{Z})$ corresponds to row operations. The matrices in (iv) are obviously inequivalent (the columns must be stabilized). □

Now consider pairs (j, j') of j-invariants of elliptic curves E, E' such that there is an isogeny $E \to E'$ of degree m. These pairs are described by the divisor of a certain polynomial φ_m:

For $j, j' \in \mathbb{C}$ choose elliptic curves E, E' having j-invariants j, j', respectively. Set

$$\varphi_m(j, j') = \varphi_m(j(E), j(E')) := \prod_{E_1' \to E'} (j(E) - j(E_1'));$$

the product is over isomorphism classes of isogenies $E_1' \to E'$ of degree m. φ_m does not depend on the choices made and is a polynomial of degree $\sigma_1(m)$ in j. For elliptic curves E, E', the condition $\varphi_m(j(E), j(E')) = 0$ is equivalent to the existence of an isogeny $E \to E'$ of degree m.

Define $\psi_m(j, j')$ by the same formula, but restrict the product to the isogenies which do not factor over some multiplication-by-n map, $n > 1$. In the above correspondence, these isogenies correspond to primitive matrices, i. e., matrices whose entries have no common divisor. We have

$$\varphi_m = \prod_{n^2|m} \psi_{m/n^2}.$$

Obviously, $\varphi_1(X, Y) = \psi_1(X, Y) = X - Y$. As we will see below, φ_m and ψ_m are polynomials; they are called *modular polynomials*.

Theorem 1.2 **([L, §5.2])**
(i) $\varphi_m, \psi_m \in \mathbb{Z}[X, Y]$.
(ii) $\psi_m(X, t)$ *is irreducible over* $\mathbb{C}(t)$.
(iii) *For* $m > 1$, *we have* $\psi_m(X, Y) = \psi_m(Y, X)$. *Consequently,* $\varphi_m(X, Y) = \pm\varphi_m(Y, X)$ *("−" precisely if* m *is a square).*

Proof
(i) First notice that the coefficients k_i of

$$\psi_m(X, j(\tau')) = \prod_{\mathrm{SL}_2(\mathbb{Z})\backslash\{A \in M_2(\mathbb{Z}) | \det A = m,\ A \text{ primitive}\}} (X - j(A\tau')) \in \mathcal{O}_{\mathbb{C}}[X]$$

are holomorphic in τ' and invariant under $\mathrm{SL}_2(\mathbb{Z})$. From the formula

$$(*) \qquad \psi_m(X, j(\tau')) = \prod_{a,b,d} \Big(X - j\Big(\frac{a\tau'+b}{d}\Big)\Big) = \prod_{a,b,d} \Big(X - \frac{1}{(q')^{a/d}\zeta_m^{ab}} - 744 - \dots\Big)$$

(a, b, d as in 1.1 (iv) and $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ primitive, $\zeta_m := \mathrm{e}^{2\pi\mathrm{i}/m}$) we see that the k_i are meromorphic at infinity. Since the q-expansion of the j-function has integral coefficients, we have

$$k_i \in \mathbb{Z}[\zeta_m][[q']]\Big[\frac{1}{q'}\Big].$$

Now there are polynomials $p_i \in \mathbb{Z}[\zeta_m, T]$ such that $k_i - p_i(j(q'))$ lies in $q'\mathbb{Z}[\zeta_m][[q']]$ and therefore, being a modular function, must vanish identically. Hence, $\psi_m \in \mathbb{Z}[\zeta_m][X, Y]$.

There are two operations of $(\mathbb{Z}/m\mathbb{Z})^\times$: first, on matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ as in 1.1 (iv) by

$$\sigma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} := \begin{pmatrix} a & \sigma b \\ 0 & d \end{pmatrix} \quad (\text{via } (\mathbb{Z}/d\mathbb{Z})^\times \text{ on } \{0, \dots, d-1\} \cong \mathbb{Z}/d\mathbb{Z}),$$

and the first product in $(*)$ is invariant under this operation. Second, $(\mathbb{Z}/m\mathbb{Z})^\times$ operates in a compatible way on $\mathbb{Z}[\zeta_m]$ by $\sigma\zeta_m = \zeta_m^\sigma$, and since the coefficients of φ_m are invariant under this operation, we find that $\psi_m \in \mathbb{Z}[X, Y]$.

(ii) By mapping $t \mapsto j$, the field of meromorphic functions on $\mathbb{H}$ becomes an extension field of $\mathbb{C}(t)$ carrying an operation of the group $\mathrm{SL}_2(\mathbb{Z})$. By the elementary divisors theorem, it permutes the zeroes of $\psi_m(X, t)$ transitively, hence $\psi_m(X, t)$ is irreducible over $\mathbb{C}(t)$.

(iii) The condition $\psi_m(j(E), j'(E)) = 0$ is equivalent to the existence of an isogeny $E \to E'$ of degree m which does not factor over a multiplication-by-n map for some $n > 1$. This last property is also true for its dual isogeny, hence $\psi_m(j(E'), j(E)) = 0$. For a fixed j_0', the irreducible polynomial $\psi_m(X, j_0')$ is therefore a divisor of $\psi_m(j_0', X)$, and conversely. It follows that $\psi_m(j, j') = \pm\psi_m(j', j)$. If the "$-$" sign is correct, $\psi_m(t, t)$ vanishes identically, so $\psi_m(X, t)$ has a zero in $\mathbb{C}(t)$, hence the degree of $\psi_m(X, t)$ must be 1. This is true precisely for $m = 1$. □

From the proof of (iii) we also see that $f_m(X) := \varphi_m(X, X)$ vanishes if and only if m is a square. If m is not a square, the degree of f_m can be read off the q-expansion in $(*)$: set $X = j(q')$, then because of $a \neq d$, the pole order of one factor is equal to $\max\{1, a/d\}$, hence the pole order of the entire product is

$$\deg f_m = \sum_{ad=m} d \max\{1, a/d\} = \sum_{ad=m} \max\{a, d\}.$$

One also sees that the leading coefficient of f_m is ± 1.

2. Intersections

We first need to fix some notation. A quadratic space (L, Q) over a ring R consists of a free R-module L of finite rank and a quadratic form Q on L. The associated bilinear form on L is defined by

$$(x, y) = Q(x + y) - Q(x) - Q(y).$$

The determinant of Q is the element of $R/(R^\times)^2$ given by the determinant of the matrix $((b_i, b_j))_{ij}$ for some basis $\{b_i\}$ of L. The diagonal of Q with respect to some fixed basis $\{b_i\}$ is defined to be the n-tuple $(Q(b_i))_i$ where n is the rank of L.

For a quadratic form F on R^m, we define the representation number $R_L(F)$ as the cardinality of the set

$$\begin{aligned}&\{(f_i) \in L^m \mid Q(x_1 f_1 + \cdots + x_m f_m) = F(x_1, \ldots, x_m) \text{ for all } x \in R^m\}\\ &= \{\text{isometries } (R^m, F) \to (L, Q)\}.\end{aligned}$$

For $R = \mathbb{Z}$ and positive definite Q, this set is finite. (For each $x = e_i$, $i = 1, \ldots, m$, there are only finitely many possible values of $x_1 f_1 + \cdots + x_m f_m = f_i$.)

For a positive integer D, let $H(D)$ be the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of positive definite binary quadratic forms over $\mathbb{Z}$ with determinant D (which is well-defined as an element of $\mathbb{Z}$), counting the forms equivalent to $ex_1^2 + ex_2^2$ and $ex_1^2 + ex_1x_2 + ex_2^2$ for some natural number e with multiplicities $1/2$ and $1/3$, respectively. If the positive integer m is not a square, we define

$$G(m) := \sum_{\substack{t \in \mathbb{Z} \\ t^2 \le 4m}} H(4m - t^2).$$

Define $T_m := V(\varphi_m) \subset \mathbb{A}^2_{\mathbb{C}}$.

Theorem 2.1 **([GK, 2.4])**. — *The curves T_{m_1} and T_{m_2} intersect properly if and only if $m = m_1 m_2$ is not a square. In this case, their intersection is supported on pairs (E, E') of elliptic curves with complex multiplication by orders whose discriminants satisfy $d(E), d(E') \ge -4m$. The intersection number is*

$$T_{m_1} \cdot T_{m_2} = \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4m}} \sum_{d \mid \gcd(m_1, m_2, t)} d \cdot H\Big(\frac{4m - t^2}{d^2}\Big) = \sum_{n \mid \gcd(m_1, m_2)} n \cdot G(m/n^2).$$

Proof. — If $m = m_1 m_2$ is a square, T_{m_1} and T_{m_2} contain $V(\psi_g)$, $g = \gcd(m_1, m_2)$, as a common component (note that m_1/g and m_2/g are coprime, hence squares themselves). Conversely, if T_{m_1} and T_{m_2} do not intersect properly, they must contain some $V(\psi_g)$ as a common component, but then $g = m_1/n_1^2 = m_2/n_2^2$, so $m = g^2 n_1^2 n_2^2$ is a square.

For a pair of elliptic curves (E, E') corresponding to an intersection point of T_{m_1} and T_{m_2}, there are isogenies $f_1, f_2 \colon E \to E'$ of degrees m_1 and m_2, respectively. Then, $\alpha := {}^t f_2 f_1$ is an endomorphism of E of degree m. Since m is not a

square, E has complex multiplication, and $\mathbb{Z}+\mathbb{Z}\alpha$ is a sublattice of $\operatorname{End} E$. Hence, its discriminant $(\operatorname{Tr}\alpha)^2-4m<0$ is divisible by $d(E)$, so

$$d(E)\geq(\operatorname{Tr}\alpha)^2-4m\geq -4m.$$

Similarly, considering $\beta:=f_2{}^t f_1$, it follows that $d(E')\geq -4m$.

Next, we compute the local intersection number at some point $(j_0,j_0')\in\mathbb{C}^2$ corresponding to a pair of elliptic curves (E,E'). Set $u_E:=\frac{1}{2}\#\operatorname{Aut}E$, similarly for E'. Choose $\tau_0'\in\mathbb{H}$ such that $j(\tau_0')=j_0'$. Locally at τ_0', the map $j\colon\mathbb{H}\to\mathbb{C}$ is a branched covering of degree $u_{E'}$, so the local intersection number in the (j,j')-plane is the intersection number in the (j,τ')-plane divided by $u_{E'}$.

In the (j,τ')-plane, the φ_{m_i} decompose into factors of the form

$$j-j(A_i\tau')\qquad\text{where } A_i\in M_2(\mathbb{Z}),\ \det A_i=m_i.$$

Therefore, it suffices to compute the local intersection number of two such factors, both vanishing at (j_0,τ_0'). This number is the zero order of

$$(**)\qquad\qquad j(A_1\tau')-j(A_2\tau')$$

at $\tau'=\tau_0'$. Since $A_1\tau_0'$ and $A_2\tau_0'$ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent, we may assume that $A_1\tau_0'=A_2\tau_0'=:\tau_0$ and $c_2=0$. Locally at τ_0,

$$j(\tau)=j(\tau_0)+s\cdot(\tau-\tau_0)^{u_E}+\text{higher order terms}$$

for some $s\neq 0$, hence $(**)$ is of the form

$$\begin{aligned}&s\Big(\frac{a_1\tau'+b_1}{c_1\tau'+d_1}-\frac{a_1\tau_0'+b_1}{c_1\tau_0'+d_1}\Big)^{u_E}-s\Big(\frac{a_2\tau'+b_2}{d_2}-\frac{a_2\tau_0'+b_2}{d_2}\Big)^{u_E}+\text{h. o. t.}\\ &=s\Big(\frac{\det A_1}{(c_1\tau_0'+d_1)^2}\cdot(\tau'-\tau_0')\Big)^{u_E}-s\Big(\frac{\det A_2}{d_2^2}\cdot(\tau'-\tau_0')\Big)^{u_E}+\text{h. o. t.}\end{aligned}$$

locally at τ_0'. We now claim that the two leading coefficients are different. (However, they have the same absolute value.) Otherwise, from

$$s\Big(\frac{\det A_1}{(c_1\tau_0'+d_1)^2}\Big)^{u_E}=s\Big(\frac{\det A_2}{d_2^2}\Big)^{u_E}$$

we get

$$\frac{c_1\tau_0'+d_1}{\sqrt{m_1}}=\omega\cdot\frac{d_2}{\sqrt{m_2}}$$

for some $2u_E$-th root of unity ω, implying

$$(***)\qquad\qquad c_1\tau_0'+d_1=\omega\cdot\frac{\sqrt{m_1m_2}}{a_2}.$$

The left-hand side is imaginary-quadratic, so by our assumption that $m=m_1m_2$ is not a square it follows that $\omega=\pm\mathrm{i}$ and $u_E=2$. But in this case, τ_0' corresponds to an elliptic curve isogenous to $E\cong\mathbb{C}/\langle 1,\mathrm{i}\rangle$, hence $\tau_0'\in\mathbb{Q}(\mathrm{i})$, contradicting $(***)$. Hence, the zero order of $(**)$ at τ_0' equals u_E.

Since the product decomposition of φ_{m_i} contains

$$\frac{1}{2u_E} \cdot \#\{f_i \in \mathrm{Hom}(E, E') \mid \deg f_i = m_i\}$$

factors vanishing at (j_0, τ_0'), the local intersection number in the (j, τ')-plane is

$$(T_{m_1} \cdot T_{m_2})_{(j_0,\tau_0')} = \frac{1}{4u_E^2} \cdot \#\{(f_1, f_2) \in \mathrm{Hom}(E, E') \mid \deg f_i = m_i\} \cdot u_E.$$

Hence, the local intersection number in the (j, j')-plane is

$$(T_{m_1} \cdot T_{m_2})_{(j_0,j_0')} = \frac{1}{4u_E u_{E'}} \cdot \#\{(f_1, f_2) \in \mathrm{Hom}(E, E') \mid \deg f_i = m_i\}.$$

Such pairs (f_1, f_2) correspond to representations of positive definite quadratic forms $Q(x_1, x_2) = \deg(x_1 f_1 + x_2 f_2)$, hence

$$\#\{(f_1, f_2) \in \mathrm{Hom}(E, E') \mid \deg f_i = m_i\} = \sum_{\substack{Q>0 \\ \mathrm{diag}\, Q=(m_1,m_2)}} R_{\mathrm{Hom}(E,E')}(Q).$$

Therefore, the global intersection number is

$$\begin{aligned} T_{m_1} \cdot T_{m_2} &= \sum_{\substack{E,E' \\ \text{ell.curves}/\mathbb{C}}} \sum_{\substack{Q>0 \\ \mathrm{diag}\, Q=(m_1,m_2)}} \frac{R_{\mathrm{Hom}(E,E')}(Q)}{4u_E u_{E'}} \\ &= \sum_{\substack{Q>0 \\ \mathrm{diag}\, Q=(m_1,m_2)}} \sum_{E,E'} \frac{R_{\mathrm{Hom}(E,E')}(Q)}{4u_E u_{E'}}. \end{aligned}$$

By Proposition 1.1 in [**Go1**], the inner sum equals

$$\sum_{d|e(Q)} d \cdot H\Big(\frac{\det Q}{d^2}\Big).$$

In our case, $Q(x_1, x_2) = m_1 x_1^2 + t x_1 x_2 + m_2 x_2^2$ for some $t \in \mathbb{Z}$ satisfying $t^2 - 4m < 0$ (as Q is positive definite), so the above sum is equal to

$$\sum_{d|\gcd(m_1,m_2,t)} d \cdot H\Big(\frac{4m - t^2}{d^2}\Big).$$

Putting everything together yields

$$T_{m_1} \cdot T_{m_2} = \sum_{\substack{t\in\mathbb{Z} \\ t^2<4m}} \sum_{d|\gcd(m_1,m_2,t)} d \cdot H\Big(\frac{4m - t^2}{d^2}\Big). \qquad \square$$

As a corollary, we get the class number relations of Kronecker and Hurwitz:

Corollary 2.2. — *If m is not a square,*

$$G(m) = \sum_{ad=m} \max\{a, d\}.$$

Proof. — By the remarks at the end of the preceding section,

$$T_1 \cdot T_m = \deg f_m = \sum_{ad=m} \max\{a, d\}. \qquad \square$$

Actually, using the convention $H(0) := \zeta(-1) = -1/12$, the above corollary is valid for all m ([**W**, §116]).

References

[Go1] U. Görtz – A sum of representation numbers, this volume, p. 9–14.

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Invent. math.* **112** (1993), p. 225–245.

[L] S. Lang – *Elliptic Functions*, Addison-Wesley, Reading, 1973.

[W] H. Weber – *Lehrbuch der Algebra, Dritter Band: Elliptische Funktionen und algebraische Zahlen*, F. Vieweg, Braunschweig, 1908.

G. Vogel, Max-Planck-Institut für Mathematik, Vivatsgasse 7, 53111 Bonn, Germany
E-mail : gunther.vogel@gmx.net

Astérisque
312, 2007, p. 9–14

3. A SUM OF REPRESENTATION NUMBERS

by

Ulrich Görtz

Abstract. — This article contains the proof of a formula stated in the paper by Gross and Keating on intersections of modular correspondences, for a certain sum of representation numbers.

***Résumé* (Une somme de nombres de représentations).** — Cet article contient la preuve d'une formule donnée dans l'article de Gross et Keating sur les intersections de correspondances modulaires, pour une certaine somme de nombres de représentations.

1. Introduction

We prove a formula for a certain sum of representation numbers, stated in the paper of Gross and Keating [**GK**] without proof, which is used in [**Vg**] in order to compute the intersection product of two modular divisors in $S_{\mathbb{C}}$. Let Q be a positive definite binary quadratic form over $\mathbb{Z}$, say

$$Q(x_1, x_2) = m_1 x_1^2 + t x_1 x_2 + m_2 x_2^2.$$

The determinant of Q is

$$\det(Q) = 4m_1 m_2 - t^2 (> 0),$$

and its content is

$$e(Q) = \gcd(m_1, m_2, t).$$

Proposition 1.1

$$\sum_{\substack{E,E' \\ \text{ell. curves } /\mathbb{C}}} \frac{R_{\mathrm{Hom}(E,E')}(Q)}{\#\operatorname{Aut}(E) \cdot \#\operatorname{Aut}(E')} = \sum_{d \mid e(Q)} d \cdot H(\det(Q)/d^2).$$

2000 ***Mathematics Subject Classification.*** — 14K22.
Key words and phrases. — Elliptic curves, complex multiplication, representation densities.

Our argument is inspired by Hirzebruch's article [**H**], where the case $m_1 = 1$ is treated.

Acknowledgments. — I am grateful to Gunther Vogel for a discussion of this problem, and to Torsten Wedhorn for proof-reading.

2. Proof of the proposition

The sum on the left hand side extends over isomorphism classes of elliptic curves, and clearly the representation number $R_{\mathrm{Hom}(E,E')}(Q)$ is 0 unless E and E' have complex multiplication and $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathrm{End}(E') \otimes \mathbb{Q}$. In particular, the sum is finite.

As in [**GK**], we denote by $H(D)$, D a positive integer, the number of $SL_2(\mathbb{Z})$-equivalence classes of positive definite binary quadratic forms over $\mathbb{Z}$ with determinant D, where the forms equivalent to $ex_1^2 + ex_2^2$ and $ex_1^2 + ex_1x_2 + ex_2^2$ for some $e \in \mathbb{Z}$ are counted with multiplicity $1/2$ and $1/3$, respectively. A quadratic form is called primitive, if its content is 1. We denote by $h(D)$ the number of primitive positive definite binary quadratic forms of discriminant D if $D > 4$, and we set $h(3) = \frac{1}{3}$, $h(4) = \frac{1}{2}$. We can also interpret $h(D)$ as the number of elliptic curves E with complex multiplication, such that the endomorphism ring $\mathrm{End}(E)$ (which is an order in some imaginary quadratic number field) has discriminant $-D$, where each such E is counted with multiplicity $2/\#\,\mathrm{Aut}(E)$.

For a positive integer N we denote by $\sigma_1(N)$ the sum of all divisors of N. Since clearly $H(D) = \sum_{d,d^2|D} h(D/d^2)$, we can then rewrite the right hand side of the formula as

$$\sum_{d,d^2|\det(Q)} \sigma_1(\gcd(m_1, m_2, t, d))h(\det(Q)/d^2).$$

Fix an elliptic curve E with complex multiplication. We use the following notation:

Write $E = \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau$ with $\tau \in \mathbb{H}$, and let $\alpha, \beta, \gamma \in \mathbb{Z}$, such that $\alpha\tau^2 + \beta\tau + \gamma = 0$, $\gcd(\alpha, \beta, \gamma) = 1$, $\alpha > 0$ (once τ is fixed, α, β and γ are uniquely determined by these conditions).

If there exists an E', such that $R_{\mathrm{Hom}(E,E')}(Q) \neq 0$, then there exists a natural number d with

$$4m_1m_2 - t^2 = \det(Q) = d^2(4\alpha\gamma - \beta^2). \tag{2.1}$$

Indeed, by assumption there exist $f_i \in \mathrm{Hom}(E, E')$, $i = 1, 2$, such that $\deg(f_i) = m_i$ and $\deg(f_1 + f_2) - \deg(f_1) - \deg(f_2) = t$. Let $g = f_1^\vee \circ f_2$. If we choose lattices Λ, Λ' such that $E \cong \mathbb{C}/\Lambda$, $E' \cong \mathbb{C}/\Lambda'$, then we get inclusions $\mathrm{Hom}(E, E') \subset \mathbb{C}$, $\mathrm{End}(E) \subset \mathbb{C}$, and have $g = m_1 f_1^{-1} f_2$ (although f_1 and f_2 as complex numbers depend on the choice of Λ and Λ', g is independent of these choices). Since g has norm m_1m_2 and trace t, the quadratic space generated by 1 and g inside $\mathrm{End}(E)$ has determinant $4m_1m_2 - t = \det(Q)$. Since the determinant of the quadratic space

$\mathrm{End}(E)$ is $4\alpha\gamma - \beta^2$, this implies the existence of d as above. In particular, (2.1) implies that $\frac{t-d\beta}{2}, \frac{t+d\beta}{2} \in \mathbb{Z}$.

From now on, in addition to fixing E as above, we let $g \in \mathbb{H}$ be the (unique) algebraic integer in $\mathbb{H}$ with norm $\mathrm{Nm}_{\mathbb{C}/\mathbb{R}}\, g = m_1 m_2$ and trace $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}\, g = t$. We define

$$\mathcal{D}_i = \{(E', f);\ E' \text{ an elliptic curve, } f \in \mathrm{Hom}(E, E'), \deg(f) = m_i, m_i | gf\}/\cong$$

Here (and similarly below) two pairs (E_1', f_1), (E_2', f_2) are called isomorphic if there exists an isomorphism $\varphi\colon E_1' \to E_2'$ such that $f_2 \circ \varphi = f_1$. By definition of the sets $\mathcal{D}_i$, the set

$$\begin{aligned}\big\{(E', f_1, f_2);\ & E' \text{ ell. curve, } f_i \in \mathrm{Hom}(E, E'),\\ & \deg(f_i) = m_i,\ \deg(f_1 + f_2) = t + m_1 + m_2\big\}/\cong\end{aligned}$$

maps bijectively to the disjoint union $\mathcal{D}_1 \cup \mathcal{D}_2$, by sending a triple (E', f_1, f_2) to f_1 or f_2, respectively, depending on whether $m_1 f_1^{-1} f_2 \in \mathbb{H}$ or $m_2 f_2^{-1} f_1 \in \mathbb{H}$, i. e. whether $m_1 f_1^{-1} f_2 = g$ or $m_2 f_2^{-1} f_1 = g$.

The key point in the proof of the proposition is the following lemma.

Lemma 2.1. — *The set $\mathcal{D}_i$ can be identified with the set of matrices $\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right) \in M_2(\mathbb{Z})$, such that:*

i) *There exists $Z | \gcd(m_1, m_2, t, d)$ such that $D = \frac{Z m_i}{\gcd(d\alpha, \frac{t-d\beta}{2}, m_i)}$, $A = \frac{m_i}{D}$.*

ii) *$0 \le B < D$, such that B satisfies a congruence of the form:*

$$B \equiv b \bmod \frac{D}{Z},$$

where $b \in \mathbb{Z}/\frac{D}{Z}\mathbb{Z}$ is an element depending on Z.

Proof. — To ease the notation a little bit, we assume that $i = 1$. Every matrix $M = \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$ with $A, B, D \in \mathbb{Z}_{\ge 0}$, $AD = m_1$ and $0 \le B < D$ defines an isogeny

$$E = \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau \longrightarrow E' := \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}(M\tau), \quad x \longmapsto Ax.$$

and —up to isomorphism— all isogenies of degree m_1 with source E arise in this way (see [**Vg**]).

We need to find out under which conditions the isogeny f corresponding to A, B, D has the property that $m_1 | gf$. This is equivalent to

$$\frac{Ag}{m_1}\mathbb{Z} \oplus \mathbb{Z}\tau \subseteq \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}(M\tau),$$

hence to

$$\begin{aligned} & g \in D\mathbb{Z} \oplus \mathbb{Z}(A\tau + B),\\ & g\tau \in D\mathbb{Z} \oplus \mathbb{Z}(A\tau + B).\end{aligned}$$

It is not hard to check that $g = \frac{t+d\beta}{2} + d\alpha\tau$ and that $g\tau = -d\gamma + \frac{t-d\beta}{2}\tau$, and we find that the conditions above are equivalent to the following:

$$A|d\alpha, \quad A\left|\frac{t-d\beta}{2}\right., \tag{2.2}$$

$$\frac{d\alpha}{A}B \equiv \frac{t+d\beta}{2} \bmod D, \tag{2.3}$$

$$\frac{t-d\beta}{2A}B \equiv -d\gamma \bmod D. \tag{2.4}$$

These congruences for B are solvable if and only if

$$\gcd\Big(\frac{d\alpha}{A}, D\Big)\left|\frac{t+d\beta}{2}\right., \qquad \text{and} \quad \gcd\Big(\frac{t-d\beta}{2A}, D\Big)\Big| d\gamma, \tag{2.5}$$

respectively, and they are solvable simultaneously if and only if in addition

$$\frac{d\gamma}{\gcd(\frac{t-d\beta}{2A}, D)} \cdot \frac{d\alpha}{A\gcd(\frac{d\alpha}{A}, D)} \equiv \frac{t+d\beta}{2\gcd(\frac{d\alpha}{A}, D)} \cdot \frac{t-d\beta}{2A\gcd(\frac{t-d\beta}{2A}, D)} \bmod \frac{D}{l},$$

where

$$l = \operatorname{lcm}\Big(\gcd\Big(\frac{d\alpha}{A}, D\Big), \gcd\Big(\frac{t-d\beta}{2A}, D\Big)\Big) = \frac{\gcd\left(\frac{d\alpha}{A}, D\right)\gcd\left(\frac{t-d\beta}{2A}, D\right)}{\gcd\left(\frac{d\alpha}{A}, \frac{t-d\beta}{2A}, D\right)},$$

and this condition is equivalent to

$$D\left|\frac{d^2\alpha\gamma - \frac{(t+d\beta)(t-d\beta)}{4}}{A\gcd(\frac{d\alpha}{A}, \frac{t-d\beta}{2A}, D)}\right. = \frac{m_1m_2}{\gcd(d\alpha, \frac{t-d\beta}{2}, m_1)}.$$

From this we see that the above congruences for B are simultaneously solvable if and only if

$$Z := \frac{D\gcd\left(d\alpha, \frac{t-d\beta}{2}, m_1\right)}{m_1}\Bigg| m_2, \tag{2.6}$$

(note that $Z \in \mathbb{Z}$ because $A|\gcd(d\alpha, \frac{t-d\beta}{2}, m_1)$) and that in this case the set of solutions is a residue class modulo $\frac{D}{Z}\mathbb{Z}$, as condition ii) asserts.

So for $A, D > 0$ with $AD = m_1$, there exists a B such that the triple (A, B, D) gives rise to an element of $\mathcal{D}_1$ if and only if A, D satisfy (2.2), (2.5) and (2.6), and what remains to show is that these conditions are equivalent to condition i) in the lemma.

However, given (A, B, D), we have already defined the Z in the lemma, such that D and A have got the desired form, so we only have to show that

1) if (A, B, D) defines an element of $\mathcal{D}_1$, and Z is defined as in (2.6), then $Z|m_1$, $Z|t$ and $Z|d$ (since we know already that $Z|m_2$),

2) if we have $Z|\gcd(m_1, m_2, t, d)$ and define A and D as in i), then $A, D \in \mathbb{Z}$, and (2.2) and (2.5) automatically hold.

ad 1) Since Z is a divisor of D, it is clear that $Z|m_1$. Note that $Z = \gcd(\frac{d\alpha}{A}, \frac{t-d\beta}{2A}, D)$, so obviously $Z|d\alpha$ and $Z|\frac{t-d\beta}{2}$. Furthermore, (2.2) implies

that $Z|\frac{t+d\beta}{2}$, $Z|d\gamma$. So for one thing, $Z|\frac{t+d\beta}{2}$ and $Z|\frac{t-d\beta}{2}$, hence $Z|t$ and $Z|d\beta$. In addition, we have seen that $Z|d\alpha$, $Z|d\beta$ and $Z|d\gamma$, and since $\gcd(\alpha,\beta,\gamma)=1$, we conclude that $Z|d$.

ad 2) Given a divisor Z of $\gcd(m_1,m_2,t,d)$, we define $D=\frac{Zm_1}{\gcd(d\alpha,\frac{t-d\beta}{2},m_1)}$, $A=\frac{m_1}{D}=\frac{gcd(d\alpha,\frac{t-d\beta}{2},m_1)}{Z}$. It is obvious that $D\in\mathbb{Z}$, and in order to prove that $A\in\mathbb{Z}$, all we need to show is that $Z|\frac{t-d\beta}{2}$. However, it is clear that $Z|t-d\beta$, $Z|t+d\beta$, and from (2.1) we get that $Z^2|\frac{(t-d\beta)(t+d\beta)}{4}$. Since $t-d\beta\equiv t+d\beta \bmod 2$, this implies $Z|\frac{t-d\beta}{2}$.

It remains to show that the conditions in (2.2) and (2.5) hold: It is clear that $A|d\alpha$ and $A|\frac{t-d\beta}{2}$. Next, let us show that $\gcd(\frac{d\alpha}{A},D)|\frac{t+d\beta}{2}$. Since we have

$$\gcd\Big(\frac{d\alpha}{A},D\Big)=\frac{Z\gcd(d\alpha,m_1)}{\gcd(d\alpha,\frac{t-d\beta}{2},m_1)},$$

it suffices to show

$$\gcd(m_1,m_2,t,d)\gcd(d\alpha,m_1)\,\Big|\,\frac{t+d\beta}{2}\gcd(d\alpha,\frac{t-d\beta}{2},m_1).$$

We use the following notation: for $x\in\mathbb{Z}$ such that $\gcd(m_1,m_2,t,d)|x$, let $\tilde{x}=\frac{x}{\gcd(m_1,m_2,t,d)}$. From (2.1) we get

$$\frac{\tilde{t}-\tilde{d}\beta}{2}\frac{\tilde{t}+\tilde{d}\beta}{2}=\tilde{m_1}\tilde{m_2}-(\tilde{d})^2\alpha\gamma,$$

which implies

$$\gcd(\tilde{d}\alpha,\tilde{m_1})\,\Big|\,\frac{\tilde{t}+\tilde{d}\beta}{2}\gcd\Big(\tilde{d}\alpha\,,\frac{\tilde{t}-\tilde{d}\beta}{2},\tilde{m_1}\Big).$$

Multiplying both sides by $\gcd(m_1,m_2,t,d)^2$, we get the desired result.

Finally, in a similar way we can show that $\gcd(\frac{t-d\beta}{2A},D)|d\gamma$. Namely, it is enough to show

$$\gcd(m_1,m_2,t,d)\gcd\Big(\frac{t-d\beta}{2},m_1\Big)\,\Big|\,d\gamma\gcd\Big(d\alpha,\frac{t-d\beta}{2},m_1\Big)\,,$$

and this follows from

$$\tilde{m_1}\tilde{m_2}-\frac{\tilde{t}-\tilde{d}\beta}{2}\frac{\tilde{t}+\tilde{d}\beta}{2}=(\tilde{d})^2\alpha\gamma.$$

This concludes the proof of 2), and hence the proof of the lemma. □

Corollary 2.2. — *We fix E as above, and use the same notation. Then*

$$\begin{aligned}&\sum_{E'}\frac{R_{\mathrm{Hom}(E,E')}(Q)}{\#\operatorname{Aut}(E')}\\ =\;&\sum_{E'}\frac{\#\{(f_1,f_2)\in\mathrm{Hom}(E,E')^2;\ \deg(f_i)=m_i,\deg(f_1+f_2)=t+m_1+m_2\}}{\#\operatorname{Aut}(E')}\\ =\;&2\sigma_1(\gcd(m_1,m_2,t,d)).\end{aligned}$$

Proof. — This follows from the lemma and the remark preceding it. □

Proof of the proposition. — Using the corollary, we can now easily prove the proposition:

$$\begin{aligned}
&\sum_{E,E'} \frac{R_{\mathrm{Hom}(E,E')}(Q)}{\#\mathrm{Aut}(E)\cdot\#\mathrm{Aut}(E')} \\
&= \sum_{\substack{d \\ d^2 \mid \det(Q)}} \sum_{\substack{E \\ \mathrm{disc}(\mathrm{End}(E))=-\det(Q)/d^2}} \frac{1}{\#\mathrm{Aut}(E)} \sum_{E'} \frac{R_{\mathrm{Hom}(E,E')}(Q)}{\#\mathrm{Aut}(E')} \\
&= \sum_{\substack{d \\ d^2 \mid \det(Q)}} \sum_{\substack{E \\ \mathrm{disc}(\mathrm{End}(E))=-\det(Q)/d^2}} \frac{2\sigma_1(\gcd(m_1,m_2,t,d))}{\#\mathrm{Aut}(E)} \\
&= \sum_{\substack{d \\ d^2 \mid \det(Q)}} \sigma_1(\gcd(m_1,m_2,t,d))h(\det(Q)/d^2). \quad \square
\end{aligned}$$

References

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Invent. math.* **112** (1993), p. 225–245.

[H] F. Hirzebruch – Kurven auf den Hilbertschen Modulflächen und Klassenzahlrelationen in *Classification of Algebraic Varieties and Compact Complex Manifolds*, Lecture Notes in Math., vol. 412, Springer, 1974.

[Vg] G. Vogel – Modular polynomials, this volume, p. 1–7.

U. Görtz, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : ugoertz@math.uni-bonn.de

Astérisque
312, 2007, p. 15–24

4. ARITHMETIC INTERSECTION NUMBERS

by

Ulrich Görtz

Abstract. — We define the arithmetic intersection number of three modular divisors and interpret it from the point of view of algebraic stacks. A criterion is given when the intersection of three modular divisors is finite. Furthermore, the final result about the arithmetic intersection numbers, as given by Gross and Keating, is stated and the strategy of its proof, carried out in the subsequent chapters, is explained.

***Résumé* (Nombres d'intersection arithmétiques).** — On définit les nombres d'intersection arithmétiques de trois diviseurs modulaires, et on donne une interprétation du point de vue des champs algébriques. On en donne un critère pour que cette intersection soit finie. En plus, on indique le résultat final sur les nombres d'intersection arithmétiques, comme donné par Gross et Keating, et la stratégie de sa preuve, effectuée dans les chapitres suivants.

1. Introduction

Let us recall some notation: Let $m \geq 1$ be an integer. In [**Vg**] we have defined the modular polynomial $\varphi_m \in \mathbb{Z}[j, j']$ (we regard j, j' as indeterminates). We denote by $T_m \subseteq \operatorname{Spec} \mathbb{Z}[j, j']$ the associated divisor. Write $S = \operatorname{Spec} \mathbb{Z}[j, j']$, and $S_{\mathbb{C}} = \operatorname{Spec} \mathbb{C}[j, j']$.

In this chapter, we will first prove a criterion for the intersection of three modular divisors over $\operatorname{Spec} \mathbb{Z}$ to be finite, which is analogous to the criterion of Hurwitz in the complex situation (see [**Vg**]).

In the second part we will prove, following [**GK**] and using results of later chapters, Gross' and Keating's explicit formula for the arithmetic intersection number: Fix positive integers m_1, m_2 and m_3. The arithmetic intersection number is, by definition,

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_S := \log \#\mathbb{Z}[j, j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3}).$$

2000 ***Mathematics Subject Classification.*** — 11G18, 14K07, 11E08.
Key words and phrases. — Modular divisors.

This number has a natural interpretation in the Arakelov theory for stacks (see below). In the proof, we use the properties of the invariants $\alpha_p(Q)$ and $\beta_\ell(Q)$ which will be established in later chapters. Altogether, this yields the proof of Theorem 1.2 in the introduction.

Acknowledgments. — I am grateful to all the participants of the ARGOS seminar for discussions and for feedback on these notes. In particular, I want to thank I. Bouw for her comments. I also profited from discussions with S. Kudla. Finally, I thank the anonymous referee for a number of helpful remarks.

2. Preliminaries, Notation

2.1. Quadratic forms and lattices in quadratic number fields. — There is a dictionary between binary quadratic forms (over $\mathbb{Z}$) and lattices in quadratic number fields (see [**BS**] II §7.5, in particular Satz 4). The exact statement we will use is the following.

Let $d < 0$ be a square-free integer. Denote by $\mathcal{L}$ the set of $\mathbb{Z}$-lattices in $\mathbb{Q}(\sqrt{d})$ up to homothety, and denote by $\mathcal{F}$ the set of positive definite primitive binary quadratic forms over $\mathbb{Z}$ which split in $\mathbb{Q}(\sqrt{d})$, up to proper equivalence. Then there is a bijection

$$\mathcal{L} \longrightarrow \mathcal{F}, \quad L \longmapsto \frac{N(\alpha x + \beta y)}{N(L)},$$

where $N\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ denotes the norm, $N(L) = \gcd(N(l);\ l \in L \setminus \{0\})$, and α, β is a basis of L such that $\frac{1}{i}(\alpha\overline{\beta} - \overline{\alpha}\beta) > 0$ (here $\bar{\cdot}$ denotes conjugation).

2.2. Stacks. — We mostly work with the coarse moduli space of (pairs of) elliptic curves, but in a few places it is more convenient to use the language of stacks. For the convenience of the reader, in this section we give a few references to the literature about the results that we need. A general reference is the book [**LM**] by Laumon and Moret-Bailly. See also Deligne's and Mumford's article [**DM**]. For the stacks that we are concerned with the main reference is the book [**KM**] of Katz and Mazur: although superficially the language of stacks is not used there, it is obvious that their results can be understood as results about stacks.

We denote by $\mathcal{M}$ the moduli stack (over $\mathbb{Z}$) of elliptic curves; this is a Deligne–Mumford stack.

We denote by $\mathcal{T}_m$ the moduli space of isogenies of elliptic curves of degree m. (In [**KM**], the notation [m-Isog] is used.) This is a Deligne–Mumford stack, too, and furthermore, we have:

Proposition 2.1. — *The morphism $\mathcal{T}_m \to \mathcal{M}$ is finite and flat, and is étale over $\mathbb{Z}[\frac{1}{m}]$. The morphism $\mathcal{T}_m \to \mathcal{M} \times \mathcal{M}$ is finite and unramified.*

Proof. — The first assertion is just [**KM**, 6.8.1], and the second one follows immediately from the rigidity theorem, see [**KM**, 2.4.2]. □

By relating the divisor T_m (inside the coarse moduli space) defined by the modular polynomials φ_m to the space $\mathcal{T}_m$, we get a description of the geometric points of T_m.

Lemma 2.2. — *Let $m \geq 1$. A geometric point of T_m corresponds to a pair (E, E') of elliptic curves such that there exists an isogeny $E \longrightarrow E'$ of degree m.*

Proof. — In characteristic 0 this is basically the definition of T_m and φ_m. In positive characteristic, we can prove this as follows: By mapping an isogeny to its source, we get a finite flat map from $\mathcal{T}_m$ to the moduli stack $\mathcal{M}$ of elliptic curves (see [**KM**, 6.8.1]). In particular, $\mathcal{T}_m$ is flat over $\mathbb{Z}$.

Now we have a map to the coarse moduli space S of pairs of elliptic curves:

$$F\colon \mathcal{T}_m \longrightarrow S, \quad (E \to E') \longmapsto (j(E), j(E')),$$

and we get a diagram

$$\begin{array}{ccc}
\mathcal{T}_{m,\mathbb{Q}_p} & \longrightarrow & \mathcal{T}_{m,\mathbb{Z}_p} \\
\downarrow & & \downarrow \\
\operatorname{im} F_{\mathbb{Q}_p} & \longrightarrow & \operatorname{im} F_{\mathbb{Z}_p} \\
\downarrow \cong & & \\
\operatorname{div}(\varphi_{m,\mathbb{Q}_p}) & \longrightarrow & \operatorname{div}(\varphi_{m,\mathbb{Z}_p}) \\
\downarrow & & \downarrow \\
S_{\mathbb{Q}_p} & \longrightarrow & S_{\mathbb{Z}_p}
\end{array}$$

Since $p \nmid \varphi_m(X, Y)$, $\operatorname{div}(\varphi_m)$ is flat over $\mathbb{Z}_p$, and because $\operatorname{im} F_{\mathbb{Z}_p}$ is flat over $\mathbb{Z}_p$, too, we get $\operatorname{im} F_{\mathbb{Z}_p} = \operatorname{div}(\varphi_m)$. Obviously the geometric points of $\operatorname{im} F_{\mathbb{Z}_p}$ correspond to pairs (E, E') of elliptic curves such that there exists an isogeny $E \to E'$ of degree m, so the lemma is proved. □

We can express the arithmetic intersection number of three 'divisors' $\mathcal{T}_{m_i}$ in $\mathcal{S} := \mathcal{M} \times \mathcal{M}$ in terms of the complete local rings of their 'intersection' $\mathcal{X} := \mathcal{T}_{m_1} \times_{\mathcal{S}} \mathcal{T}_{m_2} \times_{\mathcal{S}} \mathcal{T}_{m_3}$. (Note however that $T_{m_1} \times_S T_{m_2} \times_S T_{m_3}$ is not the coarse moduli space of $\mathcal{X}$.)

Proposition 2.3. — *Let $\mathcal{X} := \mathcal{T}_{m_1} \times_{\mathcal{S}} \mathcal{T}_{m_2} \times_{\mathcal{S}} \mathcal{T}_{m_3}$. Then*

$$\begin{aligned}
(T_{m_1} \cdot T_{m_2} \cdot T_{m_3}) &:= \log \#\mathbb{Z}[j, j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3}) \\
&= \frac{1}{2} \sum_p \log(p) \cdot \sum_{x \in \mathcal{X}(\overline{\mathbb{F}}_p)} \frac{1}{\#\mathrm{Aut}_{\mathcal{X}}(x)} \lg \widehat{\mathcal{O}}_{\mathcal{X},x}.
\end{aligned}$$

Proof. — We may assume that the intersection $T_{m_1} \cap T_{m_2} \cap T_{m_3}$ is finite, since otherwise both sides are infinite. (See the next section for a precise criterion, when this is the case.) The complete local ring of a geometric point in $\mathcal{M} \times \mathcal{M}$ is the universal

deformation ring of the corresponding pair of elliptic curves, and this ring is free of rank $\frac{\#\operatorname{Aut}(E)\#\operatorname{Aut}(E')}{4}$ over the complete local ring in the corresponding point in the coarse moduli space. This gives us (see the remarks at the beginning of section 4 for details) that the local contribution to the intersection number at a point (E, E') is

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_{(E,E')} = \sum_{f_i, i=1,2,3} \frac{1}{2\#\operatorname{Aut}(E)\#\operatorname{Aut}(E')} \lg_W \widehat{\mathcal{O}}_{\mathcal{M}\times\mathcal{M},(E,E')}/I,$$

where the sum extends over triples of isogenies $f_i \colon E \to E'$, $\deg f_i = m_i$, and where I is the smallest ideal in $\widehat{O}_{\mathcal{M}\times\mathcal{M},(E,E')}$, such that f_1, f_2, and f_3 lift to isogenies between the universal deformations of E, E' modulo I.

Now if a triple f_1, f_2, f_3 corresponds to the point $x \in \mathcal{X}(\overline{\mathbb{F}}_p)$, then $\widehat{\mathcal{O}}_{\mathcal{M}\times\mathcal{M},(E,E')}/I = \mathcal{O}_{\mathcal{X},x}$. Another triple (f_1', f_2', f_3') yields the same point in $\mathcal{X}$ if and only if there are automorphisms φ of E and φ' of E' such that $f_i' = \varphi' \circ f_i \circ \varphi^{-1}$ for $i = 1, 2, 3$. Furthermore $\operatorname{Aut}_{\mathcal{X}}(x)$ is isomorphic to the group of $(\varphi, \varphi') \in \operatorname{Aut}(E) \times \operatorname{Aut}(E')$ such that $f_i = \varphi' \circ f_i \circ \varphi^{-1}$ for $i = 1, 2, 3$. Hence by splitting up the sum above according to classes of triples which map to the same point in $\mathcal{X}$, we get the claimed equality. □

2.3. Notation. — We recall the following notation from [**Vg**]. For an elliptic curve E, we let $u_E := \frac{1}{2}\#\operatorname{Aut}(E)$.

Furthermore, given a ring R, and a quadratic space (L, D), for a quadratic form Q on R^m we define the representation number $R_L(Q)$ as the number of isogenies $(R^m, Q) \to (L, D)$.

3. When is $T_{m_1} \cap T_{m_2} \cap T_{m_3}$ finite?

We start with a lemma which guarantees the existence of elliptic curves such that the homomorphism module represents a given binary quadratic form.

Lemma 3.1. — *Let Q be a positive definite binary quadratic form over $\mathbb{Z}$. Then there exist elliptic curves E, E' (with complex multiplication) over $\mathbb{C}$ such that $Q \cong (\operatorname{Hom}(E, E'), \deg)$.*

Proof. — By the dictionary between quadratic forms and lattices in imaginary quadratic number fields (see section 2), if Q is a positive definite binary quadratic form over $\mathbb{Z}$ and $Q' = \frac{1}{r}Q$ is the associated primitive form, then there exists $d < 0$, an order $R_f = \mathbb{Z} + f\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \subseteq \mathbb{Q}(\sqrt{d})$ and an ideal $\mathfrak{a} \subseteq R_f$ with $\mathbb{Z}$-basis α, β, such that

$$Q'(x, y) \cong \frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}.$$

For the elliptic curves $\mathbb{C}/R_{fr}$ and $\mathbb{C}/\mathfrak{a}$ we then have

$$\mathrm{Hom}(\mathbb{C}/R_{fr}, \mathbb{C}/\mathfrak{a}) = \{\gamma \in \mathbb{C};\ \gamma R_{fr} \subseteq \mathfrak{a}\} = \mathfrak{a},$$

and for $\gamma \in \mathrm{Hom}(\mathbb{C}/R_{fr}, \mathbb{C}/\mathfrak{a})$,

$$\deg \gamma = [\mathfrak{a} : \gamma R_{fr}] = r \cdot [\mathfrak{a} : \gamma R_f] = r \cdot \frac{N(\gamma)}{N(\mathfrak{a})} = Q(\gamma). \qquad \square$$

It has been shown already by Hurwitz that on $S_{\mathbb{C}}$, two divisors T_{m_1} and T_{m_2} intersect in dimension 0 if and only if $m_1 m_2$ is not a square; see [**Vg**]. In other words, they intersect in dimension 0 if and only if there is no unary quadratic form Q which represents both m_1 and m_2. The following proposition gives us a completely analogous criterion for the intersection of three T_m's on S.

Proposition 3.2. — *The divisors T_{m_1}, T_{m_2} and T_{m_3} intersect in dimension 0 if and only if there is no positive definite binary quadratic form over $\mathbb{Z}$ which represents m_1, m_2 and m_3.*

In this case the support of $T_{m_1} \cap T_{m_2} \cap T_{m_3}$ is contained in the zero cycle of pairs of supersingular elliptic curves in characteristic $p < 4m_1m_2m_3$.

Proof. — First suppose that m_1, m_2, m_3 are represented by the positive definite binary quadratic form F. Let E, E' be elliptic curves in characteristic 0 (with complex multiplication) such that $\mathrm{Hom}(E, E') \cong F$. Then (E, E') corresponds to a point of $T_{m_1} \cap T_{m_2} \cap T_{m_3}$, so this intersection must have dimension ≥ 1.

If, on the other hand, there is no positive definite binary quadratic form which simultaneously represents m_1, m_2 and m_3, then for all points (E, E') of $T_{m_1} \cap T_{m_2} \cap T_{m_3}$ we must have $\mathrm{rk}\,\mathrm{Hom}(E, E') > 2$, thus E and E' are supersingular, and in particular live in positive characteristic.

Now fix a point $(E, E') \in S_{\mathbb{F}_p}$ which lies in the intersection $T_{m_1} \cap T_{m_2} \cap T_{m_3}$. To complete the proof of the proposition, we have to show that $p \leq 4m_1m_2m_3$. There exist isogenies $f_i \in \mathrm{Hom}(E, E')$ of degree m_i, $i = 1, 2, 3$.

Now consider the ternary quadratic form

$$Q(x_1, x_2, x_3) = \deg(x_1 f_1 + x_2 f_2 + x_3 f_3).$$

Since the matrix associated to Q is symmetric and positive definite, its determinant is smaller or equal than the product of the diagonal entries (see [**Be**, ch. 8, Thm. 5]), *i.e.*,

$$\Delta := \frac{1}{2} \det Q \leq 4m_1m_2m_3.$$

Note that $\Delta \in \mathbb{Z}$ (see [**B**] Lemma 1.1).

Now the proposition follows from the following lemma. $\square$

Lemma 3.3. — *With notation as above, we have*

$$p | \Delta.$$

Proof. — Let us first assume that $p > 2$.

We recall the following theorem on quadratic forms over $\mathbb{Q}_p$, see [**Se**, III Thm. 1, IV 2.1 and IV Thm. 6], for instance:

Theorem 3.4. — *If F is an anisotropic quadratic form of rank 4 over $\mathbb{Q}_p$, then its discriminant is a square, and its Hasse-Witt invariant ε_p is -1.*

Here, if we write $F = \sum_{i=1}^4 a_i x_i^2$, $a_i \in \mathbb{Q}_p$, then

$$\begin{aligned} \varepsilon_p &= \prod_{i<j} (a_i, a_j) \in \{1, -1\}, \qquad \text{where } (x, y) \text{ is the Hilbert symbol,} \\ (x, y) &= (-1)^{\alpha\beta\frac{p-1}{2}} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha}, \quad \text{if } x = p^\alpha u, y = p^\beta v, u, v \in \mathbb{Z}_p^\times, p \neq 2. \end{aligned}$$

Now $\mathrm{Hom}(E, E') \otimes \mathbb{Q}$ is isomorphic, up to scaling the form, to $\mathrm{End}(E) \otimes \mathbb{Q}$ with the quadratic form deg. But $\mathrm{End}(E) \otimes \mathbb{Q}$ is the quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞, and the degree form corresponds to the reduced norm (see [**Wd1**, 2.2]). Hence $\det(\deg|_{\mathrm{Hom}(E,E')})$ is a square. We also see that the quadratic form deg on $\mathrm{Hom}(E, E')$ is anisotropic over $\mathbb{Q}_p$, so its Hasse-Witt invariant ε_p is -1.

Since the m_i are not simultaneously represented by a binary quadratic form, the f_i are linearly independent over $\mathbb{Z}$. Now $\mathrm{Hom}(E, E')$ has square determinant and represents Q, so we have

$$\mathrm{Hom}(E, E') \otimes \mathbb{Q} \cong Q \perp \langle \Delta \rangle,$$

where $\langle \Delta \rangle$ denotes the unary quadratic form $x \mapsto \Delta x^2$. Over $\mathbb{Z}_p$ we can diagonalize Q:

$$Q(x_1, x_2, x_3) = a x_1^2 + b x_2^2 + c x_3^2, \quad a, b, c \in \mathbb{Z}_p.$$

Then $\Delta = 4abc$ and $\varepsilon_p = -1$ implies $p | abc$, by the formulas above.

For $p = 2$ the bound $p \leq 4 m_1 m_2 m_3$ holds trivially, but the stronger assertion $p|\Delta$ is true in this case too. Namely, by [**B**] Prop. 4.7, the 2-adic valuation of Δ is equal to the sum $a_1 + a_2 + a_3$ of the Gross–Keating invariants of Q (see *loc. cit.*). Furthermore, since Q is anisotropic, the a_i cannot all be 0 (*loc. cit.* Lemma 5.3).

This concludes the proof of the lemma, and thus the proof of the proposition, as well. □

We conclude this section by the following proposition which reformulates the criterion we obtained above in terms of ternary quadratic forms.

Proposition 3.5. — *Let m_1, m_2, m_3 be positive integers. The following are equivalent:*

(1) There exists no positive definite integral binary quadratic form Q which represents m_1, m_2, and m_3.

(2) Every positive semi-definite half-integral symmetric matrix T with diagonal entries m_1, m_2, m_3 is non-degenerate, i.e., $\det T \neq 0$.

(As usual, by half-integral we mean that the entries outside the diagonal lie in $\frac{1}{2}\mathbb{Z}$, and the diagonal entries are integers. We denote the set of half-integral symmetric $n \times n$ matrices by $\mathrm{Sym}(\mathbb{Z})^\vee$.)

Proof. — Given a positive semi-definite $T \in \mathrm{Sym}(\mathbb{Z})^\vee$ with $\det T = 0$, we get a Q as in (1) as follows: There exists an $x \in \mathbb{Z}^3$ such that ${}^t xTx = 0$, and we may assume that x is not divisible, *i.e.*, that it generates a direct summand in $\mathbb{Z}^3$. Choosing a complement, we get a positive-semidefinite binary quadratic form which represents the m_i. It could happen that this form is degenerate, but then we can clearly find a positive definite form which still represents all the three m_i.

On the other hand, given a Q as in (1), choose x_i, y_i, such that $Q(x_i, y_i) = m_i$, $i = 1, 2, 3$. The matrix $\left(\begin{smallmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{smallmatrix}\right)$ defines a map $\mathbb{Z}^3 \to \mathbb{Z}^2$, and expressing the ternary quadratic form which we get as the composition of this map with Q, we obtain a positive semi-definite half-integral symmetric matrix T with diagonal (m_1, m_2, m_3) which is obviously degenerate. □

4. A formula for the intersection number

From now on, we assume that T_{m_1}, T_{m_2} and T_{m_3} intersect in dimension 0. We want to explain the final formula which we get for the intersection number, see Theorem 4.3 below. The proofs of the main steps will follow in later chapters.

We write

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_S = \sum_p n(p) \log p,$$

with

$$n(p) = \lg_{\mathbb{Z}_p} \mathbb{Z}_p[j, j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3})$$

(and $n(p) = 0$ for $p > 4m_1m_2m_3$).

Furthermore, $n(p)$ is the sum of the intersection multiplicities in points (E, E') given by pairs of supersingular elliptic curves in characteristic p. Denote by $j^{(E)}, j^{(E')}$ their j-invariants.

Let $W = W(\overline{\mathbb{F}}_p)$ be the ring of Witt vectors of $\overline{\mathbb{F}}_p$, let $\tilde{j}^{(E)}, \tilde{j}^{(E')} \in W$ be lifts of $j^{(E)}, j^{(E')}$, respectively, and let R_0 be the completion of $W[j, j']$ in the ideal $\mathfrak{m} = (p, j - \tilde{j}^{(E)}, j' - \tilde{j}^{(E')})$. Then

$$R_0 \cong W[[j - \tilde{j}^{(E)}, j' - \tilde{j}^{(E')}]].$$

On the other hand, if R denotes the universal deformation ring of the pair (E, E'), then $R \cong W[[t, t']]$, and R_0 is isomorphic to the ring $R^{\mathrm{Aut}(E) \times \mathrm{Aut}(E')}$ of invariants under the finite group $\mathrm{Aut}(E) \times \mathrm{Aut}(E')$ (cf. [**KM**, 8.2.3]). Since R_0 is regular, R is free over R_0 (see [**Ma**, Theorem 23.1]) and since $\pm\,\mathrm{id}$ are the only automorphisms of the whole universal deformation, we have $\mathrm{rk}_{R_0} R = u_E u_{E'}$.

We denote by $(\mathbb{E}, \mathbb{E}')$ the universal pair of elliptic curves over $\mathrm{Spf}\, R$.

Lemma 4.1. — *In R, the modular polynomial φ_m factors as follows:*

$$\varphi_m = \prod_{\substack{f\colon E\to E' \text{ isog. of} \\ \text{degree } m, \bmod \pm 1}} \varphi_{m,f},$$

such that for each f, $(\varphi_{m,f}) \subseteq R$ is the smallest ideal $I \subseteq R$ such that f lifts to an isogeny $\tilde{f}\colon \mathbb{E} \longrightarrow \mathbb{E}'$ modulo I.

Proof. — Let $f\colon E \to E'$ be an isogeny of degree m. Then its deformation functor Def_f is pro-represented by a closed subscheme of $\mathrm{Spf}\, R$ (by the rigidity theorem), and this closed subscheme is a divisor, say $\mathrm{div}(\varphi_{m,f})$, $\varphi_{m,f} \in R$. (This is proved in [**KM**, (6.8)] if m is a power of p, but the proof given there works in general. If p does not divide m, then Def_f is actually smooth.)

Claim. — *If f and g are isogenies $E \to E'$ of degree m, then the elements $\varphi_{m,f}$ and $\varphi_{m,g}$ are coprime unless $f = \pm g$.*

To prove the claim, suppose that f and g are given such that $\varphi_{m,f}$ and $\varphi_{m,g}$ are not coprime. Then $\mathrm{div}(\varphi_{m,f})$ and $\mathrm{div}(\varphi_{m,g})$ have a common component C. Now $C \otimes \mathbb{Q}$ must have dimension 1, so $\mathrm{End}(\mathbb{E} \otimes_{\mathrm{Spf}\, R} C) = \mathrm{End}(\mathbb{E}' \otimes_{\mathrm{Spf}\, R} C) = \mathbb{Z}$

By definition of C, we have isogenies $f, g\colon \mathbb{E} \otimes_{\mathrm{Spf}\, R} C \to \mathbb{E}' \otimes_{\mathrm{Spf}\, R} C$ of degree m. Since ${}^t f \circ f$ and ${}^t f \circ g$ are elements in $\mathrm{End}(\mathbb{E} \otimes_{\mathrm{Spf}\, R} C) = \mathbb{Z}$ of the same degree, we see that $f = \pm g$. This proves the claim.

Thus we get for the scheme-theoretic union

$$\bigcup_{f \bmod \pm 1} \mathrm{Def}_f = \mathrm{div}\Big(\prod_{f \bmod \pm 1} \varphi_{m,f}\Big).$$

Since

$$\bigcup_{f \bmod \pm 1} \mathrm{Def}_f(S) = \mathrm{div}(\varphi_m)(S)$$

for all $S \to \mathrm{Spf}\, R$, we obtain that (after possibly changing one of the $\varphi_{m,f}$'s by a unit)

$$\varphi_m = \prod_{f \bmod \pm 1} \varphi_{m,f}. \qquad \square$$

Lemma 4.2. — *Let A be a ring, B an A-algebra, and let $x_1, \ldots, x_n \in B$. If none of the x_i is a zero-divisor, then*

$$\mathrm{lg}_A B/(x_1 \cdots x_n) = \sum_{i=1}^{n} \mathrm{lg}_A B/(x_i). \quad \square$$

We can write

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3}) = \sum_p \log(p) \sum_{(E,E')\text{s.s. in char } p} (T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_{(E,E')},$$

and by applying Lemma 4.1 to φ_{m_i} for $i = 1, 2, 3$, and applying lemma 4.2 successively, we get that the local contribution in a point (E, E') is

$$\begin{aligned}(T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_{(E,E')} &= \lg_W R_0/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3}) \\ &= \sum_{f_1}\sum_{f_2}\sum_{f_3} \frac{1}{u_E u_{E'}} \lg_W R/(\varphi_{m_1,f_1}, \varphi_{m_2,f_2}, \varphi_{m_3,f_3}) \\ &= \sum_{f_i, i=1,2,3} \frac{1}{u_E u_{E'}} \lg_W R/I, \qquad (4.1)\end{aligned}$$

where the sums are over isogenies $f_i \colon E \to E'$ of degree m_i, up to ± 1, and where I is the smallest ideal in R such that f_1, f_2 and f_3 lift to isogenies $\tilde{f}_i \colon \mathbb{E} \to \mathbb{E}'$ mod I.

We write, using the notation of [**R**],

$$\alpha(f_1, f_2, f_3) = \lg_W R/I.$$

By the theorem of Serre-Tate, this global question about elliptic curves can be reduced to a local question about formal groups. This is the reason why we study deformations of isogenies between formal groups in detail in the following chapters.

From [**R**, Theorem 1.1] we get that $\alpha(f_1, f_2, f_3)$ depends only on the $\mathbb{Z}_p$-isomorphism class of the ternary quadratic form $Q \colon (x_1, x_2, x_3) \mapsto \deg(\sum x_i f_i)$. We thus write $\alpha_p(Q)$ instead of $\alpha(f_1, f_2, f_3)$. Loc. cit. gives an explicit expression for $\alpha_p(Q)$ in terms of the coefficients of Q. The number of occurrences of Q in (4.1) is $\frac{1}{8} R_{\mathrm{Hom}(E,E')}(Q)$ (because we count the isogenies up to ± 1, but the representation number counts each triple (f_1, f_2, f_3)). Furthermore, for a positive definite ternary form Q, $R_{\mathrm{Hom}(E,E')}(Q) = 0$ unless Q is isotropic over $\mathbb{Q}_\ell$ for all $\ell \neq p$, and anisotropic over $\mathbb{Q}_p$. The reason is that $\mathrm{Hom}(E, E') \otimes \mathbb{Q} \cong \mathrm{End}(E) \otimes \mathbb{Q}$, and $\mathrm{End}(E) \otimes \mathbb{Q}_\ell \cong M_2(\mathbb{Q}_\ell)$ for $\ell \neq p$, and $\mathrm{End}(E) \otimes \mathbb{Q}_p$ is a division algebra (see [**Wd1**, 2.2]). On the other hand, in the latter case there exists a pair of supersingular elliptic curves E, E' in characteristic p, such that Q is represented by $\mathrm{Hom}(E, E')$ (see [**Wd1**, Proposition 3.2]).

We have now

$$n(p) = \frac{1}{8} \sum_{(E,E') \text{ supersingular}} \left(\sum_Q \frac{R_{\mathrm{Hom}(E,E')}(Q)}{u_E u_{E'}} \alpha_p(Q) \right).$$

Further Corollary 4.4 in [**Wd1**] states that there are invariants $\beta_\ell(Q) \in \mathbb{Z}_{\geq 1}$ which depend only on the isomorphism class of the ternary form Q over $\mathbb{Z}_\ell$, such that

$$\sum_{(E,E') \text{ s.s.}} \frac{R_{\mathrm{Hom}(E,E')}(Q)}{u_E u_{E'}} = 4 \prod_{\substack{\ell \mid \Delta \\ \ell \neq p}} \beta_\ell(Q). \qquad (4.2)$$

The invariants β_ℓ are computed explicitly in [**Wd2**, Proposition 2.1]. Altogether, we get the following theorem.

Theorem 4.3. — *If T_{m_1}, T_{m_2} and T_{m_3} intersect in dimension 0, then*

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_S = \log \#\mathbb{Z}[j,j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3}) = \sum_p n(p) \log p$$

with

$$n(p) = \frac{1}{2} \sum_Q \left(\prod_{\substack{\ell \mid \Delta \\ \ell \neq p}} \beta_\ell(Q) \right) \alpha_p(Q),$$

where the sum runs over all positive definite ternary quadratic forms Q over $\mathbb{Z}$ with diagonal (m_1, m_2, m_3) which are isotropic over $\mathbb{Q}_\ell$ for all $\ell \neq p$.

In this way we get a very explicit formula for the intersection numbers.

References

[Be] R. Bellmann – *Introduction to Matrix Analysis*, 2nd ed., Tata McGraw-Hill, 1974.

[BS] S. Borewicz & I. Šafarevič – *Zahlentheorie*, Birkhäuser, 1966.

[B] I. Bouw – Invariants of ternary quadratic forms, this volume, p. 113–137.

[DM] P. Deligne & D. Mumford – The irreducibility of the space of curves of given genus, *Publ. Math. Inst. Hautes Études Sci.* **36** (1969), p. 75–109.

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Invent. math.* **112** (1993), p. 225–245.

[KM] N. Katz & B. Mazur – *Arithmetic Moduli of Elliptic Curves*, Ann. Math. Studies, vol. 108, Princeton University Press, 1985.

[LM] G. Laumon & L. Moret-Bailly – *Champs algébriques*, Erg. Math. Grenzg. 3. Folge, Band, vol. 39, Springer, 2000.

[Ma] H. Matsumura – *Commutative Ring theory*, Cambridge University Press, 1986.

[R] M. Rapoport – Deformations of isogenies of formal groups, this volume, p. 139–169.

[Se] J.-P. Serre – *A Course in Arithmetic*, Graduate Texts in Math., vol. 7, Springer, 1973.

[Vg] G. Vogel – Modular polynomials, in this volume, p. 1–7.

[Wd1] T. Wedhorn – The genus of the endomorphisms of a supersingular elliptic curve, this volume, p. 25–47.

[Wd2] ———, Calculation of representation densities, this volume, p. 179–190.

U. Görtz, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : ugoertz@math.uni-bonn.de

Astérisque
312, 2007, p. 25–47

5. THE GENUS OF THE ENDOMORPHISMS OF A SUPERSINGULAR ELLIPTIC CURVE

by

Torsten Wedhorn

***Abstract.* —** We describe the genus of the quadratic space $\mathrm{Hom}(E', E)$ of homomorphisms of two supersingular elliptic curves E and E' and study the map $(E', E) \mapsto \mathrm{Hom}(E', E)$ from the set of pairs of supersingular elliptic curves over $\bar{\mathbb{F}}_p$ to the set of proper classes in this genus. We show that this map is surjective and determine its fibres. In the last section we use the Minkowski-Siegel formula to express the mean value of the representation of a ternary quadratic form in this genus by local representation densities.

***Résumé* (Le genre des endomorphismes d'une courbe elliptique supersingulière)**

Nous décrivons le genre de l'espace quadratique $\mathrm{Hom}(E', E)$ des homomorphismes de deux courbes elliptiques supersingulières E et E' et nous étudions l'application $(E', E) \mapsto \mathrm{Hom}(E', E)$ de l'ensemble des paires de courbes elliptiques supersingulières sur $\bar{\mathbb{F}}_p$ vers l'ensemble des classes propres dans ce genre. Dans le dernier paragraphe, on utilise la formule de Minkowski-Siegel pour exprimer la moyenne de la représentation d'une forme quadratique ternaire dans ce genre en termes de densités de représentation locales.

Introduction

Let $p > 0$ be a prime and let D be the unique quaternion division algebra with center $\mathbb{Q}$ which is ramified precisely at p and at infinity. The reduced norm Nrd is a quadratic form on D. We will study lattices and maximal orders in D. Recall that two lattices Λ and Λ' are said to be in the same proper class if there exists a $g \in \mathrm{SO}(D, \mathrm{Nrd})$ such that $g\Lambda = \Lambda'$.

We will relate the lattices and the maximal orders in D to supersingular elliptic curves. Many of these results, although formulated somewhat differently, can already be found in [**Do**] (see also [**GZ**]).

2000 ***Mathematics Subject Classification.* —** 11E08, 14K07, 11E12.
***Key words and phrases.* —** Supersingular elliptic curve, quaternion algebra, genus, Minkowski-Siegel formula.

Fix a supersingular elliptic curve E_0 over $\overline{\mathbb{F}}_p$ set $O = \mathrm{End}(E_0)$. Then O is a maximal order in the quadratic space $O \otimes_{\mathbb{Z}} \mathbb{Q}$, where the quadratic form is given by the degree, and we can and will identify the rational quadratic spaces $O \otimes_{\mathbb{Z}} \mathbb{Q}$ with D.

The first result is the following (proved in sections 2.9 and 2.15):

Theorem. — *Consider isomorphism classes of pairs (E, φ) where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and $\varphi\colon E \to E_0$ is a quasi-isogeny.*

(1) *The map $(E, \varphi) \mapsto \varphi \mathrm{Hom}(E_0, E)$ induces a bijection of the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and the set of right ideal classes of O.*

(2) *The map $(E, \varphi) \mapsto \varphi \mathrm{End}(E)\varphi^{-1}$ induces a surjection from the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ to the set of conjugacy classes of maximal orders in D. Two supersingular elliptic curves E and E' are sent to the same conjugacy class if and only if there exists a $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ such that $E' \cong E^{(\sigma)}$.*

For all pairs (E', E) of supersingular elliptic curves it is possible to choose quasi-isogenies $\varphi\colon E \to E_0$ and $\varphi'\colon E' \to E_0$ with $\deg(\varphi) = \deg(\varphi')$. Then $\varphi \mathrm{Hom}(E', E)\varphi'^{-1}$ is a lattice in D whose proper class is independent of the choice of φ and φ'. In this way we can consider $\mathrm{Hom}(E', E)$ as a proper class of lattices in D.

The second theorem describes these proper classes (see sections 3.1 and Proposition 3.2).

Theorem. — *Let Λ be a lattice in D. Then the proper class $[\Lambda]$ of Λ is the proper class associated to $\mathrm{Hom}(E', E)$ if and only if Λ is in the same genus as O.*

It follows that the map $((E, \varphi), (E', \varphi')) \mapsto \varphi \mathrm{Hom}(E', E)\varphi'^{-1}$ induces a surjection $(E, E') \mapsto [\mathrm{Hom}(E', E)]$ from the set of pairs of isomorphism classes of supersingular elliptic curves onto the set of proper classes of lattices in D which are locally isomorphic to O. The next theorem describes the fibres of this map and number of automorphisms of the quadratic space $\mathrm{Hom}(E, E')$ (see Proposition 3.3 and Corollary 3.5).

Theorem

(1) *Two pairs (E, E') and (F, F') are sent to the same proper class if and only if there exists a $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ such that $F = E^{(\sigma)}$ and $F' = E'^{(\sigma)}$.*

(2) *For all (E, E')*

$$\#\mathrm{SO}([\mathrm{Hom}(E', E)]) = \begin{cases} \#\mathrm{Aut}(E)\#\mathrm{Aut}(E'), & E,\ E' \text{ both defined over } \mathbb{F}_p; \\ \frac{1}{2}\#\mathrm{Aut}(E)\#\mathrm{Aut}(E'), & \text{otherwise.} \end{cases}$$

Now fix a positive definite ternary quadratic form Q over $\mathbb{Z}$. By the theorems above we can consider the expression

$$2\left(\sum_{E}\frac{1}{\#\operatorname{Aut}(E)}\right)^{-2}\sum_{(E',E)}\frac{R_{\operatorname{Hom}(E',E)}(Q)}{\#\operatorname{Aut}(E')\#\operatorname{Aut}(E)}$$

as the mean value of the representation of Q by the genus of $\operatorname{End}(E_0)$ (here E and E' run through all isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and $R_{\operatorname{Hom}(E',E)}(Q)$ denotes the number of isometries $Q \to \operatorname{Hom}(E',E)$). Hence it can be expressed as a product of local representation densities $\alpha_l(Q,\operatorname{End}(E_0))$ (see 4.3) by the Minkowski-Siegel formula. We obtain (theorem 4.3):

Theorem. — *The mean value is given by*

$$\sum_{(E',E)}\frac{R_{\operatorname{Hom}(E',E)}(Q)}{\#\operatorname{Aut}(E')\#\operatorname{Aut}(E)}=2\left(\frac{p-1}{12}\right)^2\frac{\pi^4}{p^3}\prod_l\alpha_l(Q,\operatorname{End}(E_0)),$$

where l runs through all prime numbers l.

This article is organized as follows. In the first section some definitions and results on quadratic spaces and quaternion algebras are recalled. The second section addresses the correspondence between supersingular elliptic curves, right ideal classes, and conjugacy classes of maximal orders. In the third section the above results on the quadratic spaces $\operatorname{Hom}(E',E)$ are proved. The Minkowski-Siegel formula is applied in the last section.

Acknowledgements. — I am very grateful to S. Kudla for his helpful remarks and to M. Rapoport, T. Yang and the referee for their comments.

1. Preliminaries on quadratic spaces and quaternion algebras

1.1. In this section we recall some definitions and results on quadratic spaces.

If R is a commutative ring, a *quadratic space over* R is a free R-module M together with a map $Q\colon M \to R$, such that

(a) $Q(rm) = r^2Q(m)$ for all $r \in R$ and $m \in M$.

(b) The form $b_Q(x,y) = Q(x+y) - Q(x) - Q(y)$ is R-bilinear and nondegenerate (*i.e.*, the R-linear map $M \to M^*$ corresponding to b_Q is injective).

The map Q is called the *quadratic form* of the quadratic space (M,Q).

Two quadratic spaces (M,Q) and (M',Q') over R are said to be *isomorphic* if there exists an R-linear isomorphism $f\colon M \to M'$ such that $Q'(f(m)) = Q(m)$ for all $m \in M$. We then write $(M,Q) \cong (M',Q')$.

The group of automorphisms of a quadratic space will be denoted by $\mathrm{O}(M,Q)$, the subgroup of automorphisms $g \in \mathrm{O}(M,Q)$ with $\det(g) = 1$ is denoted by $\mathrm{SO}(M,Q)$.

1.2. In the sequel we will only consider quadratic spaces (M, Q) over integral domains R whose field of fractions has characteristic not equal to 2. Then we write $\mathrm{Sym}_n(R)^\vee$ for the set of symmetric matrices n by n matrices $A = (a_{ij})$ with coefficients in $\mathrm{Quot}(R)$ such that $a_{ii} \in R$ for all i and such that $2a_{ij} \in R$ for all i, j. Moreover, we denote by B_Q the $\mathrm{Quot}(R)$-valued bilinear form

$$B_Q \colon M \times M \longrightarrow \mathrm{Quot}(R), \qquad (x, y) \longmapsto \frac{1}{2}(Q(x+y) - Q(x) - Q(y)).$$

Let $\mathcal{B} = (e_1, \ldots, e_n)$ be an R-basis of M. The matrix

$$S_Q = (B_Q(e_i, e_j)) \in \mathrm{Sym}_n(R)^\vee$$

is called the matrix associated to $(M, Q, \mathcal{B})$.

We denote by $\det(M) = \det((M, Q))$ the class of $\det(S_Q)$ modulo $(R^\times)^2$. This is independent of the choice of $\mathcal{B}$.

1.3. Very often we will consider quadratic spaces which arise as follows: Let (V, Q) be a quadratic space over $\mathbb{Q}$ and let Λ be a $\mathbb{Z}$-lattice of V (*i.e.*, a finitely generated $\mathbb{Z}$-submodule Λ such that $\Lambda\mathbb{Q} = V$). If $Q(\Lambda) \subset \mathbb{Z}$, the restriction of Q to Λ defines a quadratic form on Λ over $\mathbb{Z}$.

If l is a finite place of $\mathbb{Q}$, $\Lambda_l = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is a lattice in the $\mathbb{Q}_l$-vector space $V_l = V \otimes \mathbb{Q}_l$. Recall that to give a $\mathbb{Z}$-lattice Λ in V is the same as to give a $\mathbb{Z}_l$-lattice Λ_l for all l such that there exists a $\mathbb{Z}$-lattice Γ of V with $\Lambda_l = \Gamma_l$ for almost all l.

Denote by $\mathbb{A}_f$ the ring of finite adeles of $\mathbb{Q}$. An element $g \in GL(V \otimes \mathbb{A}_f)$ is an element $(g_l) \in \prod_l GL(V_l)$ where l runs over all finite places of $\mathbb{Q}$ such that $g_l(\Lambda_l) = \Lambda_l$ for almost all l (this condition is independent of Λ). Hence $g = (g_l)$ acts on the set of lattices by setting

$$g(\Lambda) = \bigcap_l (V \cap g_l(\Lambda_l)).$$

We obtain an action of $GL(V \otimes \mathbb{A}_f)$ on the set of lattices in V and in particular an action of the subgroups $\mathrm{O}(V \otimes \mathbb{A}_f)$ and $\mathrm{SO}(V \otimes \mathbb{A}_f)$.

Definition 1.1. — We say that two quadratic spaces M and M' over $\mathbb{Z}$ are *related* if M and M' are isomorphic over $\mathbb{Z}_l$ for all places l of $\mathbb{Q}$ (with the convention $\mathbb{Z}_\infty = \mathbb{R}$).

1.4. If M and M' are related, they are of course also isomorphic over $\mathbb{Q}_l$ for all places l and hence they are isomorphic over $\mathbb{Q}$ by the weak approximation theorem for quadratic spaces. If we choose an isomorphism of rational quadratic spaces $M \otimes \mathbb{Q} \cong M' \otimes \mathbb{Q}$, we can consider M and M' both as lattices in the same quadratic space V over $\mathbb{Q}$. Moreover, the fact that M and M' are related just means that there exists a $g \in \mathrm{O}(V)(\mathbb{A}_f)$ with $g(M) = M'$. This leads us to the following definition:

Definition 1.2. — Let V be a quadratic space over $\mathbb{Q}$. We say that two lattices Λ and Λ' in V are *related* if there exists a $g \in \mathrm{O}(V)(\mathbb{A}_f)$ such that $g(\Lambda) = \Lambda'$.

An $\mathrm{O}(V)(\mathbb{A}_f)$-orbit of lattices in V is called a *genus*.

Lemma 1.3. — *Let l be a prime number and let (M, Q) be a quadratic space over $\mathbb{Z}_l$. Then there exists a reflection in $\mathrm{O}(M, Q)$.*

Proof. — Let $x \in M$ be an element such that the l-adic valuation of $Q(x)$ is minimal among the elements in M. Then an easy calculation shows that the reflection associated to x preserves M. □

Corollary 1.4. — *Let V be a quadratic space over $\mathbb{Q}$. Two lattices Λ and Λ' in V are in the same genus if and only if there exists a $g \in \mathrm{SO}(V \otimes \mathbb{A}_f)$ such that $g(\Lambda) = \Lambda'$.*

Definition 1.5. — Let V be a quadratic space over $\mathbb{Q}$. Two lattices Λ and Λ' in V are said to be in the same *proper class* or to be *properly equivalent* if there exists a $g \in \mathrm{SO}(V)$ such that $g(\Lambda) = \Lambda'$.

They are in the same *class* or *equivalent* if there exists a $g \in \mathrm{O}(V)$ such that $g(\Lambda) = \Lambda'$.

Obviously, every genus of a lattice is the disjoint union of classes and every class is the disjoint union of one or two proper classes. Moreover, it is well known (*e.g.*, [**Ki**, 6.1.2]) that in each genus there are only finitely many proper classes.

The class of a lattice Λ is equal to the proper class of Λ if and only if there exists a $g \in \mathrm{O}(V)$ with $\det(g) = -1$ such that $g(\Lambda) = \Lambda$, *i.e.*, if and only if $\mathrm{SO}(\Lambda) \neq \mathrm{O}(\Lambda)$.

1.5. We will be mostly interested in quadratic spaces which arise from quaternion algebras: By a quaternion algebra over a field F we mean a central simple algebra D over F of dimension 4. We write Trd and Nrd for the reduced trace and the reduced norm on D, respectively, and we denote by $x \mapsto \bar{x} := \mathrm{Trd}(x) - x$ the canonical involution on D.

Assume that F is the field of fractions of Dedekind domain A (*e.g.*, $A = \mathbb{Z}$ or $A = \mathbb{Z}_l$). Let Λ be some A-lattice of D. Then we set

$$O_l(\Lambda) = \{\, d \in D \mid d\Lambda \subset \Lambda \,\}, \tag{1.1}$$

$$O_r(\Lambda) = \{\, d \in D \mid \Lambda d \subset \Lambda \,\}. \tag{1.2}$$

These are orders in D. We call them the *left order* (resp. *right order*) of Λ. We say that Λ is *normal* if $O_l(\Lambda)$ and $O_r(\Lambda)$ are maximal orders.

Lemma 1.6. — *Let F be a field with $\mathrm{char}(F) \neq 2$ and let D be a quaternion algebra over F. We set*

$$S(D) := \{\, (d, d') \in D^\times \times D^\times \mid \mathrm{Nrd}(d) = \mathrm{Nrd}(d') \,\}.$$

Consider the group homomorphism

$$\begin{aligned} \alpha \colon S(D) &\longrightarrow \mathrm{O}(D, \mathrm{Nrd}), \\ (d, d') &\longmapsto (\delta \longmapsto d\delta d'^{-1}). \end{aligned}$$

Then we have

$$\mathrm{Im}(\alpha) = \mathrm{SO}(D, \mathrm{Nrd})\,, \qquad \mathrm{Ker}(\alpha) = F^\times$$

where $F^\times$ is embedded diagonally in $D^\times \times D^\times$.

Proof. — We give two proofs for this. The first is elementary: Clearly, we have $\mathrm{Ker}(\alpha) = F^\times$. Let $d \in D$ be an element with $\mathrm{Nrd}(d) \neq 0$ and denote by $\tau_d \colon D \to D$ the reflection with respect d. Then we have for $\delta \in D$:

$$\tau_d\delta = \delta - \frac{\mathrm{Trd}(\delta\bar{d})}{\mathrm{Nrd}(d)}d = -d\bar{\delta}\bar{d}^{-1}. \tag{1.3}$$

Every element in $\mathrm{SO}(D)$ is a product of elements of the form $\tau_d\tau_{d'}$ as $\mathrm{char}(F) \neq 2$. It follows from (1.3) that for all $\delta \in D$ we have

$$\tau_d\tau_{d'}(\delta) = dd'^{-1}\delta\bar{d}'\bar{d}^{-1}$$

and this proves that $\mathrm{SO}(D)$ is contained in the image of α.

Conversely, let $\sigma \colon \delta \mapsto d\delta d'^{-1}$ with $\mathrm{Nrd}(d) = \mathrm{Nrd}(d')$ be in the image of α. The determinant of left or right multiplication with any element $\tilde{d} \in D$ is given by $\mathrm{Nrd}(\tilde{d})^2$ (this can be checked over an algebraic closure and for a matrix algebra this is elementary). Hence we see

$$\det(\sigma) = \mathrm{Nrd}(d)^2\,\mathrm{Nrd}(d')^{-2} = 1.$$

The second proof is as follows. By Hilbert 90 we have $H^1(F, \mathbb{G}_m) = 0$ and therefore it suffices to show that α induces an exact sequence of algebraic groups over F

$$1 \longrightarrow \mathbb{G}_{m,F} \longrightarrow S(D) \xrightarrow{\alpha} \mathrm{SO}(D, \mathrm{Nrd}) \longrightarrow 0.$$

We can replace F by its algebraic closure. Then it is clear that $S(D)$ is a connected algebraic group of dimension 7. This implies that $\mathrm{Im}(\alpha)$ must be contained in the conected component of 1 of $\mathrm{O}(D, \mathrm{Nrd})$ which is $\mathrm{SO}(D, \mathrm{Nrd})$. Again it is obvious that $\mathrm{Ker}(\alpha) = \mathbb{G}_m$. It follows that $\dim(\mathrm{Im}(\alpha)) = 6 = \dim(\mathrm{SO}(D, \mathrm{Nrd}))$ which shows $\mathrm{Im}(\alpha) = \mathrm{SO}(D, \mathrm{Nrd})$. □

Corollary 1.7. — *Let D be a quaternion algebra over $\mathbb{Q}$. And let Λ and Λ' be $\mathbb{Z}$-lattices of D.*

(1) *They are in the same genus if and only if there exist $d = (d_l)$, $d' = (d'_l) \in (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ with $\mathrm{Nrd}(d_l) = \mathrm{Nrd}(d'_l)$ for all l such that $d\Lambda = \Lambda' d'$.*
(2) *They are in the same proper class if and only if there exist d, $d' \in D^\times$ with $\mathrm{Nrd}(d) = \mathrm{Nrd}(d')$ such that $d\Lambda = \Lambda' d'$.*

1.6. From now on, D will denote a quaternion algebra over $\mathbb{Q}$. For every place v of $\mathbb{Q}$ we set $D_v = D \otimes_{\mathbb{Q}} \mathbb{Q}_v$. Then D_v is a quaternion algebra over $\mathbb{Q}_v$. For all v there are up to isomorphism two quaternion algebras over $\mathbb{Q}_v$. One is isomorphic to the ring of matrices $M_2(\mathbb{Q}_v)$ and the other one is a quaternion division algebra. If $D_v \cong M_2(\mathbb{Q}_v)$ we say that D is *split* at v otherwise D is said to be *ramified* at v.

We know that D is split at almost all places v and that the number of ramified places is even. Conversely, for every set of places S of $\mathbb{Q}$ with an even number of elements there exists a quaternion algebra D over $\mathbb{Q}$ such that D is ramified at v if and only if $v \in S$.

1.7. Let l be a prime number and let D_l be a quaternion algebra over $\mathbb{Q}_l$. We recall some well-known facts on maximal orders and ideals in D_l:

Assume first that $D_l = \mathrm{End}(V)$ where V is a two-dimensional $\mathbb{Q}_l$-vector space. For every $\mathbb{Z}_l$-lattice L in V the ring

$$\mathrm{End}(L) = \{\, d \in \mathrm{End}(V) \mid d(L) \subset L \,\}$$

is a maximal order of $\mathrm{End}(V)$. Conversely, every maximal order O is of this form. As $GL(V) = D^\times$ acts transitively on the set of all lattices in V, we see that all maximal orders of D are conjugate.

If we choose a basis for L, the Cartan decomposition can be written as

$$GL_2(\mathbb{Q}_l) = GL_2(\mathbb{Z}_l) \cdot T \cdot GL_2(\mathbb{Z}_l)$$

where T consists of the diagonal matrices of the form $\mathrm{diag}(l^a, l^b)$ for $a, b \in \mathbb{Z}$. Using this decomposition, an easy calculation shows that the normalizer of a maximal order $O = \mathrm{End}(L)$ in $D_l^\times$ is given by

$$N_{D_l^\times}(O) = l^{\mathbb{Z}} O^\times. \tag{1.4}$$

A $\mathbb{Z}_l$-lattice Λ is normal (see 1.5) if and only if there exist lattices L and L' in V such that

$$\Lambda = \mathrm{Hom}(L', L) = \{\, d \in D_l \mid d(L') \subset L \,\}.$$

Conversely, $\mathrm{Hom}(L', L)$ is clearly a normal lattice of $\mathrm{End}(V)$ for all lattices L, L' of V. We have

$$O_l(\mathrm{Hom}(L', L)) = \mathrm{End}(L), \qquad O_r(\mathrm{Hom}(L', L)) = \mathrm{End}(L')$$

and as a left $\mathrm{End}(L)$-module (resp. as a right $\mathrm{End}(L')$-module) $\mathrm{Hom}(L', L)$ is generated by any one element d such that $d(L') = L$.

1.8. Now assume that D_l is a quaternion division algebra over $\mathbb{Q}_l$. Then there exists a unique maximal order $\mathcal{O}_{D_l}$ of D_l, namely

$$\mathcal{O}_{D_l} = \{\, d \in D_l \mid \mathrm{Nrd}(d) \in \mathbb{Z}_l \,\}.$$

Moreover, $\mathcal{O}_{D_l}$ has a unique maximal ideal $\mathfrak{m}$ which is a principal ideal. Every nonzero one-sided ideal of $\mathcal{O}_{D_l}$ is a power of $\mathfrak{m}$, in particular it is a two-sided ideal.

As $d\mathcal{O}_{D_l}d^{-1}$ is again a maximal order of D_l for all $d \in D_l^\times$, we see that

$$N_{D_l^\times}(\mathcal{O}_{D_l}) = D_l^\times. \tag{1.5}$$

2. Supersingular elliptic curves

2.1. From now on we fix a prime number p. We consider supersingular elliptic curves E over $\overline{\mathbb{F}}_p$. Recall that any supersingular elliptic curve is already defined over $\mathbb{F}_{p^2}$. For two supersingular elliptic curves we denote by $\mathrm{Hom}(E', E)$ the set of homomorphism $E' \to E$ which are defined over $\overline{\mathbb{F}}_p$. We set $\mathrm{End}(E) = \mathrm{Hom}(E, E)$.

We denote by $W(\overline{\mathbb{F}}_p)$ the ring of Witt vectors of $\overline{\mathbb{F}}_p$ and write σ for the Frobenius on $W(\overline{\mathbb{F}}_p)$.

2.2. For any prime $l \neq p$ let $T_l(E)$ be the Tate module. It is a free $\mathbb{Z}_l$-module of rank 2. For $l = p$ we denote by $T_p(E)$ the (covariant) Dieudonné module of E. It as a free $W(\overline{\mathbb{F}}_p)$-module of rank 2 with σ-linear operator Φ such that

$$pT_p(E) \subsetneq \Phi(T_p(E)) \subsetneq T_p(E)$$

where σ is the Frobenius in $W(\overline{\mathbb{F}}_p)$. In fact, there exists a $W(\overline{\mathbb{F}}_p)$-basis (e, f) of $T_p(E)$ such that $\Phi(e) = f$ and $\Phi(f) = pe$.

We denote by $\mathrm{Hom}(T_p(E'), T_p(E))$ the $\mathbb{Z}_p$-module of $W(\overline{\mathbb{F}}_p)$-linear homomorphisms $T_p(E') \to T_p(E)$ which commute with Φ. It is easily checked that this is a free $\mathbb{Z}_p$-module of rank 4. Moreover, $\mathrm{End}(T_p(E)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is "the" quaternion division algebra over $\mathbb{Q}_p$ and $\mathrm{End}(T_p(E))$ is its maximal order.

We set $T^p(E) = \prod_{l \neq p} T_l(E)$, $V^p(E) = T^p(E) \otimes_{\mathbb{Z}} \mathbb{Q}$, $V_p(E) = T_p(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $V(E) = V^p(E) \times V_p(E)$.

These are free modules of rank 2 over the rings $\mathbb{Z}^p = \prod_{l \neq p} \mathbb{Z}_l$, $\mathbb{A}_f^p = \mathbb{Z}^p \otimes \mathbb{Q}$, $\mathbb{Q}_p$, and $\mathbb{A}_f$, respectively.

2.3. We fix a supersingular elliptic curve E_0, set $\mathcal{O}_D = \mathrm{End}(E_0)$ and $D = \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Q}$. It follows from 2.2 (see also 3.1 below) that D is a quaternion division algebra over $\mathbb{Q}$ which is ramified precisely at p and ∞. As $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is a maximal order in $D_l = D \otimes_{\mathbb{Q}} \mathbb{Q}_l$ for all primes l, $\mathcal{O}_D$ is a maximal order in D.

The reduced norm Nrd is a positive definite quadratic form on D and the induced homomorphism $\mathrm{Nrd}\colon D^\times \to \mathbb{Q}^{>0}$ is surjective.

2.4. Denote by Y^p be the set of $\widehat{\mathbb{Z}}^p$-lattices in $V^p(E_0)$ and by Y_p the set of $W(\overline{\mathbb{F}}_p)$-lattices L in $V_p(E_0)$ such that $pL \subsetneq \Phi(L) \subsetneq L$. Then $Y^p \times Y_p$ describes quasi-isogenies with target E_0 as follows: Consider pairs (E, φ) where E is a supersingular elliptic curve and $\varphi\colon E \to E_0$ a quasi-isogeny. We call two such pairs (E, φ) and (E', φ') equivalent if there exists a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E_0 \\ \wr\downarrow & & \downarrow\wr \\ E' & \xrightarrow{\varphi'} & E_0, \end{array}$$

where the vertical arrows are isomorphisms. Then $Y^p \times Y_p$ corresponds to the set $\mathcal{L}$ of equivalence classes of such pairs (E, φ) as above (see [**Mi**, 6] for the general description of an isogeny class of an abelian variety with endomorphisms).

The group $GL(V^p(E_0))$ acts transitively on the elements in Y^p and therefore we have a bijection

$$Y^p \longleftrightarrow GL(V^p(E_0))/GL(T^p(E_0)).$$

Moreover, if we denote by $\mathrm{Aut}(V_p(E_0))$ the automorphisms of $V_p(E_0))$ which commute with Φ, it follows from the existence of a normal form for lattices in Y_p (see 2.2) that $\mathrm{Aut}(V_p(E_0))$ acts transitively on Y_p. Therefore we have a bijection

$$Y_p \longleftrightarrow \mathrm{Aut}(V_p(E_0))/\mathrm{Aut}(T_p(E_0)).$$

If we choose isomorphisms $\alpha_l \colon \mathrm{End}(T_l(E_0)) \xrightarrow{\sim} \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_l$ for all primes l, we obtain a bijection

$$\mathcal{L} \longleftrightarrow (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / (\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times \tag{2.1}$$

which is independent of the choice of the α_l by the theorem of Skolem-Noether. Explicitly this bijection is given by the associating to $d = (d_l) \in (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ the equivalence class of the pair (E, φ) such that $T_l(\varphi)(T_l(E)) = d_l T_l(E_0)$ for all primes l.

2.5. Let $d \in (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ and let $[(E, \varphi)] \in \mathcal{L}$ be the associated quasi-isogeny. Then we have

$$\deg(\varphi) = \prod_l l^{v_l(\mathrm{Nrd}(d_l))}$$

where l runs over all prime numbers.

2.6. For example, the relative Frobenius $E_0^{(p)} \to E_0$ corresponds via the bijection (2.1) to the class of an element Π in $(D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ which has a uniformizing element of $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p$ as p-th component and a unit of $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_l$ as l-th component for all primes $l \neq p$.

More generally, if O is any maximal order of D, we call an element $\Pi = (\Pi_l)_l \in D \otimes_{\mathbb{Q}} \mathbb{A}_f$ a *Frobenius element in a quaternion algebra with respect to* O if $\Pi_l \in (O \otimes_{\mathbb{Z}} \mathbb{Z}_l)^\times$ for all $l \neq p$ and Π_p is a uniformizing element of $\mathcal{O}_{D_p}$.

2.7. Consider the natural map

$$\begin{aligned} \mathcal{L} &\longrightarrow \mathcal{I} := \left\{ \begin{array}{c} \text{isomorphism classes of} \\ \text{supersingular elliptic curves over } \overline{\mathbb{F}}_p \end{array} \right\}, \\ [(E, \varphi)] &\longmapsto E. \end{aligned}$$

Using the identification (2.1), two elements d, $d' \in (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / (\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times$ have the same image in $\mathcal{I}$ if and only if there exists a $\delta \in D^\times = (\mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q})^\times$ such that $\delta d = d'$. Hence we get:

Theorem 2.1. — *There is a natural identification*

$$D^\times\backslash(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times/(\mathcal{O}_D\otimes_{\mathbb{Z}}\widehat{\mathbb{Z}})^\times \longleftrightarrow \left\{\begin{matrix}\text{isomorphism classes of}\\ \text{supersingular elliptic}\\ \text{curves over } \overline{\mathbb{F}}_p\end{matrix}\right\}. \tag{2.2}$$

2.8. Let O be any order in D. A $\mathbb{Z}$-lattice Λ of D is called a *right ideal of* O if $O\subset O_r(\Lambda)$ (cf. 1.5). If O is a maximal order, this is of course equivalent to $O=O_r(\Lambda)$. Two right ideals Λ and Λ' of O are said to be *in the same right ideal class* if there exists a $d\in D^\times$ with $d\Lambda=\Lambda'$.

Let Λ be a lattice in D. It can be easily checked locally that $O_l(\Lambda)$ is a maximal order of D if and only if $O_r(\Lambda)$ is a maximal order. Hence all right ideals of our fixed maximal order $\mathcal{O}_D$ are normal lattices in the sense of 1.5.

By 1.7 and 1.8 we know that locally all right ideals of $\mathcal{O}_D$ are principal ideals. Hence it follows that for every right ideal Λ of $\mathcal{O}_D$ there exists a $d\in(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$ such that $\Lambda=d\mathcal{O}_D$. Therefore $(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$ acts transitively on the set of all right ideals of $\mathcal{O}_D$. Moreover, an easy local calculation shows that the stabilizer of the right ideal $\mathcal{O}_D$ in $(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$ is equal to $(\mathcal{O}_D\otimes_{\mathbb{Z}}\widehat{\mathbb{Z}})^\times$. Thus we have a natural bijection

$$(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times/(\mathcal{O}_D\otimes_{\mathbb{Z}}\widehat{\mathbb{Z}})^\times \longleftrightarrow \{\text{right ideals of } \mathcal{O}_D\}. \tag{2.3}$$

Composing this bijection with (2.1) we get a bijection of $\mathcal{L}$ with the set of right ideals of $\mathcal{O}_D$. Explicitly, this associates to each equivalence class $[(E,\varphi)]$ the right ideal $\varphi\operatorname{Hom}(E_0,E)$ of $\mathcal{O}_D=\operatorname{End}(E_0)$.

2.9. The bijection (2.3) induces a bijection of the set of right ideal classes of $\mathcal{O}_D$ with $D^\times\backslash(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times/(\mathcal{O}_D\otimes_{\mathbb{Z}}\widehat{\mathbb{Z}})^\times$. Composing this with (2.2) we obtain:

Proposition 2.2. — *There exists a natural bijection*

$$\left\{\begin{matrix}\text{right ideal classes}\\ \text{of } \mathcal{O}_D\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{isomorphism classes of}\\ \text{supersingular elliptic}\\ \text{curves over } \overline{\mathbb{F}}_p\end{matrix}\right\}. \tag{2.4}$$

2.10. By 1.7 and 1.8 we know that locally all maximal orders in D are conjugate to each other. Therefore $(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$ acts transitively by conjugation on the set of maximal orders in D. The stabilizer of the maximal order $\mathcal{O}_D$ is the normalizer of $\mathcal{O}_D$ in $(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$. It can be computed locally and by (1.4) and (1.5) we have

$$N_{(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times}(\mathcal{O}_D)=\mathbb{Q}^\times(D_p^\times\times(\mathcal{O}_D\otimes_{\mathbb{Z}}\widehat{\mathbb{Z}}^p)^\times). \tag{2.5}$$

2.11. Let O be a maximal order of D and $d\in(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$ such that $O=d\mathcal{O}_Dd^{-1}$. Then it follows at once from the definition of a Frobenius element in 2.6 that if $\Pi\in(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$ is a Frobenius element with respect to $\mathcal{O}_D$, $d\Pi d^{-1}$ is a Frobenius element with respect to O.

2.12. For $d \in (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ let $[(E,\varphi)]$ be the associated element in $\mathcal{L}$ via the bijection (2.1). Let Π be a Frobenius element with respect to $\mathcal{O}_D$. Then the pair $[(E',\varphi')]$ associated to $d\Pi$ is given by $E' = E^{(p^{-1})}(= E^{(p)})$ and $\varphi' = F_{E_0} \circ \varphi^{(p^{-1})}$ where $F_{E_0} : E_0^{(p^{-1})} \to E_0$ is the relative Frobenius.

Moreover, if $\Lambda = d\mathcal{O}_D$ is the right ideal of $\mathcal{O}_D$ corresponding to $[(E,\varphi)]$ via the bijection (2.3), the right ideal corresponding to $[(E',\varphi')]$ is given by $d\Pi\mathcal{O}_D = \tilde{\Pi} d\mathcal{O}_D = \tilde{\Pi}\Lambda$ where $\tilde{\Pi} = d\Pi d^{-1}$ is a Frobenius element with respect to $O = O_l(\Lambda)$.

2.13. Let $\mathfrak{m}_p \subset \mathcal{O}_{D_p}$ be the maximal ideal. For a maximal order O of D let $\mathfrak{p} = O \cap \mathfrak{m}_p$ be the unique prime ideal of O which lies over p. Let Λ be any left ideal of O and let Π be a Frobenius element with respect to O. Then arguing locally one sees that

$$\Pi\Lambda = \mathfrak{p}\Lambda.$$

2.14. It is easy to check that the canonical projection

$$\begin{aligned} &\{\text{right ideals of } \mathcal{O}_D\} = (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / (\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times \\ \longrightarrow\ &\{\text{maximal orders of } D\} = (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / N_{(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times}(\mathcal{O}_D) \end{aligned} \tag{2.6}$$

is given by $\Lambda \mapsto O_l(\Lambda)$.

The projection (2.6) induces a map from the set of right ideal classes of $\mathcal{O}_D$ to the set of $D^\times$-conjugacy classes of maximal orders in D whose adelic version is the projection

$$\begin{aligned} D^\times\backslash(D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / (\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times &\longrightarrow D^\times\backslash(D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / N_{(D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times}(\mathcal{O}_D) \\ &= D^\times\backslash(D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / (D_p^\times \times (\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^p)^\times). \end{aligned} \tag{2.7}$$

Lemma 2.3. — *Let $\{O\}$ be a conjugacy class of maximal orders in D. Let $\mathcal{R}(\{O\})$ be the set of classes of right ideals of $\mathcal{O}_D$ which are sent to $\{O\}$ under the map* (2.7). *Then $\mathcal{R}(\{O\})$ consists either of one or two elements. It consists of one element if and only if O contains an element d with* $\mathrm{Nrd}(d) = p$ *for one (or equivalently for all) $O \in \{O\}$.*

Proof. — We consider the map (2.7). Hence we are in the following situation: Let G be a group, H and G_2 be subgroups, and let G_1 be a normal subgroup of G_2. Consider the canonical projection

$$\varpi : H\backslash G/G_1 \longrightarrow H\backslash G/G_2.$$

Let $g_0 \in G$ and set $F_{g_0} = \varpi^{-1}(\varpi(Hg_0G_1))$. Then $G_1\backslash G_2$ acts transitively from the right on F_{g_0} and the stabilizer of Hg_0G_1 is $(g_0^{-1}Hg_0 \cap G_2)G_1/G_1$.

In the special case of (2.7) we have $H = D^\times$, $G = (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, $G_1 = (\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times$ and $G_2 = D_p^\times \times (\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^p)^\times$. Therefore G_2/G_1 is the free cyclic group generated by a Frobenius element Π (cf. 2.6). Moreover, $\Pi^2 G_1 \subset \mathbb{Q}^\times G_1 \subset (g_0^{-1}Hg_0 \cap G_2)G_1/G_1$ for all $g_0 \in G$. Therefore the fibres of (2.7) consist of at most two elements.

Now fix g_0 and let $O = g_0\mathcal{O}_D g_0^{-1}$ be the associated maximal order of D. A fibre F_{g_0} consists of one element if and only if there exists in $g_0^{-1}D^\times g_0$ a Frobenius element. If there exists a $d \in D^\times$ such that $g_0^{-1}dg_0$ is a Frobenius element (and hence an element of $\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$), we necessarily have $d \in g_0\mathcal{O}_D g_0^{-1} = O$. Moreover, $g_0^{-1}dg_0$ is a Frobenius element if and only if

$$\mathrm{Nrd}(g_0^{-1}dg_0)_l \in \begin{cases} \mathbb{Z}_l^\times, & \text{if } l \neq p; \\ p\mathbb{Z}_p, & \text{if } l = p. \end{cases}$$

Hence we see that F_{g_0} consists of one element if and only if there exists an element $d \in O$ such that $\mathrm{Nrd}(d) = p$ (the case $\mathrm{Nrd}(d) = -p$ can of course not occur). □

2.15. In 2.8 we have seen that every right ideal of $\mathcal{O}_D$ is of the form $\varphi\,\mathrm{Hom}(E_0, E)$ for some quasi-isogeny $\varphi\colon E \to E_0$. As we have

$$O_l(\varphi\,\mathrm{Hom}(E_0, E)) = \varphi\,\mathrm{End}(E)\varphi^{-1}$$

we see that every maximal order of D is of the form $\varphi\,\mathrm{End}(E)\varphi^{-1}$. Moreover, the $D^\times$-conjugacy class of $\varphi\,\mathrm{End}(E)\varphi^{-1}$ depends only on E. We denote it by $\{\mathrm{End}(E)\}$.

Proposition 2.4. — *Let O be a maximal order and let E be a supersingular elliptic curve such that O is in the conjugacy class $\{End(E)\}$. Let $\mathfrak{p}$ be the unique (two-sided) prime ideal of O which lies over p.*

(1) *The following assertions are equivalent:*
   (a) *The elliptic curve E is defined over $\mathbb{F}_p$.*
   (b) *Up to isomorphism there exists a unique supersingular elliptic curve E such that the conjugacy class of O is equal to $\{\mathrm{End}(E)\}$.*
   (c) *The prime ideal $\mathfrak{p}$ is a principal ideal.*
   (d) *The subgroup $\mathbb{Q}^\times O^\times$ of the normalizer $N_{D^\times}(O)$ is of index 2.*

(2) *If these equivalent conditions do not hold, we have:*
   (a) *Up to isomorphism there are precisely two elliptic curves E and E' such that $\{O\} = \{\mathrm{End}(E)\} = \{\mathrm{End}(E')\}$ and for them $E' \cong E^{(p)}$.*
   (b) *$N_{D^\times}(O) = \mathbb{Q}^\times O^\times$.*

Proof. — It follows from Proposition 2.2 and Lemma 2.3 that (1)(b) is equivalent to the existence of a $d \in O$ such that $\mathrm{Nrd}(d) = p$. As $\mathfrak{p} = \mathfrak{m}_p \cap O$ such an element generates $\mathfrak{p}$. Conversely, for every generator d of $\mathfrak{p}$ we have $\mathrm{Nrd}(d) = p$. This proves the equivalence of (1)(b) and (1)(c).

An easy calculation shows that $d \in N_{D^\times}(O)$ implies $d \in l^{\mathbb{Z}}(O \otimes_{\mathbb{Z}} \mathbb{Z}_l)^\times$ for all primes $l \neq p$. Therefore we have an injective homomorphism

$$\nu\colon N_{D^\times}(O)/(\mathbb{Q}^\times O^\times) \hookrightarrow (D \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times/\mathbb{Q}^\times(O \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \cong \mathbb{Z}/2\mathbb{Z}$$

where the isomorphism is given by $v_p \circ \mathrm{Nrd}$. In particular, we see that if (1)(d) does not hold, (2)(b) holds.

The homomorphism ν is surjective if and only if there exists an element $d \in N_{D^\times}(O)$ such that $v_p(\mathrm{Nrd}(d)) = 1$. For all $d \in N_{D^\times}(O)$ we have $v_l(\mathrm{Nrd}(d)) \in 2\mathbb{Z}$ for all $l \neq p$. Therefore, if $d \in N_{D^\times}(O)$ satisfies $v_p(\mathrm{Nrd}(d)) = 1$, we can find a $\lambda \in \mathbb{Q}^\times$ such that $\mathrm{Nrd}(d\lambda) = p$. As $d\lambda \in N_{D^\times}(O)$, we can write $d\lambda = l^m a$ for all $l \neq p$ where $m \in \mathbb{Z}$ and $a \in (O \otimes_{\mathbb{Z}} \mathbb{Z}_l)^\times$. As $v_l(\mathrm{Nrd}(d\lambda)) = 0$, we have $d\lambda \in (O \otimes_{\mathbb{Z}} \mathbb{Z}_l)^\times$. Moreover, $\mathrm{Nrd}(d\lambda) = p$ also implies that $d\lambda \in O \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathcal{O}_{D_p}$. Hence $d\lambda \in O$. Altogether we have seen that ν is surjective if and only if there exists a $d \in O \cap N_{D^\times}(O)$ with $\mathrm{Nrd}(d) = p$. Such an element generates $\mathfrak{p}$ and thus (1)(d) implies (1)(c).

Conversely, for every $d \in O$ with $\mathrm{Nrd}(d) \in p^{\mathbb{Z}}$ we have $d(O \otimes_{\mathbb{Z}} \mathbb{Z}_l)d^{-1} = (O \otimes_{\mathbb{Z}} \mathbb{Z}_l)$ for all primes l and hence $d \in N_{D^\times}(O)$. Therefore the converse implication does also hold.

Next we show that for any supersingular elliptic curve E we have

$$\{\mathrm{End}(E)\} = \{\mathrm{End}(E^{(p^{-1})})\}.$$

Choose a quasi-isogeny $\varphi\colon E \to E_0$ and let $I = \varphi\,\mathrm{Hom}(E_0, E)$ be the corresponding right ideal of $\mathcal{O}_D$. The right ideal corresponding to the quasi-isogeny $E_0^{(p^{-1})} \to E_0 \to^{\varphi} E$ (where the first arrow is the relative Frobenius) is the right ideal ΠI where $\Pi \in (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ is a Frobenius element with respect to the maximal order $O_l(I)$ (cf. 2.6). Using a local calculation it follows at once that $O_l(\Pi I) = \Pi O_l(I)\Pi^{-1} = O_l(I)$.

We have already seen in the proof of Lemma 2.3 that if $I = d\mathcal{O}_D$ and $I' = d'\mathcal{O}_D$ (with d, $d' \in (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$) are two right ideals of $\mathcal{O}_D$ with $\{O_l(I)\} = \{O_l(I')\}$ then there exists a Frobenius element Π with respect to $\mathcal{O}_D$ and an integer n such that the right ideal class of $d'\mathcal{O}_D$ is equal to the right ideal class of $d\Pi^n\mathcal{O}_D$. Writing $d\Pi = \tilde{\Pi}d$ for a Frobenius element $\tilde{\Pi}$ with respect to $O_l(I)$ (see 2.11), we see that the right ideal classes of I' and $\tilde{\Pi}^n I$ are equal. Let E be the supersingular elliptic curve corresponding to the class of I and let E' be the supersingular elliptic curve corresponding to the class of I'. Then this implies that there exists an integer n such that $E' \cong E^{(p^n)}$ and this completes the proof. □

2.16. Note that the proof of Proposition 2.4 also shows that every supersingular elliptic curve is already defined over $\mathbb{F}_{p^2}$.

Moreover we have seen:

Corollary 2.5. — *Let O be a maximal order of D and set $N := N_{D^\times}(O)$. Consider the subgroups $O^\times \subset \mathbb{Q}^\times O^\times \subset N$. Then*

$$O^\times = \{\, d \in N \mid \mathrm{Nrd}(d) = 1 \,\},$$
$$\mathbb{Q}^\times O^\times = \{\, d \in N \mid \mathrm{Nrd}(d) \in (\mathbb{Q}^\times)^2 \,\}.$$

3. The genus of the quadratic space $\mathrm{Hom}(E', E)$

3.1. For any two supersingular elliptic curves E and E' we will consider the free $\mathbb{Z}$-module $\mathrm{Hom}(E', E)$ together with the quadratic form given by the degree.

As E and E' are supersingular, $\mathrm{Hom}(E', E)$ has rank 4 as a $\mathbb{Z}$-module. We have a canonical map of $\mathbb{Z}_l$-modules

$$\alpha\colon \mathrm{Hom}(E', E) \otimes_{\mathbb{Z}} \mathbb{Z}_l \longrightarrow \mathrm{Hom}(T_l(E'), T_l(E)).$$

As the union of the l^n-torsion $E[l^n]$ for $n \geq 1$ is scheme-theoretically dense in E, α is injective. Moreover, the cokernel of α is torsionfree: Indeed, let $\tau \in \mathrm{Hom}(T_l(E'), T_l(E))$ be such that $l\tau = \alpha(\varphi)$ for some $\varphi \in \mathrm{Hom}(E', E) \otimes \mathbb{Z}_l$. We write φ as the limit of sequence of $\varphi_n \in \mathrm{Hom}(E', E)$ converging to φ. For large n we have $T_l(\varphi_n) = l\tau_n$ for some $\tau_n \in \mathrm{Hom}(T_l(E'), T_l(E)$, and therefore the restriction of φ_n to the l-torsion $E[l]$ is zero. But this implies that φ is divisible by l.

As both sides have rank 4, it follows that α is an isomorphism. Choosing an identification $T_l(E') \cong T_l(E)$, we can consider the right hand side as a lattice in the quaternion algebra $\mathrm{End}(T_l(E)) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and the quadratic form given by the degree on the left hand side corresponds via α to the reduced norm on the right hand side.

Therefore the isomorphism class of the quadratic space $\mathrm{Hom}(E', E) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is independent of E and E' for all l. In other words (Definition 1.1), $\mathrm{Hom}(E', E)$ and $\mathrm{Hom}(F', F)$ are related for all supersingular elliptic curves E, E', F, and F'.

Lemma 3.1. — *Let E and E' be two supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Then there exists a quasi-isogeny $\varphi\colon E' \to E$ of degree 1.*

Proof. — As $\mathrm{Hom}(E', E)$ and $\mathrm{End}(E)$ are related, we can choose an isomorphism of quadratic spaces $\mathrm{Hom}(E', E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Via this isomorphism we identify $\mathrm{Hom}(E', E)$ with a sublattice of $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Choose an integer $N \geq 1$ such that $N\,\mathrm{End}(E) \subset \mathrm{Hom}(E', E)$. Then $N\,\mathrm{id}_E$ corresponds to an isogeny $\varphi'\colon E' \to E$ of degree N^2 and $\varphi = (1/N)\varphi'$ is a quasi-isogeny of degree 1. □

3.2. If E and E' are two supersingular elliptic curves, we can choose quasi-isogenies $\varphi\colon E \to E_0$ and $\varphi'\colon E' \to E_0$ such that $\deg(\varphi) = \deg(\varphi')$ by Lemma 3.1. Then

$$\iota_{\varphi,\varphi'}\colon \mathrm{Hom}(E', E) \longrightarrow D, \qquad \alpha \longmapsto \varphi \circ \alpha \circ \varphi'^{-1}$$

is an isometry. If we choose another pair (φ_1, φ_1') as above, we have

$$\iota_{\varphi,\varphi'}(\mathrm{Hom}(E', E)) = d\iota_{\varphi_1,\varphi_1'}(\mathrm{Hom}(E', E))d'^{-1}$$

for d, $d' \in D$ with $\mathrm{Nrd}(d) = \mathrm{Nrd}(d')$. Hence it follows from Corollary 1.7 that the proper class of $\iota_{\varphi,\varphi'}(\mathrm{Hom}(E', E))$ is independent of the choice of (φ, φ'). We denote this class by $[\mathrm{Hom}(E', E)]$.

Proposition 3.2. — *Every proper class in the genus of $\mathrm{End}(E_0) \subset D$ is of the form $[\mathrm{Hom}(E', E)]$ for two supersingular elliptic curves E and E'.*

Proof. — Let $\Lambda \subset D$ be a lattice in the genus of $\mathcal{O}_D$. By Corollary 1.7 there exist d, $d' \in (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ with $\mathrm{Nrd}(d_l) = \mathrm{Nrd}(d'_l)$ for all primes l such that $\Lambda = d\mathcal{O}_D d'^{-1}$. Denote by $[(E,\varphi)]$, $[(E',\varphi')] \in \mathcal{L}$ the quasi-isogenies associated to d, d', respectively, via bijection 2.1. Then $\varphi \operatorname{Hom}(E',E)\varphi'^{-1} \subset D$ depends only on the classes of (E,φ) and (E',φ') in $\mathcal{L}$. Recall that $\operatorname{Hom}(E',E) \otimes \mathbb{Z}_l = \operatorname{Hom}(T_l(E'), T_l(E))$ for all primes l (see 3.1). Therefore we have by 2.4:

$$\begin{aligned}
\varphi \operatorname{Hom}(E',E)\varphi'^{-1} &= \bigcap_l \big((\varphi \operatorname{Hom}(T_l(E'),T_l(E))\varphi'^{-1}) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cap D\big) \\
&= \bigcap_l (T_l(\varphi) \operatorname{Hom}(T_l(E'),T_l(E)) T_l(\varphi')^{-1} \cap D) \\
&= \bigcap_l (d_l \operatorname{Hom}(T_l(E_0),T_l(E_0)) d_l'^{-1} \cap D) \\
&= d\mathcal{O}_D d'^{-1} = \Lambda.
\end{aligned}$$

Moreover, it follows from 2.5 that the condition $\mathrm{Nrd}(d_l) = \mathrm{Nrd}(d'_l)$ implies $\deg(\varphi) = \deg(\varphi')$. Thus Λ lies in the proper class $[\operatorname{Hom}(E',E)]$. □

Proposition 3.3. — *Let E, E', E_1 and E'_1 be supersingular elliptic curves. Then we have $[\operatorname{Hom}(E',E)] = [\operatorname{Hom}(E'_1,E_1)]$ if and only if there exists an integer n such that $E'_1 \cong E'^{(p^n)}$ and $E_1 \cong E^{(p^n)}$.*

Proof. — Choose quasi-isogenies $\varphi\colon E \to E_0$, $\varphi'\colon E' \to E_0$, $\varphi_1\colon E_1 \to E_0$ and $\varphi'_1\colon E'_1 \to E_0$ such that $\deg(\varphi) = \deg(\varphi')$ and $\deg(\varphi_1) = \deg(\varphi'_1)$. We set $\Lambda = \iota_{\varphi,\varphi'}(\operatorname{Hom}(E',E))$ and $\Lambda_1 = \iota_{\varphi_1,\varphi'_1}(\operatorname{Hom}(E'_1,E_1))$. Let d, d', d_1, $d'_1 \in (D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ be elements such that the associated pairs in $\mathcal{L}$ via the bijection (2.1) are equal to $[(E,\varphi)]$, $[(E',\varphi')]$, $[(E_1,\varphi_1)]$, $[(E'_1,\varphi'_1)]$ respectively. Then

$$\Lambda = d\mathcal{O}_D d'^{-1}, \qquad \Lambda_1 = d_1\mathcal{O}_D d_1'^{-1}.$$

We set $\hat{\mathcal{O}}_D^\times := (\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times$. If $E'_1 \cong E'^{(p^{-n})}$ and $E_1 \cong E^{(p^{-n})}$, we can choose $\varphi'_1 = F^n_{E_0} \circ \varphi'^{(p^n)}$ and $\varphi_1 = F^n_{E_0} \circ \varphi^{(p^n)}$ where $F^n_{E_0}\colon E_0^{(p^{-n})} \to E_0$ is the relative Frobenius. Then we have $d'_1\hat{\mathcal{O}}_D^\times = d'\Pi^n\hat{\mathcal{O}}_D^\times$ and $d_1\hat{\mathcal{O}}_D^\times = d\Pi^n\hat{\mathcal{O}}_D^\times$ for a Frobenius element Π with respect to $\mathcal{O}_D$. Note that $\Pi^n\hat{\mathcal{O}}_D^\times = \hat{\mathcal{O}}_D^\times\Pi^n$ and $\varepsilon\mathcal{O}_D = \mathcal{O}_D = \mathcal{O}_D\varepsilon$ for $\varepsilon \in \hat{\mathcal{O}}_D^\times$. Therefore

$$\Lambda_1 = d_1\mathcal{O}_D d_1'^{-1} = d\Pi^n\mathcal{O}_D\Pi^{-n}d'^{-1} = d\mathcal{O}_D d'^{-1} = \Lambda.$$

Conversely, assume that Λ and Λ_1 are in the same proper class. By Corollary 1.7 there exist δ, $\delta' \in D^\times$ with $\mathrm{Nrd}(\delta) = \mathrm{Nrd}(\delta')$ such that $\delta\Lambda = \Lambda_1\delta'$. Then the maximal orders $O_l(\Lambda)$ and $O_l(\Lambda_1)$ are in the same conjugacy class. Hence we see that $\{\mathrm{End}(E)\} = \{\mathrm{End}(E_1)\}$ and then Proposition 2.4 implies that there exists an integer n such that $E_1 \cong E^{(p^n)}$. Considering $O_r(\Lambda)$ and $O_r(\Lambda_1)$ we see that there also exists an integer n' such that $E'_1 \cong E'^{(p^{n'})}$.

It remains to show that we can choose $n = n'$. As all supersingular elliptic curves are defined over $\mathbb{F}_{p^2}$, we can assume that $n, n' \in \{0, 1\}$. If one elliptic curve X is defined over $\mathbb{F}_p$ we have $X = X^{(p)}$ and therefore we can assume that all four elliptic curves are not defined over $\mathbb{F}_p$. Then we have to show that the following case cannot occur: $E_1' \cong E'$ and $E_1 \ncong E$. Note that we know already that $E_1 \ncong E$ implies $E_1 \cong E^{(p)}$.

We can assume that $O_r(\Lambda) = O_r(\Lambda_1) =: O$. Then $\delta\Lambda = \Lambda_1\delta'$ implies that $\delta' \in N_{D^\times}(O)$. As $E' = E_1'$ is not defined over $\mathbb{F}_p$ we have $N_{D^\times}(O) = \mathbb{Q}^\times O^\times$ by Proposition 2.4. Thus there exists a $\delta_1 \in D^\times$ with $\mathrm{Nrd}(\delta_1) = 1$ such that $\delta_1\Lambda = \Lambda_1$. Now $E_1 = E^{(p)}$ implies by 2.13 that there exists a $\delta_1' \in D^\times$ such that $\Lambda_1 = \delta_1'\mathfrak{p}\Lambda$ where $\mathfrak{p}$ is the prime ideal of $O_l(\Lambda)$ which lies over (p). But this implies

$$\delta_1 O = \Lambda_1\Lambda^{-1} = \delta_1'\mathfrak{p}$$

and this is a contradiction as $\mathfrak{p}$ is not a principal ideal by Proposition 2.4. □

3.3. Let E and E' be two supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Consider the natural map

$$\begin{aligned} \alpha\colon \mathrm{Aut}(E) \times \mathrm{Aut}(E') &\longrightarrow \mathrm{O}(\mathrm{Hom}(E', E)) \\ (\varphi, \varphi') &\longmapsto (x \longmapsto \varphi x \varphi'^{-1}) \end{aligned}$$

Proposition 3.4. — *The image of α lies in $\mathrm{SO}(\mathrm{Hom}(E', E))$ and the kernel of α consists of $\{\pm 1\}$ (diagonally embedded in $\mathrm{Aut}(E) \times \mathrm{Aut}(E')$). The image of α is equal to $\mathrm{SO}(\mathrm{Hom}(E', E))$ if and only if E or E' is not defined over $\mathbb{F}_p$. If both curves are defined over $\mathbb{F}_p$ the image of α has index 2 in $\mathrm{SO}(\mathrm{Hom}(E', E))$.*

Proof. — We choose quasi-isogenies $\varphi\colon E \to E_0$ and $\varphi'\colon E' \to E_0$ of the same degree. Set $\Lambda = \varphi\,\mathrm{Hom}(E', E)\varphi'^{-1} \subset D$, $O_l := O_l(\Lambda)$ and $O_r = O_r(\Lambda)$. By Lemma 1.6 we know

$$\mathrm{SO}(\Lambda) = \{\, (d, d') \in D^\times \times D^\times \mid d\Lambda = \Lambda d',\ \mathrm{Nrd}(d) = \mathrm{Nrd}(d') \,\}/\mathbb{Q}^\times$$

where $\mathbb{Q}^\times$ is embedded diagonally. Note that the condition $d\Lambda = \Lambda d'$ already implies $\mathrm{Nrd}(d) = \mathrm{Nrd}(d')$. Moreover, $d\Lambda = \Lambda d'$ implies $O_l = O_l(d\Lambda)$ and hence $d \in N_{D^\times}(O_l)$. Similarly $d' \in N_{D^\times}(O_r)$. Thus we see

$$\mathrm{SO}(\Lambda) = \{\, (d, d') \in N_{D^\times}(O_l) \times N_{D^\times}(O_r) \mid d\Lambda = \Lambda d' \,\}/\mathbb{Q}^\times.$$

For $(d, d') \in \mathrm{SO}(\Lambda)$ we have by Corollary 2.5:

$$d \in \mathbb{Q}^\times O_l^\times \iff d' \in \mathbb{Q}^\times O_r^\times. \tag{3.1}$$

Further $\mathbb{Q}^\times \cap O_l^\times = \mathbb{Q}^\times \cap O_r^\times = \{\pm 1\}$.

Now consider the case where E is not defined over $\mathbb{F}_p$. By Proposition 2.4 this is equivalent to $N_{D^\times}(O_l) = \mathbb{Q}^\times O_l^\times$. Therefore

$$\begin{aligned}\mathrm{SO}(\Lambda) &= \{\,(d,d') \in \mathbb{Q}^\times O_l^\times \times \mathbb{Q}^\times O_r^\times \mid d\Lambda = \Lambda d'\,\}/\mathbb{Q}^\times \\ &= \{\,(d,d') \in O_l^\times \times O_r^\times\,\}/\{\pm 1\}\end{aligned}$$

which proves the proposition in this case. The case that E' is not defined over $\mathbb{F}_p$ is proved by the same argument.

It remains to consider the case that E and E' are both defined over $\mathbb{F}_p$. Then $\mathbb{Q}^\times O_l^\times \subset N_{D^\times}(O_l)$ and $\mathbb{Q}^\times O_r^\times \subset N_{D^\times}(O_r)$ are subgroups of index 2 by Proposition 2.4. Moreover it follows from (3.1) that $\{\,(d,d') \in O_l^\times \times O_r^\times\,\}/\{\pm 1\}$ is a subgroup of index 2 of $\mathrm{SO}(\Lambda)$. This finishes the proof. □

Corollary 3.5. — *Let E and E' be two supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Then we have*

$$\#\mathrm{SO}(\mathrm{Hom}(E',E)) \;=\; \begin{cases} \#\operatorname{Aut}(E)\#\operatorname{Aut}(E'), & \text{if } E,\ E' \text{ both defined over } \mathbb{F}_p; \\ \frac{1}{2}\#\operatorname{Aut}(E)\#\operatorname{Aut}(E'), & \text{otherwise.} \end{cases}$$

3.4. We now sketch an alternative formulation in the language of groupoids of some of the above results suggested by the referee. We start with some general notations.

Let X be a set and let H be a group acting on X from the left. Then we denote by $[H\backslash X]$ the category whose objects are the elements of X and whose morphisms are for $x, x' \in X$

$$\mathrm{Hom}_{[H\backslash X]}(x,x') = \{\,h \in H \mid hx = x'\,\}.$$

Composition of morphisms is given by the multiplication in the group H. Clearly, this category is a groupoid (*i.e.*, every morphism is an isomorphism), and two objects $x, x' \in X$ are isomorphic if and only if they are in the same H-orbit.

If X is of the form G/H' for some group G and some subgroup H' and if H is a subgroup of G acting in the natural way on X, we have by definition

$$\mathrm{Hom}_{[H\backslash(G/H')]}(g_1H', g_2H') = G \cap g_2H'g_1^{-1}. \tag{3.2}$$

We denote by $\mathcal{M}$ the following category. The objects are supersingular elliptic curves over $\overline{\mathbb{F}}_p$. For two such supersingular elliptic curves E' and E the morphisms from E' to E in $\mathcal{M}$ are by definition the isomorphisms of elliptic curves from E' to E over $\overline{\mathbb{F}}_p$. Then Theorem 2.1 can be made more precise by saying that (2.2) induces an equivalence of categories

$$[D^\times\backslash((D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times/(\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times)] \approx \mathcal{M}.$$

This follows from (3.2) and the arguments in 3.2.

Let $\mathrm{SL}(\mathcal{O}_D)$ be the algebraic group over $\mathbb{Z}$ of elements with reduced Norm equal to 1. Then Lemma 3.1 is by 2.5 equivalent to the fact that the canonical functor

$$[\mathrm{SL}(\mathcal{O}_D)(\mathbb{Q})\backslash(\mathrm{SL}(\mathcal{O}_D)(\mathbb{A}_f)/\mathrm{SL}(\mathcal{O}_D)(\widehat{\mathbb{Z}}))] \longrightarrow [D^\times\backslash((D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times/(\mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times)]$$

is essentially surjective (which also can easily be proved directly). Moreover it follows from the definition of a morphism in the above categories that this functor is indeed an equivalence of categories.

Arguing as in the second proof of Lemma 1.6 one sees that the morphism

$$\alpha\colon \mathrm{SL}(D)\times\mathrm{SL}(D)\to\mathrm{SO}(D),\quad (d,d')\longmapsto(\delta\longmapsto d\delta d'^{-1})$$

is a surjection of algebraic groups with $\mathrm{Ker}(\alpha)=\mu_2$ (embedded diagonally in $\mathrm{SL}(D)\times\mathrm{SL}(D)$). Then α induces a functor

$$\begin{aligned} A\colon\ & [\mathrm{SL}(\mathcal{O}_D)(\mathbb{Q})\backslash(\mathrm{SL}(\mathcal{O}_D)(\mathbb{A}_f)/\mathrm{SL}(\mathcal{O}_D)(\widehat{\mathbb{Z}}))]^2 \\ & \longrightarrow [\mathrm{SO}(D)(\mathbb{Q})\backslash(\mathrm{SO}(D)(\mathbb{A}_f)/\mathrm{SO}(\mathcal{O}_D)(\widehat{\mathbb{Z}}))]. \end{aligned} \tag{3.3}$$

As we have seen, we can identify the left hand side with $\mathcal{M}\times\mathcal{M}$. The set of isomorphism classes of the right side is the set of proper classes in the genus of $\mathcal{O}_D=\mathrm{End}(E_0)$ (Corollary 1.4 and 1.5). Then Proposition 3.2 asserts that A is essentially surjective. Moreover, Proposition 3.3 describes the fibres of the induced surjective map on isomorphism classes and Proposition 3.4 is the analysis in which way A fails to be fully faithful.

Finally, Proposition 4.1 below can also be expressed in the language of groupoids using the notion of direct and inverse image for functions (or more generally for sheaves) with respect to the functor A. We omit the details.

4. Local densities

4.1. Recall that for two quadratic spaces Q and L over $\mathbb{Z}$ we write $R_L(Q)$ for the number of isometries $Q\to L$. Note that $R_L(Q)$ depends only on the classes of L and Q. In this section we are going to express

$$\sum_{(E',E)}\frac{R_{\mathrm{Hom}(E',E)}(Q)}{u_E u_{E'}} \tag{4.1}$$

in terms of local densities. Here the (E',E) runs through all pairs of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, Q is a fixed ternary positive definite quadratic form over $\mathbb{Z}$, and $u_E=\frac{1}{2}\#\mathrm{Aut}(E)$.

Proposition 4.1. — *Fix a supersingular elliptic curve E_0. Then we have*

$$\sum_{(E',E)}\frac{R_{\mathrm{Hom}(E',E)}(Q)}{u_E u_{E'}}=4\sum_L\frac{R_L(Q)}{\#\mathrm{SO}(L)}. \tag{4.2}$$

Here on the right hand side, L runs through the proper classes of the genus of $\mathrm{End}(E_0)$.

Proof. — By Proposition 3.2 we know that the proper classes $[\mathrm{Hom}(E',E)]$ exhaust the genus of $\mathrm{End}(E_0)$ if (E',E) runs through all pairs of supersingular elliptic curves. If E and E' are both defined over $\mathbb{F}_p$, the class L of $\mathrm{Hom}(E',E)$ occurs once in the sum on the left hand side of (4.2) by Proposition 3.3, and we have $\#\mathrm{SO}(L)=4u_Eu_{E'}$ by

Corollary 3.5. Otherwise, the class L of $\mathrm{Hom}(E', E)$ occurs twice in the sum on the left hand side of (4.2) and we have $\#\mathrm{SO}(L) = 2u_E u_{E'}$. This proves the proposition. □

4.2. Let M be a quadratic space over $\mathbb{Z}_p$. We denote by $Q_M \colon M \to \mathbb{Z}_p$ its quadratic form and let B_M the bilinear form given by

$$B_M(x, y) = \frac{1}{2}(Q_M(x + y) - Q_M(x) - Q_M(y)).$$

4.3. Let M and N be two quadratic spaces over $\mathbb{Z}_p$ of ranks m and n, respectively. We choose bases (μ_i) and (ν_i) of M, N respectively and let $T = (B_M(\mu_i, \mu_j)) \in \mathrm{Sym}_m(\mathbb{Z}_p)^\vee$ and $S = (B_N(\nu_i, \nu_j)) \in \mathrm{Sym}_n(\mathbb{Z}_p)^\vee$ be the corresponding matrices. For $r \geq 0$ we define $A_{p^r}(M, N) = A_{p^r}(T, S)$ as

$$\begin{aligned} &\#\{\, X \in M_{n,m}(\mathbb{Z}_p/p^r\mathbb{Z}_p) \mid {}^t XSX - T \in p^r \,\mathrm{Sym}_m(\mathbb{Z}_p)^\vee \,\} \\ =&\#\{\, \sigma \colon M/p^rM \to N/p^rN \mid Q_N(\sigma(x)) \equiv Q_M(x) \bmod p^r \,\}. \end{aligned}$$

For $r \gg 0$ we set

$$\alpha_p(M, N) = \alpha_p(T, S) = 2^{-\delta_{mn}}(p^r)^{m(m+1)/2 - mn} A_{p^r}(M, N).$$

It is shown in [**Ki**, 5.6] that this is independent of r if r is sufficiently big. We call $\alpha_p(T, S)$ the *local representation density*. Note that for $p = 2$ our representation density is $2^{m(m-1)/2}$-times the representation density α_p defined in [**Ki**].

4.4. For any class N of lattices in a positive definite quadratic space over $\mathbb{Q}$ we set

$$o(N) = \#\mathrm{O}(N), \qquad so(N) = \#\mathrm{SO}(N).$$

Moreover, we set

$$w(N) := \sum_{\substack{N' \text{ class} \\ \text{in gen}(N)}} \frac{1}{o(N')}$$

where N' runs through all classes within the genus of N. We call $w(N)$ the *weight of* N.

Then we have $o(N) = so(N)$ if and only if there exist two proper classes in N. Therefore

$$w(N) = \frac{1}{2} \sum_{\substack{N' \text{ proper class} \\ \text{in gen}(N)}} \frac{1}{so(N')}. \tag{4.3}$$

Let M and N be lattices in positive definite quadratic spaces over $\mathbb{Q}$. By the *mean value of the representation of M by N* we mean

$$m(M,N) = w(N)^{-1} \sum_{\substack{N' \text{ class} \\ \text{in } \mathrm{gen}(N)}} \frac{R_{N'}(M)}{o(N')}$$
$$= \left(\sum_{\substack{N' \text{ proper class} \\ \text{in } \mathrm{gen}(N)}} \frac{1}{so(N')} \right)^{-1} \sum_{\substack{N' \text{ proper class} \\ \text{in } \mathrm{gen}(N)}} \frac{R_{N'}(M)}{so(N')}.$$

Clearly, $m(M,N)$ depends only on the genus of N.

4.5. We recall the Minkowski-Siegel formula (cf. [**Ki**, 6.8]): Let M and N be lattices in positive definite quadratic spaces over $\mathbb{Q}$. For any prime l we define $\alpha_l(M,N) := \alpha_l(M \otimes_{\mathbb{Z}} \mathbb{Z}_l, N \otimes_{\mathbb{Z}} \mathbb{Z}_l)$. Put $m := \mathrm{rank}(M)$ and $n := \mathrm{rank}(N)$. Set

$$\epsilon_{m,n} := \begin{cases} \frac{1}{2}, & \text{if either } n = m+1 \text{ or } n = m > 1; \\ 1, & \text{otherwise.} \end{cases}$$

We also define

$$\alpha_\infty(M,N) := \pi^{m(2n-m+1)/4} \left(\prod_{i=0}^{m-1} \Gamma\big((n-i)/2\big)^{-1} \right) \times \big(\det(N)\big)^{-m/2} \big(\det(M)\big)^{(n-m-1)/2}.$$

Here Γ denotes the gamma function.

Theorem 4.2 **(Minkowski, Siegel)**

$$m(M,N) = \epsilon_{m,n} 2^{-m(m-1)/2} \alpha_\infty(M,N) \prod_l \alpha_l(M,N) \tag{4.4}$$

where l runs through all prime numbers.

Theorem 4.3. — *Let M be a positive definite ternary quadratic space over $\mathbb{Z}$ and let N be the genus of* $\mathrm{End}(E_0)$ *for a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Then*

$$\sum_{(E',E)} \frac{R_{\mathrm{Hom}(E',E)}(M)}{u_E u_{E'}} = 8 \left(\frac{p-1}{12} \right)^2 \frac{\pi^4}{p^3} \prod_l \alpha_l(M,N)$$

where l runs through all prime numbers l.

Proof. — We apply the Minkowski-Siegel formula: We have $m = 3$ and $n = 4$. We first compute $\det(N)$. As N is positive definite, it suffices to compute $\mathrm{ord}_l(N \otimes \mathbb{Z}_l)$ for every prime l. For $l \neq p$ the quadratic $\mathbb{Z}_l$-spacc $N \otimes \mathbb{Z}_l$ is isomorphic to $(M_2(\mathbb{Z}_l), \det)$

and with respect to the basis $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&0\\-1&0\end{smallmatrix}\right)$ the associated matrix is equal to

$$S_l = \frac{1}{2}\begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}. \tag{4.5}$$

For $l = p$ we have $N \otimes \mathbb{Z}_l \cong (\mathcal{O}_{D_p}, \mathrm{Nrd})$ and hence there exists a basis such that the associated matrix is equal to

$$S_p = \begin{cases} \mathrm{diag}(1, -\delta, p, -\delta p), & \text{if } p \neq 2, \\ \begin{pmatrix} 1 & 1/2 & & \\ 1/2 & 1 & & \\ & & 2 & 1 \\ & & 1 & 2 \end{pmatrix}, & \text{if } p = 2, \end{cases} \tag{4.6}$$

where δ is some element in $\mathbb{Z}_p^\times \setminus (\mathbb{Z}_p^\times)^2$ (see [**Ki**, 5.2]).

If follows that $\det(N)$ is equal to $2^{-4}p^2$ and hence we get

$$\alpha_\infty(M, N) = \frac{\pi^{9/2}}{\Gamma(1)\Gamma(3/2)\Gamma(2)}(2^{-4}p^2)^{-3/2} = 2^7\frac{\pi^4}{p^3}.$$

By (4.3) we can calculate the weight of N as

$$w(N) = \frac{1}{2}\sum_{\substack{N' \text{ proper class} \\ \text{in } \mathrm{gen}(N)}} \frac{1}{so(N')}.$$

Using Proposition 3.3 and Corollary 3.5, it follows that

$$\begin{aligned} w(N) &= \frac{1}{2}\sum_{(E',E)} \frac{1}{\#\operatorname{Aut}(E)\#\operatorname{Aut}(E')} \\ &= \frac{1}{2}\left(\sum_E \frac{1}{\#\operatorname{Aut}(E)}\right)^2 \\ &= \frac{1}{2}\left(\frac{p-1}{24}\right)^2 \end{aligned}$$

where in the last equality we used Eichler's mass formula.

Now using Proposition 4.1, the Minkowski-Siegel formula tells us

$$\begin{aligned}\sum_{(E',E)} \frac{R_{\mathrm{Hom}(E',E)}(M)}{u_E u_{E'}} &= 4 \sum_{\substack{N' \text{ in proper class} \\ \text{of gen}(N)}} \frac{R_{N'}(M)}{\#\mathrm{SO}(N')} \\ &= 8w(N)m(M,N) \\ &= 4\left(\frac{p-1}{24}\right)^2 \epsilon_{3,4} 2^{-3} \alpha_\infty(M,N) \prod_l \alpha_l(M,N) \\ &= 8\left(\frac{p-1}{12}\right)^2 \frac{\pi^4}{p^3} \prod_l \alpha_l(M,N). \qquad \square\end{aligned}$$

4.6. In [**Wd2**] we will give explicit expressions for the local representation densities $\alpha_l(M,N)$ for arbitrary positive definite ternary quadratic spaces M and all primes l. We deduce (cf. [**GK**, 6.23]):

Corollary 4.4. — *Define* $\beta_l(M) = (1-l^{-2})^{-2}\alpha_l(M,N)$ *and* $\Delta(M) = 4\det(M)$. *Assume that* M *is a positive definite ternary quadratic space over* $\mathbb{Z}$ *which is isotropic over* $\mathbb{Q}_l$ *for all* $l \neq p$. *Then* M *is anisotropic over* $\mathbb{Q}_p$ *and*

$$\sum_{(E',E)} \frac{R_{\mathrm{Hom}(E',E)}(M)}{u_E u_{E'}} = 4 \prod_{l|\Delta(M), l\neq p} \beta_l(M).$$

Proof. — We have $\alpha_p(M,N) = 2(p+1)^2 p^{-1}$ by [**Wd2**, Theorem 1.1], and hence $\beta_p(M) = 2p^3/(p-1)^2$. Moreover we know by [**Wd2**, Corollary 2.2], that $\beta_l(M) = 1$ for all $l \neq p$ which do not divide $\Delta(M)$. Therefore we have

$$\begin{aligned}\prod_l \alpha_l(M,N) &= \frac{2p^3}{(p-1)^2} \prod_l (1-l^{-2})^2 \prod_{l|\Delta(M), l\neq p} \beta_l(M) \\ &= \frac{2p^3}{(p-1)^2} \zeta(2)^{-2} \prod_{l|\Delta(M), l\neq p} \beta_l(M).\end{aligned}$$

As $\zeta(2) = \pi^2/6$, the corollary follows from Theorem 4.3. $\square$

References

[Do] D. Dorman – Global orders in definite quaternion algebras as endomorphism rings for reduced CM elliptic curves, in *Théorie des nombres (Quebec, PQ, 1987)*, de Gruyter, Berlin, 1989, p. 108–116.

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Inventiones Math.* **112** (1993), p. 225–245.

[GZ] B. Gross & D. Zagier – On singular moduli, *J. Reine Angew. Math.* **355** (1985), p. 191–220.

[Ki] Y. Kitaoka – *Arithmetic of quadratic forms*, Cambridge University Press, 1993.

[Mi] J. MILNE – Points on Shimura varieties mod p, in *Automorphic forms, representations and L-functions (Oregon State Univ., Corvallis, 1977), Part 2*, Proc. Sympos. Pure Math., p. 165–184.

[Wd2] T. WEDHORN – Calculation of representation densities, this volume, p. 179–190.

T. WEDHORN, Institut für Mathematik der Universität Paderborn, Warburger Straße 100, 33098 Paderborn, Germany • *E-mail :* wedhorn@math.uni-paderborn.de
Url : www2.math.uni-paderborn.de/people/torsten-wedhorn.html

Astérisque
312, 2007, p. 49–55

6. LUBIN-TATE FORMAL GROUPS

by

Volker Meusers

Abstract. — We give an exposition of the theory of formal complex multiplication in local fields after Lubin and Tate. We recall the construction of Lubin-Tate modules, the structure of torsion points of their generic fibre and explicit local class field theory. We follow the original exposition of Lubin and Tate, and the exposition in Neukirch's book.

***Résumé* (Groupes formels de Lubin-Tate).** — Nous donnons une exposition de la théorie de la multiplication complexe formelle dans les corps locaux d'après Lubin et Tate. On rappelle la construction des modules de Lubin-Tate, la structure de leurs modules de torsion de leur fibre générique et la théorie du corps de classes locale explicite. On suit l'article original de Lubin et Tate, et le livre de Neukirch.

1. Construction of Lubin-Tate Modules

Let K be a field complete with respect to some discrete valuation. Let $\mathcal{O}_K$ be its ring of integers, $\mathfrak{p}$ its maximal ideal. Assume the residue field $\mathcal{O}_K/\mathfrak{p}$ to be finite and let q be the number of its elements. Prime elements of $\mathcal{O}_K$ are denoted by π or $\overline{\pi}$. Let k be an algebraic closure of $\mathcal{O}_K/\mathfrak{p}$. Let K^{sep} be a fixed separable closure of K and $K^{\mathrm{nr}} \subseteq K^{\mathrm{sep}}$ the maximal unramified extension of K. Let M and C denote the completions of K^{nr} and K^{sep}. Denote by $\mathcal{O}_M$ (resp. $\mathcal{O}_C$) the ring of integers of M (resp. C). Let $\widehat{\mathcal{C}}$ be the category of complete local noetherian $\mathcal{O}_K$-algebras with residue field k.

Definition 1.1. — Let $i\colon \mathcal{O}_K \to R$ be an $\mathcal{O}_K$-algebra, e.g. $\mathcal{O}_K$, $\mathcal{O}_M$ or k. A formal $\mathcal{O}_K$-module over R is a pair (H, γ_H) consisting of a (one-dimensional commutative) formal group law $H(X,Y) \in R[[X,Y]]$ together with a ring homomorphism

2000 ***Mathematics Subject Classification.*** — 11S31, 14K22, 14L05.
Key words and phrases. — Lubin-Tate formal groups, local class field theory, complex multiplication.

$\gamma_H\colon \mathcal{O}_K \to \mathrm{End}_R(H) \subset R[[T]]$ given by sending an element $a \in \mathcal{O}_K$ to the endomorphism $\gamma_H(a)(T) \in R[[T]]$ of $H(X,Y)$. As a normalization condition we require that the $\mathcal{O}_K$-algebra structure on R induced by the isomorphism

$$\mathcal{O}_K \xrightarrow{\cong} \mathrm{Lie}(H),\ a \longmapsto \left.\frac{\partial \gamma_H(a)(T)}{\partial T}\right|_{T=0}.$$

agrees with the structure given by $i\colon \mathcal{O}_K \to R$, in other words we require $\gamma_H(a)(T)$ to be of the form

$$\gamma_H(a)(T) = i(a)T + \cdots \in R[[T]].$$

We write $[a](T)$ for $\gamma_H(a)(T)$ and $a = i(a) \in R$ if no confusion is possible.

For $R \in \widehat{\mathcal{C}}$ write $H(R)$ for the abelian group $(\mathfrak{m}_R, +_H)$ where we have set $x +_H y = H(x,y)$ for $x, y \in \mathfrak{m}_R$. This converges since R is assumed to be complete. This group is also an (ordinary) $\mathcal{O}_K$-module by setting $ax = a \cdot_H x = [a](x)$. Note that unless (H, γ_H) is the formal additive group, *i.e.*, $(\widehat{\mathbb{G}}_a(X,Y) = X+Y, \gamma_{\widehat{\mathbb{G}}_a}(a)(T) = aT)$, this $\mathcal{O}_K$-module structure is not the standard structure on $\mathfrak{m}_R$ as an ideal of R. For a finite extension $L|K$ with ring of integers $\mathcal{O}_L \in \widehat{\mathcal{C}}$ and maximal ideal $\mathfrak{m}_L \subset \mathcal{O}_L$ we set $H(L) = H(\mathfrak{m}_L)$. Similarly for infinite extensions after completion.

The goal of this section is to construct, as for ordinary complex multiplication (see Remark 3.5 below), a formal $\mathcal{O}_K$-module (G, γ_G) over $\mathcal{O}_M$ such that

$$G[\mathfrak{p}] = \bigcap_{a \in \mathfrak{p}} \mathrm{Ker}(a) = G[\pi]$$

is isomorphic to the kernel of the Frobenius $G \otimes k \to (G \otimes k)^{(q)}$ when reduced modulo the maximal ideal of $\mathcal{O}_M$. Lubin and Tate construct G as a base change $G = H_\pi \otimes_{\mathcal{O}_K} \mathcal{O}_M$ of a formal $\mathcal{O}_K$-module H_π over $\mathcal{O}_K$, the so called Lubin-Tate module associated to the prime element $\pi \in \mathcal{O}_K$. As we will see H_π depends on the chosen π while G will be independent of it.
By our normalization condition $\gamma_G(\pi)(T)$ is of the form

$$\gamma_G(\pi)(T) = \pi T + \cdots \in \mathcal{O}_K[[T]].$$

The condition on the Frobenius requires that

$$\gamma_G(\pi)(T) \equiv T^q \bmod \pi.$$

This justifies the following definition:

Definition 1.2. — A power series $f(T) = \pi T + \cdots \in \mathcal{O}_K[[T]]$ such that

$$f(T) \equiv T^q \bmod \pi$$

is called a Lubin-Tate series associated to π. The set of Lubin-Tate series for π is denoted by $\mathcal{F}_\pi$. A formal $\mathcal{O}_K$-module (H, γ_H) over $\mathcal{O}_K$ with $\gamma_H(\pi)(T) \in \mathcal{F}_\pi$ is called Lubin-Tate module.

Examples 1.3

(1) The simplest example of a Lubin-Tate-series is

$$f(T) = \pi T + T^q \in \mathcal{F}_\pi.$$

(2) In the cyclotomic case, *i.e.*, for $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$ and $\pi = p \in \mathbb{Z}_p$ the polynomial

$$f(T) = (T+1)^p - 1 = pT + p(\dots) + T^p \in \mathcal{F}_\pi.$$

is a Lubin-Tate-series associated to $\pi = p$. One easily checks that in this case the formal multiplicative group

$$\widehat{\mathbb{G}}_m(X,Y) = (1+X)(1+Y) - 1$$

is a Lubin-Tate module associated to $f(T)$.

The construction of Lubin-Tate-modules is based on the following lemma.

Lemma 1.4. — *Let $\pi, \overline{\pi}$ be two prime elements of M and $f(T) \in \mathcal{F}_\pi$ resp. $g(T) \in \mathcal{F}_{\overline{\pi}}$. Let $L(X_1, \dots, X_n) = \sum_{i=1}^n a_i X_i$ be a linear form with coefficients in $\mathcal{O}_M$ such that*

$$\pi L(X_1, \dots, X_n) = \overline{\pi} L^\sigma(X_1, \dots, X_n)$$

where σ is the continuous extension of the Frobenius in $\mathrm{Gal}(K^{nr}|K)$ to M. Then there exists a unique power series $F(X_1, \dots, X_n) \in \mathcal{O}_M[[X_1, \dots, X_n]]$ such that

$$F(X_1, \dots, X_n) \equiv L(X_1, \dots, X_n) \bmod (X_1, \dots, X_n)^2 \tag{1.1}$$

and

$$f(F(X_1, \dots, X_n)) = F^\sigma(g(X_1), \dots, g(X_n)). \tag{1.2}$$

where $(X_1, \dots, X_n)$ denotes the ideal generated by $X_1, \dots, X_n$. If the coefficients of f, g, L lie in $\mathcal{O}_K$ then F also has coefficients in $\mathcal{O}_K$.

The idea of the proof is to construct F inductively modulo powers of the ideal generated by $X_1, \dots, X_n$ and then use the completeness of the power series ring. The induction starts with (1.1). For the induction step one plugs in (1.2) and uses that f and g are Lubin-Tate series to see that the coefficients are in $\mathcal{O}_M$. See [**N**] for a detailed proof.

We use the lemma to construct Lubin-Tate modules as follows:
For $f(T) \in \mathcal{F}_\pi$ let $H_f(X,Y)$ be the unique solution of the equations

$$H_f(X,Y) \equiv X + Y \bmod (X,Y)^2$$

and

$$f(H_f(X,Y)) \equiv H_f(f(X), f(Y))$$

For each $a \in \mathcal{O}_K$ and $f(T), g(T) \in \mathcal{F}_\pi$ let $[a]_{f,g}(T)$ be the unique solution of

$$[a]_{f,g}(T) \equiv aT \bmod T^2$$

and

$$f([a]_{f,g}(T)) \equiv [a]_{f,g}(g(T))$$

To simplify notations we shall write $[a]_f$ instead of $[a]_{f,f}$. The following theorem shows that the series $H_f(X,Y)$ together with $\gamma_{H_f}(a)(T) = [a]_f(T)$ is in fact a Lubin-Tate module associated to $f(T)$.

Theorem 1.5. — *For any $f(T) \in \mathcal{F}_\pi$ the series $H_f(X,Y)$ is a formal group law over $\mathcal{O}_K$, i.e., the following identities hold:*

$$\begin{aligned} H_f(X,Y) &= H_f(Y,X) \\ H_f(H_f(X,Y),Z) &= H_f(X,H_f(Y,Z)) \\ H_f(X,0) &= X \\ H_f(0,Y) &= Y \\ H_f(X,[-1]_f(X)) &= 0. \end{aligned}$$

For $g,h \in \mathcal{F}_\pi$ and $a,b \in \mathcal{O}_K$ we have

$$\begin{aligned} H_f([a]_{f,g}(X),[a]_{f,g}(Y)) &= [a]_{f,g}(H_g(X,Y)) \\ [a]_{f,g}([b]_{g,h}(T)) &= [ab]_{f,h}(T) \\ [a+b]_{f,g}(T) &= H_f([a]_{f,g}(T),[b]_{f,g}(T)) \\ [\pi]_f(T) &= f(T) \\ [1]_f(T) &= T. \end{aligned}$$

In particular $(H_f(X,Y),\gamma_{H_f})$ with $\gamma_{H_f}(a)(T) = [a]_f(T)$ is a Lubin-Tate-module such that $\gamma_{H_f}(\pi)(T) = f(T)$. For two series $f(T),g(T) \in \mathcal{F}_\pi$ we have the canonical isomorphism

$$[1]_{f,g}(T)\colon H_g \xrightarrow{\cong} H_f$$

of formal $\mathcal{O}_K$-modules over $\mathcal{O}_K$.

The equalities in the Theorem are all true modulo squares and follow from the uniqueness assertion of Lemma 1.4. For a detailed proof see [**N**, proof of Theorem V.4.6].

Remark 1.6. — Although H_f does not depend on the particular choice $f \in \mathcal{F}_\pi$ it does depend on the particular choice of the uniformizing element $\pi \in \mathcal{O}_K$. They become isomorphic over $\mathcal{O}_M$ because of the following lemma.

Lemma 1.7. — *Let π and $\overline{\pi}$ be two prime elements of $\mathcal{O}_K$ with $\pi = u\overline{\pi}$ for some unit $u \in \mathcal{O}_K^\times$. Let σ be the Frobenius of M as above. There exists some $\epsilon \in \mathcal{O}_M^\times$ such that $u = \epsilon^{\sigma-1}$. Let $f(T) \in \mathcal{F}_\pi$ and $g(T) \in \mathcal{F}_{\overline{\pi}}$ be Lubin-Tate series. Then there exists a unique power series $\theta(X) \in \mathcal{O}_M[[X]]$ such that $\theta(X) = \epsilon X$ modulo $(X)^2$ and $f \circ \theta = \theta^\sigma \circ g$. Furthermore $\theta(X)$ induces an isomorphism $H_g \xrightarrow{\cong} H_f$ of Lubin-Tate modules (defined over $\mathcal{O}_M$).*

This is proved using Lemma 1.4. For a detailed proof see [**N**, Corollary V.2.3], and also [**LT**, Lemma 2].

2. Torsion points of the Generic Fibre

Now fix some $f \in \mathcal{F}_\pi$. We want to describe the structure of torsion points of the generic fibre of $H_f(C)$ as a Galois module. Recall that for every separable algebraic extension $K \subset L \subset C$ we set $H_f(L) = H_f(\widehat{\mathcal{O}}_L)$. If $L_1 \subset L$ then $H_f(L_1) \subset H_f(L)$. If $L|L_1$ is Galois then $\mathrm{Gal}(L|L_1)$ operates naturally on $H_f(L)$ in a manner compatible with the $\mathcal{O}_K$-module structure. This results from the fact that the Galois group operates continuously on $\widehat{\mathcal{O}}_L$ and that H_f is defined over $\mathcal{O}_K \subseteq \mathcal{O}_{L_1}$. In this way $H_f(L)$ becomes a $\mathrm{Gal}(L|L_1) \times \mathcal{O}_K$-module. For another $g \in \mathcal{F}_\pi$ the canonical map induced by $[1]_{f,g}(T)$ is an isomorphism of $\mathrm{Gal}(L|L_1) \times \mathcal{O}_K$-modules. It commutes with the inclusions $H_f(L_1) \subset H_f(L)$.

Set

$$\Lambda_f = \bigcup_{m \geq 0} H_f(C)[\mathfrak{p}^m] \subset H_f(C)$$

Then Λ_f is a torsion $\mathcal{O}_K$-module, *i. e.*, the union over its sub-modules $\Lambda_{f,m} = \Lambda_f[\mathfrak{p}^m]$. It is clear that the Galois extension $K \subset L_{\pi,m} = K(\Lambda_f[m])$ does not depend on $f \in \mathcal{F}_\pi$. Let us denote its Galois group by $G_{\pi,m} = \mathrm{Gal}(L_{\pi,m}|K)$.

Theorem 2.1. — *Let π be a prime element of $\mathcal{O}_K$ and $f \in \mathcal{F}_\pi$.*
(1) The $\mathcal{O}_K$-module Λ_f is divisible.
(2) For each m, the $\mathcal{O}_K$-module $\Lambda_{f,m}$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}^m$.
(3) The $\mathcal{O}_K$-module Λ_f is isomorphic to $K/\mathcal{O}_K$.
(4) For each $\tau \in G_\pi$ there exists a unique $u_\tau \in \mathcal{O}_K^\times$ such that $\tau\lambda = [u_\tau]_f(\lambda)$ for every λ in Λ_f.
(5) The map $\tau \mapsto u_\tau$ is an isomorphism of G_π onto the group $\mathcal{O}_K^\times$, under which the quotients $G_{\pi,m}$ of G_π correspond to the quotients $\mathcal{O}_K^\times/(1+\mathfrak{p}^m)$ of $\mathcal{O}_K^\times$.

See [**LT**] for a proof.

Example 2.2. — In the cyclotomic case we get $1 + \Lambda_{f,m} = \mu_{p^m}$, $1 + \Lambda_f = \mu_{p^\infty}$. We have $\widehat{\mathbb{G}}_m(\mathbb{Q}_p) = p\mathbb{Z}_p$ with addition given by the identification with $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ as a multiplicative subgroup. In this case the multiplicative structure is given by exponentiating, *i.e.*,

$$[a]_f(T) = \sum_{n=1}^{\infty} \binom{a}{n} T^n = (1+T)^a - 1$$

for $a \in \mathbb{Z}_p$.

3. Local Class Field Theory

Let $\pi \in \mathcal{O}_K$ be a fixed prime element. Since L_π is totally ramified over K, it is linearly disjoint from K^{nr} over K, and the Galois group $\mathrm{Gal}(L_\pi K^{\mathrm{nr}}|K)$ is the product of $G_\pi = \mathrm{Gal}(L_\pi|K)$ and $\mathrm{Gal}(K^{\mathrm{nr}}|K)$. For each prime π in $\mathcal{O}_K$, we can therefore define a homomorphism

$$\rho_\pi \colon K^\times \longrightarrow \mathrm{Gal}(L_\pi K^{\mathrm{nr}}|K)$$

such that
(1) For each unit $u \in \mathcal{O}_K^\times$, the automorphism $\rho_\pi(u)$ is the identity on K^{nr}, and on L_π the reciprocal τ_u^{-1} of the element $\tau_u \in G_\pi$ corresponding to u by the isomorphism of the theorem; and
(2) $\rho_\pi(\pi)$ is the identity on L_π and is the Frobenius automorphism σ on K^{nr}.

Thus for an arbitrary element $a = u\pi^m \in K^\times$ we have, by definition:

$$\rho_\pi(a) = \sigma^m \text{ on } K^{\mathrm{nr}}$$

and

$$\lambda^{\rho_\pi(a)} = [u^{-1}]_f(\lambda) \text{ for } \lambda \in \Lambda_f.$$

Theorem 3.1. — *The field $L_\pi K^{nr}$ and the homomorphism ρ_π are independent of π.*

This follows easily from Lemma 1.7. See [**LT**] for a detailed proof.

Corollary 3.2. — *The field $L_\pi K^{nr}$ is the maximal abelian extension of K, and ρ_π is the reciprocity law homomorphism for it, i.e.,*

$$\rho_\pi(a) = (a, L_\pi K^{nr}|K)$$

for every $a \in K^\times$.

See [**LT**] for a proof.

Remark 3.3. — Note that while both the field L_π and the reciprocity map ρ_π can be defined in terms of a Lubin-Tate series alone, the proofs depend heavily on the extra structure given by the associated Lubin-Tate module.

Example 3.4. — In the cyclotomic case we get for $a = up^{v_p(a)} \in \mathbb{Q}_p^\times$ that

$$(a, \mathbb{Q}_p(\zeta)|\mathbb{Q}_p)(\zeta - 1) = [u^{-1}]_f(\zeta - 1)$$

or

$$(a, \mathbb{Q}_p(\zeta)|\mathbb{Q}_p)\zeta = \zeta^{u^{-1}}$$

if $\zeta = 1 + \lambda$ is a primitive p^m-th root of unity or in other words $\lambda = \zeta - 1 \in \Lambda_{f,m}$.

Remark 3.5. — There are strong analogies with the classical theory of complex multiplication and explicit reciprocity laws for imaginary quadratic fields. In fact for every single statement presented here, there is an analogous one if one replaces the Lubin-Tate modules by elliptic curves with complex multiplication. See for example [**L**].

References

[L] S. Lang – *Elliptic functions*, Addison-Wesley, 1973.

[LT] J. Lubin & J. Tate – Formal complex multiplication in local fields, *Ann. Math.* **81** (1965), p. 380–387.

[N] J. Neukirch – *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften 322, Berlin, 1999.

V. Meusers, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : meusers@math.uni-bonn.de

Astérisque
312, 2007, p. 57–66

7. FORMAL MODULI OF FORMAL $\mathcal{O}_K$-MODULES

by

Eva Viehmann & Konstantin Ziegler

Abstract. — We define formal $\mathcal{O}_K$-modules and their heights, following Drinfeld. To describe their universal deformations we introduce a formal cohomology group.

***Résumé* (Espaces de modules formels de $\mathcal{O}_K$-modules formels).** — On définit les $\mathcal{O}_K$-modules formels et leurs hauteurs, suivant Drinfeld. Pour décrire leurs déformations universelles, on introduit un groupe de cohomologie formelle.

Notation. — *Except in the proof of Lemma 2.1, all constant coefficients of power series are assumed to be 0.*

Acknowledgements. — During the preparation of Section 3 we profited from the talk given by S. Wewers in the ARGOS seminar. We thank I. Vollaard and W. Kroworsch for helpful comments on a preliminary version.

1. Formal modules

Let A, R be commutative rings with 1 and $i : A \to R$ a homomorphism. We also write a instead of $i(a)$ for the image of a under i.

Definition 1.1

1. A *formal A-module over R* is a commutative formal group law $F(X,Y) = X + Y + \cdots \in R[[X,Y]]$ together with a ring homomorphism $\gamma : A \to \mathrm{End}_R(F)$ such that the induced map $A \to \mathrm{End}_R(\mathrm{Lie}F) \cong R$ is equal to the structure map i.
2. For $a \in A$ we write $\gamma(a)(X) = [a]_F(X) = aX + \cdots \in R[[X]]$ for the corresponding endomorphism of F. We will also use the notation $X +_F Y$ instead of $F(X,Y)$.

2000 *Mathematics Subject Classification.* — 14L05, 14B12, 13D10, 14K15.
Key words and phrases. — Formal module, formal group, universal deformation.

3. A *homomorphism of formal A-modules over R* is a homomorphism $\varphi(X) : F(X,Y) \to G(X,Y)$ of formal group laws $F(X,Y), G(X,Y)$ over R such that $\varphi \circ \gamma_F(a) = \gamma_G(a) \circ \varphi$ for all $a \in A$. Denote by $\mathrm{Hom}_R(F,G)$ the set of homomorphisms from F to G.

Definition 1.2. — For $r \geq 2$ let $\nu_r = p$, if r is a power of a prime p, and $\nu_r = 1$ else. Denote by

$$C_r(X,Y) = \frac{1}{\nu_r}((X+Y)^r - X^r - Y^r)$$

the *modified binomial form* of degree r.

Consider the functor which assigns to every A-Algebra R the set of formal A-modules over R. It is represented by an algebra Λ_A which is generated by the indeterminate coefficients of the series F and $\gamma(a)$ and whose relations are those which are required by the condition that (F,γ) is a formal module. It has a natural grading: the degree of a coefficient is one less than the degree of the corresponding monomial in X,Y. It is induced by the action of $\mathbb{G}_m$ on $\mathrm{Spf}(A[[t]])$. From this description (or by an elementary calculation) one sees that the grading is compatible with concatenation of power series. The elements of the form ab with $\deg a, \deg b \geq 1$ generate a homogeneous ideal. Let $\tilde{\Lambda}_A$ be the quotient with induced grading $\tilde{\Lambda}_A = \bigoplus \tilde{\Lambda}_A^n$.

Denote by $\mathbb{G}_{a,R}$ the additive formal group law over R. With the canonical R-action $\gamma(a) = aX$, it becomes an R-module over R.

Lemma 1.3. — *If A is an infinite field, then for each formal A-module over A there exists a unique isomorphism with $\mathbb{G}_{a,A}$ whose derivative at zero equals* 1. *In this case there is a canonical isomorphism $\Lambda_A \cong A[c_1, c_2, \dots]$ as graded algebras where* $\deg c_i = i$.

To prove this lemma, one explicitly computes the desired isomorphism, compare [**D**, Prop. 1.2]. The c_i correspond to the coefficients of a homomorphism to the additive formal group law together with the standard A-module structure.

From now on let K be a complete discretely valued field with finite residue field $\mathbb{F}_q$, where $q = p^l$ for some prime p. Denote by $\mathcal{O}_K$ the ring of integers of K. Let π be a uniformizer.

Theorem 1.4. — *$\Lambda_{\mathcal{O}_K}$ and $\mathcal{O}_K[g_1, g_2, \dots]$ are non-canonically isomorphic as graded algebras where* $\deg g_i = i$.

Proof. — First we show that $\tilde{\Lambda}^{n-1}_{\mathcal{O}_K} \cong \mathcal{O}_K$ as $\mathcal{O}_K$-modules for all $n \geq 2$. For each i let F_i and $[a]_i$ denote the polynomials of degree i obtained from the universal formal module by leaving out all summands of higher degree. We write

$$F_n(X,Y) = F_{n-1}(X,Y) + \sum_{i=1}^{n-1} c_i X^i Y^{n-i}$$

and

$$[a]_n = [a]_{n-1} + h(a)X^n.$$

Then the c_i and $h(a)$ generate $\tilde{\Lambda}^{n-1}_{\mathcal{O}_K}$. As F is a formal group law, we obtain $\sum_{i=1}^{n-1} c_i X^i Y^{n-i} = \alpha C_n(X,Y)$ (compare [**H**, Lemma 1.6.6]). Note that we need here that we consider elements in $\tilde{\Lambda}_{\mathcal{O}_K}$ and not in $\Lambda_{\mathcal{O}_K}$ itself. In particular, $\tilde{\Lambda}^{n-1}_{\mathcal{O}_K}$ is generated by α and $h(a)$. The condition that $\gamma : \mathcal{O}_K \to \mathrm{End}(F)$ is a homomorphism implies that modulo $(X,Y)^{n+1}$ we have

$$[ab]_{n-1}(X) + h(ab)X^n = [a]_{n-1}([b]_{n-1}(X) + h(b)X^n) + h(a)(bX)^n,$$

$$F_{n-1}([a]_{n-1}(X) + h(a)X^n, [b]_{n-1}(X) + h(b)X^n) + \alpha C_n(aX, bX) = [a+b]_{n-1}(X) + h(a+b)X^n,$$

and

$$[a]_{n-1}(F_{n-1}(X,Y) + \alpha C_n(X,Y)) + h(a)(X+Y)^n = F_{n-1}([a]_{n-1}(X) + h(a)X^n, [a]_{n-1}(Y) + h(a)Y^n) + \alpha C_n(aX, aY).$$

In $\tilde{\Lambda}^{n-1}_{\mathcal{O}_K}$ this leads to the relations

$$ah(b) + b^n h(a) = h(ab) \tag{1.1}$$

$$h(a+b) - h(a) - h(b) = \alpha C_n(a,b) \tag{1.2}$$

$$(a^n - a)\alpha = \begin{cases} h(a) & \text{if } n \text{ is not a power of a prime} \\ h(a)p' & \text{if } n = p'^l, \end{cases} \tag{1.3}$$

and these are all relations between the generators α, $h(a)$ of $\tilde{\Lambda}^{n-1}_{\mathcal{O}_K}$. If n is invertible in $\mathcal{O}_K$, then (1.3) shows that each $h(a)$ is a multiple of α. If n is a power of p (where $q = p^l$) but not of q itself, then there exists an $a \in \mathcal{O}_K$ with $a^n - a \notin (\pi)$. From (1.1) we obtain $(a^n - a)h(b) = (b^n - b)h(a)$, thus $h(b)$ is a multiple of $h(a)$. Finally (1.2) shows that α is also a multiple of $h(a)$. Now let n be a power of q. By choosing $h(a) \mapsto (a^n - a)/\pi$ and $\alpha \mapsto p/\pi$ we define an epimorphism of $\mathcal{O}_K$-modules $\tilde{\Lambda}^{n-1}_{\mathcal{O}_K} \to \mathcal{O}_K$. It is well defined as (1.1)-(1.3) are the only relations of $\tilde{\Lambda}^{n-1}_{\mathcal{O}_K}$. It remains to prove that $\tilde{\Lambda}^{n-1}_{\mathcal{O}_K}$ is generated by $h(\pi)$. Let $M = \tilde{\Lambda}^{n-1}_{\mathcal{O}_K}/(h(\pi))$, and denote by $\overline{x} \in M$ the image of $x \in \tilde{\Lambda}^{n-1}_{\mathcal{O}_K}$. Then (1.1) shows that $\pi\overline{h(b)} = \overline{h(\pi b)} = \pi^n \overline{h(b)}$, thus $\overline{h(\pi b)} = 0$ for all $b \in \mathcal{O}_K$. Besides, (1.3) shows $(\pi^n - \pi)\overline{\alpha} = \overline{h(\pi)p} = 0$, hence $\pi\overline{\alpha} = 0$, and M is an $\mathbb{F}_q$-vector space. As n is a power of q, (1.1) reduces to $a\overline{h(b)} + b\overline{h(a)} = \overline{h(ab)}$. This shows

$$\overline{h(a)} = \overline{h(a^n)} = n\overline{a^{n-1}h(a)} = 0$$

for all a. Then (1.2) implies that $C_n(a,b)\overline{\alpha} = 0$ for all $a, b \in \mathbb{F}_q$. By [**H**, Lemma 21.3.2], there is an $x \in \mathbb{F}_p$ with $C_n(x,1) \neq 0$ in $\mathbb{F}_p$. Thus $\overline{\alpha} = 0$ and $M = 0$.

Hence in all cases $\tilde{\Lambda}^{n-1}_{\mathcal{O}_K} \cong \mathcal{O}_K$, and we have an epimorphism of graded algebras $\mathcal{O}_K[g_1, g_2, \dots] \to \Lambda_{\mathcal{O}_K}$. Here g_i is a lift of a generator of $\tilde{\Lambda}^i_{\mathcal{O}_K}$. The construction of the isomorphism $\Lambda_K \cong K[c_1, c_2, \dots]$ in Lemma 1.3 implies that the canonical morphism $\Lambda_{\mathcal{O}_K} \otimes K \to K[c_1, c_2, \dots]$ which is compatible with the grading is also surjective. Comparing dimensions one sees that the epimorphism $\mathcal{O}_K[g_1, g_2, \dots] \to \Lambda_{\mathcal{O}_K}$ is an isomorphism. □

2. Heights

Let $\mathcal{O}_K$ be as above and let R be a local $\mathcal{O}_K$-algebra of characteristic p with residue field k.

Lemma 2.1. — *Let F, G be formal $\mathcal{O}_K$-modules over R and let $\alpha \in \mathrm{Hom}_R(F,G) \setminus \{0\}$. Then there is a unique integer $h = \mathrm{ht}(\alpha) \geq 0$ and $\beta \in R[[X]]$ with $\alpha(X) = \beta(X^{q^h})$ and $\beta'(0) \neq 0$. The integer h is called the* height $\mathrm{ht}(\alpha)$ *of α.*

This lemma is analogous to the corresponding result over a field, compare [**H**, 18.3.1]. For $\alpha = 0$ we set $\mathrm{ht}(\alpha) = \infty$.

Proof. — We first show that $\alpha(X) = \beta(X^{p^n})$ for some β with $\beta'(0) \neq 0$. To do this we assume $\alpha(X) \neq 0$ with $(\partial\alpha/\partial X)(0) = 0$ and show that $\alpha(X) = \beta(X^p)$ for some homomorphism β of (not necessarily the same) formal group laws. The claim then follows by induction.

Partial differentiation of $\alpha(F(X,Y)) = G(\alpha(X), \alpha(Y))$ with respect to Y gives

$$\frac{\partial\alpha}{\partial X}(F(X,Y))\frac{\partial F}{\partial Y}(X,Y) = \frac{\partial G}{\partial Y}(\alpha(X),\alpha(Y))\frac{\partial\alpha}{\partial X}(Y).$$

Substituting $Y = 0$ and using $(\partial\alpha/\partial X)(0) = 0$ we obtain

$$\frac{\partial\alpha}{\partial X}(X)\frac{\partial F}{\partial Y}(X,0) = 0.$$

As $(\partial F/\partial Y)(X,0) = 1 + a_1X + \cdots \in R[[X]]^\times$, we obtain $\frac{\partial\alpha}{\partial X}(X) = 0$. Hence $\alpha(X) = \beta(X^p)$ for some $\beta \in R[[X]]$. Let σ_*F be the formal group law obtained from F by raising each coefficient to the pth power. Then an easy calculation shows that β is a homomorphism from σ_*F to G.

We now have to show that p^n is a power of q. Let $a \in \mathcal{O}_K$. Then

$$[a]_G(\alpha(X)) = \alpha([a]_F(X)) = \beta'(0)i(a)^{p^n}X^{p^n} + \cdots$$

and on the other hand

$$[a]_G(\alpha(X)) = \beta'(0)i(a)X^{p^n} + \cdots .$$

This implies $\beta'(0)(i(a) - i(a^{p^n})) = 0$ with $\beta'(0) \neq 0$, hence $i(a) - i(a^{p^n}) = i(a - a^{p^n})$ maps to 0 in k. Thus $a^{p^n} = a$ for all $a \in \mathbb{F}_q$ and p^n is a power of q. □

Definition 2.2. — The *height* of a formal $\mathcal{O}_K$-module F over R is

$$\mathrm{ht}(F) = \begin{cases} h & \text{if } [\pi]_F \text{ has height } h \\ \infty & \text{if } [\pi]_F = 0. \end{cases}$$

Remark 2.3. — This definition is different from the definition of height of a formal module given in [**H**], where it is defined as the height of the reduction of the module over the residue field.

Lemma 2.4. — *Let R be as above and let (F, γ_F) be the formal $\mathcal{O}_K$-module corresponding to a homomorphism $\varphi : \Lambda_{\mathcal{O}_K} \to R$. Then* $\mathrm{ht}(F) = \min\{i | \varphi(g_{q^i-1}) \neq 0\}$.

Proof. — In the proof of Theorem 1.4 we identified the generator g_{q^i-1} of $\tilde{\Lambda}_{\mathcal{O}_K}^{q^i-1}$ with the coefficient of X^{q^i} of $[\pi](X)$. □

The following lemma reduces the examination of formal modules over fields and of their deformations to formal modules of an especially simple form. For a proof see [**D**, Prop. 1.7].

Lemma 2.5. — *Let (F,γ) be a formal $\mathcal{O}_K$-module of height $h<\infty$ over a separably closed field k of characteristic $p>0$. Then F is isomorphic to a formal module (F',γ') over k with*

$$\begin{aligned} F'(X,Y) &\equiv X+Y \pmod{\deg q^h},\\ [a]_{F'}(X) &\equiv aX \pmod{\deg q^h},\\ [\pi]_{F'}(X) &= X^{q^h}. \end{aligned}$$

Such modules are called normal modules.

Fix an integer $h>1$ and let F_0 be a formal $\mathcal{O}_K$-module of height h over k. Assume that R is a local artinian $\mathcal{O}_K$-algebra with maximal ideal $\mathfrak{m}$ and residue field k. Let $I \lhd R$ be an ideal. We set $\overline{R}=R/I$. If F is a lift of F_0 over R, we set $\overline{F}:=F\otimes_R \overline{R}$.

Lemma 2.6. — *Let F,G be lifts of F_0 over R. Then the reduction map*

$$\mathrm{Hom}_R(F,G)\to \mathrm{Hom}_{\overline{R}}(\overline{F},\overline{G}) \tag{2.1}$$

is injective.

Proof. — The reduction map in (2.1) is the composition of finitely many maps

$$\mathrm{Hom}_{R_{n+1}}(F\otimes R_{n+1}, G\otimes R_{n+1})\to \mathrm{Hom}_{R_n}(F\otimes R_n, G\otimes R_n),$$

where $R_n=R/I_n$ with $I_n=I\cap\mathfrak{m}^n$. We may therefore assume that $\mathfrak{m}\cdot I=0$. Then I is a finite dimensional k-vector space, and we have $I^2=0$. Let $\alpha(X)=a_1X+a_2X^2+\dots$ be a homomorphism from F to G such that $\alpha(X)\equiv 0 \pmod I$. We get

$$\alpha([\pi]_F(X))=[\pi]_G(\alpha(X))=0.$$

Since $\mathrm{ht}(F_0)<\infty$, we have $[\pi]_F(X)\not\equiv 0 \pmod{\mathfrak{m}}$, thus $\alpha=0$ which proves the lemma. □

From now on we may consider $\mathrm{Hom}_R(F,G)$ as a subset of $\mathrm{Hom}_{\overline{R}}(\overline{F},\overline{G})$.

3. Deformations of modules, formal cohomology

Let F be a formal $\mathcal{O}_K$-module of height $h<\infty$ over k, and let M be a finite dimensional k-vector space. A *symmetric 2-cocycle* of F with coefficients in M is a

collection of power series $\Delta(X,Y) \in M[[X,Y]]$ and $\{\delta_a(X) \in M[[X]]\}_{a\in\mathcal{O}_K}$ satisfying

$$\Delta(X,Y) = \Delta(Y,X) \tag{3.1}$$

$$\Delta(X,Y) + \Delta(F(X,Y),Z) = \Delta(Y,Z) + \Delta(X,F(Y,Z)) \tag{3.2}$$

$$\delta_a(X) + \delta_a(Y) + \Delta([a]_F(X),[a]_F(Y)) = i(a)\Delta(X,Y) + \delta_a(F(X,Y)) \tag{3.3}$$

$$\delta_a(X) + \delta_b(X) + \Delta([a]_F(X),[b]_F(X)) = \delta_{a+b}(X) \tag{3.4}$$

$$i(a)\delta_b(X) + \delta_a([b]_F(X)) = \delta_{ab}(X). \tag{3.5}$$

For any $\Psi \in M[[X]]$, the *coboundary of* Ψ is the symmetric 2-cocycle $(\Delta^\Psi, \{\delta_a^\Psi\})$ with

$$\Delta^\Psi(X,Y) = \Psi(F(X,Y)) - \Psi(X) - \Psi(Y) \tag{3.6}$$

$$\delta_a^\Psi(X) = \Psi([a]_F(X)) - i(a)\Psi(X). \tag{3.7}$$

The coboundaries form a subspace of the vector space $Z^2(F,M)$ of symmetric 2-cocycles. The quotient of the symmetric 2-cocycles by the coboundaries is a k-vector space denoted $H^2(F,M)$.

The following lemma is due to Keating, see [**K2**, Lemma 2.1].

Lemma 3.1. — *A cocycle $(\Delta;\{\delta_a\}) \in Z^2(F,M)$ is zero if and only if $\delta_\pi(X) = 0$.*

Proof. — If the cocyle is zero, then clearly $\delta_\pi(X) = 0$. Assume conversely that $\delta_\pi(X) = 0$. Substituting $a = \pi$ in (3.3) gives

$$\Delta([\pi]_F(X),[\pi]_F(Y)) = 0,$$

since $\delta_\pi(X) = 0$ and $i(\pi) = 0$. As $[\pi]_F(X) \neq 0$, this implies $\Delta(X,Y) = 0$. Condition (3.5) with $a = \pi$ together with $\delta_\pi(X) = 0$ shows $\delta_{\pi b}(X) = 0$. The same formula with $b = \pi$ and a arbitrary gives $\delta_a([\pi]_F(X)) = 0$. This implies that $\delta_a(X) = 0$, so all components of the cocycle are zero. □

In the following let R denote a local artinian $\mathcal{O}_K$-algebra with maximal ideal $\mathfrak{m}$ and residue field k. Let $I \subseteq \mathfrak{m}$ be an ideal with $\mathfrak{m}I = 0$. Then I is a k-vector space. We set $\overline{R} = R/I$. If F_0 is a formal module over k and F is a lift of F_0 over R, denote by $\overline{F} = F \otimes_R \overline{R}$ the reduction modulo I. The reduction modulo $\mathfrak{m}$ of power series over R is denoted by $\cdot^*$.

Proposition 3.2. — *In the setting above let F_0 be a formal $\mathcal{O}_K$-module over k and let $F, G \in R[[X,Y]]$ be formal $\mathcal{O}_K$-modules with $F^* = G^* = F_0$. For $\varphi(X) \in R[[X]]$ let $\overline{\varphi} \in \overline{R}[[X]]$ be the image. Assume that $\overline{\varphi}$ is a homomorphism from $\overline{F}$ to $\overline{G}$. Then*

1. *There is an element of $Z^2(F_0,I)$ defined by*
$$\Delta = \varphi(F(X,Y)) -_G \varphi(X) -_G \varphi(Y)$$
$$\delta_a = \varphi([a]_F(X)) -_G [a]_G(\varphi(X)).$$
2. *$(\Delta;\{\delta_a\}_a) = 0$ if and only if $\varphi(X) \in \mathrm{Hom}_R(F,G)$.*
3. *The class of $(\Delta;\{\delta_a\}_a)$ in $H^2(F_0,I)$ is independent of the choice of the lift φ of $\overline{\varphi}$. It vanishes if and only if $\overline{\varphi} \in \mathrm{Hom}_R(F,G) \subseteq \mathrm{Hom}_{\overline{R}}(\overline{F},\overline{G})$. If $(\Delta;\{\delta_a\})$ is the coboundary of ψ, the lift of $\overline{\varphi}$ to a homomorphism over R is given by $\varphi -_G \psi$.*

Proof. — Applying φ to the left hand side of the associativity law for F

$$(X +_F Y) +_F Z = X +_F (Y +_F Z) \tag{3.8}$$

and using the definition of Δ, we get

$$\varphi(X) +_G \varphi(Y) +_G \varphi(Z) +_G \Delta(X,Y) +_G \Delta(X +_F Y, Z). \tag{3.9}$$

Applying φ to the right hand side of (3.8), we get

$$\varphi(X) +_G \varphi(Y) +_G \varphi(Z) +_G \Delta(X, Y +_F Z) +_G \Delta(Y,Z). \tag{3.10}$$

From (3.10) and (3.9) we obtain

$$\Delta(X,Y) +_G \Delta(X +_F Y, Z) = \Delta(X, Y +_F Z) +_G \Delta(Y,Z). \tag{3.11}$$

Using the assumption $\mathfrak{m} \cdot I = 0$, we see that (3.11) implies the second cocycle rule

$$\Delta(X,Y) + \Delta(X +_{F_0} Y, Z) = \Delta(X, Y +_{F_0} Z) + \Delta(Y,Z). \tag{3.12}$$

The other cocycle rules are proved in a similar manner, replacing (3.8) by the commutativity resp. the distributivity law of F. This proves 1.

Part 2 of the proposition is a straightforward consequence of the definition of $(\Delta; \{\delta_a\})$. To prove 3., we continue with the notation used in the proof of 1. Let $\varphi'(X)$ be another lift of $\overline{\varphi}$, and let $(\Delta'; \{\delta'_a\})$ be the cocycle it defines. We can write $\varphi' = \varphi +_G \psi$, with $\psi \in I[[X]]$. Then

$$\begin{aligned} \varphi'([\pi]_F(X)) &= [\pi]_G(\varphi(X)) +_G \delta_\pi(X) +_G \psi([\pi]_F(X)) \\ &= [\pi]_G(\varphi'(X)) +_G (\delta_\pi(X) +_G \psi([\pi]_F(X))). \end{aligned}$$

For the second equality we have used that $I\mathfrak{m} = 0$. We conclude that $\delta'_\pi(X) - \delta_\pi(X) = \psi([\pi]_F(X))$ is the π-component of the coboundary of ψ. Then Lemma 3.1 implies that the two cocycles differ by the coboundary of ψ. Hence $(\Delta; \{\delta_a\})$ and $(\Delta'; \{\delta'_a\})$ lie in the same class in $H^2(F_0, I)$. It follows from 2. that this class vanishes if and only if $\overline{\varphi} \in \mathrm{Hom}_R(F,G)$. This completes the proof of 3. and the proposition. □

Lemma 3.3. — *In the setting of Proposition 3.2 let (F,γ) be a lift of F_0 to R and let $\overline{F}$ be the reduction to $\overline{R}$.*

1. *Proposition 3.2 defines a bijection between deformations of $\overline{F}$ to R and cocycles in $Z^2(F_0, I)$. Its inverse is given by assigning to $(\Delta; \{\delta_a\})$ the deformation $F_\Delta(X,Y) = X +_F Y +_F \Delta(X,Y)$ and $\gamma_\delta(a) = \gamma(a) +_F \delta_a$.*
2. *Two cocycles are in the same cohomology class if and only if the corresponding deformations are isomorphic via an isomorphism which lifts the identity of $\overline{F}$.*

Proof. — For the first assertion we have to check that $(F_\Delta, \gamma_\delta)$ is a formal module. From $I^2 = 0$ we obtain that the equations (3.1) to (3.5) also hold with F replaced by F_Δ. These equations immediately imply that $(F_\Delta, \gamma_\delta)$ is a formal module. For F_Δ, F and $\varphi = X$ we obtain the cocycle $(\Delta, \{\delta_a\})$. Then the second assertion follows from Proposition 3.2, 3. □

Corollary 3.4. — *Let F_0, R, and I be as above with $\mathrm{char}(R) = p$, $\mathrm{ht}(F_0) = h$, and $(\Delta; \{\delta_a\}) \in Z^2(F_0, I)$.*

1. *Let $g \leq h$. Then $\delta_\pi(X) \equiv 0 \pmod{X^{q^{g-1}+1}}$ if and only if $\delta_\pi \in I[[X^{q^g}]]$.*

2. *The following are equivalent:*
   (a) *The cocycle* $(\Delta; \{\delta_a\})$ *is the coboundary of some* $\psi(X) \in I[[X]]$.
   (b) $\delta_\pi \in I[[X^{q^h}]]$.
   (c) *Let* (F, γ) *be a lift of* F_0 *to a formal* $\mathcal{O}_K$*-module over* R. *Then the identity of* $\overline{F}$ *lifts to an isomorphism between* (F, γ) *and* $(F_\Delta, \gamma_\delta)$.

   If these conditions are satisfied, $(\Delta; \{\delta_a\})$ *is the coboundary of* $\psi = d \circ \beta^{-1}$ *where* $d(X^{q^h}) = \delta_\pi(X)$ *and* $\beta(X^{q^h}) = [\pi]_{F_0}(X)$.

Proof. — If $\delta_\pi(X) \equiv 0 \pmod{X^{q^{g-1}+1}}$ then

$$[\pi]_{F_\Delta}(X) = \delta_\pi(X) +_F [\pi]_F(X) \equiv 0 \pmod{(X^{q^{g-1}+1})},$$

thus $\mathrm{ht}(F_\Delta) > g - 1$. This shows that $\delta_\pi(X) = [\pi]_{F_\Delta}(X) -_F [\pi]_F(X)$ is a power series in X^{q^g}. The other assertion of 1. is trivial. The equivalence of (a) and (c) of 2. follows from Lemma 3.3. From Lemma 3.1 we see that $(\Delta; \{\delta_a\}) = (\Delta^\psi; \{\delta_a^\psi\})$ for some ψ if and only if $\delta_\pi(X) = \delta_\pi^\psi(X) = \psi([\pi]_F(X)) = \psi([\pi]_{F_0}(X))$. Here the last two equations follow from $I\mathfrak{m} = 0$. As $\mathrm{ht}(F_0) = h$, this implies (b). On the other hand assume (b) and let $d(X^{q^h}) = \delta_\pi(X)$ and $\beta(X^{q^h}) = [\pi]_{F_0}(X)$. Then the π-component of the coboundary of $\psi = d \circ \beta^{-1}$ is δ_π. □

Let $\hat{\mathcal{O}}_K^{nr}$ be the completion of the maximal unramified extension of $\mathcal{O}_K$. Denote by $\hat{\mathcal{O}}_K^{nr}[[t]] = \hat{\mathcal{O}}_K^{nr}[[t_1, \dots, t_{h-1}]]$ the power series ring over $\hat{\mathcal{O}}_K^{nr}$ in $h-1$ variables. Let $k = \hat{\mathcal{O}}_K^{nr}/(\pi)$.

Lemma 3.5. — *Let* (F, γ_F) *be a normal* $\mathcal{O}_K$*-module over* k *of height* $h < \infty$. *Then there exists a formal* $\mathcal{O}_K$*-module* (Γ, γ) *over* $\hat{\mathcal{O}}_K^{nr}[[t]]$ *which over* k *reduces to* F *with the following property: For* $1 \le i \le h-1$ *denote by* (Γ_i, γ_i) *the reduction to* $\hat{\mathcal{O}}_K^{nr}[[t]]/(t_1, \dots, t_{i-1})$. *Then*

$$\gamma_i(\pi)(X) \equiv \pi X + t_i X^{q^i} \pmod{\deg(q^i + 1)}. \tag{3.13}$$

Proof. — The module F corresponds to a map $\overline{\varphi} : \Lambda_{\mathcal{O}_K} \cong \mathcal{O}_K[g_1, g_2, \dots] \to k$ with $g_i \mapsto 0$ for all $i < q^h - 1$. Let $\varphi : \Lambda_{\mathcal{O}_K} \to \hat{\mathcal{O}}_K^{nr}$ be a lift with the same property. We choose

$$f_i = \begin{cases} t_j & \text{if } i = q^j - 1 \text{ with } 1 \le j < h-1 \\ \varphi(g_i) & \text{else.} \end{cases}$$

Let Γ be the formal $\mathcal{O}_K$-module corresponding to the map $\Lambda_{\mathcal{O}_K} \to \hat{\mathcal{O}}_K^{nr}[[t]]$ which maps g_i to f_i. Then for (Γ_i, γ_i) we see that g_{q^i-1} is the first generator which is mapped to a nonzero element in $\hat{\mathcal{O}}_K^{nr}[[t]]/(t_1, \dots, t_{i-1})$. From the description of $\tilde{\Lambda}_{\mathcal{O}_K}^{q^i-1}$ in the proof of Theorem 1.4 we see that $\gamma_i(\pi)(X)$ has the desired form. □

Note that a proof of this result can also be found in [**GH**, Section 12].

Let (F, γ_F) be a normal formal $\mathcal{O}_K$-module of height $h < \infty$ over k. Let (Γ, γ) be the deformation over $\hat{\mathcal{O}}_K^{nr}[[t]]$ defined in Lemma 3.5. Let (Γ^i, γ^i) be the reduction of (Γ, γ) to $k[[t_i]]/(t_i)^2 = R_i$ and let $(F, \gamma_F)_{R_i}$ be the base change of (F, γ_F) to R_i.

Proposition 3.6. — *For F as above we have $\dim_k H^2(F,k) = h-1$. The cocycles $(\Delta^i;\{\delta_a^i\})$ associated to the pairs of deformations $(F,\gamma_F)_{R_i}$ and (Γ^i,γ^i) with values in $t_iR_i \cong k$ satisfy*

$$\delta_\pi^i \equiv t_i X^{q^i} \pmod{\deg q^i + 1}. \tag{3.14}$$

Their classes form a basis for $H^2(F,k)$.

Proof. — Equation (3.14) immediately follows from (3.13). Corollary 3.4, 2. shows that the π-components of coboundaries are power series in X^{q^h}. Thus (3.14) implies that the classes of the cocycles $(\Delta^i;\{\delta_a^i\})$ are linearly independent in $H^2(F,k)$. Let $(\Delta;\{\delta_a\}) \in H^2(F,k)$. Then by Corollary 3.4, 1., δ_π is of the form $\beta(X^{q^g})$ with $\beta'(0) \neq 0$. If $g < h$ we subtract a suitable multiple of $(\Delta^g;\{\delta_a^g\})$ to annihilate the coefficient of X^{q^g}. In this way we can inductively represent the cocycle $(\Delta;\{\delta_a\})$ as a linear combination of the $(\Delta^i;\{\delta_a^i\})$ plus a cocycle whose π-component is congruent to 0 modulo $X^{q^{h-1}+1}$. Hence by Corollary 3.4, the cohomology class is a linear combination of the classes of the $(\Delta^i;\{\delta_a^i\})$. □

Definition 3.7. — Let R be a local ring with maximal ideal $\mathfrak{m}$. For a power series f with coefficients in R let f^* be the reduction modulo $\mathfrak{m}$. A *$*$-isomorphism* between $\mathcal{O}_K$-modules F,G over R is an isomorphism $\varphi \in \mathrm{Hom}_R(F,G)$ with $\varphi^*(X) = X$.

Let F be a fixed $\mathcal{O}_K$-module of height $h < \infty$ over $k = \hat{\mathcal{O}}_K^{nr}/(\pi)$. We consider the functor $\mathcal{D}_F$ which assigns to each complete local noetherian $\hat{\mathcal{O}}_K^{nr}$-algebra R with residue field k and maximal ideal $\mathfrak{m}$ the set of $*$-isomorphism classes of formal $\mathcal{O}_K$-modules over R that modulo $\mathfrak{m}$ reduce to F.

Theorem 3.8 **(Universal deformation)**. — *Let (F,γ_F) be an $\mathcal{O}_K$-module over k of height $h < \infty$. Then $\mathcal{D}_F$ is represented by $\hat{\mathcal{O}}_K^{nr}[[t]]$.*

Proof. — As k is separably closed, Lemma 2.5 shows that we may assume (F,γ_F) to be normal. Let (Γ,γ) be the deformation over $\hat{\mathcal{O}}_K^{nr}[[t]]$ of Lemma 3.5. Let $(\Phi,\gamma_\Phi) \in \mathcal{D}_F(R)$ for some complete local noetherian $\hat{\mathcal{O}}_K^{nr}$-algebra R with residue field k and maximal ideal $\mathfrak{m}$. As R is complete, it is enough to show that for each $r \in \mathbb{N}$ the following holds: If the projection Φ_r of Φ to $R/\mathfrak{m}^r$ corresponds to a homomorphism $\varphi_r : \hat{\mathcal{O}}_K^{nr}[[t]] \to R/\mathfrak{m}^r$, then there is a unique lift $\varphi_{r+1} : \hat{\mathcal{O}}_K^{nr}[[t]] \to R/\mathfrak{m}^{r+1}$ of φ_r corresponding to Φ_{r+1}.

Let ψ be any lift of φ_r to $R/\mathfrak{m}^{r+1}[[X]]$. Then the pair of deformations $\psi(\Gamma,\gamma)$, $(\Phi_{r+1},\gamma_{\Phi_{r+1}})$ corresponds to an element of $H^2(F,\mathfrak{m}^r/\mathfrak{m}^{r+1})$, hence to a uniquely defined linear combination of the Δ^i with coefficients a_i in $\mathfrak{m}^r/\mathfrak{m}^{r+1}$. Let $\varphi_{r+1}(t_i) = \psi(t_i) + a_i$. Then by Corollary 3.4, the deformations Φ_{r+1} and $\varphi_{r+1}(\Gamma,\gamma)$ of F over $R/\mathfrak{m}^{r+1}$ are isomorphic via an isomorphism which lifts the given isomorphism over $R/\mathfrak{m}^r$. As the classes of the Δ^i are linearly independent, φ_{r+1} is unique. □

References

[D] V. G. Drinfel'd – Elliptic modules, *Math. USSR Sbornik* **23** (1974), no. 4, p. 561–592.

[GH] B. H. Gross & M. J. Hopkins – Equivariant vector bundles on the Lubin-Tate moduli space, in *Topology and representation theory (Evanston, IL, 1992)*, Contemp. Math., vol. 158, Amer. Math. Soc., 1994, p. 23–88.

[H] M. Hazewinkel – *Formal groups and Applications*, Academic Press, 1978.

[K2] K. Keating – Lifting endomorphisms of formal A-modules, *Compos. Math.* **67** (1988), p. 211–239.

E. Viehmann, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : viehmann@math.uni-bonn.de

K. Ziegler, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : zieglerk@uni-bonn.de

Astérisque
312, 2007, p. 67–86

8. CANONICAL AND QUASI-CANONICAL LIFTINGS

by

Stefan Wewers

Abstract. — The present note gives a detailed account of the paper of Gross on canonical and quasi-canonical liftings. These are liftings of formal $\mathcal{O}$-modules with extra endomorphisms, and thus correspond to CM-points in the universal deformation space.

***Résumé* (Relèvements canoniques et quasi-canoniques).** — Nous donnons un exposé détaillé des travaux de Gross sur les relèvements canoniques et quasi-canoniques des $\mathcal{O}$-modules formels, qui correspondent aux points CM dans l'espace de déformations universel.

The present note gives a detailed account of Gross' paper [**G**] on canonical and quasi-canonical liftings. We make heavy use of results of Lubin and Tate [**LT2**] and Drinfeld [**D**] which are reviewed in [**VZ**]. All the results presented here have been generalized to the case of arbitrary finite height by J. K. Yu [**Yu**].

I thank Eva Viehmann, Inken Vollaard and Michael Rapoport for careful proofreading and helpful discussions.

1. Canonical lifts

In this section we study canonical lifts of a formal $\mathcal{O}_K$-module of height two with respect to a quadratic extension L/K. In particular, we prove the first main result of [**G**] which computes the endomorphism ring of the reduction of a canonical lift modulo some power of the prime ideal of $\mathcal{O}_K$.

2000 ***Mathematics Subject Classification.*** — 14L05, 14K22.
Key words and phrases. — Formal $\mathcal{O}$-modules, canonical liftings, Lubin-Tate theory.

1.1. Throughout this note, K denotes a field which is complete with respect to a discrete valuation v, and whose residue class field is finite, with $q = p^f$ elements. We denote by $\mathcal{O}_K$ the ring of integers of K. We fix a prime element π of K, and we assume that $v(\pi) = 1$.

Let $i : \mathcal{O}_K \to R$ be an $\mathcal{O}_K$-algebra. Recall that a *formal $\mathcal{O}_K$-module over R* is given by a commutative formal group law $F(X,Y) = X + Y + \cdots \in R[\![X,Y]\!]$ together with a ring homomorphism $\gamma : \mathcal{O}_K \to \mathrm{End}_R(F)$ such that the induced map $\mathcal{O}_K \to \mathrm{End}_R(\mathrm{Lie}F) \cong R$ is equal to the structure map i. Whenever this is not likely to be confusing, we will omit the maps i and γ from the notation. Given an element $a \in \mathcal{O}_K$, we write $[a]_F(X) = i(a)X + \cdots \in R[\![X]\!]$ for the corresponding endomorphism of F.

If F_1, F_2 are two formal $\mathcal{O}_K$-modules over R, we write $\mathrm{Hom}_R(F_1, F_2)$ for the group of homomorphisms $\alpha : F_1 \to F_2$ of formal $\mathcal{O}_K$-modules, *i.e.*, $\mathcal{O}_K$-linear homomorphisms of formal groups. Similarly, $\mathrm{End}_R(F)$ denotes the (in general non-commutative) ring of $\mathcal{O}_K$-linear endomorphisms of F. Note that $\mathrm{End}_R(F)$ is an $\mathcal{O}_K$-algebra.

1.2. Let k be an algebraic closure of the residue class field of $\mathcal{O}_K$. We regard k as an $\mathcal{O}_K$-algebra, and write $\bar{a} \in k$ for the image of an element $a \in \mathcal{O}_K$.

Let G be a formal $\mathcal{O}_K$-module over k and let $\alpha \in k[\![X]\!]$ be an endomorphism of G, with $\alpha \neq 0$. By [**VZ**, Lemma 2.1], there exists an integer $h = \mathrm{ht}(\alpha) \geq 0$, called the *height* of α, such that $\alpha(X) = \beta(X^{q^h})$, with $\beta'(0) \neq 0$. It is easy to check that the function $\mathrm{ht} : \mathrm{End}_k(G) \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ (we set $\mathrm{ht}(0) := \infty$) is a valuation on the $\mathcal{O}_K$-algebra $\mathrm{End}_k(G)$. We say that the formal $\mathcal{O}_K$-module G has *height h*, if the endomorphism $[\pi]_G$ has height h. In other words, the restriction of the valuation ht *via* the structure map $\mathcal{O}_K \to \mathrm{End}_k(G)$ is equal to $h^{-1} \cdot v$.

We recall the following fundamental result.

Theorem 1.1. — *For each natural number h, there exists a formal $\mathcal{O}_K$-module G over k of height h. It is unique up to isomorphism. The ring $\mathrm{End}_k(G)$ is isomorphic to the maximal order $\mathcal{O}_D$ of a division algebra D of dimension h^2 over K, with invariant $\mathrm{inv}(D) = 1/h$.*

Proof. — (Compare with [**D**], Proposition 1.7.) The existence of G follows from Lubin-Tate theory, as follows. Let L/K be the unramified extension of degree h. Extend the algebra map $\mathcal{O}_K \to k$ to $\mathcal{O}_L$, which gives k the structure of an $\mathcal{O}_L$-algebra. Let F be the Lubin-Tate module of $\mathcal{O}_L$ with respect to the prime element π, *i.e.*, the (unique) formal $\mathcal{O}_L$-module over $\mathcal{O}_L$ such that $[\pi]_F = \pi X + X^{q^h}$, see [**LT1**]. By restriction, we may regard F as a formal $\mathcal{O}_K$-module. Then $G := F \otimes k$ is a formal $\mathcal{O}_K$-module of height h over k.

The uniqueness of G is more difficult. See *e.g.* [**H**, Theorem 21.9.1].

Let us sketch a proof of the last statement of Theorem 1.1. Set $H := \mathrm{End}_k(G)$. We may assume that G is the reduction to k of the Lubin–Tate module for $\mathcal{O}_L$, where L/K is unramified of degree h. Since the natural map $\mathcal{O}_L = \mathrm{End}(F) \to H$ is injective (see [**VZ**, Lemma 2.6]), we have $\mathcal{O}_L \subset H$. By construction, the group law $G(X,Y) = X+Y+\dots$ and the endomorphisms $[a]_G(X) = \bar{a}X + \dots$, for $a \in \mathcal{O}_K$, are power series with coefficients in $\mathbb{F}_q$. Moreover, we have $[\pi]_G(X) = X^{q^h}$. Hence the polynomial $\Pi(X) := X^q$ defines an element $\Pi \in H$ with $\Pi^h = \pi$. One checks that

$$\Pi([a]_G(X)) = [a^\sigma]_G(\Pi(X)),$$

where $\sigma \in \mathrm{Gal}(L/K)$ is the Frobenius. From there, it is easy to see that the subalgebra $\mathcal{O}_D := \mathcal{O}_L[\Pi]$ of H is the maximal order of a division algebra D of dimension h^2 over K, with invariant $1/h$. It remains to be shown that $\mathcal{O}_D = H$.

Let $\alpha(X) = \bar{a}X + \dots$ be an element of H. Since α commutes with $[\pi]_G(X) = X^{q^h}$, the coefficients of α lie in $\mathbb{F}_{q^h} = \mathcal{O}_L/\pi\mathcal{O}_L$. Let $a \in \mathcal{O}_L$ be a lift of $\bar{a}$. Then $\alpha - [a]_G$ is an endomorphism of G with positive height, and therefore lies in the left ideal $H \cdot \Pi \subset H$. We have shown that the natural map

$$\mathcal{O}_D \longrightarrow H/(H \cdot \Pi)$$

is surjective. Now the desired equality $\mathcal{O}_D = H$ follows from the fact (which is easy to prove) that H is complete with respect to the Π-adic topology. □

1.3. For the rest of this note, we fix a formal $\mathcal{O}_K$-module G of height two over k. By Theorem 1.1, G is uniquely determined, up to isomorphism, and $\mathcal{O}_D := \mathrm{End}_k(G)$ is the maximal order in a quaternion division algebra D over K with invariant $1/2$.

Let L/K be a quadratic extension. Let π_L denote a prime element of L. By [**S**, §XIII.3, Corollaire 3], there exists a K-linear embedding $\kappa : L \hookrightarrow D$. It is unique up to conjugation by elements of $D^\times$. We choose one such embedding and consider L, from now on, as a subfield of D. Note that $\mathcal{O}_L \subset \mathcal{O}_D$. *Via* this last embedding, we may regard G as a formal $\mathcal{O}_L$-module over k. In particular, we obtain a map $\mathcal{O}_L \to \mathrm{End}(\mathrm{Lie}\, G) = k$, which extends the canonical morphism $\mathcal{O}_K \to k$.

Let A be the strict completion of $\mathcal{O}_L$ with respect to k. In other words, A is the completion of the maximal unramified extension of $\mathcal{O}_L$, together with a morphism $A \to k$ extending the morphism $\mathcal{O}_L \to k$.

Definition 1.2. — A *canonical lift* of G with respect to the embedding $\kappa : L \hookrightarrow D$ is a lift F of G over A in the category of $\mathcal{O}_L$-modules.

In more detail, a canonical lift is a formal $\mathcal{O}_K$-module F over A, together with an isomorphism of $\mathcal{O}_K$-modules $\lambda : F \otimes k \xrightarrow{\sim} G$ and an isomorphism of $\mathcal{O}_K$-algebras $\gamma : \mathcal{O}_L \xrightarrow{\sim} \mathrm{End}(F)$, such that the following holds. First, the composition of γ with the regular representation $\mathrm{End}(F) \to \mathrm{End}(\mathrm{Lie}\, F) = A$ is the canonical inclusion $\mathcal{O}_L \subset A$. Second, the composition of γ with the inclusion $\mathrm{End}(F) \hookrightarrow \mathrm{End}(G) = \mathcal{O}_D$ induced by λ is equal to κ. Note that γ is uniquely determined by the lift F and the first

condition. We will omit it from our notation and simply write $[a]_F : F \to F$ for the endomorphism $\gamma(a)$. Also, the fixed embedding κ will mostly be understood, and we write $[a]_G : G \to G$ for the endomorphism $\kappa(a)$.

Since G has height one as an $\mathcal{O}_L$-module, it follows from [**VZ**, Theorem 3.8], that a canonical lift F is uniquely determined, up to $*$-isomorphism, by the embedding κ. On the other hand, using Lubin-Tate theory and the uniqueness statement of Theorem 1.1, we also conclude that a canonical lift F exists, for any choice of κ. So it is justified to speak about *the* canonical lift F of G, with respect to κ. By choosing a suitable parameter X for F, we may always assume that

$$[\pi_L]_F(X) = \pi_L X + X^{q^{2/e}},$$

where e is the ramification index of the extension L/K.

1.4. Let F be the canonical lift of G over A, with respect to a fixed embedding $\kappa : L \hookrightarrow D$. For any positive integer n, we set

$$A_n := A/\pi_L^{n+1}A, \qquad F_n := F \otimes_A A_n, \qquad H_n := \mathrm{End}_{A_n}(F_n).$$

Since $\mathcal{O}_L \subset H_n$ for all n, we may consider the rings H_n as left $\mathcal{O}_L$-modules. We have a sequence of $\mathcal{O}_L$-linear maps, which are injective by [**VZ**, Lemma 2.6]:

$$H_n \hookrightarrow H_{n-1} \hookrightarrow \cdots \hookrightarrow H_0 = \mathcal{O}_D.$$

We shall consider H_n as an $\mathcal{O}_L$-submodules of $\mathcal{O}_D$. Since A is complete, we have

$$\cap_{n\geq 0} H_n = \mathcal{O}_L.$$

By [**VZ**, Proposition 3.2], we have an injective map

$$H_{n-1}/H_n \hookrightarrow H^2(G, M_n),$$

where $M_n := (\pi_L^n)/(\pi_L^{n+1})$.

Lemma 1.3. — *Fix $n \geq 1$ and let α be an element of $H_{n-1} - H_n$. Then $[\pi_L]_G \circ \alpha \in H_n - H_{n+1}$. In other words, multiplication with π_L induces an* injective *homomorphism of $\mathcal{O}_L$-modules*

$$H_{n-1}/H_n \hookrightarrow H_n/H_{n+1}.$$

Proof. — We may represent α by a power series $\alpha(X) \in A[\![X]\!]$, without constant coefficient, whose reduction modulo π_L^n is an endomorphism of F_{n-1}. We write α_n for the reduction of α modulo π_L^{n+1}. Set

$$\epsilon := \alpha \circ [\pi]_F -_F [\pi]_F \circ \alpha.$$

Since α_{n-1} is an endomorphism of F_{n-1}, we have $\epsilon \equiv 0 \pmod{\pi_L^n}$. Moreover, if $(\Delta, \{\delta_a\}) \in Z^2(G, M_n)$ denotes the cocycle associated to α_n by [**VZ**, Proposition 3.2], then we have

$$\epsilon \equiv \delta_\pi \pmod{\pi_L^{n+1}}.$$

By assumption, the endomorphism α_{n-1} of F_{n-1} cannot be lifted to an endomorphism of F_n. Therefore, Corollary 3.4 of [**VZ**] shows that $\epsilon(X) = cX^q + \dots$, with $c \in (\pi_L^n) - (\pi_L^{n+1})$.

Set

$$\epsilon' := [\pi_L]_F \circ \alpha \circ [\pi]_F -_F [\pi]_F \circ [\pi_L]_F \circ \alpha.$$

Since $[\pi_L]_F$ is an endomorphism of F, we actually have $\epsilon' = [\pi_L]_F \circ \epsilon$. Using our assumption $[\pi_L]_F(X) = \pi_L X + X^{q^{2/e}}$ and the congruence $\epsilon \equiv 0 \pmod{\pi_L^n}$, we see that

$$\epsilon' = \pi_L c X^q + \dots \equiv 0 \pmod{\pi_L^{n+1}}.$$

By [**VZ**, Corollary 3.4], this implies that $[\pi_L]_F \circ \alpha_n$ is an endomorphism of F_n, *i.e.*, $[\pi_L] \circ \alpha \in H_n$. Moreover, if $(\Delta', \{\delta'_a\}) \in Z^2(G, M_{n+1})$ denotes the cocycle associated to $[\pi_L] \circ \alpha_{n+1}$, then we have

$$\epsilon' \equiv \delta'_\pi \pmod{\pi_L^{n+2}}.$$

Since $\pi_L c \in (\pi_L^{n+1}) - (\pi_L^{n+2})$, Corollary 3.4 of [**VZ**] shows that $[\pi_L]_F \circ \alpha_n$ cannot be lifted to an endomorphism of F_n. This means that $[\pi_L] \circ \alpha \notin H_{n+1}$. □

We can now prove the main result of this section (Proposition 3.3 in [**G**]).

Theorem 1.4. — *For $n \geq 1$ we have $H_n = \mathcal{O}_L + \pi_L^n \mathcal{O}_D$.*

Proof. — Each group H_n is a submodule of the free rank-two $\mathcal{O}_L$-module $\mathcal{O}_D$ and contains the direct factor $\mathcal{O}_L \subset \mathcal{O}_D$. Therefore, the quotients H_{n-1}/H_n are cyclic $\mathcal{O}_L$-modules. By Lemma 1.3, these quotients are killed by π_L. Hence H_{n-1}/H_n is either 0 or isomorphic to $\mathcal{O}_L/\pi_L\mathcal{O}_L$. We claim that only the second case occurs. The case $n = 1$ is dealt with in the following lemma.

Lemma 1.5. — *We have $H_1 \neq H_0 = \mathcal{O}_D$.*

We will prove this lemma in the next subsection. Lemma 1.3 says that left multiplication with π_L induces an *injective* map $H_{n-1}/H_n \hookrightarrow H_n/H_{n+1}$. So by induction on n, Lemma 1.5 and the arguments preceding it show that $H_n/H_{n+1} \cong \mathcal{O}_L/\pi_L\mathcal{O}_L$ for all n and that $\mathcal{O}_D/H_n$ is an $\mathcal{O}_L$-module of length n, killed by π_L^n. The theorem follows immediately. □

1.5. We are now going to prove Lemma 1.5. We distinguish two cases.

Case 1: L/K is unramified. In this case, we may assume that $\pi_L = \pi$ and hence $[\pi]_F = \pi X + X^{q^2}$. Then

$$\mathcal{O}_D = \mathcal{O}_L \oplus \mathcal{O}_L \cdot \Pi,$$

where $\Pi = X^q$, see the proof of Theorem 1.1. Let $\alpha = \sum_{i \geq q} a_i X^i \in A_1[\![X]\!]$ be a lift of Π with leading term X^q. Let $(\Delta, \{\delta_a\}) \in Z^2(G, M_1)$ be the cocycle associated

to α. Using Taylor expansion, we see that

$$\begin{aligned}\delta_\pi(X) &= \alpha([\pi]_{F_1}(X)) -_{F_1} [\pi]_{F_1}(\alpha(X)) \\ &= \bigl(\alpha(X^{q^2}) + \pi\cdot\alpha'(X^{q^2})X\bigr) -_{F_1} \bigl(\pi\alpha(X) + \alpha(X)^{q^2}\bigr) \\ &= -\pi X^q + \cdots \neq 0.\end{aligned}$$

(Here we use the notation $\alpha' := \partial\alpha/\partial X$.) Therefore, by [**VZ**, Corollary 3.4], we have $\Pi \notin H_1$.

Case 2: L/K is ramified. Then π_L satisfies an Eisenstein equation over $\mathcal{O}_K$, which we may normalize to

$$\pi_L^2 + a\pi_L + \pi = 0,$$

with $a \in \pi\mathcal{O}_K$. Assuming, as usual, that $[\pi_L]_F = \pi_L X + X^q$, a short computation yields the congruence

$$[\pi]_F(X) \equiv -\pi_L X^q - X^{q^2} + \ldots \pmod{\pi}. \tag{1.1}$$

Let $j \in \mathcal{O}_D$ be an element which generates an unramified quadratic extension of K. We may assume that $j(X) = \bar{u}X + \ldots$, where $\bar{u} \in k$ generates the quadratic extension of the residue class field of $\mathcal{O}_K$. Lift j to a power series $\alpha(X) = uX + \cdots \in A_1[\![X]\!]$ modulo π, and let $(\Delta, \{\delta_a\}) \in Z^2(G, M_1)$ be the associated cocycle. Then $u^q \not\equiv u \pmod{\pi_L}$. Using the congruence (1.1), we compute

$$\begin{aligned}\delta_\pi(X) &= \alpha([\pi]_{F_1}(X)) -_{F_1} [\pi]_{F_1}(\alpha(X)) \\ &= \bigl(u(-\pi_L X^q - X^{q^2}) + \ldots\bigr) -_{F_1} \bigl(-\pi_L\alpha(X)^q - \alpha(X)^{q^2}\bigr) \\ &= \pi_L(u^q - u)X^q + \ldots\end{aligned}$$

As in Case 1, we use [**VZ**, Corollary 3.4], to conclude that $j \notin H_1$.

2. Isogenies and Tate modules

In this section we review the connection between the endomorphism ring and the isogeny classes of a formal $\mathcal{O}_K$-module on the one hand, and lattices inside the Tate module on the other hand. These results will be used in the following section on quasi-canonical lifts.

2.1. As in the previous sections, K denotes a field which is complete with respect to a discrete valuation and has a finite residue field of order $q = p^f$. We let k denote an algebraic closure of the residue field of K. Furthermore, A is a flat local $\mathcal{O}_K$-algebra which is a complete discrete valuation ring with residue field k, and M is the fraction field of A. We fix an algebraic closure $\bar{M}$ of M.

Let F be a formal $\mathcal{O}_K$-module of finite height h over A (not necessarily a canonical lift). We write

$$\Lambda(F) := F(\bar{M})_{\mathrm{tor}} = \cup_n F[\pi^n]$$

for the torsion subgroup of F and

$$T(F) := \varprojlim_n F[\pi^n]$$

for the Tate module of F. These are $\mathcal{O}_K$-modules with a continuous, $\mathcal{O}_K$-linear action of $\mathrm{Gal}(\bar{M}/M)$. As $\mathcal{O}_K$-modules, we have non-canonical isomorphisms

$$\Lambda(F) \cong (K/\mathcal{O}_K)^h, \qquad T(F) \cong \mathcal{O}_K^h.$$

Set $V(F) := T(F) \otimes_{\mathcal{O}_K} K$; then we have a canonical short exact sequence of $\mathrm{Gal}(\bar{M}/M)$-$\mathcal{O}_K$-modules

$$0 \to T(F) \longrightarrow V(F) \longrightarrow \Lambda(F) \to 0. \tag{2.1}$$

Let A' be a finite extension of A, and let F' be a formal $\mathcal{O}_K$-module over A'. An *isogeny* between F and F' defined over A' is a nonzero homomorphism $\alpha : F \otimes_A A' \to F'$ of formal $\mathcal{O}_K$-modules. If such an isogeny exists, then we say that F' is *isogenous* to F (over A'). For simplicity, we shall write $\alpha : F \to F'$, and consider α as a power series in $\mathcal{O}_{\bar{M}}[\![X]\!]$ whose coefficients generate a finite extension of A. We say that α is defined over A' if $\alpha \in A'[\![X]\!]$.

Given an isogeny $\alpha : F \to F'$, we obtain a diagram

(2.2)

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & N & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T(F) & \longrightarrow & V(F) & \longrightarrow & \Lambda(F) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle T(\alpha)} & & \cong\downarrow{\scriptstyle V(\alpha)} & & \downarrow{\scriptstyle \Lambda(\alpha)} & & \\
0 & \longrightarrow & T(F') & \longrightarrow & V(F') & \longrightarrow & \Lambda(F') & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathrm{Coker}\, T(\alpha) & & 0 & & 0 & &
\end{array}$$

with exact rows and columns. Note that N is equal to the kernel of α; it is a finite $\mathcal{O}_K$-submodule. A trivial version of the snake lemma shows that we have a canonical isomorphism $N \cong \mathrm{Coker}\, T(\alpha)$.

The following theorem states that every finite $\mathcal{O}_K$-submodule of $\Lambda(F)$ arises as the kernel of an isogeny. More precisely:

Theorem 2.1. — *Let $N \subset \Lambda(F)$ be a finite $\mathcal{O}_K$-submodule, $\Gamma' \subset \Gamma$ the stabilizer of N, $M' \subset \bar{M}$ the fixed field of Γ' and A' the valuation ring of M'. Then the formula*

$$\alpha(X) := \prod_{z \in N} (X -_F z) \in A'[\![X]\!]$$

defines an isogeny $\alpha : F \to F'$ over A'. It has the following properties.

1. $\mathrm{Ker}(\alpha) = N$.

2. *Let $\beta : F \to F''$ be an isogeny with $N \subset \mathrm{Ker}(\beta)$. Then there exists a unique isogeny $\gamma : F' \to F''$ with $\beta = \gamma \circ \alpha$.*

Proof. — See [**H**, §35.2]. □

2.2. It will be more convenient for us to reformulate Theorem 2.1 in terms of lattices $T' \subset V(F)$ (instead of finite subgroups $N \subset \Lambda(F)$). Let F be a formal $\mathcal{O}_K$-module of finite height over A. Set $T := T(F)$ and $V := V(F)$.

Corollary 2.2. — 1. *Let $T' \subset V$ be an $\mathcal{O}_K$-lattice containing the lattice T (a* superlattice*). Then there exists an isogeny $\alpha : F \to F'$ such that $T' = V(\alpha)^{-1}(T(F'))$. If T'' is a superlattice of T' and $\beta : F \to F''$ an isogeny with $T'' = V(\beta)^{-1}(T(F''))$, then there exists a unique isogeny $\gamma : F' \to F''$ such that $\beta = \gamma \circ \alpha$.*

2. *Let $T' \subset T$ be an $\mathcal{O}_K$-sublattice. Then there exists an isogeny $\alpha : F' \to F$ such that $T' = \mathrm{Im}(T(\alpha))$. If $T'' \subset T'$ is another sublattice, and $\beta : F'' \to F$ is an isogeny such that $T'' = \mathrm{Im}(T(\beta))$, then there exists a unique isogeny $\gamma : F'' \to F'$ with $\beta = \alpha \circ \gamma$.*

Proof. — Given T' as in Part 1, we set $N := T'/T$. *Via* the short exact sequence (2.1), we consider N as a (finite) $\mathcal{O}_K$-submodule of V. Let $\alpha : F \to F'$ be the isogeny with kernel N, which exists by Theorem 2.1.1. Then the diagram (2.2) shows that $T' = V(\alpha)^{-1}(T(F'))$. This proves the first assertion in Part 1. The second assertion follows from Theorem 2.1.2.

We are now going to prove Part 2 of the corollary. Let $T' \subset T$ be a sublattice. Choose an integer n such that $\pi^n T \subset T'$. By Part 1 of the corollary, there exists an isogeny $\beta : F \to F'$ such that $V(\beta)^{-1}(T(F')) = \pi^{-n}T'$. The kernel of β is isomorphic to $\pi^{-n}T'/T$, which is an $\mathcal{O}_K$-module killed by π^n. Therefore, Theorem 2.1.2 shows that there exists an isogeny $\alpha : F' \to F$ with $\alpha \circ \beta = [\pi^n]_F$. By construction, we have

$$\mathrm{Im}(T(\alpha)) = \pi^n \cdot V(\beta)^{-1}(T(F')) = T'.$$

This proves the first assertion of Part 2. The proof of the second assertion is left to the reader. □

2.3. Let F, T and V be as before. The faithful representation of $\mathrm{End}(F)$ on V extends to a faithful representation

$$\mathrm{End}^0(F) := \mathrm{End}(F) \otimes_{\mathcal{O}_K} K \hookrightarrow \mathrm{End}_K(V).$$

We will from now on consider elements of $\mathrm{End}^0(F)$ as elements of $\mathrm{End}_K(V)$.

Let T', T'' be $\mathcal{O}_K$-superlattices of T inside V. Let $\alpha : F \to F'$ and $\beta : F \to F''$ be the corresponding isogenies, as in Corollary 2.2.1. We identify $V(F')$ and $V(F'')$ with V, *via* the isomorphisms $V(\alpha)$ and $V(\beta)$. Then $T' = T(F')$ and $T'' = T(F'')$.

Corollary 2.3. — *The map which sends a homomorphism $\psi : F' \to F''$ to the induced endomorphism $\tilde{\psi} : V \cong V(F') \to V(F'') \cong V$ is a bijection*

$$\mathrm{Hom}(F', F'') \xrightarrow{\sim} \{\, \tilde{\psi} \in \mathrm{End}^0(F) \mid \tilde{\psi}(T') \subset T'' \,\}.$$

Proof. — Let $\psi : F' \to F''$ be a homomorphism and $\tilde{\psi} \in \mathrm{End}_K(V)$ the induced endomorphism of V. By definition, we have $\tilde{\psi}(T') \subset T''$. We have to show that $\tilde{\psi} \in \mathrm{End}^0(F)$. Set $\gamma := \psi \circ \alpha : F \to F''$. The isogeny γ corresponds, *via* Corollary 2.2.2, to the sublattice $\tilde{\psi}(T) \subset T''$. From the same point of view, the isogeny $\beta : F \to F''$ corresponds to the sublattice $T \subset T''$. Choose an integer n such that $\pi^n \tilde{\psi}(T) \subset T$. Then by Corollary 2.2.2, there exists an endomorphism $\phi : F \to F$ such that $\beta \circ \phi = \gamma \circ [\pi^n]_F$. One checks that $\phi = \pi^n \tilde{\psi}$, as elements of $\mathrm{End}_K(V)$, which shows that $\tilde{\psi} \in \mathrm{End}^0(F)$.

Conversely, let $\tilde{\psi}$ be an element of $\mathrm{End}^0(F) \subset \mathrm{End}_K(V)$ with $\tilde{\psi}(T') \subset T''$. By definition, we can write $\tilde{\psi} = \pi^{-n}\phi$ for some endomorphism $\phi : F \to F$. The isogeny $\alpha \circ [\pi^n]_F : F \to F'$ (resp. the isogeny $\beta \circ \phi : F \to F''$) corresponds, *via* Corollary 2.2.1, to the superlattice $\pi^{-n}T' \supset T$ (resp. the superlattice $\phi^{-1}(T'') \supset T$). The assumption $\tilde{\psi}(T') \subset T''$ together with $\tilde{\psi} = \pi^{-n}\phi$ implies $\pi^{-n}T' \subset \phi^{-1}(T'')$. Therefore, by Corollary 2.2.1, there exists an isogeny $\psi : F' \to F''$ with $\psi \circ \alpha \circ [\pi^n]_F = \beta \circ \phi$. By construction, $\tilde{\psi}$ is the image of ψ under the embedding $\mathrm{Hom}(F', F'') \hookrightarrow \mathrm{End}_K(V)$. This concludes the proof of the corollary. □

3. Quasi-canonical lifts

A quasi-canonical lift is a lift whose endomorphism ring is an order in a quadratic extension L/K. In this section we show that every quasi-canonical lift is isogenous to a canonical lift, and we determine the set of isomorphism classes of all quasi-canonical lifts together with its natural Galois action.

3.1. We now come back to the situation of Section 1. In particular, G is the (unique) formal $\mathcal{O}_K$-module of height two over k. We fix a quadratic extension L/K, an $\mathcal{O}_K$-linear embedding $\kappa : \mathcal{O}_L \hookrightarrow \mathcal{O}_D := \mathrm{End}_k(G)$. We denote by F the canonical lift of G with respect to κ. Recall that F is defined over A, the strict completion of $\mathcal{O}_L$ with respect to the map $\mathcal{O}_K \to k$ induced by the $\mathcal{O}_L$-action on $\mathrm{Lie}(G)$.

Let M denote the fraction field of A, $\bar{M}$ an algebraic closure of M and $\Gamma := \mathrm{Gal}(\bar{M}/M)$. We let $T := T(F)$ denote the Tate-module of F and $V := T \otimes_{\mathcal{O}_K} K$. Note that T has the structure of a free $\mathcal{O}_L$-module of rank one, and that the Γ-action on T is continuous and $\mathcal{O}_L$-linear. By Lubin–Tate theory, the resulting homomorphism

$$\rho : \Gamma = \mathrm{Gal}(\bar{M}/M) \longrightarrow \mathcal{O}_L^\times \tag{3.1}$$

yields an isomorphism $\Gamma^{\mathrm{ab}} \xrightarrow{\sim} \mathcal{O}_L^\times$. Identifying Γ with the inertia subgroup of $\mathrm{Gal}(\bar{L}/L)$, the homomorphism (3.1) is the inverse of the reciprocity map $L^\times \to \mathrm{Gal}(\bar{L}/L)^{\mathrm{ab}}$ of local class field theory, restricted to $\mathcal{O}_L^\times$. See [**LT1**].

Fix an integer $s \geq 0$. Let

$$\mathcal{O}_s := \mathcal{O}_K + \mathcal{O}_L \cdot \pi^s$$

denote the order of $\mathcal{O}_L$ generated by $\mathcal{O}_K$ and the ideal $\mathcal{O}_L \cdot \pi^s$. It is easy to see that every order of $\mathcal{O}_L$ containing $\mathcal{O}_K$ is equal to $\mathcal{O}_s$, for some s. Let M_s/M be the ring class field of $\mathcal{O}_s^\times$, *i.e.*, the fixed field of the subgroup $\Gamma_s \subset \Gamma$, where Γ_s is the inverse image of $\mathcal{O}_s^\times \subset \mathcal{O}_L^\times$ under the inverse reciprocity homomorphism (3.1). In other words, we have

$$\mathrm{Gal}(M_s/M) \cong \mathcal{O}_L^\times/\mathcal{O}_s^\times.$$

An easy computation shows that, for $s \geq 1$,

$$[M_s : M] = |\mathcal{O}_L^\times/\mathcal{O}_s^\times| = \begin{cases} q^{s-1}(q+1), & \text{if } L/K \text{ is unramified,} \\ q^s, & \text{if } L/K \text{ is ramified.} \end{cases}$$

Definition 3.1. — A *quasi-canonical lift of G of level s* (with respect to the embedding $\kappa : \mathcal{O}_L \hookrightarrow \mathcal{O}_D$) is a lift F of G, defined over some finite extension A'/A, together with an $\mathcal{O}_K$-algebra isomorphism $\gamma : \mathcal{O}_s \xrightarrow{\sim} \mathrm{End}(F')$, such that the following holds.

1. The composition of γ with the representation $\mathrm{End}(F') \hookrightarrow \mathrm{End}(\mathrm{Lie}\, F') = A'$ is the canonical embedding $\mathcal{O}_s \hookrightarrow A'$.
2. The composition of γ with the embedding $\mathrm{End}(F') \hookrightarrow \mathcal{O}_D$ is equal to the restriction of κ to $\mathcal{O}_s \subset \mathcal{O}_L$.

To ease the notation, we will usually omit the isomorphism γ and the embedding κ from our notation. Note that a quasi-canonical lift of level 0 is the same thing as a canonical lift (which exists and is unique). For general s, we have the following result.

Theorem 3.2. — *Let $\mathcal{O}_{M_s}$ denote the ring of integers of M_s.*

1. *Let F' be a quasi-canonical lift of level s. Then there exists an isogeny*

$$\alpha : F \longrightarrow F'$$

of degree q^s, defined over $\mathcal{O}_{M_s}$. It is unique up to composing α with an element of $\mathrm{Aut}(F) = \mathcal{O}_L^\times$. In particular, F' can be defined over $\mathcal{O}_{M_s}$.
2. *The set of $*$-isomorphism classes of all quasi-canonical lifts of level s is a principal homogeneous space under the action of $\mathrm{Gal}(M_s/M)$.*

Remark 3.3. — The proof of this theorem will show that the action of $\mathrm{Gal}(M_s/M)$ on the set of $*$-isomorphism classes can be described as follows. Let (F', λ) be a quasi-canonical lift of level s (with $\lambda : F' \otimes k \xrightarrow{\sim} G$), and $\sigma \in \Gamma$. Then the lift $(F', \lambda)^\sigma$ is $*$-isomorphic to the lift $(F', [\rho(\sigma)^{-1}]_G \circ \lambda)$. Therefore, by Theorem 3.2.2, two quasi-canonical lifts of the same level are always isomorphic as formal $\mathcal{O}_K$-modules.

3.2. Let $\alpha : F \to F'$ and $\beta : F \to F''$ be two isogenies with source F. We say that α and β are *isomorphic* if there exists an isomorphism of formal $\mathcal{O}_K$-modules $\gamma : F' \xrightarrow{\sim} F''$ with $\beta = \gamma \circ \alpha$.

Fix an isogeny $\alpha : F \to F'$. To simplify the notation, we will identify $V(F')$ with V *via* the isomorphism $V(\alpha)$. Then, by Corollary 2.2.1, α corresponds, up to isomorphism, to an $\mathcal{O}_K$-superlattice $T' \supset T$ in V. Moreover, by Corollary 2.3, α induces an isomorphism of $\mathcal{O}_K$-algebras

$$\mathrm{End}(F') \xrightarrow{\sim} \{\, \phi \in L = \mathrm{End}^0(F) \mid \phi(T') \subset T' \,\}. \tag{3.2}$$

This exhibits $\mathrm{End}(F')$ as an order of $\mathcal{O}_L$.

Lemma 3.4. — *Let T be a free $\mathcal{O}_L$-module of rank one, $V := T \otimes_{\mathcal{O}_K} K$. Let $T' \supset T$ be an $\mathcal{O}_K$-superlattice in V. Then there exists a generator t of T (*i.e., *$T = \mathcal{O}_L \cdot t$) and integers $n, s \geq 0$ such that*

$$\pi_L^n \cdot T' = (\mathcal{O}_K \cdot \pi^{-s} + \mathcal{O}_L) \cdot t.$$

Moreover, the multiplicator $\mathcal{O}_{T'}$ of T' is equal to the order $\mathcal{O}_s \subset \mathcal{O}_L$.

Proof. — For $T' \supset T$ as in Part 1, define

$$n := \max\{\, n' \mid \pi_L^{n'} T' \supset T \,\}, \qquad s := \min\{\, s' \mid \pi^{s'} \pi_L^n T' \subset T \,\}.$$

Then $\pi_L^n T'/T$ is a cyclic $\mathcal{O}_K$-module, generated by an element of the form $\pi^{-s}t$. Moreover, any t with this property is a generator of T. It follows that $\pi_L^n T' = (\mathcal{O}_K \cdot \pi^{-s} + \mathcal{O}_L) \cdot t$. The proof of the fact that $\mathcal{O}_s$ is the multiplicator of T' is standard and left to the reader. □

A superlattice $T' \supset T$ is called *minimal of level s* if $T' = (\mathcal{O}_K \cdot \pi^{-s} + \mathcal{O}_L) \cdot t$, for some generator t of T. The corresponding isogenies $\alpha : F \to F'$ are also called *minimal of level s*. We let X_s denote the set of isomorphism classes of minimal isogenies of level s. The Galois group Γ acts on X_s, in a natural way. There is also an action of $\mathcal{O}_L^\times$ on X_s, given by composing $\alpha : F \to F'$ with the automorphism $[a]_F : F \xrightarrow{\sim} F$, for $a \in \mathcal{O}_L^\times$.

Proposition 3.5. — *The actions of Γ and $\mathcal{O}_L^\times$ on X_s are anti-compatible* via *the reciprocity homomorphism $\rho : \Gamma \to \mathcal{O}_L^\times$,* i.e., *for $\sigma \in \Gamma$ there exists an isomorphism $\gamma_\sigma : (F')^\sigma \xrightarrow{\sim} F'$ such that the diagram*

$$\begin{array}{ccc} F & \xrightarrow{\alpha^\sigma} & (F')^\sigma \\ {\scriptstyle [\rho(\sigma)^{-1}]_F}\downarrow & & \downarrow{\scriptstyle \gamma_\sigma} \\ F & \xrightarrow{\alpha} & F' \end{array}$$

commutes. Furthermore, X_s is a principal homogeneous space under the induced action of $\mathrm{Gal}(M_s/M) \cong \mathcal{O}_L^\times/\mathcal{O}_s^\times$.

Proof. — If the isogeny $\alpha : F \to F'$ corresponds to the lattice T', then $\alpha \circ [a]_F : F \to F'$, for $a \in \mathcal{O}_L$, corresponds to the lattice $a^{-1} \cdot T'$. Therefore, it follows immediately from Lemma 3.4 that the action of $\mathcal{O}_L^\times$ on X_s is transitive, and the stabilizer of each element is equal to $\mathcal{O}_s^\times$. To see that this action is compatible with the Galois action, fix an element $\sigma \in \Gamma$. Clearly, the kernel of α^σ can be identified with $(T'/T)^\sigma = \rho(\sigma) \cdot T'/T$. Since this is also the kernel of $\alpha \circ [\rho(\sigma)^{-1}]_F$, the existence of γ_σ follows from Theorem 2.1. The proposition is proved. □

Proof of Theorem 3.2. — We first prove Part 1 of the theorem. Let F' be a quasi-canonical lift of level s. Set $T' := T(F')$ and $V' := T' \otimes_{\mathcal{O}_K} K$. The isomorphism $\mathcal{O}_s \xrightarrow{\sim} \mathrm{End}(F')$ extends to an isomorphism $L \xrightarrow{\sim} \mathrm{End}^0(F')$, which gives V' the structure of an L-vector space of dimension one and identifies $\mathcal{O}_s$ with the multiplicator of the lattice $T' \subset V'$.

Let $T'' \subset T'$ be a maximal $\mathcal{O}_L$-submodule of rank one. Then $T' = (\mathcal{O}_K \cdot \pi^{-s} + \mathcal{O}_L) \cdot t$ for some generator t of T'', by Lemma 3.4. Let $\alpha : F'' \to F'$ be an isogeny with $\mathrm{Im}(T(\alpha)) = T''$, see Corollary 2.2.2. By Corollary 2.3, α induces an isomorphism

$$\mathrm{End}(F'') \cong \{\, \phi \in \mathrm{End}^0(F') = L \mid \phi(T'') = T'' \,\} \cong \mathcal{O}_L.$$

Therefore, $F'' \cong F$ as formal $\mathcal{O}_K$-modules. Choosing an arbitrary isomorphism $F'' \cong F$, we can regard $\alpha : F \cong F'' \to F'$ as an element of X_s. Since $\mathcal{O}_L^\times$ acts transitively on X_s, by Proposition 3.5, we have proved Part 1 of Theorem 3.2.

Now we prove Part 2 of the theorem. In view of Part 1 and Proposition 3.5, we only need to show the following. For every minimal isogeny $\alpha : F \to F'$ of level s, there exists an isomorphism $\lambda : F' \otimes k \xrightarrow{\sim} G$ which makes F' a quasi-canonical lift. For this, we may assume that the isogeny α is given, as a power series with coefficients in $\mathcal{O}_{M_s}$, by the formula of Theorem 2.1:

$$\alpha(X) := \prod_{\gamma \in \mathrm{Ker}(\alpha)} (X -_F \gamma).$$

Here $\mathrm{Ker}(\alpha)$ is simply considered as a subset of the maximal ideal of the ring of integers of $\bar{M}$. Therefore, the reduction of α to k is $\bar{\alpha}(X) = X^{q^s}$. By the proof of Theorem 1.1, we may assume that $\Pi(X) := X^q$ is an endomorphism of G and lies in the normalizer of $\mathcal{O}_L = \mathrm{End}(F) \subset \mathcal{O}_D$. In particular, $\bar{\alpha} = \Pi^s$ is an endomorphism of G. Therefore, $F' \otimes k$ is actually *equal* to G. We define the isomorphism $\lambda : F' \otimes k \xrightarrow{\sim} G$ as the identity and claim that (F', λ) is a quasi-canonical lift.

By construction, we have an isomorphism

$$\mathrm{End}(F') \cong \{\, \phi \in L = \mathrm{End}^0(F) \mid \phi(T') = T' \,\} \cong \mathcal{O}_s. \tag{3.3}$$

Hence the image of the natural injection $\mathrm{End}(F') \hookrightarrow \mathrm{End}(\mathrm{Lie}\, F') = \mathcal{O}_{M_s}$ is an $\mathcal{O}_K$-algebra isomorphic to $\mathcal{O}_s$. It must therefore be equal to $\mathcal{O}_s$. Let $\gamma : \mathcal{O}_s \xrightarrow{\sim} \mathrm{End}(F')$ be the resulting isomorphism. Then Condition 1 of Definition 3.1 holds by construction.

Let $\kappa' : \mathcal{O}_s \hookrightarrow \mathcal{O}_D$ be the composition of γ with the embedding $\mathrm{End}(F') \hookrightarrow \mathcal{O}_D$ induced by the identification $F' \otimes k = G$. We have to show that κ' is equal to the restriction of κ to $\mathcal{O}_s$ (see Condition 2 of Definition 3.1). Tracing back the definitions, we see that $\kappa' = (\kappa|_{\mathcal{O}_s})^{\bar{\alpha}}$ is the conjugate of $\kappa|_{\mathcal{O}_s}$ by $\bar{\alpha} = \Pi^s \in \mathcal{O}_D$. Since we assumed Π to lie in the normalizer of the image of κ, we have already proved that κ' and $\kappa|_{\mathcal{O}_s}$ have the same image and are equal up to composition with an element of $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2$. However, if L/K is ramified, then the assumption that Π normalizes $\mathcal{O}_L$ already implies that $\Pi \in \mathcal{O}_L$, and we get $\kappa' = \kappa|_{\mathcal{O}_s}$ as desired. Now assume that L/K is unramified. Then it suffices to show that κ' and $\kappa|_{\mathcal{O}_s}$ agree modulo the maximal ideal $\mathcal{O}_D \cdot \Pi$. But this is a consequence of Condition 1 of Definition 3.1. This concludes the proof of Theorem 3.2. □

4. Canonical subgroups

The main result of this section is Proposition 4.6 which computes the valuation of the formal modulus of a quasi-canonical lift. The heart of the proof of this proposition is the study of *canonical subgroups* and their behavior under isogenies. The relevance of canonical subgroups was first pointed out in [**L**].

4.1. We continue with the notation used in the last section. In particular, A is the completion of the maximal unramified extension of $\mathcal{O}_L$ and M the fraction field of A. We choose an algebraic closure $\bar{M}$ of M and let $v : \bar{M} \to \mathbb{Q} \cup \{\infty\}$ denote the exponential rank-one valuation with $v(\pi) = 1$.

Let M'/M be some finite extension, and let A' denote the valuation ring of M'. Throughout this section, we will implicitly assume that the extension M'/M is 'sufficiently large'. In practice this will mean that sometimes we have to enlarge M' in order to make certain torsion points M'-rational.

For the moment, we fix an arbitrary lift F of the formal $\mathcal{O}_K$-module G, defined over A' (not necessarily the canonical lift). By [**VZ**, Theorem 3.8], F is isomorphic to the pullback of the universal deformation $\tilde{F}$ of G *via* a unique $\widehat{\mathcal{O}}_K^{\mathrm{nr}}$-algebra morphism $R^{\mathrm{univ}} \to A$. Moreover, R^{univ} can be written as a power series algebra $\widehat{\mathcal{O}}_K^{\mathrm{nr}}[\![u]\!]$. (The proof of this result in [**VZ**] does not provide us with a natural choice of the parameter u, but this is irrelevant for us by Remark 4.2 below. See [**HG**] for a more explicit choice of the parameter u.)

Definition 4.1. — The image of the parameter u under the morphism $R^{\mathrm{univ}} \to A'$ corresponding to F is denoted by $u(F)$ and is called the *formal modulus* of the lift F. The rational number $v(F) := \min\{v(u(F)), 1\}$ is called the *valuation* of F.

Remark 4.2. — It is clear that the valuation $v(F)$ is actually independent of the choice of the parameter u. Therefore, $v(F)$ depends only on the isomorphism class of F as a formal $\mathcal{O}_K$-module, and not on the chosen isomorphism $\lambda : F \otimes k \xrightarrow{\sim} G$. Indeed,

a unit $\gamma \in \mathcal{O}_D^\times$ induces an automorphism $\tilde{\gamma}$ of the universal deformation space of G (which sends the pair (F, λ) to the pair $(F, \gamma \circ \lambda)$). Applying the automorphism $\tilde{\gamma}$ amounts to replacing the parameter u by $u' := \tilde{\gamma}^* u$.

Definition 4.3. — A sub-$\mathcal{O}_K$-module $H \subset F[\pi]$ of length one is called a *canonical subgroup* if

$$v(x) > v(y)$$

for all $x \in H$ and $y \in F[\pi] - H$.

Note that a canonical subgroup, if it exists, is unique. We may therefore speak about *the* canonical subgroup of F. The two last definitions are related to each other in the following manner.

Proposition 4.4

1. *Write* $[\pi]_F = \sum_{i \geq 1} a_i X^i$, *with* $a_i \in A'$. *Then* $v(F) = \min\{v(a_q), 1\}$.
2. *The lift* F *has a canonical subgroup if and only if*

$$v(F) < \frac{q}{q+1}.$$

Proof. — It follows from the proof of [**VZ**, Theorem 3.8], that we can choose for the parameter u defining the isomorphism $R^{\mathrm{univ}} \cong \widehat{\mathcal{O}}_K^{\mathrm{nr}}[\![u]\!]$ the qth coefficient of $[\pi]_{\tilde{F}}$, where $\tilde{F}$ is the universal deformation of G. Therefore, Part 1 of the proposition is a direct consequence of the definition of $v(F)$. Now Part 2 is easily seen by looking at the Newton polygon of $[\pi]_F$. Indeed, the slope filtration on the set $F[\pi] - \{0\}$ is also a filtration of $\mathcal{O}_K$-modules. But as an $\mathcal{O}_K$-module, $F[\pi]$ has length two, so there can be at most two finite negative slopes. Also, breaks occur only at $i = 1, q^2$ and possibly at $i = q$. Since $v(a_1) = 1$ and $v(a_{q^2}) = 0$, we have a break at $i = q$ if and only if $v(F) < q/(q+1)$. □

4.2. Fix a lift F of G defined over A' and a sub-$\mathcal{O}_K$-module $H \subset F[\pi]$ of length one. Let $\alpha : F \to F'$ be the isogeny with kernel H, defined by Theorem 2.1. Recall that α is given by the power series

$$\alpha(X) := \prod_{x \in H} (X -_F x). \tag{4.1}$$

Let us choose an isomorphism $\lambda' : F' \otimes k \xrightarrow{\sim} G$. We will use λ' as an identification, *i.e.*, we will regard F' as a lift of G. As in Section 3.2, one can choose λ' in such a way that $\alpha \otimes k$ gets identified with the isogeny $\Pi = X^q : G \to G$. However, this choice is not at all canonical. In what follows, we are mainly interested in relating the two valuations $v(F)$ and $v(F')$. By Remark 4.2, the choice that we have made is irrelevant for this problem.

Let $\beta : F \to F'$ be the unique isogeny such that $[\pi]_F = \beta \circ \alpha$. Then $H' := \ker(\beta)$ is equal to the image of $F[\pi]$ under the isogeny α. Clearly, H' is an $\mathcal{O}_K$-module of length one.

Proposition 4.5

1. *Suppose that H is the canonical subgroup of F. There are two cases:*
   (a) *If $v(F) \leq \frac{1}{q}$ then $v(F') = q \cdot v(F)$ and H' is not canonical.*
   (b) *If $\frac{1}{q} < v(F) < \frac{q}{q+1}$ then $v(F') = 1 - v(F)$ and H' is the canonical subgroup of F'.*
2. *Suppose that H is* not *the canonical subgroup of F. Again we have two cases:*
   (a) *If $v(F) \leq \frac{q}{q+1}$ then $v(F') = q^{-1} \cdot v(F)$.*
   (b) *If $v(F) \geq \frac{q}{q+1}$ then $v(F') = 1/(q+1)$.*

   In both cases, H' is the canonical subgroup of F'.

Proof. — Suppose that H is canonical. By Proposition 4.4, we have $v(F) < q/(q+1)$. Moreover, the proof of this proposition shows that the Newton polygon of $[\pi]_F$ has exactly two finite negative slopes, namely

$$s_1 = -\frac{1 - v(F)}{q - 1}, \qquad s_2 = -\frac{v(F)}{q^2 - q}.$$

Here s_1 is the slope above the interval $[1, q]$ and corresponds to the canonical subgroup, whereas s_2 is the slope above $[q, q^2]$.

Pick an element $y \in F[\pi] - H$; then $v(y) = -s_2 = v(F)/(q^2 - q)$. It follows from (4.1) that the element $z := \alpha(y) \in H'$ has valuation

$$v(z) = \sum_{x \in H} v(y -_F x) = q \cdot v(y) = \frac{v(F)}{q - 1}.$$

Now if $v(F) \leq 1/q$ then $v(z) \leq 1/(q^2 - q)$. This means that $-v(z)$ is equal to the slope of the Newton polygon of $[\pi]_{F'}$ above the interval $[q, q^2]$. We conclude that

$$v(F') = (q^2 - q) \cdot v(z) = q \cdot v(F)$$

and that H' is not the canonical subgroup of F'. On the other hand, if $v(F) > 1/q$ then $v(z) > 1/(q^2 - q)$. Therefore, $v(z)$ is equal to the slope above the interval $[1, q]$. We conclude that

$$v(F') = 1 - (q - 1) \cdot v(F) = 1 - v(F)$$

and that H' is the canonical subgroup of F'. This finishes the proof of Case 1. The proof of Case 2 is similar and left to the reader. □

4.3. Let us now assume that the lift F is the canonical lift of G with respect to some fixed embedding $\kappa : L \hookrightarrow D$. Note that we have $v(F) = 1$ if L/K is unramified and $v(F) = 1/2$ if L/K is ramified. In the former case, F has no canonical subgroup, whereas in the latter case the canonical subgroup of F is the kernel of $[\pi_L]_F$.

For $s = 1, 2, \ldots$, we define isogenies $\alpha_s : F \to F_s$ inductively, as follows. First, choose a non-canonical $\mathcal{O}_K$-submodule $H \subset F[\pi]$ of height one. Set $F_1 := F/H$ and let $\alpha_1 : F \to F_1$ be the natural projection. For $s \geq 1$, choose a non-canonical $\mathcal{O}_K$-submodule $H_s \subset F_s[\pi]$ of height one, set $F_{s+1} := F_s/H_s$ and let $\alpha_{s+1} : F \to F_{s+1}$ be

the composition of α_s with the natural projection $F_s \to F_{s+1}$. As we have seen in the last section, we can see F_s as a lift of G in such a way that the isogeny α_s reduces to the endomorphism $\Pi^s : G \to G$ modulo the maximal ideal of A'. This choice is by no means canonical; however, for the statement of the next proposition, the choice that we have made is irrelevant, see Remark 3.3 and Remark 4.2.

Proposition 4.6. — *The lift F_s is quasi-canonical of level s, and we have*

$$v(F_s) = \begin{cases} \dfrac{1}{q^{s-1}(q+1)}, & \text{if } L/K \text{ is unramified and } s \geq 1, \\ \dfrac{1}{2q^s}, & \text{if } L/K \text{ is ramified.} \end{cases}$$

Proof. — We proceed by induction over s. We start the induction at $s = 1$ if L/K is unramified and at $s = 0$ in the ramified case (one has to be careful with the notation: plugging in $s = 0$ into F_s should be understood as F). If L/K is unramified, then $v(F) = 1 > q/(q+1)$, and Proposition 4.5, Case 2(b), shows that $v(F_1) = 1/(q+1)$. This is indeed as in the statement of the proposition. The statement of the proposition is also true for $s = 0$ if L/K is ramified.

Suppose now that $s \geq 1$ or that L/K is ramified. Then $v(F_s) \leq q/(q+1)$, so Proposition 4.5, Case 2(a), shows that

$$v(F_{s+1}) = \frac{v(F_s)}{q}.$$

We see that the formula for $v(F_s)$ follows by induction.

Since F_s is isogenous to F, it is a quasi-canonical lift of some level. By construction, the isogeny $\alpha_s : F \to F_s$ has degree q^s. Let n be the maximal integer such that α_s factors over $[\pi_L^n] : F \to F$. The proof of Theorem 3.2 shows that F_s is quasi-canonical of level $s' := s - 2n/e$.

Suppose $n > 0$. By the induction hypothesis, $F_{s'}$ is quasi-isogenous of level s'. Therefore, by Remark 3.3, $F_{s'}$ and F_s are isomorphic as formal $\mathcal{O}_K$-modules. But then we have $v(F_s) = v(F_{s'})$. This gives a contradiction with the formula for $v(F_s)$ which we have already proved. We conclude that $n = 0$, *i.e.*, that F_s is quasi-canonical of level s. □

Corollary 4.7. — *Let F_s be a quasi-canonical lift of level s and $\mathcal{O}_{M_s}/A$ be the smallest extension over which it can be defined. Then the formal modulus $u(F_s) \in \mathcal{O}_{M_s}$ of F_s is a uniformizer for the valuation ring $\mathcal{O}_{M_s}$.*

Proof. — It follows from Theorem 3.2 that $\mathcal{O}_{M_s}$ is the ring of integers of the extension M_s/M, the ring class field of $\mathcal{O}_s^\times$. Moreover, we may assume that F_s is the lift constructed before Proposition 4.5. Therefore, the formula for $v(F_s)$ in Proposition 4.5 shows that the valuation of $u(F_s)$ is equal to the reciprocal of the degree $[M_s : M]$. This concludes the proof. □

Corollary 4.8. — *Let F_s and F_{s+1} be quasi-canonical lifts of level s and $s+1$, respectively. Let $\beta : F_s \to F_{s+1}$ be an isogeny of height one. Then $H := \ker(\beta)$ is not the canonical subgroup, and*

$$v(\mathrm{Lie}(\beta)) = v(F_{s+1}).$$

Proof. — We note that β identifies F_{s+1} with the quotient F_s/H. It follows from the proof of Proposition 4.6 that H is not the canonical subgroup of F_s and that therefore the nonzero elements $x \in H$ have valuation

$$v(x) = \frac{v(F_s)}{q^2 - q}.$$

Set $b := \mathrm{Lie}(\beta)$. The formula for β in terms of H (see Theorem 2.1) shows that

$$v(b) = \sum_{x \in H - \{0\}} v(x) = \frac{v(F_s)}{q}.$$

By Corollary 4.7, this is equal to $v(F_{s+1})$. □

5. Some complements

We prove some technical results which are needed in [**R**].

5.1. Let K and k be as before. Let G be the formal $\mathcal{O}_K$-module of height two over k, with endomorphism ring $\mathcal{O}_D$. We have seen in [**VZ**] that the formal cohomology group $H^2(G, k)$ has dimension $h - 1 = 1$. Therefore, the universal deformation ring of G is $W[\![t]\!]$ (where $W = \hat{\mathcal{O}}_K^{\mathrm{nr}}$ is the completion of the maximal unramified extension of $\mathcal{O}_K$).

Let A be a complete local $\mathcal{O}_K$-algebra with residue field k and $I \lhd A$ an ideal with $\mathfrak{m}_A \cdot I = 0$. Set $\bar{A} := A/I$. Let F, F' be two deformations of G over A and $\bar{\alpha} : F \otimes \bar{A} \to F' \otimes \bar{A}$ a homomorphism which is defined modulo I. Then the obstruction for lifting $\bar{\alpha}$ to a homomorphism $\alpha : F \to F'$ is an element of the k-vector space

$$H^2(G, I) \cong H^2(G, k) \otimes_k I.$$

Indeed, as in [**VZ**, Section 3], a lift $\alpha(X) \in A[\![X]\!]$ of $\bar{\alpha}$ as a power series defines a cocycle $(\Delta; \delta_a)$,

$$\Delta(X, Y) := \alpha(X +_F Y) -_{F'} \alpha(X) -_{F'} \alpha(Y),$$
$$\delta_a(X) := \alpha([a]_F(X)) -_{F'} [a]_{F'}(\alpha(X)).$$

The cohomology class of this cocycle is independent of the chosen lift α. It vanishes if and only if there exists some lift α which is a homomorphism $F \to F'$. If this is the case, then the lift which is a homomorphism is unique.

Let F be the universal deformation of G over $W[\![t]\!]$, and let F' be another universal deformation over $W[\![t']\!]$. Hence the pair (F, F') is defined over the formal scheme $\mathcal{S} = \mathrm{Spf}\, R$, where $R := W[\![t, t']\!]$.

Proposition 5.1. — *Let $\alpha : G \to G$ be an isogeny,* i.e., *$\alpha \neq 0$. Let J be the minimal ideal of R such that α lifts to an isogeny $F \to F'$ modulo J. Then the closed formal subscheme $\mathcal{T}$ of $\mathcal{S}$ defined by J is a relative divisor over* $\operatorname{Spf} W$.

Proof. — We have to show that J is generated by one element which is neither a unit nor divisible by p. Suppose, for the moment, that $\alpha \notin \mathcal{O}_K$ and set $L = K(\alpha) \subset D$. Let M be the completion of the maximal unramified extension of L and F_1 the canonical lift of G with respect to $\mathcal{O}_L \subset \mathcal{O}_D$ (which is defined over $\mathcal{O}_M$). There is a unique homomorphism of $\mathcal{O}_K$-algebras $\varphi : W[\![t, t']\!] \to \mathcal{O}_M$ which induces the identity on k, such that the pair (F_1, F_1) is $*$-isomorphic to the pullback of the pair (F, F') *via* φ. By construction, J is contained in the kernel of φ. This shows $J \neq R$, at least if $\alpha \notin K$. The case $\alpha \in K$ is handled in a similar way.

Suppose that $J \subset (\pi)$. This means that α lifts to an isogeny $F \to F'$ over $k[\![t, t']\!]$. Setting $t' = 0$, the isogeny α would then induce an isogeny between $F \otimes_{W[\![t]\!]} k((t))$ and $G \otimes_k k((t))$. But $F \otimes_{W[\![t]\!]} k((t))$ has height $h - 1 = 1$ (see [**VZ**]) and is therefore not isogenous to the height-two module $G \otimes_k k((t))$. This gives a contradiction and shows that $J \not\subset (\pi)$.

Let $\mathfrak{m}$ denote the maximal ideal of R. Set $A := R/\mathfrak{m}J$ and $I := J/\mathfrak{m}J$. Then $\mathfrak{m} \cdot I = 0$, and $\bar{A} = A/I \cong R/J$. Clearly, α lifts to a homomorphism $F \otimes \bar{A} \to F' \otimes \bar{A}$ but *not* to a homomorphism $F \otimes A \to F' \otimes A$. The responsible obstruction is a nonzero element in

$$H^2(G, I) \cong H^2(G, k) \otimes_k I \cong I.$$

Let f be the image of this obstruction in I. The element f depends on the choice of an isomorphism $H^2(G, k) \cong k$, but the ideal $(f) \lhd A$ does not. Clearly, α lifts to a homomorphism $F \otimes A' \to F' \otimes A'$ over the ring $A' = A/(f)$. This implies $I = (f)$. Now Nakayama's Lemma shows that J is generated by one element. The proposition is proved. □

5.2. Let A be the ring of integers of a finite extension of the fraction field of W. Let λ denote a uniformizer of A. For each positive integer n, we set $A_n := A/(\lambda^{n+1})$ and $M_n := (\lambda^n)/(\lambda^{n+1})$.

Let F_1, F_2, F_3 be three lifts of G over A. We define

$$H_n := \operatorname{Hom}(F_1 \otimes A_n, F_2 \otimes A_n), \quad H'_n := \operatorname{Hom}(F_1 \otimes A_n, F_3 \otimes A_n).$$

As for endomorphisms, the natural reduction maps $H_n, H'_n \to \operatorname{End}(G) = \mathcal{O}_D$ are injective. We will consider H_n and H'_n as subsets of $\mathcal{O}_D$. Note that H_n and H'_n are in fact sub-$\mathcal{O}_K$-modules of $\mathcal{O}_D$. The obstruction theory reviewed above gives injective maps

$$\kappa_n : H_{n-1}/H_n \hookrightarrow H^2(G, M_n), \qquad \kappa'_n : H'_{n-1}/H'_n \hookrightarrow H^2(G, M_n).$$

Proposition 5.2. — *Let $\alpha : G \to G$ be an isogeny defined over k which does not lift to a homomorphism $F_1 \to F_2$. Let n be the unique positive integer such that $\alpha \in$*

$H_{n-1} - H_n$. Let $\beta : F_2 \to F_3$ be an isogeny defined over A, and let m denote the valuation of $b := \mathrm{Lie}(\beta) \in A$. We make the following assumptions:

1. *β has height one.*
2. *$m \leq (q-1)n$.*

Then $\beta \circ \alpha \in H'_{n+m-1} - H'_{n+m}$.

Proof. — (compare with the proof of Lemma 1.3) We may represent α as a power series with coefficients in A without constant coefficient such that α_{n-1}, the reduction of α modulo λ^n, is a homomorphism $F_1 \otimes A_{n-1} \to F_2 \otimes A_{n-1}$. We define

$$\epsilon := \alpha \circ [\pi]_{F_1} - [\pi]_{F_2} \circ \alpha.$$

Then $\epsilon \equiv 0 \pmod{\lambda^n}$. Moreover, we have $\epsilon \equiv \delta_\pi \pmod{\lambda^{n+1}}$, where $(\Delta, \{\delta_a\})$ denotes the cocycle associated to α_n. The assumption $\alpha \notin H_n$ implies $\epsilon(X) = cX^q + \ldots$, with $\mathrm{ord}_\lambda(c) = n$. Similarly, define

$$\epsilon' := \beta \circ \alpha \circ [\pi]_{F_1} - [\pi]_{F_3} \circ \beta \circ \alpha.$$

Then $\epsilon' = \beta \circ \epsilon$. Write $\beta(X) = \sum_i b_i X^i$. It follows from Assumption 1 that the Newton polygon of β has slope $-m/(q-1)$ over $[1, \ldots, q]$. This means that

$$\mathrm{ord}_\lambda(b_i) \geq \frac{q-i}{q-1} \cdot m, \quad i = 1, \ldots, q$$

(with equality for $i = 1, q$). Now Assumption 2, together with an easy calculation, shows that

$$\epsilon' = \beta \circ \epsilon = b_1 c X^q + \cdots \equiv 0 \quad (\lambda^{n+m}).$$

Since $\mathrm{ord}_\lambda(b_1 c) = n + m$, we conclude as in the proof of Lemma 1.3 that $\beta \circ \alpha \in H'_{n+m-1} - H'_{n+m}$. □

Corollary 5.3. — *Suppose that F_1, F_2, F_3 are quasi-canonical liftings of G of level $r, s, s+1$ (with respect to some embedding $\kappa : L \hookrightarrow D$). Suppose that $r \leq s$. Suppose, moreover, that A is the minimal $\mathcal{O}_K$-algebra over which the lifts F_1, F_2, F_3 can be defined. (By Theorem 3.2 and Corollary 4.7, A is the ring of integers of the ring class extension of $\mathcal{O}_{s+1}$.)*

Let $\alpha : G \to G$ be an element of $\mathcal{O}_D$ and $\beta : F_2 \to F_3$ an isogeny of height one, defined over A. We assume that α does not lift to a homomorphism $F_1 \to F_2$. Let n be the maximal integer such that α can be lifted to a homomorphism $F_1 \to F_2$ modulo λ^n. Then $\beta \circ \alpha$ can be lifted to a homomorphism $F_1 \to F_3$ modulo λ^{n+1}, but not *modulo λ^{n+2}.*

Proof. — It follows from Corollary 4.8 that $\mathrm{ord}_\lambda(\mathrm{Lie}(\beta)) = 1$. Hence we can apply Proposition 5.2, which proves the corollary. □

References

[D] V. G. Drinfel'd – Elliptic modules, *Math. USSR Sbornik* **23** (1974), no. 4, p. 561–592.

[G] B. H. Gross – On canonical and quasi-canonical liftings, *Invent. math.* **84** (1986), p. 321–326.

[H] M. Hazewinkel – *Formal groups and Applications*, Academic Press, 1978.

[HG] M. J. Hopkins & B. H. Gross – Equivariant vector bundles on the Lubin-Tate moduli space, in *Topology and representation theory (Evanston, IL, 1992)*, Contemp. Math., vol. 158, 1994, p. 23–88.

[L] J. Lubin – *Canonical subgroups of formal groups*, Trans. Amer. Math. Soc., vol. 251, 1979.

[LT1] J. Lubin & J. Tate – Formal complex multiplication in local fields, *Ann. Math.* **81** (1965), p. 380–387.

[LT2] ———, Formal moduli for one-parameter formal Lie groups, *Bull. Soc. Math. France* **94** (1966), p. 49–60.

[R] M. Rapoport – Deformations of isogenies of formal groups, this volume, p. 139–169.

[S] J.-P. Serre – *Corps locaux*, Hermann, 1968.

[VZ] E. Viehmann & K. Ziegler – Formal moduli of formal $\mathcal{O}_K$-modules, this volume, p. 57–66.

[Yu] J. K. Yu – On the moduli of quasi-canonical liftings, *Compositio Math.* **96** (1995), no. 3, p. 293–321.

S. Wewers, IWR, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
E-mail : stefan.wewers@iwr.uni-heidelberg.de

Astérisque
312, 2007, p. 87–98

9. CANONICAL AND QUASI-CANONICAL LIFTINGS IN THE SPLIT CASE

by

Volker Meusers

Abstract. — Following Gross we sketch a theory of quasi-canonical liftings when the formal $\mathcal{O}_K$-module of height two and dimension one is replaced by a divisible $\mathcal{O}_K$-module of height one and dimension one in the sense of Drinfel'd.

***Résumé* (Relèvements canoniques et quasi-canoniques dans le cas déployé).** — Suivant Gross, on donne une théorie de relèvements quasi-canoniques dans le cas où le $\mathcal{O}_K$-module de hauteur deux et de dimension un est remplacé par un $\mathcal{O}_K$-module divisible de hauteur un et de dimension un au sens de Drinfel'd.

In this paper, we follow up on a remark by Gross [**G**] and discuss a theory of quasi-canonical liftings when the formal $\mathcal{O}_K$-module of height two and dimension one considered in [**Ww1**] is replaced by a divisible $\mathcal{O}_K$-module of height one and dimension one in the sense of Drinfel'd [**D**]. In this situation the statements analogous to those in [**G**], [**Ww1**] are easy consequences of Lubin-Tate theory and of a slight modification of the Serre-Tate theorem for ordinary elliptic curves, as discussed in the appendix to [**Mes**].

1. Formal moduli of divisible $\mathcal{O}_K$-modules

Let K be a field complete with respect to some discrete valuation. Let $\mathcal{O}_K$ be its ring of integers, $\mathfrak{p} = (\pi)$ its maximal ideal. We assume the residue field $\mathcal{O}_K/\mathfrak{p}$ to be finite and let q denote the number of its elements. For any non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ we set $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$, *i.e.*, $N(\mathfrak{p}^s) = q^s$. Let k be an algebraic closure of $\mathcal{O}_K/\mathfrak{p}$. Let M be the completion of the maximal unramified extension of K in some fixed separable closure K^{sep}. Denote the completion of K^{sep} by C. Let $\mathcal{O}_M$ and $\mathcal{O}_C$ be the rings of integers in M and C respectively.

Following [**D**, §4] a formal group is a group object in the category of formal schemes. For example any group scheme or any discrete group is a formal group in this sense.

2000 ***Mathematics Subject Classification.*** — 11G15, 14K07, 14K22, 14L05.
Key words and phrases. — Quasi-canonical liftings, complex multiplication, Lubin-Tate formal groups, Serre-Tate theorem.

For a formal group F let us denote by F° its connected component. Let $\widehat{\mathcal{C}}$ be the category of complete local noetherian $\mathcal{O}_M$-algebras with residue field k.

Definition 1.1. — Let $R \in \widehat{\mathcal{C}}$. A divisible $\mathcal{O}_K$-module over R is a pair F, where F is a formal group over R and $\gamma_F \colon \mathcal{O}_K \to \mathrm{End}_R(F)$ is a homomorphism such that F° is a formal $\mathcal{O}_K$-module of height $h < \infty$ in the sense of [**VZ**], and such that

$$F/F^\circ \cong (K/\mathcal{O}_K)^j_{\mathrm{Spf}(R)}$$

for some $j < \infty$. The pair (h, j) will be called type of F.

To ease the notation, we will suppress the structure map γ_F of an $\mathcal{O}_K$-module F and simply write F.

Drinfel'd shows that a divisible $\mathcal{O}_K$-module over k is up to isomorphism given by its type (h, j) (see [**D**, §4]).

Example 1.2. — For $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$ the product group $G = \widehat{\mathbb{G}}_{m,R} \times (\mathbb{Q}_p/\mathbb{Z}_p)_R$ is an example of a divisible module of type $(h, j) = (1, 1)$ over R.

If $R \in \widehat{\mathcal{C}}$ is artinian then the category of fppf-abelian sheaves on R with $\mathcal{O}_K$-structure is an abelian category, the category of $\mathcal{O}_K$-modules over R. It is useful to view the category of divisible $\mathcal{O}_K$-modules over R as a full sub-category of this category.

Definition 1.3. — Fix a divisible $\mathcal{O}_K$-module G over k. A deformation of G to $R \in \widehat{\mathcal{C}}$ is a pair (F, ψ) consisting of a divisible $\mathcal{O}_K$-module F over R together with an isomorphism $\psi \colon F \otimes_R k \xrightarrow{\cong} G$ of $\mathcal{O}_K$-modules.

The deformations of G to $R \in \widehat{\mathcal{C}}$ form a category in a natural way. One checks that it is a groupoid and moreover that no object of this groupoid has non-trivial automorphisms. The last point is due to the fact that for a deformation F the isomorphism ψ is part of the data. Nevertheless we often omit ψ from the notation.

Definition 1.4. — For any $R \in \widehat{\mathcal{C}}$ let us denote by $\mathcal{D}_G(R)$ the set of isomorphism classes of the groupoid of deformations of G to R. Then $\mathcal{D}_G$ becomes a set-valued functor on $\widehat{\mathcal{C}}$.

Fix a formal $\mathcal{O}_K$-module H_0 of height $h = 1$ over k. It has a trivial deformation space, *i.e.*, $\mathcal{D}_{H_0}(R) = \{\text{point}\}$ for any $R \in \widehat{\mathcal{C}}$. More precisely $\mathcal{D}_{H_0}$ is representable by $\mathcal{O}_M$. This follows easily from the uniqueness of Lubin-Tate modules (see [**Me1**]; see also Remark 1.11(ii) for a far more general result of Drinfel'd). Let us denote by H the unique lift of H_0 to $\mathcal{O}_M$. We assume, as we may, that H is given as the base change

$$H = H_f \otimes_{\mathcal{O}_K} \mathcal{O}_M,$$

where H_f is the Lubin-Tate module over $\mathcal{O}_K$ corresponding to some fixed prime element $\pi \in \mathcal{O}_K$ and some fixed Lubin-Tate series $f \in \mathcal{F}_\pi$. Recall from [**Me1**, Lemma 1.7] that the isomorphism class of H does not depend on these choices. Recall further that for any $R \in \widehat{\mathcal{C}}$ we have $H(R) = \mathfrak{m}_R$ as a set. The $\mathcal{O}_K$-module structure is given as follows: For $q, q' \in H(R)$ and $z \in \mathcal{O}_K$ we have $q +_H q' = H(q, q')$ and $z \cdot_H q = [z]_f(q)$. We often omit the subscript H from the notation.

Now fix some divisible $\mathcal{O}_K$-module G over k of height $h = 1$ such that there is an isomorphism $G/G^\circ \cong (K/\mathcal{O}_K)_k$. Fix an isomorphism of divisible $\mathcal{O}$-modules

$$r \colon G \xrightarrow{\cong} H_0 \times (K/\mathcal{O}_K)_k$$

where H is the unique lift of G° to $\mathcal{O}_M$ as above. Two such isomorphisms differ by an element of the automorphism group of the right hand side. This group is described by the following easy but important lemma.

Lemma 1.5

(1) We have

$$\mathrm{Hom}_{\mathcal{O}_K,k}((K/\mathcal{O}_K)_k, H_0) = \{0\} = \mathrm{Hom}_{\mathcal{O}_K,k}(H_0, (K/\mathcal{O}_K)_k)$$

and

$$\mathrm{End}_{\mathcal{O}_K,k}(H_0) = \mathcal{O}_K = \mathrm{End}_{\mathcal{O}_K,k}((K/\mathcal{O}_K)_k).$$

(2) In particular there is a canonical isomorphism

$$\mathcal{O}_K \times \mathcal{O}_K \longrightarrow \mathrm{End}_{\mathcal{O}_K,k}(H_0 \times (K/\mathcal{O}_K)_k).$$

It induces an isomorphism

$$\mathcal{O}_K^\times \times \mathcal{O}_K^\times \longrightarrow \mathrm{Aut}_{\mathcal{O}_K,k}(H_0 \times (K/\mathcal{O}_K)_k).$$

Proof. — It clearly suffices to prove the first point. We have

$$\mathrm{Hom}_{\mathcal{O}_K,k}((K/\mathcal{O}_K)_k, H_0) = \mathrm{Hom}_{\mathcal{O}_K}(K/\mathcal{O}_K, H_0(k)) = \{0\}$$

by adjunction and because $H_0(k) = \{0\}$. We have

$$\mathrm{Hom}_{\mathcal{O}_K,k}(H_0, (K/\mathcal{O}_K)_k) = \mathrm{Hom}_{\mathcal{O}_K,k}(H_0, (K/\mathcal{O}_K)_k^\circ) = \{0\}$$

because H_0 is connected and $(K/\mathcal{O}_K)^\circ = \{0\}$. We have

$$\mathrm{End}_{\mathcal{O}_K,k}(H_0) = \mathcal{O}_K$$

because by Lubin-Tate theory every endomorphism of H_0 is uniquely given by its differential at zero. We have

$$\mathrm{End}_{\mathcal{O}_K,k}((K/\mathcal{O}_K)_k) = \mathrm{End}_{\mathcal{O}_K}(K/\mathcal{O}_K)$$

by adjunction. Since the natural map

$$\mathcal{O}_K \longrightarrow \mathrm{End}_{\mathcal{O}_K}(K/\mathcal{O}_K)$$

is well known to be an isomorphism we are done. □

We want to sketch a proof of the following theorem (compare the analogous statement in [**VZ**, Theorem 3.8]):

***Theorem 1.6* (Universal deformation).** — *For any $R \in \widehat{\mathcal{C}}$ and fixed isomorphism r there is a natural isomorphism*

$$\eta_R \colon \mathcal{D}_G(R) \xrightarrow{\cong} H(R).$$

In particular $\mathcal{D}_G$ can be given the structure of an $\mathcal{O}_K$-module (depending on r of course). Since we assume $H = H_f \otimes_{\mathcal{O}_K} \mathcal{O}_M$, the $\mathcal{O}_K$-module structure is given by Lubin-Tate theory as recalled above.

The proof will take up the rest of this section. One proceeds as in [**Mes**, appendix]: In the course of the proof we will identify both, $\mathcal{D}_G(R)$ and $H(R)$ for $R \in \widehat{\mathcal{C}}$ artinian, with a certain Ext-group. So let us briefly recall the definition and some basic properties of these groups. A careful discussion can be found in [**Mt**, chapter VII].

For objects M'' and M' of an abelian category $\mathcal{A}$ let

$$\mathcal{E}xt_{\mathcal{A}}(M'', M')$$

denote the groupoid of extensions $(M, p, i) \colon M' \overset{i}{\hookrightarrow} M \overset{p}{\twoheadrightarrow} M''$. It is well known that the map

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{A}}(M'', M') & \longrightarrow & \mathrm{Aut}_{\mathcal{E}xt_{\mathcal{A}}(M'', M')}((M, p, i)) \\ \varphi & \longmapsto & \mathrm{id}_M + i \circ \varphi \circ p \end{array}$$

is an isomorphism of groups. In particular the automorphism group of (M, p, i) is trivial if and only if $\mathrm{Hom}_{\mathcal{A}}(M'', M')$ is. Let

$$\mathrm{Ext}_{\mathcal{A}}(M'', M')$$

be the class of isomorphism classes of $\mathcal{E}xt_{\mathcal{A}}(M'', M')$. Assume it to be a set. Sometimes we will not distinguish an extension from its isomorphism class. Using Baer-addition $\mathrm{Ext}_{\mathcal{A}}(M'', M')$ becomes an abelian group in the usual way. For $N' \in \mathcal{A}$ let

$$\delta_{(M,p,i),N'} \colon \mathrm{Hom}_{\mathcal{A}}(M', N') \longrightarrow \mathrm{Ext}_{\mathcal{A}}(M'', N'). \tag{1.1}$$

be the boundary homomorphism.

Apply this in the case that $\mathcal{A}$ is the category of $\mathcal{O}_K$-modules on some fixed artinian $R \in \widehat{\mathcal{C}}$. In this case the Ext-groups are in fact $\mathcal{O}_K$-modules.

***Definition 1.7*.** — Let $R \in \widehat{\mathcal{C}}$ be artinian. For any two $\mathcal{O}_K$-modules M' and M'' over R let

$$\mathrm{Ext}_{\mathcal{O}_K, R}(M'', M')$$

denote the $\mathcal{O}_K$-module of extension classes of M'' by M' constructed above.

Recall that we view the category of divisible $\mathcal{O}_K$-modules on artinian R as a full sub-category of the category of all $\mathcal{O}_K$-modules.

Lemma 1.8 (compare [**Mes**, I.2.4.3]). — *Let $R \in \widehat{\mathcal{C}}$ be artinian. Given an extension of the form*

$$H_R \overset{i}{\hookrightarrow} F \overset{p}{\hookrightarrow} (K/\mathcal{O}_K)_R$$

of $\mathcal{O}_K$-modules over R, then F is a divisible $\mathcal{O}_K$-module such that $F^\circ \cong H_R$ and $F/F^\circ \cong (K/\mathcal{O}_K)_R$. If one uses the isomorphism $r\colon G \overset{\cong}{\to} H_0 \times (K/\mathcal{O}_K)_k$ then F becomes a deformation of G to R. This association yields a functor between the groupoid of extensions of $(K/\mathcal{O}_K)_R$ by H_R and the groupoid of deformations of G to R.

Proof. — Since $(K/\mathcal{O}_K)_R$ is totally disconnected and H_R is connected it follows that $i\colon H_R \overset{\cong}{\to} F^\circ$. The snake lemma implies that p induces an isomorphism $p'\colon F/F^\circ \overset{\cong}{\to} (K/\mathcal{O}_K)_R$. It follows that F is divisible. Since $H_R(k) = \{0\}$ the extension $H_R \hookrightarrow F \twoheadrightarrow (K/\mathcal{O}_K)_R$ yields an injective map $F(k) \hookrightarrow (K/\mathcal{O}_K)_R(k) = K/\mathcal{O}_K$. Since k is algebraically closed it is an isomorphism. This isomorphism gives us a canonical splitting map $(K/\mathcal{O}_K)_k \hookrightarrow F \otimes k$. Thus the extension is canonically split over k. Together with the identification $r\colon G \overset{\cong}{\to} H_0 \times (K/\mathcal{O}_K)_k$ we get an isomorphism $\psi\colon F \otimes k \overset{\cong}{\to} G$ such that the pair (F, ψ) is a deformation of G. One checks that it is functorial. □

Proposition 1.9 (compare [**Mes**, appendix Prop.2.1]). — *Assume $R \in \widehat{\mathcal{C}}$ to be artinian. Then the functor of the preceding lemma is an equivalence of groupoids and there is a natural isomorphism*

$$\epsilon_R\colon \mathcal{D}_G(R) \overset{\cong}{\longrightarrow} \mathrm{Ext}_{\mathcal{O}_K,R}((K/\mathcal{O}_K)_R, H_R).$$

Proof. — fully faithful: It is enough to see that every object in either groupoid has a trivial automorphism group. For deformations, this was noted above. For extensions, recall that the automorphism group is isomorphic to $\mathrm{Hom}_{\mathcal{O}_K,R}((K/\mathcal{O}_K)_R, H_R) = \{0\}$.

essentially surjective: Let F be a deformation of G to R. We need to define homomorphisms $i\colon H_R \hookrightarrow F$ and $p\colon F \twoheadrightarrow (K/\mathcal{O}_K)_R$ such that $p \circ i = 0$. For this we let p on R-valued points be defined as follows :

$$F(R) \longrightarrow\!\!\!\!\!\rightarrow F(k) = F \otimes k(k) \underset{r\circ\psi}{\overset{\cong}{\longrightarrow}} H_0(k) \times (K/\mathcal{O}_K)_k(k) \underset{\mathrm{pr}_2}{\longrightarrow\!\!\!\!\!\rightarrow} K/\mathcal{O}_K = (K/\mathcal{O}_K)_R(R).$$

Since $K/\mathcal{O}_K$ is discrete the kernel of p equals F°. Because R is artinian local it follows that $F^\circ \otimes k = (F \otimes k)^\circ \cong G^\circ \cong H_0$. Since H_R is the unique lift of H_0 to R it follows that F° is isomorphic to H_R and we get the map $i\colon H_R \cong F^\circ \hookrightarrow F$. This proves the first assertion. The second follows by passage to isomorphism classes. □

To calculate the Ext-group, we use

Proposition 1.10. — *For any artinian $R \in \widehat{\mathcal{C}}$ the connecting homomorphism associated to the sequence $\mathcal{O}_K \hookrightarrow K \longrightarrow\!\!\!\!\!\rightarrow K/\mathcal{O}_K$ is an isomorphism*

$$\delta_R\colon H(R) = \mathrm{Hom}_{\mathcal{O}_K,R}(\mathcal{O}_K, H_R) \overset{\cong}{\longrightarrow} \mathrm{Ext}_{\mathcal{O}_K,R}((K/\mathcal{O}_K)_R, H_R).$$

Proof. — Assume $\mathfrak{m}_R^{n+1} = 0$ for some $n >> 0$. Then H is killed by $\mathfrak{p}^n$ (compare [**K**, Lemma 1.1.2]). Associated to the short exact sequence

$$(\mathcal{O}_K)_R \overset{i}{\hookrightarrow} K_R \overset{p}{\twoheadrightarrow} (K/\mathcal{O}_K)_R$$

and H_R we have the boundary map (1.1)

$$\delta_{(K_R,p,i),H_R} \colon \mathrm{Hom}_{\mathcal{O}_K,R}((\mathcal{O}_K)_R, H_R) \longrightarrow \mathrm{Ext}_{\mathcal{O}_K,R}((K/\mathcal{O}_K)_R, H_R).$$

If we identify $H(R)$ with $\mathrm{Hom}_{\mathcal{O}_K,R}((\mathcal{O}_K)_R, H_R)$ this gives us the desired map δ_R. Because the prime element $\pi \in \mathcal{O}_K$ acts invertibly on K and nilpotently on H one sees easily that

$$\mathrm{Hom}_{\mathcal{O}_K,R}(K, H) = \{0\} = \mathrm{Ext}_{\mathcal{O}_K,R}(K, H).$$

By the exactness of the long Ext-sequence, it follows that δ_R is an isomorphism. □

Proof of Theorem 1.6. — Combining Proposition 1.9 and Proposition 1.10 we get the desired isomorphism for artinian $R \in \widehat{\mathcal{C}}$ as

$$\eta_R = \delta_R^{-1} \circ \epsilon_R.$$

For general R we can pass to the limit over its artinian quotients. □

Remark 1.11

(i) How does one calculate the inverse of δ_R? For $R = k$ both sides are trivial and so is δ_k. In the general case δ_R^{-1} can be computed by an approximation process with respect to the "$\mathfrak{p}$-adic topology" on both $\mathrm{Ext}_{\mathcal{O}_K,R}(\mathcal{O}_K, H_R)$ and $H(R)$. For details we refer to [**K**, page 151f], [**Mes**, appendix].

(ii) In particular it follows from this theorem that the formal moduli space of the divisible module $G = H_0 \times (K/\mathcal{O}_K)_k$ is representable by a formal power series ring in one variable over $\mathcal{O}_M$. More generally, Drinfel'd shows that the formal moduli space of a divisible module of type (h, j) over k is representable by a power series ring in $h + j - 1$ variables (compare [**D**, Prop.4.5]).

Definition 1.12. — For $R \in \widehat{\mathcal{C}}$ and fixed r, let F be a lift of G to R. Let us set

$$q(F, r) = \eta_R(\text{ isom. class of } F) \in H(R).$$

We simply write $q(F)$ if γ_F and r are understood. As in [**Ww1**], Definition 4.1 we refer to the element $q(F) \in H(R) = \mathfrak{m}_R$ as the formal modulus or coordinate of the lift F.

Example 1.13. — If $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$, and $H = \widehat{\mathbb{G}}_m$ we are in the situation of [**Mes**], Appendix. If we let $q_{\mathrm{Tate}}(F) \in 1 + \widehat{\mathbb{G}}_m(R)$ denote the coordinate introduced in [**Mes**], then the relations are simply

$$q_{\mathrm{Tate}}(F) = 1 + q(F) \in 1 + \widehat{\mathbb{G}}_m(R).$$

and

$$q_{\mathrm{Tate}}(F)^z = (1 + q(F))^z = 1 + z \cdot_{\widehat{\mathbb{G}}_m} q(F).$$

2. Lifting endomorphisms

Let F and F' be deformations of G to R with coordinates $q = q(F), q' = q(F') \in H(R)$. We want to describe in terms of our chosen coordinates which endomorphisms $\rho_0 \in \mathrm{End}_{\mathcal{O}_K,R}(G)$ lift to homomorphisms $\rho\colon F \to F'$.

Proposition 2.1 (compare [**Mes**, Appendix Prop.3.3]). — *Let $\rho_0\colon F_0 \to F_0'$ be given by multiplication by z_1 on $(K/\mathcal{O}_K)_R$ and by multiplication by z_0 on $H(R)$. Then ρ_0 lifts to a (necessarily unique) homomorphism $\rho\colon F \to F'$ if and only if we have the equality*

$$z_1 q - z_0 q' = 0 \in H(R),$$

where the last expression is more precisely written as $[z_1]_H(q) -_H [z_0]_H(q')$.

Sketch of proof. — This follows from rigidity (see [**VZ**, Lemma 2.6], for formal $\mathcal{O}_K$-modules), the description of lifts in terms of extensions and the following well known and simple lemma applied to $M' = N' = H$, $M'' = N'' = K/\mathcal{O}_K$ and $\varphi = z_1$ and $\psi = z_0$. □

Lemma 2.2 (compare [**CE**, chap.XIV, exercise 18]). — *Let*

$$\begin{array}{ccccc} M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' \\ \downarrow{\scriptstyle\varphi} & & & & \downarrow{\scriptstyle\psi} \\ N' & \xrightarrow[i']{} & N & \xrightarrow[p']{} & N'' \end{array}$$

be a commutative diagram in an arbitrary abelian category. Then it can be completed by a homomorphism $\rho\colon M \to N$ if and only if the extension obtained by pushing out the upper sequence along φ is isomorphic to the extension obtained by pulling back the lower sequence along ψ.

Example 2.3. — For reasons explained above (see [**Me1**, Example 1.3]), the analogous formula of [**Mes**], Appendix reads:

$$(q_{\mathrm{Tate}})^{z_1}(q'_{\mathrm{Tate}})^{-z_0} = (1+q)^{z_1}(1+q')^{-z_0} = 1 + (z_1 q -_{\widehat{\mathbb{G}}_m} z_0 q') = 1.$$

Specialize to $R = \mathcal{O}_C$. As a consequence of proposition (1.9) we can describe the ring of endomorphisms of a lift F of F_0 to $\mathcal{O}_C$.

Corollary 2.4. — *Let F be a lift F of G to $\mathcal{O}_C$ with $q = q(F, r) \in H(\mathcal{O}_C)$. Then there are two cases:*

(i) If the annihilator of q in $\mathcal{O}_K$ is zero then the endomorphism ring of F equals $\mathcal{O}_K$.

(ii) If the annihilator of q in $\mathcal{O}_K$ is $\mathfrak{p}^s$ for some $0 \leq s < \infty$ then the endomorphism ring of F, as a subring of the ring of endomorphisms of G, is strictly bigger then $\mathcal{O}_K$ and is isomorphic to

$$\mathrm{End}_{\mathcal{O}_K,\mathcal{O}_C}(F) \cong \{(z_0, z_1) \in \mathcal{O}_K \times \mathcal{O}_K | z_0 - z_1 \in \mathfrak{p}^s\} \subseteq \mathcal{O}_K \times \mathcal{O}_K.$$

Proof. — This follows directly from the proposition with $q = q'$. Note that in this case

$$(z_1 \cdot_H q) -_H (z_0 \cdot_H q) = (z_1 - z_0) \cdot_H q = 0 \in H(R). \quad \square$$

3. Quasi-canonical lifts in the split case

We now show that the results on canonical and quasi-canonical liftings in [**Ww1**] and [**G**] have analogues in the present case. To bring out this analogy we introduce the following definitions:

Definition 3.1

(i) Set $L = K \times K$ and $\mathcal{O}_L = \mathcal{O}_K \times \mathcal{O}_K$. Embed K resp. $\mathcal{O}_K$ diagonally into L resp. $\mathcal{O}_L$.

(ii) From Lemma 1.5 we get an $\mathcal{O}_K$-linear isomorphism

$$\kappa\colon \mathcal{O}_L \xrightarrow{\cong} \mathrm{End}_{\mathcal{O}_K,k}(G).$$

(iii) The "completion of the maximal unramified extension" of L is given by $M_L = M \times M$ whose "separable closure" is $M_L^{\mathrm{sep}} = M^{\mathrm{sep}} \times M^{\mathrm{sep}}$.

(iv) Set

$$\Gamma_L = \mathrm{Gal}(M_L^{\mathrm{sep}}|M_L) = \mathrm{Gal}(M^{\mathrm{sep}}|M) \times \mathrm{Gal}(M^{\mathrm{sep}}|M).$$

By Lubin-Tate theory we have a reciprocity isomorphism

$$\rho_K^{\mathrm{ab}}\colon \mathrm{Gal}(M^{\mathrm{sep}}|M)^{\mathrm{ab}} \xrightarrow{\cong} \mathcal{O}_K^\times.$$

It induces a reciprocity isomorphism

$$\rho_L^{\mathrm{ab}} = (\rho_K^{\mathrm{ab}}, \rho_K^{\mathrm{ab}})\colon \Gamma_L^{\mathrm{ab}} \xrightarrow{\cong} \mathcal{O}_L^\times.$$

(v) For any integer $s \geq 0$ let

$$\mathcal{O}_s = \mathcal{O}_K + \mathfrak{p}^s\mathcal{O}_L = \{(z_0, z_1) \in \mathcal{O}_L | z_0 - z_1 \in \mathfrak{p}^s\}$$

be the "order" containing $\mathcal{O}_K$ of conductor $\mathfrak{p}^s$ or level s in $\mathcal{O}_L$.

(vi) For $s \geq 1$ let $M_s|M$ be the fixed field in M^{sep} of the inverse image under the reciprocity isomorphism ρ_K^{ab} of $(1 + \mathfrak{p}^s) \subset \mathcal{O}_K^\times$ in $\mathrm{Gal}(M^{\mathrm{sep}}|M))$, *i.e.*, such that reciprocity gives an isomorphism

$$\rho_K^{\mathrm{ab}}\colon \mathrm{Gal}(M_s|M) \xrightarrow{\cong} \mathcal{O}_K^\times/(1 + \mathfrak{p}^s).$$

Remark 3.2. — One easily sees that the map $\mathcal{O}_L^\times \to \mathcal{O}_K^\times$ given by sending $(x, y) \in \mathcal{O}_L^\times$ to the quotient $xy^{-1} \in \mathcal{O}_K^\times$ induces an isomorphism

$$\mathcal{O}_L^\times/\mathcal{O}_s^\times \xrightarrow{\cong} \mathcal{O}_K^\times/(1 + \mathfrak{p}^s).$$

If we let $\Gamma_s \subset \Gamma_L^{\mathrm{ab}}$ be the inverse image of $\mathcal{O}_s^\times$ in Γ_L^{ab} under ρ_L^{ab}, then we have the following commutative diagram

$$\begin{array}{ccc}
\Gamma_L^{\mathrm{ab}} & \xrightarrow[\cong]{\rho_L^{\mathrm{ab}}} & \mathcal{O}_L^\times \\
\downarrow & & \downarrow \\
\Gamma_L^{\mathrm{ab}}/\Gamma_s & \xrightarrow{\cong} & \mathcal{O}_L^\times/\mathcal{O}_s^\times \\
{\scriptstyle (\sigma,\tau)\mapsto\sigma\tau^{-1}}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle (x,y)\mapsto xy^{-1}} \\
\mathrm{Gal}(M_s|M) & \xrightarrow[\cong]{} & \mathcal{O}_K^\times/(1+\mathfrak{p}^s)
\end{array}$$

where "$\cong$" denotes isomorphisms. In this sense we may consider $M_s|M$ to be the "ring class field" of the "order" $\mathcal{O}_s \subseteq \mathcal{O}_L$.

Definition 3.3. — A quasi-canonical lift of G of level $s \geq 0$ (with respect to κ) is a lift F of G to $\mathcal{O}_C$ already defined over the ring of integers of some finite extension of M, together with an $\mathcal{O}_K$-algebra isomorphism $\mathcal{O}_s \xrightarrow{\cong} \mathrm{End}_{\mathcal{O}_K,\mathcal{O}_C}(F')$. A quasi-canonical lift of level $s = 0$ is also called canonical.

Proposition 3.4 (compare [**Ww1**, §1.3]). — *Let F be a lift of G. Then the following statements are equivalent:*

(1) The lift F is canonical, i.e., *defined over some finite extension of M and such that* $\mathrm{End}_{\mathcal{O}_K,\mathcal{O}_C}(F) = \mathrm{End}_{\mathcal{O}_K,k}(G) \cong \mathcal{O}_K \times \mathcal{O}_K$.

(2) The lift F is isomorphic to $H_{\mathcal{O}_M} \times (K/\mathcal{O}_K)_{\mathcal{O}_M}$.

In particular there exists a canonical lift and it is unique up to unique isomorphism. The formal modulus of a canonical lift F_{can} is $q(F_{can}) = 0$ and thus independent of the chosen isomorphism r.

Proof. — Clearly, the lift $F = H_{\mathcal{O}_M} \times (K/\mathcal{O}_K)_{\mathcal{O}_M}$ is canonical. To show that any canonical lift is isomorphic to the product, note that the endomorphism ring of a canonical lift contains the images e_{inf} and e_{et} of $(1,0) \in \mathcal{O}_L$ and $(0,1) \in \mathcal{O}_L$. They satisfy $e_{\mathrm{inf}}^2 = e_{\mathrm{et}}^2 = 1$ and $e_{\mathrm{inf}} + e_{\mathrm{et}} = 1$ and hence define a splitting

$$F \cong \mathrm{Im}(e_{\mathrm{inf}}) \times \mathrm{Im}(e_{\mathrm{et}})$$

as claimed. Given two canonical lifts, the element $(1,1) \in \mathcal{O}_L$ induces a canonical isomorphism. For the last claim simply observe that the split extension is the image of $0 \in H(\mathcal{O}_C)$ under $\delta_{\mathcal{O}_C}$ by construction. □

Proposition 3.5 (compare [**Ww1**, §3] and [**G**, Prop.5.3])

(1) Quasi-canonical liftings F_s exist for all levels $s \geq 0$.

(2) Liftings of level s are rational over the ring of integers $\mathcal{O}_{M_s}$ of M_s. Their isomorphism classes are permuted simply transitively under the action of the Galois group

$$\mathrm{Gal}(M_s|M) \cong \mathcal{O}_L^\times/\mathcal{O}_s^\times \cong (\mathcal{O}_L/\mathfrak{p}^s\mathcal{O}_L)^\times/(\mathcal{O}_K/\mathfrak{p}^s)^\times$$

which has order

$$|\operatorname{Gal}(M_s|M)| = \begin{cases} q^s\left(1-\frac{1}{q}\right) & : \quad s \geq 1 \\ 1 & : \quad s = 0 \end{cases}$$

In particular M_s is the smallest extension of M over which a quasi-canonical lift can be defined.

(3) The formal modulus $q(F_s) \in H(\mathcal{O}_{M_s}) = H(\mathcal{O}_C)$ of a quasi-canonical lift of level s is a uniformizing element of $\mathcal{O}_{M_s}$. In particular, for $s \geq 1$ the $\mathcal{O}_K$-modules F_s and F_{can} are not isomorphic over $\mathcal{O}_{M_s}/\mathfrak{m}_{M_s}^2$.

Proof. — For the first point recall that it follows from Lubin-Tate theory that $H(\mathcal{O}_C)_{\text{torsion}} \cong K/\mathcal{O}_K$ as $\mathcal{O}_K$-modules. Thus there are elements $q_s \in H(\mathcal{O}_C)$ with annihilator $\mathfrak{p}^s$ for any given $s \geq 0$. This implies the existence of a lift $F_s/\mathcal{O}_C$ with formal modulus q_s. By Corollary 2.4 the endomorphism ring of F_s is isomorphic to $\mathcal{O}_s$. If $s = 0$ then $F_{can} = H \times K/\mathcal{O}_K$ is a canonical lift and it is clearly defined over M. If $s \geq 1$ then the stabilizer of the formal modulus q_s, *i.e.*, $1 + \operatorname{Ann}(q_s)$, equals $1 + \mathfrak{p}^s \subset \mathcal{O}_K^\times$. Thus again by Lubin-Tate theory its isomorphism class is stable under the Galois group $\operatorname{Gal}(M^{\text{sep}}|M_s)$ since the identification of $\mathcal{D}_{F_0}(\mathcal{O}_C)$ with $H(\mathcal{O}_C)$ is compatible with the action of $\operatorname{Gal}(M^{\text{sep}}|M)$. Since deformations have no non-trivial automorphisms, this induces a Galois action on the chosen lift $F_s/\mathcal{O}_C$ itself. It follows that F_s descends to a formal $\mathcal{O}_K$-module over $\mathcal{O}_{M_s} = \mathcal{O}_C \cap M_s$.

For the second point note that the first isomorphism follows from Remark 3.2. One checks easily that the natural map

$$\mathcal{O}_L^\times/\mathcal{O}_s^\times \longrightarrow (\mathcal{O}_L/\mathfrak{p}^s\mathcal{O}_L)^\times/(\mathcal{O}_K/\mathfrak{p}^s)^\times$$

is an isomorphism. For $s \geq 1$ it follows from Lubin-Tate theory that

$$|\mathcal{O}_K^\times/1+\mathfrak{p}^s| = N(\mathfrak{p})^{s-1}(N(\mathfrak{p})-1) = |\operatorname{Gal}(M_s|M)|$$

as claimed .

The last point also follows from Lubin-Tate theory (see [**Me1**]), for one knows that $N_{M_s|M}(-q_s) = \pi$ and hence

$$v_{M_s|M}(q_s) = \frac{1}{[M_s:M]} v_M(N_{M_s|M}(q_s)) = \frac{1}{[M_s:M]}$$

as claimed. Therefore $q_s \in \mathfrak{m}_{M_s} \backslash \mathfrak{m}_{M_s}^2$ for $s \geq 1$. But the canonical lift has formal modulus $q_{can} = 0 \in \mathfrak{m}_{M_s}^2$. It follows that $q_s \not\equiv q_{can} \bmod \mathfrak{m}_{M_s}^2$. □

Remark 3.6

(i) The degree formula in the proposition can be written in a uniform way as

$$|\operatorname{Gal}(M_s|M)| = N(\mathfrak{p}^s) \prod_{\mathfrak{l}|\mathfrak{p}^s} \left(1 - \left(\frac{L}{\mathfrak{l}}\right) \frac{1}{N(\mathfrak{l})}\right)$$

where one formally sets

$$\left(\frac{L}{\mathfrak{l}}\right) = +1, -1, 0$$

according as $\mathfrak{l} = \mathfrak{p}$ is split (our case), inert or ramified (the cases treated in [**Ww1**]) in the extension $L|K$.

(ii) Let E_0 be an ordinary elliptic curve over $\overline{\mathbb{F}}_p$. Then one knows that its endomorphism ring is isomorphic to some order $\mathcal{O} \subset L$ in some imaginary quadratic field L. Let $c_0 \in \mathbb{Z}$ be the conductor of $\mathcal{O}$. It is known that p does not divide c_0. Set $c_s = p^s c_0$ and $\mathcal{O}_s = \mathbb{Z} + p^s\mathcal{O}$. Let $M_s|L$ be the ring class field of the order $\mathcal{O}_s$. For example if $c_0 = 1$ and $s = 0$ then $M_s = M$ is the Hilbert class field of L, *i.e.*, the maximal unramified abelian extension of L. In this situation one has Deuring's lifting theorem (compare [**L**, chap.13,§4,§5]). It guarantees the existence of an elliptic curve E_s over M_s with complex multiplication by $\mathcal{O}_s$ and such that the reduction of E_s at some prime of degree one over p is isomorphic to E_0 (same notational conflict as in the local case). The j-invariants of the different curves E_s are permuted simply transitively by the Galois group $\mathrm{Gal}(M_s|M)$. By the well known formula for the class numbers of orders in imaginary quadratic fields (see [**S**, exercise 4.12]) the Galois group has order

$$|\operatorname{Gal}(M_s|M)| = \frac{h(\mathcal{O}_s)}{h(\mathcal{O})} = \frac{|\mathcal{O}_s^\times|}{|\mathcal{O}^\times|} \cdot \frac{c_s}{c_0} \prod_{l|\frac{c_s}{c_0}} \left(1 - \left(\frac{L}{l}\right)\frac{1}{l}\right).$$

where the symbol $\left(\frac{L}{l}\right)$ is defined as in (i). The extra factor $\frac{|\mathcal{O}_s^\times|}{|\mathcal{O}^\times|}$ is due to the presence of nontrivial automorphisms in this situation. It is trivial for $L \neq \mathbb{Q}(i), \mathbb{Q}(e^{\frac{2\pi i}{3}})$. This statement of a global nature is thus completely analogous to the local statement of Proposition 3.5.

References

[CE] H. Cartan & S. Eilenberg – *Homological algebra*, 1956.

[D] V. G. Drinfel'd – Elliptic modules, *Math. USSR, Sb.* **23** (1974), p. 561–592.

[G] B. H. Gross – On canonical and quasi-canonical liftings, *Invent. Math.* **84** (1986), p. 321–326.

[K] N. Katz – Serre-Tate local moduli, in *Surfaces algebriques, Sémin. de géométrie algébrique, Orsay 1976-78*, Springer Lect. Notes Math., vol. 868, 1981, p. 138–202.

[L] S. Lang – *Elliptic functions*, Addison-Wesley, 1973.

[Mes] W. Messing – *The crystals associated to Barsotti-Tate groups: with applications to Abelian schemes*, Springer Lect. Notes Math., vol. 264, 1972.

[Me1] V. Meusers – Lubin-Tate formal groups, this volume, p. 49–55.

[Mt] B. Mitchell – *Theory of categories*, 1965.

[S] G. Shimura – *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, 1971.

[VZ] E. Viehmann & K. Ziegler – Formal moduli of formal $\mathcal{O}_K$-modules, this volume, p. 57–66.

[Ww1] S. Wewers – Canonical and quasi-canonical liftings, this volume, p. 67–86.

V. Meusers, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : meusers@math.uni-bonn.de

Astérisque
312, 2007, p. 99–104

10. LIFTING ENDOMORPHISMS OF FORMAL $\mathcal{O}_K$-MODULES

by

Eva Viehmann

Abstract. — We present Keating's results on lifts of endomorphisms of formal $\mathcal{O}_K$-modules over a power series ring. Let k be a separably closed field of characteristic p. Let K a complete discretely valued field of characteristic p with finite residue field and $\mathcal{O}_K$ its ring of integers. Let F be a formal $\mathcal{O}_K$-module over $k[[t]]$ with generic fiber of height $h-1$ and special fiber of height h. We compute the endomorphism ring of the reduction of F to $k[[t]]/(t^{n+1})$.

***Résumé* (Relèvements des endomorphismes de $\mathcal{O}_K$-modules formels).** — On présente les résultats de Keating sur les relèvements des endomorphismes de $\mathcal{O}_K$-modules formels sur un anneau de séries formelles. Soit k un corps de charactéristique p séparablement clos. Soit $\mathcal{O}_K$ un anneau de valuation discrète complète de charactéristique p à corps résiduel fini et soit K son corps des fractions. Soit F un $\mathcal{O}_K$-module formel sur $k[[t]]$ à fibre générique de hauteur $h-1$ et fibre speciale de hauteur h. On calcule l'anneau des endomorphismes de la réduction de F à $k[[t]]/(t^{n+1})$.

The following is an exposition of results in [**K2**].

1. Results

Let K be a complete discretely valued field of arbitrary characteristic with finite residue field $\mathbb{F}_q$, where $q = p^f$ for some prime p. Denote by $\mathcal{O}_K$ the ring of integers in K and let π be a uniformizer.

Let $1 < h < \infty$ and let (F_0, γ_0) be a formal $\mathcal{O}_K$-module of height h over a field k of characteristic p with $\mathcal{O}_K$-algebra structure $i : \mathcal{O}_K \to k$. The discrete valuation ring $R = k[[t]]$ has a canonical $\mathcal{O}_K$-algebra structure given by $\mathcal{O}_K \to k \hookrightarrow k[[t]] = R$. Let (F, γ) be a deformation of F_0 of height $g = h-1$ over R, that is a formal $\mathcal{O}_K$-module F over R with $F \equiv F_0 \pmod{(t)}$. For $a \in \mathcal{O}_K$ let $[a]_F = \gamma(a) \in \mathrm{End}_R(F)$. Let

2000 ***Mathematics Subject Classification.*** — 14L05, 11G07, 11S31, 14K07.
Key words and phrases. — Endomorphisms of formal $\mathcal{O}_K$-modules.

$R_n = R/(t^{n+1})$, $M_n = (t^n R_n)$, and $F_n = F \otimes_R R_n$. As F is an $\mathcal{O}_K$-module of height $g < h$, Lemma 2.1 of [**VZ**] shows that

$$[\pi]_F(X) = a_0 X^{q^g} + \cdots \in R[[X^{q^g}]] \tag{1.1}$$

with $a_0 \in R \setminus \{0\}$ and $v_t(a_0) \geq 1$.

The aim is to compute the endomorphism ring

$$H_n = \mathrm{End}_{R_n}(F_n) = \mathrm{End}_R(F_n)$$

for every n. Lemma 2.6 of [**VZ**] implies that the reduction maps $R_n \to R_{n-1}$ induce injections $H_n \hookrightarrow H_{n-1}$. By [**Ww1**, Theorem 1.1] we have $H_0 = \mathrm{End}_k(F_0) = \mathcal{O}_D$, where $\mathcal{O}_D$ is the maximal order in a division algebra D of degree h^2 and invariant $\frac{1}{h}$ over K. Hence the rings H_n can be identified with $\mathcal{O}_K$-subalgebras of $\mathcal{O}_D$. Obviously $\mathcal{O}_K \subseteq \bigcap_n H_n$. Let π_D be a uniformizer of $\mathcal{O}_D$.

For $m \geq 0$ we define

$$a(gm) = \frac{(q^h - 1)(q^{gm} - 1)}{(q^g - 1)(q - 1)}.$$

Theorem 1.1. — *Let F_0, F, and a_0 be as above, $v_t(a_0) = 1$, k separably closed, and*

$$f_0 \in (\mathcal{O}_K + \pi_D^l \mathcal{O}_D) \setminus (\mathcal{O}_K + \pi_D^{l+1} \mathcal{O}_D) \subseteq \mathcal{O}_D$$

for some $l \geq 0$. Write $l = hm + b$ with integers m, b and $0 \leq b < h$. Then $f_0 \in H_{n-1} \setminus H_n$ for

$$n = a(gm) + q^{gm} \frac{q^b - 1}{q - 1} + 1.$$

Using this result, we can easily calculate H_n:

Theorem 1.2. — *In the setting of Theorem 1.1 we have*

$$H_n = \mathcal{O}_K + \pi_D^{j(n)} \mathcal{O}_D$$

with $j(n) = hm + b$, where m and b are the uniquely defined integers with $0 \leq b < h$ and

$$a(gm) - q^{gm} + 1 \leq n < a(gm) + 1 \quad \text{if} \quad b = 0$$

$$a(gm) + q^{gm} \frac{q^{b-1} - 1}{q - 1} + 1 \leq n < a(gm) + q^{gm} \frac{q^b - 1}{q - 1} + 1 \quad \text{if} \quad 0 < b < h.$$

Keating ([**K2**, Thm. 3.4]) also calculates H_n without making the assumptions $v_t(a_0) = 1$ and k separably closed.

To prove Theorem 1.1 we need the following two propositions.

Proposition 1.3. — *Let f_0 be as in Theorem 1.1 with $0 \leq l \leq h$. Then $f_0 \in H_{n-1} \setminus H_n$ where $n = \frac{q^l - 1}{q - 1} + 1$.*

Proposition 1.4. — *Let $f_0 \in \mathcal{O}_K + \pi_D \mathcal{O}_D$ and $n > 1$ such that $f_0 \in H_{n-1} \setminus H_n$. Then $[\pi]_{F_0} \circ f_0 \in H_{n'-1} \setminus H_{n'}$ where $n' = q^g n + \frac{q^g - 1}{q - 1} + 1$.*

The first proposition says that the theorem holds for $l \leq h$. The second calculates the maximal lifting of $[\pi]_{F_0} \circ f_0$ given the maximal lifting of f_0. As the elements of $\mathcal{O}_K$ lift to all levels, an inductive argument shows that the two propositions imply Theorem 1.1.

2. Proof of the Lifting Theorem

We use the notation of the preceding section. Without further mention we assume that the constant coefficients of all power series in this section are 0.

Let $f_{n+1} \in R_{n+1}[[X]]$ be a lift of $f_n \in H_n$. We recall the definition of the associated symmetric 2-cocycle with coefficients in $(t^{n+1})k[[t]]/(t^{n+2})$ from [**VZ**, Prop. 3.2]:

$$\begin{aligned} \Delta(X,Y) &= f_{n+1}(X +_{F_{n+1}} Y) -_{F_{n+1}} f_{n+1}(X) -_{F_{n+1}} f_{n+1}(Y) \\ \delta_a(X) &= f_{n+1} \circ [a]_{F_{n+1}}(X) -_{F_{n+1}} [a]_{F_{n+1}} \circ f_{n+1}(X) \qquad (a \in A) \end{aligned}$$

The cocycle vanishes if and only if $f_{n+1} \in H_{n+1} = \mathrm{End}_{R_{n+1}}(F)$.

Corollary 2.1. — *Let $f_n(X) \in R_n[[X]]$ be a lift of $f_0(X) \in H_0$. Then $f_n \in H_n$ if and only if f_n commutes with $[\pi]_{F_n}$.*

Proof. — This follows by induction on $i \in [0,n]$ from [**VZ**, Prop. 3.2, 2. and Lemma 3.1]. □

Lemma 2.2. — *Let $f_n \in H_n$ with $f_n(X) \in R_n[[X^{q^r}]]$ of the form $f_n(X) = b_0 X^{q^r} + \cdots$ for some $r > 0$ and $b_0 \in R_n \setminus \{0\}$.*

1. *There exists a lift $f_{n+1} \in H_{n+1}$ of f_n.*
2. *If the degree of the leading term of δ_π is greater than q^{r+g}, the leading term of f_{n+1} has degree q^r.*
3. *Otherwise the degree of the leading term of δ_π is q^{r+g} and the leading term of f_{n+1} has degree q^{r-1}.*

Proof. — Let $f'_{n+1} \in R_{n+1}[[X^{q^r}]]$ be an arbitrary lift of f_n and let $(\Delta; \{\delta_a\})$ be the corresponding cocycle. As $[\pi]_{F_{n+1}}(X) \in R_{n+1}[[X^{q^g}]]$, the degree of the leading term of δ_π is at least q^{r+g}. The assumption $r > 0$ together with [**VZ**, Cor. 3.4 1.] implies that $\delta_\pi(X) \in M_{n+1}[[X^{q^h}]]$. Hence by [**VZ**, Cor. 3.4, 2. and Prop. 3.2, 3.] we get a lift $f_{n+1} = f'_{n+1} -_{F_{n+1}} \varepsilon$. If the degree of the leading term of δ_π is q^{r+g}, the leading term of $\varepsilon = d \circ p^{-1}$ has degree $q^{r+g-h} = q^{r-1}$. Otherwise the leading term of ε has degree greater than q^{r-1}. Thus the degree of the leading term of f_{n+1} is greater than q^{r-1}. As it is a lift of f_n, its degree is at most q^r. But the degree has to be a power of q, as $f_{n+1} \in H_{n+1} = \mathrm{End}_{R_{n+1}}(F_{n+1})$ (compare [**VZ**, Lemma 2.1]). Hence it has to be q^r. □

Let F, F_0, a_0 as in Theorem 1.1. Let $f_0 \in H_0$ and let $f_{n-1} \in H_{n-1}$ be a lift, *i.e.*, $f_{n-1} \equiv f_0 \pmod{(t)}$. We can write $f_{n-1}(X) = b_0 X^{q^r} + \cdots$ for some $r \geq 0$ and $b_0 \in R_{n-1} \setminus \{0\}$. Let $m = v_t(b_0)$. As $b_0 \neq 0$ in R_{n-1}, we have $m < n$.

Lemma 2.3. — *Suppose that in the above situation $m+q^r < q^g m+1$. Then*

1. $m+q^r \geq n$.
2. *If $m+q^r > n$, then f_{n-1} lifts to $f'_n \in H_n$ of the form $f'_n(X) = b'_0 X^{q^r} + \cdots$ with $v_t(b'_0) = m$.*
3. *If $m+q^r = n$ and $r > 0$, then f_{n-1} lifts to $f'_n \in H_n$ of the form $f'_n(X) = b'_0 X^{q^{r-1}} + \cdots$ with $v_t(b'_0) = n = m+q^r$.*
4. *A lift of f_{n-1} to H_n again satisfies the assumption of the lemma.*
5. *If $m+q^r = n$ and $r = 0$, then f_{n-1} does not lift to an element of H_n.*
6. *f_{n-1} lifts to $H_{n'-1}$ with $n' = m + \frac{q^{r+1}-1}{q-1}$ but not to $H_{n'}$.*

Proof. — We assumed $v_t(a_0) = 1$, where a_0 is as in (1.1). By the assumption of the lemma the valuation of the leading coefficient of δ_π is

$$v_t(b_0 a_0^{q^r} - a_0 b_0^{q^g}) = m + q^r.$$

As $f_{n-1} \in H_{n-1}$, this coefficient is in (t^n) and 1. follows. Since $f_{n-1} \in H_{n-1}$ has leading term of degree q^r, it has to be a power series in X^{q^r}. Let $f_n \in R_n[[X^{q^r}]]$ be a lifting with

$$f_n(X) = \tilde{b}_0 X^{q^r} + \cdots .$$

For the corresponding 2-cocycle we have

$$\delta_\pi(X) = (\tilde{b}_0 a_0^{q^r} - a_0 \tilde{b}_0^{q^g}) X^{q^{r+g}} + \cdots .$$

If $m+q^r > n$, the first term vanishes modulo (t^{n+1}), so the degree of δ_π is greater than q^{r+g}. Besides, r has to be positive, thus 2. follows from Lemma 2.2, 2. If $m+q^r = n$, the leading term of δ_π has degree q^{r+g}, hence 3. follows from Lemma 2.2, 3. The values of m and r for a lift of f_{n-1} to H_n are either the same as for f_{n-1} or they change to n and $r-1$. In both cases the assumption of the lemma is satisfied. This shows 4. for the case $r > 0$. If $r = 0$, the statement is trivial. To show 5., we assume that there exists a lift. By 4. it satisfies the assumption of the lemma with $r = 0$ and $m = n-1$. Thus 1. implies $n-1+1 \geq n+1$ which is a contradiction. The last assertion follows by applying 2.-4. until the assumption of 5. holds. □

Proof of Proposition 1.4. — We write $f_0 = a + f'_0$ with $a \in \mathcal{O}_K$ and $f'_0 \in \pi_D \mathcal{O}_D$. Since $\mathcal{O}_K \subseteq H_n$ for every n, we may assume $f_0 = f'_0 \in \pi_D \mathcal{O}_D$. We assumed that f_0 lifts to $f_{n-1} \in H_{n-1}$ with $f_{n-1}(X) = b_0 X^{q^r} + \cdots$ for some $b_0 \in R_{n-1} \setminus \{0\}$ but not to H_n. Lemma 2.2 implies $r = 0$. We have $f_{n-1} \equiv f_0 \pmod{(t)}$ and $f_0 \in \pi_D \mathcal{O}_D$. Hence $m = v_t(b_0) > 0$ and the assumption of Lemma 2.3 is satisfied. As f_{n-1} does not lift to H_n, the lemma shows that $v_t(b_0) = n-1$.

We lift f_{n-1} arbitrarily to $f(X) \in R[[X]]$. This lift is unique modulo (t^n), so $[\pi]_F \circ f$ is unique modulo $(t^{q^g n+1})$. Here we use that $[\pi]_F(X) = a_0 X^{q^g} + \cdots$ with $v_t(a_0) = 1$. We next show that the reduction $\phi_{q^g n}$ of $[\pi]_F \circ f$ modulo $(t^{q^g n+1})$ is in $H_{q^g n}$. By Lemma 2.1, 2. it suffices to verify that

$$[\pi]_F \circ ([\pi]_F \circ f) \equiv ([\pi]_F \circ f) \circ [\pi]_F \pmod{(t^{q^g n+1})}$$

which follows from $[\pi]_F \circ f \equiv f \circ [\pi]_F \pmod{(t^n)}$. Now we determine the maximal lifting of $\phi_{q^g n}$. We have

$$\begin{aligned} \phi_{q^g n} &\equiv [\pi]_F \circ f(X) \\ &\equiv a_0 b_0^{q^g} X^{q^g} + \cdots \pmod{(t^{q^g n+1})} \end{aligned}$$

and $v_t(a_0 b_0^{q^g}) = 1 + q^g(n-1)$. The assumption of Lemma 2.3 applied to $\phi_{q^g n}$ reads

$$(1 + q^g(n-1)) + q^g < q^g\,(1 + q^g(n-1)) + 1.$$

It is satisfied because $n > 1$ and $g \geq 1$. We get that $\phi_{q^g n}$ lifts to $H_{n'-1}$ but not to $H_{n'}$ where $n' = q^g n + \frac{q^g-1}{q-1} + 1$. □

For the proof of Proposition 1.3 we need the following lemma.

Lemma 2.4. — *Let $f_{n-1} \in H_{n-1}$ with $f_{n-1}(X) = b_0 X^{q^r} + \cdots$ and $m = v_t(b_0)$ as before. Assume $m + q^r > q^g m + 1 = n$. Then f_{n-1} lifts to $f'_n \in H_n$ of the form $f'_n(X) = b'_0 X^{q^{r-1}} + \cdots$ with $v_t(b'_0) = q^g m + 1$.*

Proof. — We lift f_{n-1} arbitrarily to $f_n(X) \in R_n[[X^{q^r}]]$ with $f_n(X) = \tilde{b}_0 X^{q^r} + \cdots$. As before let $(\Delta, \{\delta_a\})$ be the corresponding cocycle with coefficients in M_n. We have

$$\begin{aligned} \delta_\pi(X) &= f_n \circ [\pi]_{F_n}(X) -_{F_n} [\pi]_{F_n} \circ f_n(X) \\ &= (\tilde{b}_0 a_0^{q^r} - a_0 \tilde{b}_0^{q^g}) X^{q^{r+g}} + \cdots . \end{aligned}$$

The assumptions imply $v_t(\tilde{b}_0 a_0^{q^r} - a_0 \tilde{b}_0^{q^g}) = q^g m + 1 = n$. Therefore the first nonvanishing term of δ_π has degree q^{r+g}. As $m < n$, the assumption $m + q^r > n$ implies $r > 0$, and by Lemma 2.2, 3., f_{n-1} lifts to $f'_n \in H_n$ with leading term of degree q^{r-1}. □

Proof of Proposition 1.3

Case 1: $l = 0$**.** In this case $f_0 \in \mathcal{O}_D \setminus (\mathcal{O}_K + \pi_D \mathcal{O}_D)$ has the form $f_0(X) = b_0 X + \cdots$ with $b_0 \in \mathbb{F}_{q^h} \setminus \mathbb{F}_q$. Let $f_1(X) \in R_1[[X]]$ with $f_1(X) = b_0 X + \cdots$ be an arbitrary lift of f_0. We have to show that $f_1 \notin H_1$. For the corresponding cocycle with coefficients in M_1 we have $\delta_\pi(X) = (b_0 a_0 - a_0 b_0^{q^g}) X^{q^g} + \cdots$. Since $b_0 \in \mathbb{F}_{q^h} \setminus \mathbb{F}_q$, we have $v_t(b_0 - b_0^{q^g}) = 0$. Thus $b_0 a_0 - a_0 b_0^{q^g}$ is nonzero in R_1 and $\delta_\pi(X) \neq 0$, which shows $f_1 \notin H_1$.

Case 2: $0 < l < h$**.** Here

$$(\mathcal{O}_K + \pi_D^l \mathcal{O}_D) \setminus (\mathcal{O}_K + \pi_D^{l+1} \mathcal{O}_D) \subseteq \mathcal{O}_K + (\pi_D^l \mathcal{O}_D \setminus \pi_D^{l+1} \mathcal{O}_D).$$

As elements of $\mathcal{O}_K$ lift to all levels, it is enough to consider $f_0 \in \pi_D^l \mathcal{O}_D \setminus \pi_D^{l+1} \mathcal{O}_D$. Then f_0 is of the form $f_0(X) = b_0 X^{q^l} + \cdots$ with $b_0 \in k^\times$. As $m = 0$, Lemma 2.4 shows that f_0 lifts to $f'_1 \in H_1$ of the form $f'_1(X) = b'_0 X^{q^{l-1}} + \cdots$ with $v_t(b'_0) = 1$. For f'_1 the assumption of Lemma 2.3 is satisfied, so f_0 lifts to H_{n-1} but not to H_n with $n = \frac{q^l-1}{q-1} + 1$.

Case 3: $l = h$**.** Here

$$(\mathcal{O}_K + \pi_D^h \mathcal{O}_D) \setminus (\mathcal{O}_K + \pi_D^{h+1} \mathcal{O}_D) \subseteq \mathcal{O}_K + \pi_D^h (\mathcal{O}_D \setminus (\mathcal{O}_K + \pi_D \mathcal{O}_D)).$$

Similarly to the second case it suffices to consider $f_0 \in \pi_D^h(\mathcal{O}_D \setminus (\mathcal{O}_K + \pi_D\mathcal{O}_D))$, that is $f_0 = \pi g_0$ for some $g_0 \in \mathcal{O}_D \setminus (\mathcal{O}_K + \pi_D\mathcal{O}_D)$. Then $g_0(X) = b_0X + \cdots$ with $b_0 \in \mathbb{F}_{q^h} \setminus \mathbb{F}_q$. Let $g(X) \in R[[X]]$ be an arbitrary lift of g_0. From

$$[\pi]_F \circ g \equiv g \circ [\pi]_F \pmod{(t)}$$

we get

$$[\pi]_F \circ ([\pi]_F \circ g) \equiv ([\pi]_F \circ g) \circ [\pi]_F \pmod{(t^{q^g+1})}.$$

Lemma 2.1 shows that

$$\begin{aligned} f_{q^g}(X) &\equiv [\pi]_F \circ g(X) \\ &\equiv a_0 b_0^{q^g} X^{q^g} + \cdots \pmod{(t^{q^g+1})} \end{aligned}$$

is in H_{q^g}. Let $f_{q^g+1} \in R_{q^g+1}[[X^{q^g}]]$ with $f_{q^g+1}(X) = c_0X^{q^g} + \cdots$ and $c_0 \equiv a_0b_0^{q^g} \pmod{(t^{q^g+1})}$ be a lift of f_{q^g}. The corresponding cocycle satisfies

$$\begin{aligned} \delta_\pi(X) &= f_{q^g+1} \circ [\pi]_{F_{q^g+1}}(X) - {}_{F_{q^g+1}}[\pi]_{F_{q^g+1}} \circ f_{q^g+1}(X) \\ &= (c_0a_0^{q^g} - a_0c_0^{q^g})X^{q^{2g}} + \cdots \\ &\equiv a_0^{q^g+1}(b_0^{q^g} - b_0^{q^{2g}})X^{q^{2g}} + \cdots \pmod{(t^{q^g+2})}. \end{aligned}$$

Since $b_0 \in \mathbb{F}_{q^h} \setminus \mathbb{F}_q$, we have $b_0^{q^g} \neq b_0^{q^{2g}}$ in $\mathbb{F}_{q^h}$. Hence $a_0^{q^g+1}(b_0^{q^g} - b_0^{q^{2g}})$ is nonzero in M_{q^g+1} and δ_π has leading term of degree $q^{2g} = q^{r+g}$. So Lemma 2.2, 3. shows that f_{q^g} lifts to $f'_{q^g+1} \in H_{q^g+1}$ with leading term of degree q^{g-1}. As f'_{q^g+1} satisfies the assumption of Lemma 2.3, it lifts to H_{n-1} but not to H_n where $n = \frac{q^h-1}{q-1} + 1$. □

References

[K2] K. Keating – Lifting endomorphisms of formal A-modules, *Compos. Math.* **67** (1988), p. 211–239.

[VZ] E. Viehmann & K. Ziegler – Formal moduli of formal $\mathcal{O}_K$-modules, this volume, p. 57–66.

[Ww1] S. Wewers – Canonical and quasi-canonical liftings, this volume, p. 67–86.

E. Viehmann, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : viehmann@math.uni-bonn.de

Astérisque
312, 2007, p. 105–112

11. ENDOMORPHISMS OF QUASI-CANONICAL LIFTS

by

Inken Vollaard

Abstract. — We present Keating's result on the locus of deformation of an endomorphism of a quasi-canonical lifting. At the same time, this determines the endomorphism ring of the reduction of quasi-canonical liftings to Artin rings.

***Résumé* (Endomorphismes de relèvements quasi-canoniques).** — On donne le résultat de Keating concernant le lieu de déformation d'un endomorphisme d'un relèvement quasi-canonique. En même temps, ceci détermine l'anneau des endomorphismes de la réduction d'un relèvement quasi-canonique à des anneaux artiniens.

In this paper we prove a lifting theorem for endomorphisms of a formal $\mathcal{O}_K$-module to a quasi-canonical lift. For the canonical lift, a similar lifting theorem is proved in [**Ww1**]. This work is due to K. Keating ([**K1**]).

I thank S. Wewers for helpful comments on this manuscript.

1. Notation

Let K be a complete discretely valued field, let $\mathcal{O}_K$ be its ring of integers and let π be a uniformizing element of $\mathcal{O}_K$. We will assume that the residue field of $\mathcal{O}_K$ is equal to the field $\mathbb{F}_q$ of characteristic p. Denote by k an algebraic closure of $\mathbb{F}_q$. Let L be a quadratic extension of K and let $A = \widehat{\mathcal{O}}_L^{ur}$ be the completion of the maximal unramified extension of $\mathcal{O}_L$. Denote by M the quotient field of A.

Let F_0 be a formal $\mathcal{O}_K$-module of height 2 over k. By [**Ww1**] Theorem 1.1, the ring of $\mathcal{O}_K$-linear endomorphisms $\mathrm{End}_k F_0$ is isomorphic to the maximal order $\mathcal{O}_D$ in a division algebra D of dimension 4 over K and invariant $1/2$. We identify $\mathrm{End}_k F_0$ with $\mathcal{O}_D$. Let F be the canonical lift of F_0 over A with respect to an embedding

$$\mathcal{O}_L \hookrightarrow \mathcal{O}_D.$$

2000 ***Mathematics Subject Classification.*** — 14L05, 11G07, 11S31, 14K07.
Key words and phrases. — Quasi-canonical lift, endomorphism ring, formal module.

We consider a quasi-canonical lift F' of F_0 of level s ([**Ww1**, Def. 3.1]). By definition, $\mathrm{End}_{A'} F'$ is an order $\mathcal{O}_s := \mathcal{O}_K + \pi^s \mathcal{O}_L$ in $\mathcal{O}_L$. Note that a quasi-canonical lift of level 0 is a canonical lift and therefore can be defined over A. A quasi-canonical lift of level $s \geq 1$ can be defined over a totally ramified Galois extension M'/M of degree

$$[M' : M] = \begin{cases} q^s + q^{s-1} & \text{if } L/K \text{ is unramified} \\ q^s & \text{if } L/K \text{ is ramified} \end{cases}$$

([**Ww1**, Thm. 3.2]). Denote by A' the ring of integers of M' and denote by π' a uniformizing element of A'. If s is equal to 0, the ring A' is equal to A. Let $e_s = e(A'/\mathcal{O}_K)$ be the ramification index of A' over $\mathcal{O}_K$, *i.e.*,

$$e_s = \begin{cases} 2q^s & \text{if } L/K \text{ is ramified.} \\ q^s + q^{s-1} & \text{if } L/K \text{ is unramified and } s \neq 0. \\ 1 & \text{if } L/K \text{ is unramified and } s = 0. \end{cases}$$

By [**Ww1**, Proposition 4.4 and Proposition 4.6], the endomorphism $[\pi]_{F'}$ is given by a power series

$$[\pi]_{F'} = \pi X + \cdots + uX^q + \cdots + vX^{q^2} + \cdots \in A'[[X]] \tag{1.1}$$

with $v_{\pi'}(u) = 1$ and $v_{\pi'}(v) = 0$.

Denote by $A'_n = A'/(\pi')^{n+1}$ the reduction of A' modulo $(\pi')^{n+1}$ and by $F'_n = F' \otimes_{A'} A'_n$ the reduction of F' to A'_n. We obtain

$$\mathcal{O}_s = \mathrm{End}_{A'} F' \subset \cdots \subset \mathrm{End}_{A'_n} F'_n \subset \cdots \subset \mathrm{End}_k F_0 = \mathcal{O}_D$$

([**VZ**, Lem. 2.6]), hence we will consider $\mathrm{End}_{A'_n} F'_n$ as a subring of $\mathrm{End}_k F_0 = \mathcal{O}_D$. We write $\mathrm{End}\, F'_n$ instead of $\mathrm{End}_{A'_n} F'_n$.

For $n \leq e_s$ the ring $A'/(\pi')^n$ is of characteristic p and one can define the height of the module F'_n ([**VZ**, Def. 2.2]). By construction, F'_n is of height 1 if $0 < n \leq e_s$ and F_0 is of height 2. Denote by a_i the coefficients of $[\pi]_{F'}$. Then $v_{\pi'}(a_i) \geq e_s$ if $q \nmid i$, and $v_{\pi'}(a_i) \geq e_s$ if $q \mid i$ and $q^2 \nmid i$.

2. Results

The goal of this paper is to compute the endomorphism rings $\mathrm{End}\, F'_n$ as subrings of $\mathcal{O}_D$. In the case of the canonical lift, these rings are calculated in [**Ww1**]. Denote by $a(k)$ the rational number

$$a(k) = \frac{(q^k - 1)(q + 1)}{q - 1}$$

for every integer k. We have $a(0) = 0$ and $a(k) = (q + 1)(\sum_{i=0}^{k-1} q^i)$ for $k \geq 1$.

Theorem 2.1. — *Let F' be a quasi-canonical lift of F_0 of level s. Let $l \geq 0$ be an integer and let*

$$f_0 \in (\mathcal{O}_s + \pi_D^l \mathcal{O}_D) \setminus (\mathcal{O}_s + \pi_D^{l+1} \mathcal{O}_D).$$

Then f_0 lifts to $\operatorname{End} F'_{n_l-1}$ *and not to* $\operatorname{End} F'_{n_l}$ *with*

$$n_l = n_l(s) = n_l(L/K, s) = \begin{cases} a(\frac{l}{2}) + 1 & \text{if } l \leq 2s \text{ and } l \text{ even.} \\ a(\frac{l-1}{2}) + q^{\frac{l-1}{2}} + 1 & \text{if } l \leq 2s \text{ and } l \text{ odd.} \\ a(s-1) + q^{s-1} + (\frac{l+1}{2} - s)e_s + 1 & \text{if } l \geq 2s-1. \end{cases}$$

Remark 2.2. — The rational number n_l of the theorem is an integer. Indeed, if L/K is ramified, the ramification index e_s is even. If L/K is unramified and $l \geq 2s$ is even, then

$$\mathcal{O}_s + \pi_D^l \mathcal{O}_D = \mathcal{O}_s + \pi_D^{l+1} \mathcal{O}_D.$$

Theorem 2.3. — *Consider the same situation as in Theorem 2.1. Then* $\operatorname{End} F'_n = \mathcal{O}_s + \pi_D^{j(n)} \mathcal{O}_D$ *where*

$$j(n) = \begin{cases} 2k & \text{if } n \in]a(k-1) + q^{k-1}; a(k)] \text{ for } k < s. \\ 2k+1 & \text{if } n \in]a(k); a(k) + q^k] \text{ for } k < s. \\ k & \text{if } n \in]a(s-1) + q^{s-1} + (\frac{k}{2} - s)e_s; a(s-1) + q^{s-1} + (\frac{k+1}{2} - s)e_s] \\ & \text{for } k \geq 2s. \end{cases}$$

Note that the above intervals form a disjoint cover of the set of positive integers. The integer $j(n)$ is uniquely determined unless L/K is unramified and $j(n) \geq 2s$. In this case we have $\mathcal{O}_s + \pi_D^{j(n)} \mathcal{O}_D = \mathcal{O}_s + \pi_D^{j(n)+1} \mathcal{O}_D$ for every even $j(n)$.

Proof. — This theorem follows from Theorem 2.1. □

Remark 2.4. — If F' is the canonical lift of F_0, *i.e.*, if $s = 0$, Theorem 2.1 and Theorem 2.3 have already been proved in [**Ww1**] Theorem 1.4. We obtain in this case

$$\operatorname{End} F_n = \mathcal{O}_L + \pi_L^n \mathcal{O}_D$$

and

$$n_l(0) = \begin{cases} l+1 & \text{if } L/K \text{ is ramified.} \\ \frac{l+1}{2} & \text{if } L/K \text{ is unramified.} \end{cases}$$

3. Proofs

We will assume in the following that s is greater or equal than 1. We will split the proof of Theorem 2.1 into two propositions similar to the proof of Theorem 1.1 in [**Vi**].

Proposition 3.1. — *Let $l \leq 2s+1$ and let $s \geq 1$. Let*

$$f_0 \in (\mathcal{O}_s + \pi_D^l \mathcal{O}_D) \setminus (\mathcal{O}_s + \pi_D^{l+1} \mathcal{O}_D).$$

Then f_0 lifts to $\operatorname{End} F'_{n_l - 1} \setminus \operatorname{End} F'_{n_l}$ with

$$n_l = \begin{cases} a(\frac{l}{2}) + 1 & \text{if } l \leq 2s \text{ and } l \text{ even.} \\ a(\frac{l-1}{2}) + q^{\frac{l-1}{2}} + 1 & \text{if } l \leq 2s \text{ and } l \text{ odd.} \\ a(s-1) + q^{s-1} + e_s + 1 & \text{if } l = 2s+1. \end{cases}$$

Proposition 3.2. — *Let $s \geq 1$ and let $f_0 \in \operatorname{End} F'_{n-1} \setminus \operatorname{End} F'_n$ with $n \geq \frac{e_s - 1}{q-1}$. Then $[\pi] \circ f_0$ lifts to $\operatorname{End} F'_{n'-1} \setminus \operatorname{End} F'_{n'}$ with $n' = n + e_s$.*

Proof of Theorem 2.1. — Theorem 2.1 follows by induction from Proposition 3.1 and Proposition 3.2. Let $l > 2s+1$ and let $f_0 \in (\mathcal{O}_s + \pi_D^l \mathcal{O}_D) \setminus (\mathcal{O}_s + \pi_D^{l+1} \mathcal{O}_D)$. Write $f_0 = c + [\pi]_{F_0} \circ g_0$ with $c \in \mathcal{O}_s$ and $g_0 \in \pi_D^{l-2} \mathcal{O}_D \setminus (\mathcal{O}_s + \pi_D^{l-1} \mathcal{O}_D)$. By induction g_0 lifts to $\operatorname{End} F'_{n_{l-2}-1} \setminus \operatorname{End} F'_{n_{l-2}}$ with

$$\begin{aligned} n_{l-2} &= a(s-1) + q^{s-1} + (\frac{l-1}{2} - s)e_s + 1 \\ &= \frac{2q^s - 2}{q-1} + (\frac{l-1}{2} - s)e_s \geq \frac{e_s - 1}{q-1}. \end{aligned}$$

By Proposition 3.2 the endomorphism $[\pi]_{F_0} \circ g_0$, hence f_0, lifts to $\operatorname{End} F'_{n'-1} \setminus \operatorname{End} F'_{n'}$ with $n' = n_{l-2} + e_s = n_l$. □

Remark 3.3. — We now split the proof of Proposition 3.1 into two cases. As we will see below, we can use the results of [**Vi**] in the case $n_l + 1 \leq e_s$. Note that n_l is a strictly increasing sequence.

An easy computation shows that there exists an integer l_0 such that $n_{l_0} + 1 \leq e_s < n_{l_0+1}$. We obtain

- $l_0 = 2s$ if L/K is ramified and $q \geq 3$.
- $l_0 = 2s-1$ if $\begin{cases} L/K \text{ is unramified and } q \geq 3. \\ L/K \text{ is unramified, } q = 2 \text{ and } s = 1. \\ L/K \text{ is ramified and } q = 2. \end{cases}$
- $l_0 = 2s-2$ if L/K is unramified, $q = 2$ and $s \neq 1$.

Proof of Proposition 3.1 in the case of $n_l + 1 \leq e_s$. — Since $A'/\widehat{\mathcal{O}}_K$ is a totally ramified extension of ramification index e_s, we obtain for $n \leq e_s$ an isomorphism of $\mathcal{O}_K$-algebras

$$\begin{aligned} A'/(\pi')^n &\cong (\widehat{\mathcal{O}}_K/(\pi))[\pi']/(\pi')^n \\ &\cong k[t]/(t)^n. \end{aligned}$$

Let $f_0 \in (\mathcal{O}_s + \pi_D^l \mathcal{O}_D) \setminus (\mathcal{O}_s + \pi_D^{l+1}\mathcal{O}_D)$ with $n_l + 1 \leq e_s$, *i.e.*, with $l \leq l_0$ (Rem. 3.3). Then F'_{n_l} is a lift of F_0 of height 1 over $k[t]/(t)^{n_l+1}$ and we will prove the proposition by using the results of [**Vi**].

We have $\mathcal{O}_s + \pi_D^l \mathcal{O}_D = \mathcal{O}_K + \pi_D^l \mathcal{O}_D$ for $l \leq 2s$ and by an easy computation $\mathcal{O}_s + \pi_D^{2s+1}\mathcal{O}_D = \mathcal{O}_K + \pi_D^{2s+1}\mathcal{O}_D$ if L/K is ramified. Hence [**Vi**] Theorem 1.1, shows that f_0 lifts to $\operatorname{End} F'_{n_l-1} \setminus \operatorname{End} F'_{n_l}$. This proves the proposition in this case. □

3.1. Let f_0 be an element of $\operatorname{End} F'_{n-1}$. By $f_{n-1} \in A'_{n-1}[[X]]$ we always denote the unique lift of f_0 as an endomorphism of F'_{n-1}. Let $f \in A'[[X]]$ be a lift of f_{n-1} as a power series without constant coefficient. As we are interested in endomorphisms of formal groups, we make the general assumption that all power series in this article have no constant coefficient. We write f_k for the residue class of the power series f in $A'_k[[X]]$. Denote by ϵ the commutator

$$\epsilon = f \circ [\pi]_{F'} - {}_{F'}\, [\pi]_{F'} \circ f \in A'[[X]]$$

using the additive operation on $A'[[X]]$ induced by F'. Then ϵ has coefficients in $(\pi')^n$ because f_{n-1} is an endomorphism of F'_{n-1}.

The main technique to prove the lifting theorem is the cohomology theory as in [**VZ**]. Denote by I_n the 1-dimensional k-vector space $(\pi')^n/(\pi')^{n+1}$. Consider the cohomology group $H^2(F_0, I_n)$ as in [**VZ**] Chapter 3. For $f_{n-1} \in \operatorname{End} F'_{n-1}$ one can define a cocycle $(\Delta, \{\delta_a\}) \in H^2(F_0, I_n)$. Then f_{n-1} lifts to $\operatorname{End} F'_n$ if and only if $(\Delta, \{\delta_a\}) \equiv 0$, *i.e.*, if and only if δ_π is a power series in X^{q^2} ([**VZ**] Prop. 3.2, Cor. 3.4). We have

$$\delta_\pi = \epsilon \bmod (\pi')^{n+1}.$$

Lemma 3.4. — *The cohomology group $H^2(F_0, I_n)$ is a k-vector space of dimension 1. For a cocycle $(\Delta, \{\delta_a\}) \in H^2(F_0, I_n)$, the element $\delta_\pi = \beta(X^q)$ is a power series in X^q and $(\Delta, \{\delta_a\}) \not\equiv 0$ if and only if $\beta'(0) \neq 0$.*

Proof. — By [**VZ**, Lemma 2.5], every formal module over k is isomorphic to a normal module. Then [**VZ**, Proposition 3.6], shows that $H^2(F_0, k)$ is a k-vector space of dimension 1. A basis is given by a cocycle $(\Delta, \{\delta_a\})$ such that $\delta_\pi = \beta(X^q)$ is a power series in X^q with $\beta'(0) \neq 0$. This proves the lemma. □

Remark 3.5. — Let $f_0 \in \operatorname{End} F'_{n-1}$. By Lemma 3.4 the power series ϵ is a power series in X^q modulo $(\pi')^{n+1}$,

$$\epsilon \equiv aX^q + \dots \bmod (\pi')^{n+1}. \tag{3.1}$$

Furthermore, $v_{\pi'}(a) \geq n$ and $v_{\pi'}(a) = n$ if and only if $f_0 \notin \operatorname{End} F'_n$.

Lemma 3.6. — *Let $f_0 \in \operatorname{End} F'_{n-1}$ and let $k = \min\{n + e_s, 1 + qn\}$. Then $[\pi]_{F_0} \circ f_0$ lifts to $\operatorname{End} F'_{k-1}$.*

(i) *If $1 + qn < n + e_s$, the endomorphism $[\pi]_{F_0} \circ f_0$ lifts to $\operatorname{End} F'_k$.*

(ii) *If* $k = n + e_s$ *and* $f_0 \notin \operatorname{End} F'_n$, *the endomorphism* $[\pi]_{F_0} \circ f_0$ *does not lift to* $\operatorname{End} F'_k$.

Proof. — We use the notations of 3.1. By equation (1.1) we obtain

$$[\pi]_{F'} \circ f \circ [\pi]_{F'} -_{F'} [\pi]^2_{F'} \circ f = [\pi]_{F'} \circ \epsilon$$

$$= \pi\epsilon + \cdots + u\epsilon^q + \cdots + v\epsilon^{q^2} + \dots \tag{3.2}$$

Since ϵ has coefficients in $(\pi')^n$, we have

$$[\pi]_{F'} \circ \epsilon \equiv 0 \bmod (\pi')^k.$$

Thus $[\pi]_{F'_{k-1}} \circ f_{k-1}$ commutes with $[\pi]_{F'_{k-1}}$, hence it is an element of $\operatorname{End} F'_{k-1}$ ([**VZ**, Cor. 3.1]). We obtain by (3.2)

$$\delta_\pi([\pi]_{F'_{k-1}} \circ f_{k-1}) \equiv \pi\epsilon + \cdots + u\epsilon^q + \cdots + v\epsilon^{q^2} + \dots \bmod (\pi')^{k+1}. \tag{3.3}$$

If $1 + qn < n + e_s$, the power series (3.3) is a power series in X^{q^2} as ϵ is a power series in X^q modulo $(\pi')^{n+1}$. Hence $[\pi]_{F_0} \circ f_0$ lifts to $\operatorname{End} F'_k$.

If $k = n + e_s$, we obtain

$$\delta_\pi([\pi]_{F'_{k-1}} \circ f_{k-1}) \equiv \pi a X^q + \dots \bmod (\pi')^{k+1}$$

with $v_{\pi'}(\pi a) = n + e_s$. Hence $[\pi]_{F'_{n'-1}} \circ f_{n'-1}$ does not lift to $\operatorname{End} F'_k$. □

Proof of Proposition 3.2. — Since $n \geq \frac{e_s - 1}{q-1}$, we obtain $\min\{n + e_s, 1 + qn\} = n + e_s = n'$. The proposition follows from Lemma 3.6. □

Proof of Proposition 3.1 in the case of $n \geq e_s$. — By Remark 3.3 we have to prove the following cases.

1. L/K unramified and $l = 2s + 1$.
2. L/K ramified and $l = 2s + 1$.
3. L/K ramified, $q = 2$ and $l = 2s$.
4. L/K unramified, $q = 2$, $l = 2s - 1$ and $s \neq 1$.

Note that $l \geq 2$. Let f_0 be an element of $(\mathcal{O}_s + \pi_D^l \mathcal{O}_D) \setminus (\mathcal{O}_s + \pi_D^{l+1} \mathcal{O}_D)$. Write $f_0 = c + [\pi]_{F_0} \circ g_0$ with $c \in \mathcal{O}_s$ and $g_0 \in \pi_D^{l-2} \mathcal{O}_D \setminus (\mathcal{O}_s + \pi_D^{l-1} \mathcal{O}_D)$. Since elements of $\mathcal{O}_s$ lift to $\operatorname{End} F'$, it is enough to show that $[\pi]_{F_0} \circ g_0$ satisfies the claim. As g_0 is an element of $\pi_D^{2s-1} \mathcal{O}_D \setminus (\mathcal{O}_s + \pi_D^{2s} \mathcal{O}_D)$, it lifts to $\operatorname{End} F'_{n-1} \setminus \operatorname{End} F'_n$ with $n = n_{l-2}$. We have

$$n = a(s-1) + q^{s-1} + 1 = \frac{2q^s - 2}{q-1}. \tag{3.4}$$

In the first case, we obtain $n_{l-2} \geq \frac{e_s - 1}{q-1}$ and the claim follows from the case $l = 2s - 1$ from Proposition 3.2.

Now consider the other cases. Note that in these cases $n + 1 \leq e_s$ (Rem. 3.3). Let $n' = n_l$. We have to show that $[\pi]_{F_0} \circ g_0$ lifts to $\operatorname{End} F'_{n'-1} \setminus \operatorname{End} F'_{n'}$. An easy

calculation shows that in each case $n' = qn + 2$. By equation (3.4) we see that $e_s + n = qn$ in the second case, and $e_s + n > qn + 2$ in the other cases. Now we can use Lemma 3.6 (ii) to see that $\pi \circ g_0$ lifts to $\operatorname{End} F'_{n'-1}$. Let $h_{n'-1} \in \operatorname{End} F'_{n'-1}$ be a lift of $[\pi]_{F'_0} \circ g_0$. It remains to show that $h_{n'-1}$ does not lift to $\operatorname{End} F'_{n'}$, *i.e.*, $\delta_\pi(h_{n'-1}) \in A'_{n'}[[X]]$ is not equal to zero modulo $(X)^{q^2}$.

Let $h_{n'} \in A'_{n'}[[X]]$ be a lift of $h_{n'-1}$ as a power series. Then $h_{n'} = [\pi]_{F'_{n'}} \circ g_{n'} +_{F'_{n'}} \psi$ with a power series $\psi = bX + \cdots \in (\pi')^{n'-1}[[X]]$. Using the notation of 3.1, we obtain

$$\begin{aligned} \delta_\pi(h_{n'-1}) &= \delta_\pi(\pi_{F'_{n'-1}} \circ g_{n'-1}) +_{F'_{n'}} \psi \circ [\pi]_{F'_{n'}} -_{F'_{n'}} [\pi]_{F'_{n'}} \circ \psi \\ &\equiv [\pi]_{F'_{n'}} \circ \epsilon +_{F'_{n'}} \psi \circ [\pi]_{F'_{n'}} \bmod (\pi')^{n'+1}. \end{aligned} \tag{3.5}$$

By (3.1) we obtain from equation (3.5)

$$\delta_\pi(h_{n'-1}) \equiv (\pi a + bu)X^q + \dots \bmod (\pi')^{n'+1}.$$

It is sufficient to prove the following claim.

Claim. — We have

$$\pi a + bu \not\equiv 0 \bmod (\pi')^{n'+1}.$$

Indeed, we have $\delta_\pi(h_{n'-1}) \equiv 0 \bmod (\pi')^{n'}$ since $h_{n'-1}$ is an endomorphism. We obtain from equation (3.5) that

$$\begin{aligned} \delta_\pi(h_{n'-1}) &\equiv (u\epsilon^q + \cdots + v\epsilon^{q^2} + \dots) +_{F'_{n'}} (bvX^{q^2} + \dots) \bmod (\pi')^{n'} \\ &\equiv (ua^q + bv)X^{q^2} + \dots \bmod (\pi')^{n'}, \end{aligned}$$

hence we have

$$ua^q + bv \equiv 0 \bmod (\pi')^{n'}. \tag{3.6}$$

Since $v_{\pi'}(a) = n$ (Rem. 3.5) and $n' = qn + 2$, we obtain that $v_{\pi'}(b) = n' - 1$.

We first consider the last two cases. In these cases, we have $e_s + n > n'$. Therefore, $\pi a \equiv 0 \bmod (\pi')^{n'+1}$ and the claim is satisfied. Thus the proposition is proved in these cases.

Now consider the second case. Let

$$g = \alpha X + \cdots \in A'[[X]].$$

Since $n + 1 \leq e_s$, we obtain from the definition of ϵ

$$\epsilon \equiv u(\alpha - \alpha^q)X^q + \dots \bmod (\pi')^{n+1},$$

hence

$$a = u(\alpha - \alpha^q).$$

As $v_{\pi'}(a) = n$, we have $v_{\pi'}(\alpha) = n - 1$.

Using equation (3.6), we obtain

$$\pi a + bu \equiv \pi a - v^{-1}u^2 a \equiv \pi u\alpha - v^{-1}u^{q+2}\alpha^q \bmod (\pi')^{n'+1}.$$

The idea is to analyze the solutions of the equation

$$\pi\alpha - v^{-1}u^{q+1}\alpha^q \equiv 0 \bmod (\pi')^{n'}. \tag{3.7}$$

There are q different solutions of this equation for $\alpha \in (\pi')^{n-1}/(\pi')^n$. We will identify these solutions as first coefficients of endomorphisms corresponding to elements of $\mathcal{O}_s$.

Consider the following general situation. Let f_0 and f_0' be two elements of $\pi_D^{2s+1}\mathcal{O}_D$ which are not equivalent modulo $\pi_D^{2s+2}\mathcal{O}_D$. As before, we write $f_0 = [\pi]_{F_0'} \circ g_0$ and $f_0' = [\pi]_{F_0'} \circ g_0'$. We obtain

$$g_0 - g_0' \in \pi_D^{2s-1}\mathcal{O}_D \setminus \pi_D^{2s}\mathcal{O}_D = \pi_D^{2s-1}\mathcal{O}_D \setminus (\mathcal{O}_s + \pi_D^{2s}\mathcal{O}_D).$$

Hence the endomorphism $g_0 - g_0'$ lifts to $\operatorname{End} F_{n-1}' \setminus \operatorname{End} F_n'$. Write $g = \alpha X + \dots$ and $g' = \alpha' X + \dots$ as before. We obtain $v_{\pi'}(\alpha - \alpha') = n - 1$, hence α and α' are not equivalent modulo $(\pi')^n$. Thus different equivalence classes of endomorphisms belong to different equivalence classes of coefficients. As L/K is a ramified extension in the division algebra D, we have

$$\begin{aligned}(\mathcal{O}_s \cap \pi_D^{2s+1}\mathcal{O}_D)/\pi_D^{2s+2}\mathcal{O}_D &= ((\mathcal{O}_K + \pi^s\mathcal{O}_L) \cap \pi_D^{2s+1}\mathcal{O}_D)/\pi_D^{2s+2}\mathcal{O}_D \\ &= \pi^{s+1}\mathcal{O}_L/(\pi_D^{2s+2}\mathcal{O}_D \cap \pi^{s+1}\mathcal{O}_L) \\ &= \mathcal{O}_L/\pi_L\mathcal{O}_L \cong \mathbb{F}_q.\end{aligned}$$

Thus the q different solutions of (3.7) correspond to the equivalence classes of endomorphisms of $\mathcal{O}_s$ in $\operatorname{End} F_{n'}'$. By our assumption $[\pi]_{F_0'} \circ g_0 \notin \mathcal{O}_s + \pi_D^{2s+2}\mathcal{O}_D$, hence equation (3.7) is not satisfied which proves the claim. □

References

[K1] K. Keating – Lifting endomorphisms of formal groups, Ph.D. Thesis, Harvard, 1987.

[Vi] E. Viehmann – *Lifting endomorphisms of formal $\mathcal{O}_K$-modules*, this volume, p. 99–104.

[VZ] E. Viehmann & K. Ziegler – Formal moduli of formal $\mathcal{O}_K$-modules, this volume, p. 57–66.

[Ww1] S. Wewers – Canonical and quasi-canonical liftings, this volume, p. 67–86.

I. Vollaard, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : vollaard@math.uni-bonn.de

Astérisque
312, 2007, p. 113–137

12. INVARIANTS OF TERNARY QUADRATIC FORMS

by

Irene I. Bouw

***Abstract.* —** This paper deals with Gross–Keating invariants of ternary quadratic forms over $\mathbb{Z}_\ell$. The main technical difficulties arise in residue characteristic $\ell = 2$. In this case, we define the Gross–Keating invariants in terms of a normal form. We give an alternative, less computational approach for anisotropic quadratic forms.

***Résumé* (Invariants de Gross–Keating pour les formes quadratiques ternaires)**

Cet article concerne les invariants de Gross–Keating pour les formes quadratiques ternaires sur $\mathbb{Z}_\ell$. Les difficultés principales n'apparaissent qu'en caractéristique résiduelle $\ell = 2$. Dans ce cas, nous déterminons les invariants de Gross–Keating en termes d'une forme normale. Pour les formes anisotropes nous donnons une approche plus directe.

This note provides details on [**GK**, Section 4]. The main goal is to define and compute the Gross–Keating invariants a_1, a_2, a_3 of ternary quadratic forms over $\mathbb{Z}_\ell$ (Definition 1.2). If $a_1 \equiv a_2 \bmod 2$ and $a_3 > a_2$ we define an additional invariant $\epsilon \in \{\pm 1\}$ (Definition 2.7, Definition 4.8). If $\ell \neq 2$ every quadratic form over $\mathbb{Z}_\ell$ is diagonalizable, and it is easy to determine these invariants from the diagonal form (Section 2). If $\ell = 2$ not every quadratic form is diagonalizable. Moreover, even for diagonal quadratic forms it is not straightforward to determine the Gross–Keating invariants. We determine a normal form in Section 3 and compute the invariants in terms of this normal form (Section 4). In Section 5 we determine explicitly when a ternary quadratic form is anisotropic. A complete table can be found in Proposition 5.2 (non diagonalizable case) and Theorem 5.7 (diagonalizable case). In Section 6, we give an alternative definition of the Gross–Keating invariants for anisotropic quadratic forms. The results of Section 6 are due to Stefan Wewers, following a hint in [**GK**, Section 4].

Our main reference on quadratic forms over $\mathbb{Z}_\ell$ is [**C**, Chapter 8]. Most of the results of this paper can also be found in the work of Yang, in a somewhat different

2000 ***Mathematics Subject Classification.* —** 11E08.
***Key words and phrases.* —** Ternary quadratic forms, Gross–Keating invariants, anisotropic quadratic forms.

form. The Gross–Keating invariants are computed in [**Y1**, Appendix B]. The question whether a given form over $\mathbb{Z}_2$ is isotropic or not (Section 5) is discussed in [**Y2**].

I would like to thank M. Rapoport for comments on an earlier version.

1. Definition of the invariants a_i

In this section we give the general definition of the Gross–Keating invariants a_i of quadratic forms over $\mathbb{Z}_\ell$ which are used in [**GK**].

Let L be a free $\mathbb{Z}_\ell$-module of rank n and choose a (for the moment) arbitrary basis $\boldsymbol{\psi} = \{\psi_1, \psi_2, \dots, \psi_n\}$. For the application to [**GK**] we are only interested in the case $n = 3$ of ternary quadratic forms. Let (L, Q) be an integral quadratic form over $\mathbb{Z}_\ell$, that is,

$$Q(x) = Q\Big(\sum x_i\psi_i\Big) = \sum_{i\le j} b_{ij}x_ix_j, \qquad \text{with } b_{ij} \in \mathbb{Z}_\ell.$$

Put $b_{ji} = b_{ij}$ for $j > i$. If we want to stress the dependence of the b_{ij} on the basis, we write $b_{ij}(\boldsymbol{\psi})$ for b_{ij}. We write $(x, y) = Q(x + y) - Q(x) - Q(y)$ for the corresponding symmetric bilinear form and $B = ((\psi_i, \psi_j))$ for the corresponding matrix. Note that

$$B = \big(B_{ij}\big), \qquad \text{where} \qquad B_{ij} = \begin{cases} b_{ij}, & \text{if } i < j, \\ 2b_{ij}, & \text{if } i = j. \end{cases}$$

In the rest of the paper we only use the b_{ij} and not the B_{ij}, for simplicity. We denote by ord the ℓ-adic valuation on $\mathbb{Z}_\ell$. We always suppose that Q is regular, that is, $\det(B) \neq 0$.

Changing the basis multiplies the determinant of B by an element of $(\mathbb{Z}_\ell^\times)^2$. Therefore the determinant is a well defined element of $\mathbb{Z}_\ell/(\mathbb{Z}_\ell^\times)^2$.

Lemma 1.1. — *Suppose that either $\ell \neq 2$ or n is odd. Define*

$$\Delta = \Delta(Q) = \frac{1}{2}\det(B).$$

Then $\Delta \in \mathbb{Z}_\ell$.

Proof. — The lemma is obvious if $\ell \neq 2$. Suppose that $\ell = 2$ and n odd. Write $\Delta = \sum_{\sigma\in S_n} 2^{\delta(\sigma)}d(\sigma)$, where $d(\sigma) = (-1)^{\operatorname{sgn}(\sigma)}\prod_{i=1}^n b_{i\sigma(i)}$ and $\delta(\sigma)+1$ is the number of $i \in \{1, 2, \dots, n\}$ which are fixed by σ. The only problematic terms are those with $\delta(\sigma) = -1$. Suppose that σ acts without fixed points on $\{1, 2, \dots, n\}$. Then $\sigma^{-1} \neq \sigma$, since n is odd. The matrix $((\psi_i, \psi_j))$ is symmetric. It follows that $d(\sigma) = d(\sigma^{-1})$, hence $2^{\delta(\sigma)}d(\sigma) + 2^{\delta(\sigma^{-1})}d(\sigma^{-1}) \in \mathbb{Z}_\ell$. □

We now come to the definition of the Gross–Keating invariants of a quadratic form. Let $\boldsymbol{\psi} = (\psi_1, \psi_2, \dots, \psi_n)$ be a basis of L. We write $S(\boldsymbol{\psi})$ for the set of tuples $\mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathbb{Z}^n$ such that

$$y_1 \le y_2 \le \cdots \le y_n, \qquad \frac{y_i + y_j}{2} \le \operatorname{ord}(b_{ij}(\boldsymbol{\psi})) \quad \text{for } 1 \le i \le j \le n. \tag{1.1}$$

Let $S = \cup S(\boldsymbol{\psi})$. We order tuples $(y_1, \dots, y_n) \in S$ lexicographically, as follows. For given $(y_1, \dots, y_n)$, $(z_1, \dots, z_n) \in S$, let j be the largest integer such that $y_i = z_i$ for all $i < j$. Then $(y_1, \dots, y_n) > (z_1, \dots, z_n)$ if $y_j > z_j$.

Definition 1.2. — The *Gross–Keating invariants* $a_1, \dots, a_n$ are the maximum of $(y_1, \dots, y_n) \in S$. A basis $\boldsymbol{\psi}$ is called *optimal* if $(a_1, \dots, a_n) \in S(\boldsymbol{\psi})$.

If $\boldsymbol{\psi}$ is optimal, then

$$a_i + a_j \leq 2\,\mathrm{ord}(b_{ij}(\boldsymbol{\psi})) \quad \text{for} \quad 1 \leq i \leq j \leq n, \quad \text{and} \quad a_1 \leq a_2 \leq \cdots \leq a_n. \tag{1.2}$$

Since Δ is well defined up to $(\mathbb{Z}_\ell^\times)^2$, the integer $\mathrm{ord}(\Delta)$ is well defined. The following lemma will be useful in computing the Gross–Keating invariants.

Lemma 1.3

(a) *Suppose that n is odd, then*

$$\mathrm{ord}(\Delta) \geq a_1 + a_2 + \cdots + a_n.$$

(b) *We have*

$$a_1 = \min_{x,y \in L} \mathrm{ord}\,(x, y)\,.$$

(c) *Define $\rho := \min_A \mathrm{ord}(\det(A))$, where A runs through the 2 by 2 minors of B. Then*

$$a_1 + a_2 \leq \rho.$$

Proof. — This lemma is proved in [**Y1**, Lemma B.1, Lemma B.2]. Note that the matrix T in [**Y1**] differs by a factor 2 from our matrix B. Let $\boldsymbol{\varphi}$ be an optimal basis. We use the notation of the proof of Lemma 1.1.

First suppose that $\ell = 2$. Write $\mathbb{S}$ for the set of equivalence classes in S_n under the equivalence relation $\sigma \sim \sigma^{-1}$. The proof of Lemma 1.1 shows that $\Delta = \sum_{\sigma \in \mathbb{S}} (-1)^{\mathrm{sgn}(\sigma)} 2^{\delta'(\sigma)} d(\sigma)$, where $\delta'(\sigma) \geq 0$. The choice of $\boldsymbol{\varphi}$ implies that

$$\mathrm{ord}(2^{\delta'(\sigma)} d(\sigma)) = \delta'(\sigma) + \mathrm{ord}\Big(\prod_i b_{i\sigma(i)}\Big) \geq \sum_{i=1}^n \frac{a_i + a_{\sigma(i)}}{2} = \sum_{i=1}^n a_i.$$

This proves (a) in this case.

If $\ell \neq 2$, define $\delta'(\sigma) = 0$ for all $\sigma \in S_n$. Then the proof works also in this case.

Since $a_1 \leq a_2 \leq \cdots \leq a_n$, it follows from (1.2) that $\mathrm{ord}(b_{ij}(\boldsymbol{\varphi})) \geq a_1$ for all $i \leq j$. On the other hand, it is obvious that $a_1 \geq \min_{x,y \in L} \mathrm{ord}\,(x, y)$. This implies (b).

Part (c) is similar to (a), compare to Lemma B1.ii in [**Y1**]. Let $i_1, i_2, j_1, j_2 \in \{1, 2, \dots, n\}$ be integers such that $i_1 \neq i_2$ and $j_1 \neq j_2$. Write $B(i_1, i_2; j_1, j_2)$ for the corresponding minor of B. After renumbering, we may suppose that $i_1 \neq j_2$ and $i_2 \neq j_1$. Then $\det(B(i_1, i_2; j_1, j_2)) = \pm(2^\alpha b_{i_1,j_1} b_{i_2,j_2} - b_{i_1,j_2} b_{i_2 j_1})$, where $\alpha \in \{0, 1, 2\}$ is the number of equalities $i_1 = j_1, i_2 = j_2$ that hold. We conclude that $\mathrm{ord}(\det(B(i_1, i_2; j_1, j_2)) \geq (a_{i_1} + a_{i_2} + a_{j_1} + a_{j_2})/2 \geq a_1 + a_2$. (Here we use that $a_1 \leq a_2 \leq \cdots \leq a_n$ and $i_1 \neq i_2$ and $j_1 \neq j_2$.) This proves (c). □

2. Definition of the Gross–Keating invariants for $\ell \neq 2$

We start this section with an elementary lemma which holds without assumption on ℓ.

Lemma 2.1. — *Choose a basis $\boldsymbol{\psi} = (\psi_1, \dots, \psi_n)$ of L. Let $\gamma_1, \dots, \gamma_m \in L$ be linearly independent. The following are equivalent.*

(a) *There exists $\gamma_{m+1}, \dots, \gamma_n \in L$ such that the (γ_i) form a basis.*
(b) *The matrix $(\gamma_1, \dots, \gamma_m)$, expressing the γ_i in terms of the basis $\boldsymbol{\psi}$, contains a $m \times m$ minor whose determinant is a p-adic unit.*
(c) *If $\sum_{i=1}^n v_i \gamma_i \in L$ for some $v_i \in \mathbb{Q}_\ell$, then $v_i \in \mathbb{Z}_\ell$.*

Proof. — This is straightforward. See also [**C**, Chapter 8, Lemma 2.1]. □

In particular, a vector $\alpha = \sum_i \alpha_i \psi_i \in L$ is part of a basis of L if and only if $\min_j \operatorname{ord}(\alpha_j) = 0$. We call such vectors *primitive*.

We have that

$$2\,(x,y) = 2[Q(x+y) - Q(x) - Q(y)] = (x+y, x+y) - (x,x) - (y,y)\,. \tag{2.1}$$

If $\ell \neq 2$, this implies that

$$\min_{x,y \in L} \operatorname{ord}(x,y) = \min_{x \in L} \operatorname{ord}(x,x)\,. \tag{2.2}$$

In the rest of this section, we suppose that $\ell \neq 2$. There is a $x \in L$ for which the minimum in (2.2) is attained. This vector x is primitive. Lemma 2.1 implies that x can be extended to a basis of L. We will see in Section 4 that (2.2) does not hold for $\ell = 2$; this is the main reason why things are more difficult for $\ell = 2$.

Proposition 2.2. — *Suppose that $\ell \neq 2$. Then there exists a basis $\boldsymbol{\psi}$ of L such that*

$$Q(x) = Q\Big(\sum x_i \psi_i\Big) = \sum_i b_{ii} x_i^2, \qquad \textit{where} \qquad \operatorname{ord}(b_{11}) \leq \operatorname{ord}(b_{22}) \leq \cdots \leq \operatorname{ord}(b_{nn}).$$

Proof. — Our proof follows [**C**, Chapter 8, Theorem 3.1].

The discussion before the statement of the theorem shows that we may choose φ_1 such that

$$\operatorname{ord}(Q(\varphi_1)) = \operatorname{ord}(\varphi_1, \varphi_1) = \min_{x,y \in L} \operatorname{ord}(x,y)\,.$$

Here we use the equality (2.2).

Choose $\varphi_2, \dots, \varphi_n \in L$ such that $\boldsymbol{\varphi} = \{\varphi_1, \varphi_2 \dots, \varphi_n\}$ is a basis of L. As before we write $Q(\sum_i x_i \varphi_i) = \sum_{1 \leq i \leq j \leq n} b_{ij}(\boldsymbol{\varphi}) x_i x_j$. Then

$$Q(x) = b_{11} \left(x_1 + \frac{b_{12}}{2b_{11}} x_2 + \cdots \frac{b_{1n}}{2b_{11}} x_n \right)^2 + \tilde{Q}(x_2, \dots, x_n),$$

for some integral quadratic form $\tilde{Q}$ in $n-1$ variables.

We define a new basis by $\psi_1 = \varphi_1$, and $\psi_i = \varphi_i - (b_{1i}/2b_{11})\varphi_1$ for $i \neq 1$. The choice of ψ_1 ensures that $\psi_i \in L$, since $e = \mathrm{ord}(2b_{11}) \leq \mathrm{ord}(b_{1i})$. With respect to this new basis, the quadratic form is

$$Q(x) = b_{11}(\boldsymbol{\psi})x_1^2 + \tilde{Q}\Big(\sum_{i\geq 2} x_i\psi_i\Big).$$

The proposition follows by induction. □

Remark 2.3. — Cassels ([**C**, Chapter 8, Theorem 3.1]) proves a stronger statement than Proposition 2.2. Namely, he gives a list of pairwise nonisomorphic quadratic forms such that every integral quadratic form is isomorphic to one of these. This stronger statement implies that the definition of the invariants a_i of Proposition 2.6 does not depend of the choice of the orthogonal basis.

We can give a simpler definition of the invariants a_i in terms of a basis $\boldsymbol{\psi}$ as in Proposition 2.2. If $\gamma \in L$ is an element such that $Q(\gamma) \neq 0$, we may define a reflection τ_γ by

$$\tau_\gamma(x) = x - \frac{2\,(x,\gamma)}{(\gamma,\gamma)}\gamma.$$

This is the reflection in the orthogonal complement of γ. Clearly, τ_γ is defined over $\mathbb{Z}_\ell$ if and only if $\mathrm{ord}\,(\gamma,\gamma) = \min_{x\in L} \mathrm{ord}\,(x,x)$. (In fact, this also holds for $\ell = 2$.) Since τ_γ is a reflection, it is clearly invertible. The following lemma is a partial analog of Witt's Lemma ([**C**, Corollary to Theorem 2.4.1]) which holds for quadratic forms over fields.

Lemma 2.4. — *Suppose that $\psi, \varphi \in L$ satisfy*

$$Q(\psi) = Q(\varphi), \qquad \mathrm{ord}(Q(\psi)) = \mathrm{ord}(Q(\varphi)) = \min_{x\in L} \mathrm{ord}(Q(x)).$$

Then there exists an integral isometry σ of (L,Q) such that $\sigma(\psi) = \varphi$. Moreover, σ may be taken as a product of reflections τ_γ.

Proof. — This is [**C**, Lemma 8.3.3]. Our assumptions on ψ and φ imply that $Q(\psi+\varphi) + Q(\psi-\varphi) = 2Q(\psi) + 2Q(\varphi) = 4Q(\psi)$. Since $\mathrm{ord}(Q(\psi)) = \mathrm{ord}\,(\psi,\psi) = \min_{x\in L} \mathrm{ord}\,(x,x) =: e$, it follows that one of the following holds:

(a) $\mathrm{ord}\,Q(\psi+\varphi) = e$,
(b) $\mathrm{ord}\,Q(\psi-\varphi) = e$.

Since $\ell \neq 2$, it is also possible that both hold. If (a) holds, then $\tau_{\psi+\varphi}$ is integral and sends ψ to φ. If (b) holds, define $\sigma = \tau_{\psi-\varphi} \circ \tau_\psi$. □

Lemma 2.5. — *Suppose $u, v \in \mathbb{Z}_\ell^\times$. Then $ux_1^2 + vx_2^2 \sim_{\mathbb{Z}_\ell} x_1^2 + uvx_2^2$.*

Proof. — This is proved in the second corollary to [**C**, Lemma 8.3.3]. We give the idea. Since $\ell \neq 2$, there exists $a, c \in \mathbb{Z}_\ell$ such that $a^2u + c^2v = 1$. We may assume that a is a unit. Then

$$C = \begin{pmatrix} a & -cv \\ c & au \end{pmatrix}$$

defines the equivalence of the lemma. □

Proposition 2.6

(a) *Let $\boldsymbol{\psi} = (\psi_1, \psi_2, \ldots, \psi_n)$ be an orthogonal basis of L as in Proposition 2.2 Write $Q(x) = \sum_i b_i x_i^2$. Then the invariants a_i (Definition 1.2) satisfy*

$$a_i = \operatorname{ord}(b_i).$$

In particular, $\boldsymbol{\psi}$ is optimal.

(b) *Suppose that n is odd. Then*

$$\operatorname{ord}(\Delta) = a_1 + \cdots + a_n.$$

Proof. — Let $\boldsymbol{\varphi}$ be a basis such that the inequalities (1.2) hold. We claim that $\operatorname{ord}(\varphi_1, \varphi_1) = a_1$. Part (b) of Lemma 1.3 implies that $a_1 = \min_{x \in L} \operatorname{ord}(x, x)$. The choice of $\boldsymbol{\varphi}$ implies moreover that $\operatorname{ord}(\varphi_1, \varphi_1) = \min_{x \in L} \operatorname{ord}(x, x)$. The definition of a_1 implies therefore that $a_1 = \operatorname{ord}(\varphi_1, \varphi_1)$.

We apply the diagonalization process of the proof of Proposition 2.2 to the basis $\boldsymbol{\varphi}$. Define $\psi_1 = \varphi_1$ and $\psi_i = \varphi_i - (b_{1i}/2b_{11})\varphi_1$ for $i \neq 1$. One computes that

$$(\psi_j, \psi_1) = 0, \qquad (\psi_j, \psi_j) = \frac{b_{1j}^2}{2b_{11}} + 2b_{jj}, \qquad (\psi_i, \psi_j) = -\frac{b_{1i}b_{1j}}{2b_{11}} + b_{ij},$$

for $j \neq 1$ and $i \neq 1, j$. The inequalities (1.2) imply that $\operatorname{ord}(\psi_j, \psi_j) \geq a_j$ and $2\operatorname{ord}(\psi_i, \psi_j) \geq a_i + a_j$. Therefore the new basis also satisfies the inequalities (1.2). This implies that there exists an orthogonal basis $\boldsymbol{\psi}$ which satisfies (1.2). It follows that the Gross–Keating invariants $(a_1, \ldots, a_n)$ are the maximum of $\cup S(\boldsymbol{\psi})$, where the union is taken over the orthogonal bases and $\cup S(\boldsymbol{\psi})$ is as in (1.1).

Let $\boldsymbol{\varphi}$ and $\boldsymbol{\psi}$ be two orthogonal bases. Write $Q(x) = b_1x_2^2 + b_2x_2^2 + \cdots + b_nx_n^2$ with respect to the basis $\boldsymbol{\psi}$ and $Q(x) = d_1x_1^2 + d_2x_2^2 + \cdots + d_nx_n^2$ with respect to the basis $\boldsymbol{\varphi}$. We suppose that $\operatorname{ord}(b_1) \leq \operatorname{ord}(b_2) \leq \cdots \leq \operatorname{ord}(b_n)$ and $\operatorname{ord}(d_1) \leq \operatorname{ord}(d_2) \leq \cdots \leq \operatorname{ord}(d_n)$. We suppose moreover that $\boldsymbol{\varphi}$ satisfies (1.2). (Such $\boldsymbol{\varphi}$ exists by the above argument.) We have to show that $\boldsymbol{\psi}$ satisfies (1.2), also. Write $C = (c_{ij})$ for the change of basis matrix expressing $\boldsymbol{\varphi}$ in terms $\boldsymbol{\psi}$. As before, Lemma 1.3.(b) implies that $\operatorname{ord}(b_1) = \operatorname{ord}(d_1) = a_1$. Write $b_1 = ud_1$, for some unit u.

Suppose that $\operatorname{ord}(b_2) > \operatorname{ord}(b_1)$. Then

$$d_1 = \sum_{j=1}^{n} c_{j1}^2 b_j \equiv c_{11}^2 b_1 \bmod \ell^{a_1+1}.$$

This implies that u is a quadratic residue. To prove the claim, we may therefore assume that $Q(\psi_1) = Q(\varphi_1)$ in this case.

Suppose that $\mathrm{ord}(b_1) = \mathrm{ord}(b_2)$. Then Lemma 2.5 implies that Q is $\mathbb{Z}_\ell$-equivalent to $d_1x_1^2 + ub_2x_2^2 + b_3x_3^2 + \cdots$. Hence also in this case we may assume that $Q(\psi_1) = Q(\varphi_1)$.

Lemma 2.4 implies that there exists an isometry σ of Q which sends ψ_1 to φ_1. Then $D := \sigma^{-1}C$ fixes ψ_1. Write

$$D = \begin{pmatrix} 1 & D_1 \\ 0 & D_2 \end{pmatrix}, \qquad B := \begin{pmatrix} 2b_1 & & 0 \\ & \ddots & \\ 0 & & 2b_n \end{pmatrix}$$

where D_2 is an $(n-1) \times (n-1)$ matrix. One computes that

$$D^t B D = \begin{pmatrix} 2\gamma^2 b_1 & 2\gamma D_1 \\ 2\gamma D_1^t & * \end{pmatrix}.$$

Our assumption implies that D^tBD is a diagonal matrix, with diagonal entries $2d_i$. This implies that $D_1 = (0, \ldots, 0)$. We conclude that D restricts to an integral and invertible map from the sublattice of L spanned by $\psi_2, \ldots, \psi_n$ to the sublattice spanned by $\varphi_2, \ldots, \varphi_n$. This implies (a).

Part (b) follows immediately from (a). □

Definition 2.7. — Suppose that $n = 3$ and $\ell \neq 2$. Assume $a_1 \equiv a_2 \bmod 2$, and $a_3 > a_2$. Choose a basis $\boldsymbol{\psi} = (\psi_1, \psi_2, \psi_3)$ of L as in Proposition 2.2. Write $b_{ii} = \ell^{a_i}u_i$. We define an invariant $\epsilon = \epsilon(\boldsymbol{\psi})$ by the Legendre symbol

$$\epsilon = \left(\frac{-u_1u_2}{\ell}\right). \tag{2.3}$$

Lemma 2.8. — *Assumptions and notations are as in Definition 2.7.*

(a) *The invariant $\epsilon(\boldsymbol{\psi})$ does not depend on the choice of the orthogonal basis $\boldsymbol{\psi}$.*

(b) *We have that $\epsilon = 1$ if and only if the subspace of $L \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ spanned by ψ_1 and ψ_2 is isotropic.*

Proof. — Let $\boldsymbol{\psi} = (\psi_1, \psi_2, \psi_3)$ be a basis of L as in Proposition 2.6, in particular $\boldsymbol{\psi}$ is orthogonal and the valuation of $b_i = (\psi_i, \psi_i)/2$ is equal to a_i, for $i = 1, 2, 3$.

Suppose that $a_2 \equiv a_1 \bmod 2$ and $a_3 > a_2$. Write $a_2 = a_1 + 2\gamma$. Write Q' for the restriction of Q to the sublattice of L spanned by ψ_1 and ψ_2. Then $Q'(x) = b_1x_1^2 + b_2x_2^2$ is equivalent to $\ell^{a_1}(x_1^2 + u_1u_2\ell^{2\gamma}x_2^2)$ (Lemma 2.5). It follows that Q' is isotropic if $\epsilon = 1$ and anisotropic if $\epsilon = -1$. This proves (b).

Let $\boldsymbol{\varphi}$ be another orthogonal basis and write $Q(\sum_i x_i\varphi_i) = d_1x_1^2 + d_2x_2^2 + d_3x_3^2$. We assume that $\mathrm{ord}(d_i) = a_i$. Write C for the matrix expressing $\boldsymbol{\varphi}$ in terms of $\boldsymbol{\psi}$. The argument of the proof of Proposition 2.6 together with the assumption that $a_2 < a_3$

implies that there exists an isometry σ such that

$$\sigma^{-1}C = \begin{pmatrix} v_1 & 0 & 0 \\ 0 & v_2 & 0 \\ 0 & 0 & v_3 \end{pmatrix},$$

where the v_i are units. This shows that $d_i = v_i^2 b_i$. The lemma follows. □

3. A normal form for quadratic forms over $\mathbb{Z}_2$

Not every quadratic form over $\mathbb{Z}_2$ is diagonalizable. In this section we give a normal form for ternary quadratic forms over $\mathbb{Z}_2$, following [**C**, Section 8.4]. Cassels uses a slightly stronger notion of integrality, namely he supposes that $b_{ij}/2 \in \mathbb{Z}_\ell$, for all $i \neq j$. However, this does not make any difference.

Lemma 3.1. — *Suppose $\ell = 2$. Let Q be a regular quadratic form over $\mathbb{Z}_2$. Then Q is $\mathbb{Z}_2$-equivalent to a sum of quadratic forms of the form*

$$2^e u x^2, \tag{3.1}$$

for $e \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}_2^\times$, and

$$2^e (b_1 x_1^2 + u x_1 x_2 + b_2 x_2^2), \tag{3.2}$$

with $e \in \mathbb{Z}_{\geq 0}$, and $u \in \mathbb{Z}_2^\times$.

The equality (2.1) holds for $\ell = 2$, but (2.2) does not. However, (2.1) implies that

$$\min_{x,y \in L} \operatorname{ord}(x,y) + 1 \geq \min_{x \in L} \operatorname{ord}(x,x).$$

Therefore $\min_{x,y\in L} \operatorname{ord}(x,y)$ equals either $\min_{x\in L} \operatorname{ord}(x,x)$ or $\min_{x\in L} \operatorname{ord}(x,x) - 1$.

Proof. — Let $e = \min_{x,y\in L} \operatorname{ord}(x,y)$. We distinguish two cases.

(a) There exists a $\gamma \in L$ such that $\operatorname{ord}(\gamma,\gamma) = e$.
(b) For all $\gamma \in L$ we have that $\operatorname{ord}(\gamma,\gamma) > e$.

Suppose we are in case (a). Then $\operatorname{ord}(\psi_1,\psi_i) \geq e$, by definition. We can now proceed as in the proof of Proposition 2.2. Namely, $2b_{11} = 2Q(\psi_1) = (\psi_1,\psi_1)$. Therefore b_{11} has valuation $e-1$. For $i \neq 1$, we have that $\operatorname{ord}(b_{1i}) = \operatorname{ord}(\psi_1,\psi_i) \geq e$. Therefore

$$\varphi_i = \psi_i - \left(\frac{b_{1i}}{2b_{11}}\right)\psi_1.$$

is an element of L and $\psi_1, \varphi_2, \ldots, \varphi_n$ form a basis. With respect to this basis the quadratic form Q becomes $Q(x) = b_{11}x_1^2 + \tilde{Q}(x_2,\ldots,x_n)$, for some quadratic form $\tilde{Q}$ in $n-1$ variables.

Suppose we are in case (b). Then $\operatorname{ord}(\gamma,\gamma) > e$ for all $\gamma \in L$. We may choose $\psi_1, \psi_2 \in L$ such that $\operatorname{ord}(\psi_1,\psi_2) = e$. The definition of e implies that $(\psi_1+\psi_2)/2 \notin L$. Lemma 2.1 implies therefore that ψ_1, ψ_2 can be extended to a basis $\psi_1, \ldots, \psi_n$ of L.

The choice of ψ_1 and ψ_2 implies that the determinant of the matrix

$$\begin{pmatrix} 2b_{11}2^{-e} & b_{12}2^{-e} \\ b_{12}2^{-e} & 2b_{22}2^{-e} \end{pmatrix}$$

is a unit in $\mathbb{Z}_\ell$. Therefore we can find λ_1^j, λ_2^j such that

$$-2\lambda_1^j b_{11} - \lambda_2^j b_{12} + b_{1j} = 0, \qquad -2\lambda_2^j b_{22} - \lambda_1^j b_{12} + b_{2j} = 0,$$

for $j = 3, \dots, n$. Define $\varphi_j = \psi_j - \lambda_1^j \psi_1 - \lambda_2^j \psi_2$. The choice of the λ_i^j implies that $(\varphi_j, \psi_1) = (\varphi_j, \psi_2) = 0$, for $j = 3, \dots, n$.

With respect to the basis $(\psi_1, \psi_2, \varphi_3, \dots, \varphi_n)$ the quadratic form Q becomes

$$Q(x) = 2^e(b_{11}x_1^2 + b_{12}x_1x_2 + b_{22}x_2^2) + \tilde{Q}(x_3, \dots, x_n).$$

This proves the lemma. □

Lemma 3.2. — *Let $Q_2(x) = b_{11}x_1^2 + b_{12}x_1x_2 + b_{22}x_2^2$ be a binary quadratic form over $\mathbb{Z}_2$ and L_2 the corresponding free $\mathbb{Z}_2$-lattice of rank two.*

(a) *If* $\min(\mathrm{ord}(b_{11}), \mathrm{ord}(b_{22})) < \mathrm{ord}(b_{12})$ *then Q_2 is diagonalizable.*

(b) *Suppose that Q_2 is not diagonalizable. Then Q_2 is anisotropic if and only if* $\mathrm{ord}(b_{12}) = \mathrm{ord}(b_{11}) = \mathrm{ord}(b_{22})$.

(c) *Suppose Q_2 is anisotropic and not diagonalizable. Then Q_2 is equivalent to*

$$2^e(x_1^2 + x_1x_2 + x_2^2),$$

for some e.

(d) *Suppose that Q_2 is isotropic and not diagonalizable. Then Q_2 is equivalent to*

$$2^e x_1 x_2,$$

for some e.

Proof. — Part (a) follows from the proof of Lemma 3.1.

Suppose that Q_2 is not diagonalizable. Then $\mathrm{ord}(b_{12}) \leq \min(\mathrm{ord}(b_{11}), \mathrm{ord}(b_{22}))$, by (a). Part (b) is an elementary Hilbert-symbol computation using [**S**, Theorem IV.6].

Suppose that Q_2 is anisotropic and not diagonalizable. Then (b) implies that $e := \mathrm{ord}(b_{12}) = \mathrm{ord}(b_{11}) = \mathrm{ord}(b_{22})$. Part (c) now follows from an elementary computation.

Suppose that Q_2 is isotropic and not diagonalizable. There exists a primitive vector ψ_1 such that $Q(\psi_1) = 0$. Lemma 2.1 together with the fact that the quadratic form is nondegenerate, implies that there exists a vector $\psi_2 \in L_2$ such that ψ_1, ψ_2 form a basis of L_2 and $(\psi_1, \psi_2) \neq 0$. After multiplying ψ_2 with a unit, we may suppose that $(\psi_1, \psi_2) = 2^e$, for some $e \geq 0$.

We claim that $\operatorname{ord}(\psi_2,\psi_2) > \operatorname{ord}(\psi_1,\psi_2)$. Namely, if $\operatorname{ord}(\psi_2,\psi_2) \leq \operatorname{ord}(\psi_1,\psi_2)$ then Q_2 is diagonalizable by (a), but this contradicts our assumptions. Therefore

$$\psi_2' := \psi_2 - \frac{(\psi_2,\psi_2)}{2\,(\psi_1,\psi_2)}\psi_1 \in L_2.$$

Now ψ_1, ψ_2' form a basis of L and $(\psi_2',\psi_2') = 0$. This proves (d). □

Proposition 3.3. — *Let (L,Q) be a ternary quadratic form over $\mathbb{Z}_2$. One of the following two possibilities occurs.*

(a) *The form Q is diagonalizable; there exists a basis such that*

$$Q(x) = b_1x_1^2 + b_2x_2^2 + b_3x_3^3, \quad \textit{with} \quad 0 \leq \operatorname{ord}(b_1) \leq \operatorname{ord}(b_2) \leq \operatorname{ord}(b_3).$$

(b) *The form Q is not diagonalizable; there exists a basis such that*

$$Q(x) = u_1 2^{\mu_1} x_1^2 + 2^{\mu_2}(vx_2^2 + x_2x_3 + vx_3^2), \quad \textit{with} \quad v \in \{0,1\}, \quad \mu_i \geq 0 \quad \textit{and} \quad u_1 \in \mathbb{Z}_2^\times.$$

Proof. — This follows immediately from Lemma 3.1 and Lemma 3.2. □

This classification is the same as the classification used (but not explicitly stated) in [**Y1**, Appendix B]. Note that Yang's matrix T differs by a factor 2 from the matrix B we use. In particular, the invariant β used in [**Y1**, Proposition B.4] satisfies $\beta \geq -1$ rather than $\beta \geq 0$.

4. The Gross–Keating invariants for $\ell = 2$

In this section we compute the Gross–Keating invariants of ternary quadratic forms (L,Q) over $\mathbb{Z}_2$ in terms of the normal form of Proposition 3.3. The computation of the a_i can be found in Proposition 4.1 (non-diagonalizable case) and Proposition 4.2 (diagonalizable case). The computation of ϵ can be found in Proposition 4.9. This section is based on [**Y1**, Appendix B].

We start by considering quadratic forms which are not diagonalizable. Recall from Proposition 3.3 that if Q is not diagonalizable then there exists a basis $\boldsymbol{\psi}$ of L with respect to which we have

$$Q(x) = u_1 2^{\mu_1} x_1^2 + 2^{\mu_2}(vx_2^2 + x_2x_3 + vx_3^2), \quad \text{with} \quad v \in \{0,1\}, \quad u_1 \in \mathbb{Z}_2^\times. \tag{4.1}$$

We do not suppose that $\mu_1 \leq \mu_2$.

Proposition 4.1. — *Suppose that Q is given by (4.1). Then*

$$(a_1,a_2,a_3) = \begin{cases} (\mu_1,\mu_2,\mu_2), & \textit{if } \mu_1 \leq \mu_2, \\ (\mu_2,\mu_2,\mu_1), & \textit{if } \mu_1 > \mu_2. \end{cases}$$

Proof. — Lemma 1.3.(b) implies that $a_1 = \min(\mu_1,\mu_2)$. We distinguish two cases.

Suppose that $\mu_1 \leq \mu_2$. Then $a_1 = \mu_1$ and $\operatorname{ord}(\Delta) = \mu_1 + 2\mu_2 \geq a_1 + a_2 + a_3$ (Lemma 1.3.(a)). Therefore $a_2 \leq (a_2+a_3)/2 \leq \mu_2$. The existence of a basis $\boldsymbol{\psi}$ as in (4.1) implies that $(\mu_1,\mu_2,\mu_2) \in S(\boldsymbol{\psi})$. We conclude that $a_2 = a_3 = \mu_2$.

Suppose that $\mu_1 > \mu_2$. In this case we have that $a_1 = \mu_2$. Recall that we defined ρ as the minimum of the valuation of the determinant of the 2×2-minors of B. One computes that $\rho = \min(2\mu_2, 1 + \mu_1 + \mu_2) = 2\mu_2$, since we assumed that $\mu_1 \geq \mu_2 + 1$. Lemma 1.3.(c) implies that $\rho \geq a_1 + a_2$, hence $a_2 \leq \mu_2$. The existence of a basis $\boldsymbol{\psi}$ as in (4.1) implies that $(\mu_2, \mu_2, \mu_1) \in S(\boldsymbol{\psi})$. We conclude that $(a_1, a_2, a_3) = (\mu_2, \mu_2, \mu_1)$. □

We now consider diagonalizable quadratic forms Q. Contrary to the situation for $\ell \neq 2$, a basis $\boldsymbol{\psi}$ which diagonalizes Q is not optimal (Definition 1.2).

Proposition 4.2. — *Suppose that Q is diagonalizable. Let $\boldsymbol{\psi}$ be a basis of L such that*

$$Q(x) = b_1 x_1^2 + b_2 x_2^2 + b_3 x_3^2, \text{ with } b_i = u_i 2^{\mu_i},\ u_i \in \mathbb{Z}_2^\times \text{ and } \mu_1 \leq \mu_2 \leq \mu_3. \tag{4.2}$$

(a) *Suppose that $\mu_1 \not\equiv \mu_2 \bmod 2$. Then $(a_1, a_2, a_3) = (\mu_1, \mu_2, \mu_3 + 2)$.*
(b) *Suppose that $\mu_1 \equiv \mu_2 \bmod 2$.*
  (i) *If $u_1 + u_2 \equiv 2 \bmod 4$ or $\mu_3 \leq \mu_2 + 1$, then $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$.*
  (ii) *Otherwise, $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 2, \mu_3)$.*

The proof of this proposition is divided in several lemmas. We use the notation of Proposition 4.2. In particular, $\boldsymbol{\psi}$ is a basis of L with respect to which Q is as in (4.2). Let $\boldsymbol{\varphi}$ be an optimal basis, *i.e.*, suppose that the inequalities (1.2) hold. We write $C = (c_{ij})$ for the change of basis matrix expressing $\boldsymbol{\varphi}$ in terms of $\boldsymbol{\psi}$. We write the quadratic form Q in terms of the basis $\boldsymbol{\varphi}$ as $Q(x) = \sum_{i \leq j} d_{ij} x_i x_j$. In other words, the d_{ij} are the coefficients of the matrix obtained by dividing the diagonal elements of $C^t B C$ by two. One computes that

$$d_{ii} = c_{1i}^2 b_1 + c_{2i}^2 b_2 + c_{3i}^2 b_3. \tag{4.3}$$

Lemma 4.3. — *Suppose that Q is diagonal and $\mu_1 \not\equiv \mu_2 \bmod 2$. Then $(a_1, a_2, a_3) = (\mu_1, \mu_2, \mu_3 + 2)$.*

Proof. — We have already seen that $a_1 = \mu_1$. Therefore it follows from the definition of the a_i that $a_2 \geq \mu_2$. We claim that $a_2 = \mu_2$. Suppose that $a_2 > \mu_2$.

Write $\mu_2 = \mu_1 + 2\gamma + 1$. The inequalities (1.2) imply that $\operatorname{ord}(d_{22}) \geq a_2 \geq \mu_2 + 1$ and $\operatorname{ord}(d_{33}) \geq a_3 \geq a_2 \geq \mu_2 + 1$. Since $\mu_1 \not\equiv \mu_2 \bmod 2$, it follows from (4.3) that $\operatorname{ord}(c_{12}) \geq \gamma + 1$ and $\operatorname{ord}(c_{13}) \geq \gamma + 1$.

We first suppose that $\mu_3 > \mu_2$. Then $\operatorname{ord}(c_{22}) \geq 1$ and $\operatorname{ord}(c_{33}) \geq 1$. But this implies that $\det(C) \equiv 0 \bmod 2$. This gives a contradiction.

If $\mu_2 = \mu_3$, we proceed similarly. In this case $c_{22} \equiv c_{32} \bmod 2$ and $c_{23} \equiv c_{33} \bmod 2$. This implies again that $\det(C) \equiv 0 \bmod 2$. We conclude that $a_2 = \mu_2$.

Since $\operatorname{ord}(\Delta) = \operatorname{ord}(\det(B)) + 2 = \mu_1 + \mu_2 + \mu_3 + 2$, it follows from Lemma 1.3.(a) that $a_3 \leq \mu_3 + 2$. To show that $a_3 = \mu_3 + 2$ it suffices to find a basis $\boldsymbol{\varphi}$ such that $(\mu_1, \mu_2, \mu_3 + 2) \in S(\boldsymbol{\varphi})$. We now construct such a basis.

Our assumptions imply that μ_3 is congruent to μ_1 or μ_2 (modulo 2). We suppose that $\mu_3 \equiv \mu_1 \bmod 2$. (The case $\mu_3 \equiv \mu_2 \bmod 2$ is similar.) Write $\mu_2 = \mu_1 + 2\gamma + 1$ and $\mu_3 = \mu_1 + 2\lambda$. We distinguish two cases:

- $u_1 + u_3 \equiv 0 \bmod 4$,
- $u_1 + u_3 \equiv 2 \bmod 4$.

In the first case define

$$C = \begin{pmatrix} 1 & 0 & 2^\lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + b_2x_2^2 + 2^{\lambda+1}b_1x_1x_3 + (b_3 + 2^{2\lambda}b_1)x_3^2$.

In the second case we define

$$C = \begin{pmatrix} 1 & 0 & 2^\lambda \\ 0 & 1 & 2^{\lambda-\gamma} \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + b_2x_2^2 + 2^{\lambda+1}b_1x_1x_3 + (b_3 + 2^{2\lambda}b_1 + 2^{2(\lambda-\gamma)}b_2)x_3^2 + 2^{\lambda-\gamma+1}b_2x_2x_3$. It is easy to check that the basis $\boldsymbol{\varphi}$ corresponding to C satisfies (1.2) for $a_1 = \mu_1$, $a_2 = \mu_2$ and $a_3 = \mu_3 + 2$. This proves the lemma. □

The proof of Lemmas 4.4, 4.5 and 4.6 follows the same pattern as the proof of Lemma 4.3.

Lemma 4.4. — *Suppose that Q is diagonalizable, $\mu_1 \equiv \mu_2 \bmod 2$ and $\mu_3 \leq \mu_2 + 1$. Then $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$.*

Proof. — Since $a_1 = \mu_1$ and $\operatorname{ord}(\Delta) = \mu_1 + \mu_2 + \mu_3 + 2$ it follows from Lemma 1.3 that $a_1 + 2a_2 \leq a_1 + a_2 + a_3 \leq \mu_1 + \mu_2 + \mu_3 + 2 \leq \mu_1 + 2\mu_2 + 3$. This implies that $a_2 \leq \mu_2 + 1$.

We now construct a basis $\boldsymbol{\varphi}$ such that $(\mu_1, \mu_2+1, \mu_3+1) \in S(\boldsymbol{\varphi})$. The lemma follows from this. Let C be the corresponding change of basis matrix. Write $\mu_2 = \mu_1 + 2\gamma$.

If $\mu_2 = \mu_3$ define

$$C = \begin{pmatrix} 1 & 2^\gamma & 2^\gamma \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + (2^{2\gamma}b_1 + b_2)x_2^2 + 2^{\gamma+1}b_1(x_1x_2 + x_1x_3) + (b_3 + 2^{2\gamma}b_1)x_3^2 + 2^{1+2\gamma}b_1x_2x_3$.

If $\mu_3 = \mu_2 + 1$ and $u_1 + u_2 \equiv 2 \bmod 4$ define

$$C = \begin{pmatrix} 1 & 2^\gamma & 2^\gamma \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + (b_2 + 2^{2\gamma}b_1)x_2^2 + 2^{\gamma+1}b_1(x_1x_2 + x_1x_3) + (b_3 + 2^{2\gamma}b_1 + b_2)x_3^2 + (2^{2\gamma+1}b_1 + 2b_2)x_2x_3$.

If $\mu_3 = \mu_2 + 1$ and $u_1 + u_2 \equiv 0 \bmod 4$ define

$$C = \begin{pmatrix} 1 & 2^\gamma & 2^\gamma \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2+(2^{2\gamma}b_1+b_2+b_3)x_2^2+2^{\gamma+1}b_1(x_1x_2+x_1x_3)+(4b_3+2^{2\gamma}b_1+b_2)x_3^2+(2^{2\gamma+1}b_1+2b_2+4b_3)x_2x_3$.

In each of these cases one checks that $(\mu_1, \mu_2+1, \mu_3+1) \in S(\boldsymbol{\varphi})$. □

Lemma 4.5. — *Suppose that Q is diagonal, $\mu_1 \equiv \mu_2 \bmod 2$ and $u_1 + u_2 \equiv 2 \bmod 4$. Then $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$.*

Proof. — By Lemma 4.4 we may assume that $\mu_3 \geq \mu_2+2$. We claim that $a_2 \leq \mu_2+1$. Suppose that $a_2 \geq \mu_2+2$. As before, we suppose that $\boldsymbol{\varphi}$ is an optimal basis. As before, we write $C = (c_{ij})$ for the change of basis matrix and $D = C^tBC = (d_{ij})$ for the matrix corresponding to the new basis. Write $\mu_2 = \mu_1 + 2\gamma$.

The assumption $a_2 \geq \mu_2 + 2$ implies that $\operatorname{ord}(d_{22}) \geq a_2 \geq \mu_2 + 2$ and $\operatorname{ord}(d_{33}) \geq a_3 \geq a_2 \geq \mu_2 + 2$. It follows from (4.3) that $\operatorname{ord}(c_{12}) \geq \gamma$ and $\operatorname{ord}(c_{13}) \geq \gamma$. Suppose that $\operatorname{ord}(c_{12}) = \gamma$. Then $\operatorname{ord}(c_{22}) = 1$ and $d_{22} \equiv 2^{\mu_2}(u_1 + u_2) \not\equiv 0 \bmod 2^{\mu_2+2}$. This gives a contradiction. Similarly, we obtain a contradiction if $\operatorname{ord}(c_{13}) = \gamma$. Therefore $\operatorname{ord}(c_{1j}) > \gamma$ for $j = 2, 3$ and $d_{22} \equiv c_{22}^2 b_2 \bmod 2^{\mu_2+2}$. Since $\operatorname{ord}(d_{22}) \geq \mu_2 + 2$ and $\operatorname{ord}(b_2) = \mu_2$, we conclude that $\operatorname{ord}(c_{22}) > 0$. Similarly, $d_{33} \equiv c_{23}^2 b_2 \bmod 2^{\mu_2+2}$; this implies that $\operatorname{ord}(c_{23}) > 0$. But then $\det(C) \equiv 0 \bmod 2$. This gives a contradiction. We conclude that $a_2 \leq \mu_2 + 1$.

To prove the lemma, we construct a basis $\boldsymbol{\varphi}$ such that $(\mu_1, \mu_2 + 1, \mu_3 + 1) \in S(\boldsymbol{\varphi})$. We distinguish two subcases:

- $\mu_3 \equiv \mu_1 \bmod 2$,
- $\mu_3 \not\equiv \mu_1 \bmod 2$.

Suppose that $\mu_3 \equiv \mu_1 \bmod 2$. Write $\mu_2 = \mu_1 + 2\gamma$ and $\mu_3 = \mu_1 + 2\lambda$. Let $\boldsymbol{\varphi}$ be the basis of L corresponding to the change of basis matrix

$$C = \begin{pmatrix} 1 & 2^\gamma & 2^\lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + (2^{2\gamma}b_1 + b_2)x_2^2 + 2^{\gamma+1}b_1x_1x_2 + 2^{\lambda+1}b_1x_1x_3 + (b_3 + 2^{2\lambda}b_1)x_3^2 + 2^{\gamma+\lambda+1}b_1x_2x_3$.

Suppose that $\mu_3 \not\equiv \mu_1 \bmod 2$. Write $\mu_2 = \mu_1 + 2\gamma$ and $\mu_3 = \mu_1 + 2\lambda + 1$. Let $\boldsymbol{\varphi}$ be the basis of L corresponding to the change of basis matrix

$$C = \begin{pmatrix} 1 & 2^\gamma & 2^\lambda \\ 0 & 1 & 2^{\lambda-\gamma} \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to the new basis we have $Q(x) = b_1x_1^2 + (2^{2\gamma}b_1 + b_2)x_2^2 + 2^{\gamma+1}b_1x_1x_2 + 2^{\lambda+1}b_1x_1x_3 + (b_3 + 2^{2\lambda}b_1 + 2^{2(\lambda-\gamma)}b_2)x_3^2 + (2^{\gamma+\lambda+1}b_1 + 2^{\lambda-\gamma+1}b_2)x_2x_3$.

In each of these cases one checks that $(\mu_1, \mu_2 + 1, \mu_3 + 1) \in S(\boldsymbol{\varphi})$. □

Lemma 4.6. — *Suppose that Q is diagonal, $\mu_1 \equiv \mu_2 \bmod 2$, $\mu_3 \geq \mu_2 + 2$ and $u_1 + u_2 \equiv 0 \bmod 4$. Then $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 2, \mu_3)$.*

Proof. — Write $\mu_2 = \mu_1 + 2\gamma$. We already know that $a_1 = \mu_1$. We claim that $a_2 \leq \mu_2 + 2$. Suppose $a_2 \geq \mu_2 + 3$. The same reasoning as in the beginning of the proof of Lemma 4.4 shows that we may assume that $\mu_3 \geq \mu_2 + 4$. If $c_{22} \equiv c_{23} \equiv 0 \bmod 2$, we conclude as in the proof of Lemma 4.5 that $\det(C) \equiv 0 \bmod 2$. This gives a contradiction, hence either c_{22} or c_{23} is a unit.

Suppose that c_{22} is a unit. (The argument in the case that c_{23} is a unit is similar, and we omit it.) Then $\mathrm{ord}(c_{12}) = \gamma$. One computes that

$$d_{12} \equiv 2c_{12}c_{11}b_1 + 2c_{21}c_{22}b_2 \bmod 2^{\mu_2+3}. \tag{4.4}$$

It follows from (1.2) that $2\,\mathrm{ord}(d_{12}) \geq a_1 + a_2 \geq \mu_1 + \mu_2 + 3 = 2\mu_1 + 2\gamma + 3$. Hence

$$\mathrm{ord}(d_{12}) \geq \mu_1 + \gamma + 2. \tag{4.5}$$

Recall that Lemma 1.3.(b) implies that $\mathrm{ord}(d_{11}) = a_1$.

First suppose that $\mu_1 < \mu_2$, that is $\gamma \neq 0$. Since d_{11} has valuation a_1, c_{11} is a unit. It follows from (4.4) that $\mathrm{ord}(d_{12}) = \mu_1 + \gamma + 1$. This contradicts (4.5).

Now suppose that $\mu_1 = \mu_2$. Since $d_{11} \equiv c_{12}^2b_1 + c_{21}^2b_2 \bmod 2^{\mu_1+1}$. Since d_{11} has valuation $a_1 = \mu_1$, it follows that either

(i) $c_{12} \equiv 1 \bmod 2$ and $c_{21} \equiv 0 \bmod 2$, or
(ii) $c_{12} \equiv 0 \bmod 2$ and $c_{21} \equiv 1 \bmod 2$.

Since $\mathrm{ord}(d_{12}) \geq \mu_1 + 2$, it follows from (4.4) that (i) holds and that $c_{11} \equiv 0 \bmod 2$. One computes that

$$d_{23} \equiv 2c_{12}c_{13}b_1 + 2c_{22}c_{23}b_2 \equiv 2c_{13}b_1 + 2c_{23}b_2 \bmod 2^{\mu_1+2},$$

since c_{12} and c_{22} are units. It follows that $c_{13} \equiv c_{23} \bmod 2$. But this implies that $\det(C) \equiv 0 \bmod 2$. (In case $u_1 + u_2 \equiv 4 \bmod 8$ one could alternatively argue as in the proof of Lemma 4.5.)

Let $\boldsymbol{\varphi}$ be the basis of L corresponding to the change of basis matrix

$$C = \begin{pmatrix} 1 & 2^\gamma & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then $b_{22}(\boldsymbol{\varphi}) \equiv 0 \bmod 2^{\mu_2+2}$. With respect to the new basis we have $Q(x) = b_1x_1^2 + (2^{2\gamma}b_1 + b_2)x_2^2 + 2^{\gamma+1}b_1x_1x_2 + b_3x_3^2$. Therefore $(\mu_1, \mu_2 + 1, \mu_3) \in S(\boldsymbol{\varphi})$. This proves the lemma. □

The following proposition is an immediate consequence of the computation of the invariants a_i. It illustrates that the a_i satisfy similar properties for $\ell = 2$ and $\ell \neq 2$, which is not so clear from the definition.

Proposition 4.7. — *Let Q be a ternary quadratic form over $\mathbb{Z}_\ell$ for $\ell \geq 2$. Then*

$$\operatorname{ord}(\Delta) = a_1 + a_2 + a_3.$$

Proof. — For $\ell \neq 2$ this is Proposition 2.6.(b). For $\ell = 2$ the theorem follows from the Propositions 4.1 and 4.2. □

In the rest of this section we define the Gross–Keating invariant ϵ for $\ell = 2$ and show that it is well defined (compare to Lemma 2.8).

Definition 4.8. — Suppose that $a_1 \equiv a_2 \bmod 2$ and $a_3 > a_2$. Let $\boldsymbol{\varphi}$ be an optimal basis. We define $\epsilon = \epsilon(\boldsymbol{\varphi})$ by $\epsilon = 1$ if the subspace of $L \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$ spanned by φ_1 and φ_2 is isotropic, and $\epsilon = -1$, otherwise.

Proposition 4.9. — *Suppose that $a_1 \equiv a_2 \bmod 2$ and $a_3 > a_2$.*

(a) *The invariant ϵ does not depend on the choice of the basis.*

(b) (i) *If Q is not diagonalizable we may write $Q(x) = u_1 2^{\mu_1} x_1^2 + 2^{\mu_2}(v x_2^2 + x_2 x_3 + v x_3^2)$ with $v \in \{0, 1\}$ and $\mu_1 > \mu_2$. In this case*

$$\epsilon = (-1)^v.$$

(ii) *If Q is diagonalizable we may write $Q(x) = u_1 2^{\mu_1} x_1^2 + u_2 2^{\mu_2} x_2^2 + u_3 2^{\mu_3} x_3^2$ with $u_1 + u_2 \equiv 0 \bmod 4$, $\mu_1 \equiv \mu_2 \bmod 2$ and $\mu_3 \geq \mu_2 + 2$. We have that*

$$\epsilon = (-1)^{(u_1+u_2)/4}.$$

Proof. — The fact that one of the two cases of (b) holds follows immediately from Propositions 4.1 and 4.2.

Suppose that Q is not diagonalizable. Write $Q(x) = u_1 2^{\mu_1} x_1^2 + 2^{\mu_2}(v x_2^2 + x_2 x_3 + v x_3^2)$, as in the statement of the proposition, and let $\boldsymbol{\psi}$ be the corresponding basis. Write Q_2 for the restriction of Q to the sublattice spanned by the basis vectors ψ_2, ψ_3. Lemma 3.2 implies that Q_2 is isotropic if and only $v = 0$. This implies that $\epsilon(\boldsymbol{\psi}) = (-1)^v$.

We now show that ϵ is well defined in this case. It suffices to show that $\epsilon(\boldsymbol{\varphi}) = \epsilon(\boldsymbol{\psi})$ for optimal bases $\boldsymbol{\varphi}$ and $\boldsymbol{\psi}$ with respect to which Q is in a normal form as in Proposition 3.3. By assumption, Q is not diagonalizable. (In fact, it follows from Proposition 4.2 that no quadratic form $Q(x) = u_1 2^{\mu_1} x_1^2 + 2^{\mu_2}(v x_2^2 + x_2 x_3 + v x_3^2)$ with $v \in \{0, 1\}$ and $\mu_1 > \mu_2$ is diagonalizable. Hence we could have dropped this assumption from the statement of the proposition.) Write $Q'(x) = u_1' 2^{\mu_1} x_1^2 + 2^{\mu_2}(v' x_2^2 + x_2 x_3 + v' x_3^2)$ for Q expressed with respect to the basis $\boldsymbol{\varphi}$. Since $\Delta(Q) = \Delta(Q')$ we have that $u_1(4v^2 - 1) = u_1'(4(v')^2 - 1)$, therefore $v = v'$ implies that $u_1 = u_1'$.

Hence, to show that $\epsilon(\boldsymbol{\varphi}) = \epsilon(\boldsymbol{\psi})$, it suffices to show that $v = v'$. We assume that $v = 1$ and $v' = 0$, and derive a contradiction.

The basis vector φ_2 is isotropic. Write $\varphi_2 = c_1\psi_1 + c_2\psi_2 + c_3\psi_3$. The fact that $Q(\varphi_2) = 0$ implies that $\mu_1 \equiv \mu_2 \bmod 2$. Moreover, it follows that $\operatorname{ord}(c_j) \geq (\mu_1 - \mu_2)/2 > 0$ for $j = 2, 3$. Since φ_2 is primitive, it follows that $c_1 \equiv 1 \bmod 2$. An easy computation shows that $\operatorname{ord}(\varphi_2, \psi_i) > \mu_2$ for $i = 1, 2, 3$. In particular $\operatorname{ord}(\varphi_2, \varphi_3) > \mu_2$. But this contradicts the assumption that $\operatorname{ord}(\varphi_2, \varphi_3) = \mu_2$.

Next we assume that Q is diagonalizable, and let $Q(x)$ be as in the statement of (b.ii). Write $\boldsymbol{\psi}$ for the corresponding basis of L. Let Q_2 be the restriction of Q to the subspace spanned by ψ_1, ψ_2. Then Q_2 is isotropic if and only if $-\det(Q)$ is a square ([**S**, Theorem IV.6]). It is easy to see that this happens if and only if $u_1 + u_2 \equiv 0 \bmod 8$.

We now show that ϵ is independent of the choice of the optimal basis in this case. Let $\boldsymbol{\varphi}$ be an optimal basis. Let $C = (c_{ij})$ be the corresponding change of basis matrix expressing $\boldsymbol{\varphi}$ in terms of $\boldsymbol{\psi}$. Write $\mu_1 = \mu_2 + 2\gamma$.

We suppose that $\mu_2 > \mu_1$, that is $\gamma > 0$. (The case $\mu_1 = \mu_2$ is analogous and left to the reader.) We use the notation of the proof of Lemma 4.6. In particular, we write $Q(x) = \sum_{i \leq j} d_{ij} x_i x_j$ for the representation of Q in terms of the basis $\boldsymbol{\varphi}$.

We showed in the proof of Lemma 4.6 that either c_{22} or c_{23} is a unit. Suppose that $c_{22} \equiv 0 \bmod 2$ and $c_{23} \equiv 1 \bmod 2$. It follows that $\operatorname{ord}(d_{33}) \geq a_3 = \mu_3 \geq \mu_2 + 3$. Therefore (4.3) implies that $\operatorname{ord}(c_{13}) = \gamma$. We showed in the proof of Lemma 4.6 that c_{11} is a unit. Since $d_{13} \equiv 2c_{11}c_{13}b_1 + 2c_{21}c_{23}b_2 \bmod 2^{\mu_3+1}$, we conclude that $2\operatorname{ord}(d_{13}) = 2 + 2\gamma + 2\mu_1 = \mu_1 + \mu_2 + 2$. (Here we use that $\gamma > 0$.) But this contradicts $2\operatorname{ord}(d_{13}) \geq a_1 + a_3 = \mu_1 + \mu_3 \geq \mu_1 + \mu_2 + 3$. We conclude that c_{22} is a unit. Recall from the proof of Lemma 4.6 that this implies that $c_{12} \equiv 1 \bmod 2$ and $c_{21} \equiv 0 \bmod 2$. Therefore the determinant of the submatrix

$$\tilde{C} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

of C is a unit. We may define

$$D = \begin{pmatrix} \tilde{C}^{-1} & 0 \\ 0 & 1 \end{pmatrix}.$$

With respect to the basis corresponding to CD, the quadratic form Q becomes $Q(x) = (b_1 + \delta_1^2 b_3)x_1^2 + (b_2 + \delta_2^2 b_3)x_2^2 + 2\delta_1 b_3 x_1 x_2 + x_3(\text{other terms})$, for certain $\delta_1, \delta_2 \in \mathbb{Z}_2$. Since $\operatorname{ord}(b_3) \geq \operatorname{ord}(b_2) + 3$ this implies that the subspace spanned by φ_1 and φ_2 is isotropic if and only if the space spanned by ψ_1 and ψ_2 is isotropic. □

5. Anisotropic quadratic forms

The goal is to classify all anisotropic ternary quadratic forms over $\mathbb{Z}_2$, starting from the normal form of Proposition 3.3. We will see that for anisotropic forms we may

choose an optimal basis $\boldsymbol{\varphi}$ so that $\operatorname{ord}(Q(\varphi_i)) = a_i$, similar to what we had for $\ell \neq 2$ (Corollary 5.8).

Proposition 5.1. — *Let Q be a ternary quadratic form over $\mathbb{Q}_\ell$. Write $Q(x) = b_1x_1^2 + b_2x_2^2 + b_3x_3^2$. We denote by $\det(Q) = b_1b_2b_3$ the determinant of Q. Then Q is isotropic if and only if*

$$(-1, -\det(Q)) = \prod_{i<j}(b_i, b_j).$$

Here $(\cdot,\cdot)$ denotes the Hilbert symbol.

Proof. — This is [**S**, Theorem IV.6.ii]. □

Proposition 5.2. — *Let Q be a ternary quadratic form over $\mathbb{Z}_2$ which is not diagonalizable. Let $\boldsymbol{\psi}$ be an optimal basis such that $Q(x) = u_1 2^{\mu_1}x_1^2 + 2^{\mu_2}(vx_2^2 + x_2x_3 + vx_3^2)$ with $v \in \{0, 1\}$. Then Q is isotropic if and only if $v = 0$ or $\mu_1 \equiv \mu_2 \bmod 2$.*

Proof. — If $v = 0$ then Q is obviously isotropic. Therefore suppose that $v = 1$. To decide whether Q is isotropic, we may consider Q as quadratic form over $\mathbb{Q}_2$. We have $Q(x) \sim_{\mathbb{Q}_2} u_1 2^{\mu_1}x_1^2 + 2^{\mu_2}(x_2^2 + 3x_3^2)$. The proposition follows from Proposition 5.1 by direct verification using the formula for the Hilbert symbol [**S**, Theorem III.1]. □

Lemma 5.3. — *Let Q be a ternary quadratic form over $\mathbb{Z}_\ell$. We do not assume that $\ell = 2$. Suppose that $a_1 \equiv a_2 \equiv a_3 \bmod 2$. Then Q is isotropic.*

Proof. — If Q is not diagonalizable then the lemma follows from Proposition 5.2, since $(a_1, a_2, a_3) \in \{(\mu_1, \mu_2, \mu_2), (\mu_2, \mu_2, \mu_1)\}$.

Suppose that Q is diagonalizable. Write $Q(x) = u_1\ell^{\mu_1}x_1^2 + u_2\ell^{\mu_2}x_2^2 + u_3\ell^{\mu_3}x_3^2$. If $\ell \neq 2$ we have that $\mu_i = a_i$ hence $\mu_1 \equiv \mu_2 \equiv \mu_3 \bmod 2$. To show that Q is isotropic, it suffices to consider Q over $\mathbb{Q}_\ell$. After multiplying the basis vectors by a suitable constant, we may assume that $\mu_1 = \mu_2 = \mu_3 = 0$. The lemma now follows immediately from Proposition 5.1, since the Hilbert symbol is trivial on units for $\ell \neq 2$.

Suppose that $\ell = 2$ and Q is diagonalizable. Proposition 4.2 implies that $\mu_1 \equiv \mu_2 \equiv \mu_3 \bmod 2$ and $u_1 + u_2 \equiv 0 \bmod 4$. As for $\ell \neq 2$, it is no restriction to suppose that $Q(x) = u_1x_2^2 + u_2x_2^2 + u_3x_3^2$. One computes that this quadratic form is anisotropic if and only if $u_1 \equiv u_2 \equiv u_3 \bmod 4$. Hence in our case Q is isotropic. □

For future reference we record from the proof of Lemma 5.3 when a diagonal ternary form over $\mathbb{Z}_2$ is anisotropic.

Lemma 5.4. — *Let $Q(x) = u_1 2^{\mu_1}x_1^2 + u_2 2^{\mu_2}x_2^2 + u_3 2^{\mu_3}x_3^2$ be a diagonal, ternary quadratic form over $\mathbb{Z}_2$. Suppose that $\mu_1 \equiv \mu_2 \equiv \mu_3 \bmod 2$. Then Q is anisotropic if and only if $u_1 \equiv u_2 \equiv u_3 \bmod 4$.*

Lemma 5.5. — *Let* $Q(x) = u_1 2^{\mu_1} x_1^2 + u_2 2^{\mu_2} x_2^2 + u_3 2^{\mu_3} x_3^2$ *be a diagonal, ternary quadratic form over* $\mathbb{Z}_2$. *Suppose that* $\mu_1 \equiv \mu_2 \bmod 2$ *and* $\mu_3 \not\equiv \mu_1 \bmod 2$.

(a) *Suppose that* $u_1 \equiv u_2 \equiv u_3 \bmod 4$. *Then* Q *is anisotropic if and only if* $u_2 \equiv \pm u_1 \bmod 8$.
(b) *Suppose that the* u_i *are not all equivalent modulo* 4. *Then* Q *is anisotropic if and only if* $u_2 \equiv \pm 3u_1 \bmod 8$.

Proof. — The proof is similar to the proof of Lemma 5.3 and is left to the reader. □

Notation 5.6. — *Let* Q *be a ternary quadratic form with Gross–Keating invariants* (a_1, a_2, a_3). *For every* $1 \leq i < j \leq 3$ *we define*

$$\delta_{ij} = \lceil \frac{a_i + a_j}{2} \rceil,$$

where $\lceil a \rceil$ is the smallest integer greater than or equal to a.

Theorem 5.7. — *Let* $Q(x) = u_1 2^{\mu_1} x_1^2 + u_2 2^{\mu_2} x_2^2 + u_3 2^{\mu_3} x_3^2$ *be a diagonal anisotropic quadratic form over* $\mathbb{Z}_2$ *with* $\mu_1 \leq \mu_2 \leq \mu_3$. *Then one of the following cases occurs.*

(a) *Suppose* $\mu_1 \equiv \mu_3 \not\equiv \mu_2 \bmod 2$ *and* $u_1 \equiv 3u_3 \bmod 8$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2, \mu_3 + 2)$ *and* $a_1 \not\equiv a_2 \bmod 2$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1} u_1 x_1^2 + 2^{a_2} u_2 x_2^2 + 2^{\delta_{13}} u_1 x_1 x_3 + 2^{a_3} u_1 x_3^2.$$

(b) *Suppose* $\mu_1 \equiv \mu_3 \not\equiv \mu_2 \bmod 2$ *and* $u_1 \equiv u_3 \bmod 4$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2, \mu_3 + 2)$ *and* $a_1 \not\equiv a_2 \bmod 2$. *Moreover,* $u_2 \equiv u_1 \bmod 4$ *if* $u_3 \equiv u_1 \bmod 8$ *and* $u_2 \equiv -u_1 \bmod 4$ *if* $u_3 \equiv 5u_1 \bmod 8$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1} u_1 x_1^2 + 2^{a_2} u_2 x_2^2 + 2^{\delta_{13}} u_1 x_1 x_3 + 2^{\delta_{23}} u_2 x_2 x_3 + 2^{a_3} u_1 v x_3^2.$$

Here $v = (u_1 + u_2)/2$ *if* $u_2 \equiv u_1 \bmod 4$ *and* $v = (3u_1 + u_2)/2$ *if* $u_2 \equiv -u_1 \bmod 4$.

(c) *Suppose* $\mu_1 \not\equiv \mu_2 \equiv \mu_3 \bmod 2$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2, \mu_3 + 2)$ *and* $a_2 \not\equiv a_1 \bmod 2$. *The quadratic form with respect to an optimal basis is as in (a) and (b) with the role of* x_1 *and* x_2 *reversed.*

(d) *Suppose* $\mu_1 \equiv \mu_2 \bmod 2$ *and* $\mu_2 = \mu_3$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_1 \not\equiv a_2 \bmod 2$. *Moreover,* $u_1 \equiv u_2 \equiv u_3 \bmod 4$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1} u_1 x_1^2 + 2^{a_2} v_2 x_2^2 + 2^{\delta_{13}} u_1 (x_1 x_2 + x_1 x_3) + 2^{\delta_{23}} u_1 x_2 x_3 + 2^{a_3} v_3 x_3^2.$$

Here $v_i = (u_1 + u_i)/2$ *for* $i = 2, 3$.

(e) *Suppose* $\mu_1 \equiv \mu_2 \bmod 2$, $\mu_3 = \mu_2 + 1$ *and* $u_1 \equiv u_2 \bmod 4$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_2 \not\equiv a_1 \bmod 2$. *Moreover,* $u_2 \equiv u_1 \bmod 8$ *if* $u_3 \equiv u_1 \bmod 4$ *and* $u_2 \equiv 5u_1 \bmod 8$ *if* $u_3 \equiv -u_1 \bmod 4$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}u_1x_1^2 + 2^{a_2}v_2x_2^2 + 2^{\delta_{13}}u_1(x_1x_2 + x_1x_3) + 2^{\delta_{23}}v_2x_2x_3 + 2^{a_3}v_3x_3^2.$$

Here $v_2 = (u_1 + u_2)/2$ *and* $v_3 = (u_1 + u_3)/2$ *(resp.* $(3u_1 + u_3)/2$*) depending on whether* $u_3 \equiv u_1 \bmod 4$ *or not.*

(f) *Suppose* $\mu_1 \equiv \mu_2 \bmod 2$, $\mu_3 = \mu_2 + 1$ *and* $u_1 \equiv -u_2 \bmod 4$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_1 \equiv a_2 \bmod 2$. *Moreover,* $u_2 \equiv 3u_1 \bmod 8$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}u_1x_1^2 + 2^{a_2}v_2x_2^2 + 2^{\delta_{13}}u_1(x_1x_2 + x_1x_3) + 2^{\delta_{23}}v_{23}x_2x_3 + 2^{a_3}v_3x_3^2.$$

Here $v_2 = (u_1 + u_2 + 2u_3)/2$, $v_{23} = (u_1 + u_2 + 4u_3)/2$ *and* $v_3 = u_1 + 2u_3$.

(g) *Suppose* $\mu_1 \equiv \mu_2 \equiv \mu_3 \bmod 2$ *and* $u_1 \equiv u_2 \bmod 4$ *and* $\mu_3 \geq \mu_2 + 2$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_2 \not\equiv a_1 \bmod 2$. *Moreover,* $u_3 \equiv u_1 \bmod 4$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}u_1x_1^2 + 2^{a_2}v_2x_2^2 + 2^{\delta_{12}}u_1x_1x_2 + 2^{\delta_{13}}u_1x_1x_3 + 2^{\delta_{23}}u_1x_2x_3 + 2^{a_3}v_3x_3^2.$$

Here $v_i = (u_1 + u_i)/2$ *for* $i = 2, 3$.

(h) *Suppose* $\mu_1 \equiv \mu_2 \not\equiv \mu_3 \bmod 2$ *and* $u_1 \equiv u_2 \bmod 4$ *and* $\mu_3 \geq \mu_2 + 2$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 1, \mu_3 + 1)$ *and* $a_2 \not\equiv a_1 \bmod 2$. *One of the following two cases holds:*

$$\begin{cases} u_2 \equiv u_1 \bmod 8 \text{ and } u_3 \equiv u_1 \bmod 4, \\ u_2 \equiv 5u_1 \bmod 8 \text{ and } u_3 \equiv -u_1 \bmod 4. \end{cases}$$

There exists an optimal basis with respect to which

$$Q(x) = 2^{a_1}u_1x_1^2 + 2^{a_2}v_2x_2^2 + 2^{\delta_{12}}u_1x_1x_2 + 2^{\delta_{13}}u_1x_1x_3 + 2^{\delta_{23}}v_2x_2x_3 + 2^{a_3}v_3x_3^2.$$

Here $v_2 = (u_1 + u_2)/2$ *and* $v_3 = (u_1 + u_3)/2$ *(resp.* $v_3 = (3u_1 + u_3)/2$*) depending on whether* $u_1 \equiv u_3 \bmod 4$ *or not.*

(i) *Suppose* $\mu_1 \equiv \mu_2 \not\equiv \mu_3 \bmod 2$, $\mu_3 \geq \mu_2 + 2$ *and* $u_2 \equiv 3u_1 \bmod 8$. *Then* $(a_1, a_2, a_3) = (\mu_1, \mu_2 + 2, \mu_3)$ *and* $a_1 \equiv a_2 \bmod 2$. *There exists an optimal basis with respect to which*

$$Q(x) = 2^{a_1}u_1x_1^2 + 2^{a_2}v_2x_2^2 + 2^{\delta_{12}}u_1x_1x_2 + 2^{a_3}u_3x_3^2.$$

Here $v_2 = (u_1 + u_2)/2$.

Proof. — This follows from the results of Section 4 together with the Lemmas 5.4, 5.5. □

Corollary 5.8. — *Suppose that* Q *is anisotropic. Then there exists an optimal basis* $\boldsymbol{\varphi}$ *such that*

$$\operatorname{ord}(b_{ii}(\boldsymbol{\varphi})) = a_i$$

for $i = 1, 2, 3$.

Proof. — This follows immediately from Theorem 5.7 (diagonal case) and Proposition 5.2 (non-diagonal case). □

In Section 6, we give a more conceptual proof of Corollary 5.8. In fact, we prove that *any* optimal basis has the property in Corollary 5.8. The following lemma gives a list of the small cases.

Lemma 5.9. — *Let Q be an anisotropic ternary quadratic form over $\mathbb{Z}_2$ and suppose that $a_3 \leq 1$. Then one of the following possibilities occurs.*

(a) *We have $(a_1, a_2, a_3) = (0, 0, 1)$. In this case Q is not diagonalizable; it is of the form*
$$Q(x) = x_1^2 + x_1x_2 + x_2^2 + u_3 2x_3^2.$$
(b) *We have $(a_1, a_2, a_3) = (0, 1, 1)$ and Q is not diagonalizable. Then Q is of the form*
$$Q(x) = u_1x_1^2 + 2(x_2^2 + x_2x_3 + x_3^2).$$
(c) *We have $(a_1, a_2, a_3) = (0, 1, 1)$ and Q is diagonalizable. Then Q is as in Theorem 5.7.(d) with $a_1 = \delta_{13} = 0$ and $a_2 = a_3 = \delta_{23} = 1$.*

6. Alternative version of the Gross–Keating invariants for anisotropic forms

We fix an arbitrary prime number ℓ and a free quadratic module (L, Q) over $\mathbb{Z}_\ell$ of rank n. We assume that (L, Q) is anisotropic, *i.e.*, that $Q(\psi) = 0$ implies $\psi = 0$. Under this assumption, there is an alternative definition of the Gross–Keating invariants and a very useful characterization of optimal bases; see the remark at the end of section 4 in [**GK**]. In this section we do not suppose that $n = 3$ to streamline some arguments. Recall that $n \geq 5$ implies that (L, Q) is isotropic ([**S**, Theorem IV.6]). Therefore the only additional case is anisotropic quadratic forms in four variables.

We define a function $v : L \to \mathbb{Z} \cup \{\infty\}$ by the rule
$$v(\psi) := \operatorname{ord}_\ell Q(\psi).$$
For $\psi \in L$ and $x \in \mathbb{Z}_p$ we have
$$v(x\psi) = 2\operatorname{ord}_\ell(x) + v(\psi). \tag{6.1}$$

Lemma 6.1. — *The function v satisfies the triangle inequality*
$$v(\psi + \psi') \geq \min(v(\psi), v(\psi')). \tag{6.2}$$
Moreover, if the inequality in (6.2) *is strict we have $v(\psi) = v(\psi')$.*

Proof. — If ψ and ψ' are linearly dependent the claim is obvious. We may hence assume that they are linearly independent. For $x, y \in \mathbb{Z}_\ell$ we write

$$Q(x\psi + y\psi') = ax^2 + y^2 b + cxy.$$

Suppose that $v(\psi + \psi') < v(\psi), v(\psi')$. Then $\mathrm{ord}_\ell(a+b+c) < \mathrm{ord}_\ell(a), \mathrm{ord}_\ell(b)$. The usual triangle inequality for ord_ℓ implies

$$\mathrm{ord}_\ell(c) = \mathrm{ord}_\ell(a+b+c) < \mathrm{ord}_\ell(a), \mathrm{ord}_\ell(b).$$

Lemma 3.2.(b) implies that (L, Q) is isotropic. This and proves (6.2). The second assertion of the lemma follows from (6.2), applied to a suitable combination of the vectors $\pm\psi$, $\pm\psi'$ and $\psi + \psi'$. □

Remark 6.2. — If $n \leq 3$, one gets an alternative proof of Lemma 6.1 by noting that (L, Q) is represented by the quaternion division algebra D over $\mathbb{Q}_\ell$, equipped with its norm form. The function v is then the restriction of the standard valuation of D.

Let $\boldsymbol{\psi} = (\psi_i)$ be a basis of L. For $i = 1, \ldots, n$, let $L_{i-1} \subset L$ be the subspace (of rank $i-1$) spanned by $\psi_1, \ldots, \psi_{i-1}$. We define a function $\tilde{v}_i : L/L_{i-1} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by the rule

$$\tilde{v}_i(\psi + L_{i-1}) := \max(v(\psi') | \psi' \in \psi + L_{i-1}).$$

Note that $\tilde{v}_i(\psi) = \infty$ if and only of $\psi \in L_{i-1}$.

Definition 6.3. — A basis $\boldsymbol{\psi} = (\psi_i)$ of L is called *ideal*, if

$$v(\psi_i) = \tilde{v}_i(\psi_i + L_{i-1}) = \min_{\psi \in L}(\tilde{v}_i(\psi + L_{i-1}))$$

holds for $i = 1, \ldots, n$.

It is clear that there exists an ideal basis of L. The next lemma gives a useful characterization of an ideal basis.

Lemma 6.4. — *A basis $\boldsymbol{\psi} = (\psi_i)$ of L is ideal if and only if*

$$v(\psi_i) \leq v(\psi_j) \quad \text{for } i \leq j, \tag{6.3}$$

and for all $(x_i) \in \mathbb{Z}_\ell^n$ we have

$$v\Big(\sum_i x_i \psi_i\Big) = \min_i v(x_i \psi_i). \tag{6.4}$$

Proof. — Let $\boldsymbol{\psi} = (\psi_i)$ be a basis of L. If (6.3) and (6.4) hold, then one easily checks from Definition 6.3 that $\boldsymbol{\psi}$ is ideal.

Conversely, suppose that $\boldsymbol{\psi}$ is ideal. The inequality (6.3) follows directly from Definition 6.3. It remains to prove (6.4). Fix $(x_i) \in \mathbb{Z}_\ell^n$ and k with $1 \leq k \leq n$. Set $\varphi_k := \sum_{i<k} x_i \psi_i$. We claim that

$$v(\varphi_k + x_k \psi_k) = \min(v(\varphi_k), v(x_k \psi_k)). \tag{6.5}$$

From this claim, (6.4) follows by induction.

For $k = 1$, the claim is obvious. To prove it for $k > 1$ we may assume that it holds for $k' = k - 1$. Also, by the triangle inequality (6.2), the left hand side of (6.5) is greater than or equal to the right hand side. Suppose that the left hand side is strictly greater than the right hand side. Then we have $v(\varphi_k) = v(x_k\psi_k)$. Using (6.1), (6.3) and the claim for $k' = k - 1$, we find that $\mathrm{ord}_\ell(x_k) \leq \mathrm{ord}_\ell(x_i)$ for all $i \leq k$. After dividing by x_k, we may therefore assume that $x_k = 1$. However, by the definition of an ideal basis we have

$$v(\varphi_k) = v(\psi_k) \geq v(\varphi_k + \psi_k).$$

This contradicts our assumption and proves the claim. □

Let us fix an ideal basis $\boldsymbol{\psi} = (\psi_1, \ldots, \psi_n)$ of L, and set

$$a_i := v(\psi_i), \quad i = 1, \ldots, n.$$

We want to show that the a_i are the Gross–Keating invariants of (L, Q). We first check that (a_i) lies in the set S (Section 1). For this we write the quadratic form Q as follows:

$$Q\Big(\sum_i x_i\psi_i\Big) = \sum_{i\leq j} b_{ij}x_ix_j.$$

We set $a_{ij} := \mathrm{ord}_\ell(b_{ij})$. Note that $a_i = a_{ii}$.

Proposition 6.5. — *For $1 \leq i \leq j \leq n$ we have*

$$a_{ij} \geq \frac{a_i + a_j}{2}.$$

Proof. — The case $i = j$ being trivial, we may assume that $i < j$. Our proof is by contradiction. First we assume that $2a_{ij}+1 < a_i+a_j$. We set $c := \max(a_{ij}-a_i+1, 0)$ and look at the right hand side of

$$Q(\ell^c\psi_i + \psi_j) = b_{ii}\ell^{2c} + b_{jj} + b_{ij}\ell^c.$$

The three terms of this sum have ℓ-valuation $a_i + 2c$, a_j and $a_{ij} + c$, respectively. By our choice of c we have

$$a_{ij} + c < \min(a_i + 2c, a_j).$$

It follows that

$$v(\ell^c\psi_i + \psi_j) = a_{ij} + c < \min(v(\ell^c\psi_i), v(\psi_j)).$$

This contradicts the triangle inequality and excludes the case $2a_{ij} + 1 < a_i + a_j$.

It remains to exclude the case $2a_{ij} + 1 = a_i + a_j$. Since $a_i \leq a_j$ we have $c := a_{ij} - a_i \geq 0$. Let $x \in \mathbb{Z}_\ell^\times$ be a ℓ-adic unit. Then

$$Q(\ell^c x\psi_i + \psi_j) = b_{ii}\ell^{2c}x^2 + b_{jj} + b_{ij}\ell^c x. \tag{6.6}$$

By our choice of c we have

$$a_i + 2c = a_j - 1 = a_{ij} + c.$$

We see that on the right hand side of (6.6), the first and the last term have the minimal valuation $a_j - 1$, while the middle term has valuation a_j. Therefore, for an appropriate choice of x, we get

$$v(\ell^c x\psi_i + \psi_j) \geq a_j > \min(v(\ell^c x\psi_i), v(\psi_j)).$$

But this contradicts Lemma 6.4, (6.4). The proposition follows. □

Proposition 6.6. — *An ideal basis is also optimal (Definition 1.2). Moreover, if $\boldsymbol{\psi} = (\psi_i)$ is an ideal basis of L, then $(a_i := v(\psi_i))$ are the Gross–Keating invariants of (L, Q).*

Proof. — The previous proposition says that (a_i) is an element of S. It remains to show that (a_i) is a maximal element, with respect to the lexicographical ordering.

Let $\boldsymbol{\psi}' = (\psi'_i)$ be an arbitrary basis of L, and let (a'_i) be an element of $S(\boldsymbol{\psi}')$ (Section 1). We will show that $a'_k \leq a_k$ for $k = 1, \ldots, n$, which proves the proposition. Write

$$\psi'_i = \sum_j x_{ij}\psi_j, \qquad \text{with} \qquad (x_{ij}) \in \mathrm{GL}_n(\mathbb{Z}_\ell).$$

The condition $(a'_i) \in S(\boldsymbol{\psi}')$ together with Lemma 6.4 shows that

$$a'_i \leq v(\psi'_i) = \min_j(a_j + 2\,\mathrm{ord}_\ell(x_{ij})). \tag{6.7}$$

Using that (x_{ij}) is invertible, one shows that there exists at least one pair of indices (ij) with $k \leq i$ and $j \leq k$ such that x_{ij} is a unit. Applying (6.7) and (6.3) we get

$$a'_k \leq a'_i \leq a_j \leq a_k.$$

This is what we had to prove. □

Corollary 6.7. — *Let $\boldsymbol{\psi} = (\psi_i)$ be an ideal basis of L and $(y_i) \in \mathbb{Q}_\ell^n$ with $y_i \neq 0$. Set $\boldsymbol{\psi}' := (\psi'_i)$, where $\psi'_i := y_i\psi_i \in L \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, and let L' denote the $\mathbb{Z}_\ell$-lattice spanned by $\boldsymbol{\psi}'$. Let (a_i) be the Gross–Keating invariants of L.*

(a) *The basis $\boldsymbol{\psi}'$ of L' is ideal.*

(b) *The Gross–Keating invariants of L' are the numbers*

$$a'_i := a_i + 2\,\mathrm{ord}_\ell(y_i),$$

in some order.

Proof. — Choose an integer r such that $\ell^r y_i \in \mathbb{Z}_\ell$, for all i. For $(x_i) \in \mathbb{Z}_\ell^n$, Lemma 6.4 shows that

$$\begin{aligned} v\Big(\sum_i x_i\psi'_i\Big) &= v\Big(\sum_i \ell^r x_i y_i \psi_i\Big) - 2r \\ &= \min_i(v(\ell^r x_i y_i \psi_i)) - 2r \\ &= \min_i(v(x_i\psi'_i)). \end{aligned}$$

Again by Lemma 6.4 we conclude that $\boldsymbol{\psi}'$ (in some order) is an ideal basis of L'. This proves (a). Part (a) of the corollary follows now from the previous proposition. □

Remark 6.8. — Corollary 6.7 (a) is false without the assumption that (L, Q) is anisotropic. Consider, for instance, the (isotropic) quadratic form $Q(x) = x_1^2 - x_2^2 + 4x_3^2$ over $\mathbb{Z}_2$. Dividing the last vector of the standard basis by 2 we obtain the quadratic form $Q'(x) = x_1^2 - x_2^2 + x_3^2$. According to Proposition 4.2(b), the Gross–Keating invariants of Q are $(0, 2, 2)$, while the invariants of Q' are $(0, 1, 1)$.

Proposition 6.9. — *Let (L, Q) be an anisotropic free quadratic module over $\mathbb{Z}_\ell$. Then every optimal basis is an ideal basis.*

The proof of this proposition uses the following lemma.

Lemma 6.10. — *Let $(a_1, \ldots, a_n)$ be the Gross–Keating invariants of (L, Q), and let $\boldsymbol{\psi}$ be an optimal basis. Then $v(\psi_i) = a_i$.*

Proof. — Let $\boldsymbol{\psi}$ be an optimal basis and suppose that $v(\psi_i) > a_i$, for some i. It follows from the definition of the Gross–Keating invariants (Definition 1.2) that there exists a $j \neq i$ such that

$$\operatorname{ord}(b_{ij}) = (a_i + a_j)/2.$$

In particular, we have that $a_i \equiv a_j \bmod 2$. Lemma 5.3 implies therefore that $a_k \not\equiv a_i \bmod 2$ for all $k \neq i, j$, since (L, Q) is anisotropic. (The case that $n = 4$ easily reduces to the case that $n = 3$ by using the existence of an ideal basis.)

Consider the restriction Q_1 of Q to $L_1 = \langle \psi_i, \psi_j \rangle$. We distinguish three cases. First suppose that $a_i = a_j$. Then (L_1, Q_1) is isotropic by Lemma 3.2.(b).

Next we suppose that $a_i < a_j$. Then $i < j$. We have already seen that $a_k \not\equiv a_i \bmod 2$ for all $k \neq i, j$. Renumbering the indices, if necessary, we may assume that $a_i < a_{i+1}$ and $a_{j-1} < a_j$. Define $(\tilde{a}_i)$ by $\tilde{a}_i = a_i + 1$ and $\tilde{a}_j = a_j - 1$, and $\tilde{a}_k = a_k$ for all $k \neq i, j$. Then $(\tilde{a}_k) \in S(\boldsymbol{\psi})$. This contradicts the definition of the Gross–Keating invariants.

Finally, we suppose that $a_i > a_j$. Then $i > j$. If $v(\psi_j) > a_j$, we interchange i and j and obtain a contradiction by the previous case. Therefore $v(\psi_j) = a_j$. Since $a_i \equiv a_j \bmod 2$, Lemma 3.2.(b) implies that L_1 is isotropic. This gives a contradiction. We conclude that $v(\psi_i) = a_i$ for all i. □

Proof of Proposition 6.9. — Let $\boldsymbol{\psi}$ be an optimal basis which is not ideal. Lemma 6.10 implies that $v(\psi_i) = a_i$ for all i. Let k be minimal such that there exists a $\varphi = \sum_{i=1}^{k} x_i \psi_i \in L$ with $v(\varphi) \neq \min_i(x_i \psi_i)$. Lemma 6.4 implies that k exists. It follows from the triangle inequality that $v(\varphi) > \min_i(x_i \psi_i)$. Write $\tilde{\varphi} = \sum_{i=1}^{k-1} x_i \psi_i$. The choice of k implies that $v(\tilde{\varphi}) = \min_{i<k} v(x_i \psi_i)$. Since $v(\varphi) = v(\tilde{\varphi} + x_k \psi_k)$, we conclude from Lemma 6.1 that $v(\tilde{\varphi}) = v(x_k \psi_k)$. This implies that

$$2 \operatorname{ord}(x_i) + a_i \geq 2 \operatorname{ord}(x_k) + a_k. \tag{6.8}$$

In particular, $\mathrm{ord}(x_i) \geq \mathrm{ord}(x_k)$, for all i. Therefore it is no restriction to assume that x_k is a unit.

We define a new basis $\boldsymbol{\varphi} = (\varphi_i)$ by $\varphi_i = \psi_i$ if $i \neq k$ and $\varphi_k = \varphi$. Write

$$\tilde{Q}\Big(\sum_i y_i\varphi_i\Big) = \sum_{i\leq j} \tilde{b}_{ij} y_i y_j.$$

One computes that

$$\tilde{b}_{jk} = \begin{cases} 2x_j b_{jj} + \sum_{i\neq j} b_{ij}x_i & \text{for } j < k, \\ \sum_i b_{ij}x_i & \text{for } j > k. \end{cases}$$

Equation (6.8) implies that $\mathrm{ord}(\tilde{b}_{jk}) \geq (a_j + a_k)/2$. Therefore $\boldsymbol{\varphi}$ is again an optimal basis. But $v(\varphi_k) = v(\varphi) > \min_i v(x_i\psi_i) = v(x_k\psi_k) = a_k$. This contradicts Lemma 6.10. □

Lemma 6.11. — *Let $M \subset L$ be a sublattice,* i.e., *a sub-$\mathbb{Z}_\ell$-module of rank n. Let $b_1, \ldots, b_n$ be the Gross–Keating invariants of $(M, Q|_M)$. Then $b_i \geq a_i$.*

Proof. — We choose ideal bases $(\psi_1, \ldots, \psi_n)$ for L and $(\varphi_1, \ldots, \varphi_n)$ for M. Then $a_i = v(\psi_i)$ and $b_i = v(\varphi_i)$. Let us fix an index $i \in \{1, \ldots, n\}$ and show $b_i \geq a_i$. For an element $\psi = \sum_j x_j\psi_j$ of L, we set $\psi' := \sum_{j<i} x_j\psi_j$ and $\psi'' := \sum_{j\geq i} x_j\psi_j$. Then $\psi = \psi' + \psi''$ and $v(\psi'') \geq a_i$. Since the vectors $\varphi'_1, \ldots, \varphi'_i$ lie in a subspace of rank $i-1$, there exist $x_1, \ldots, x_i \in \mathbb{Z}_\ell$, not all zero, such that $\sum_{j\leq i} x_j\varphi'_j = 0$. Then

$$\sum_{j\leq i} x_j\varphi_j = \sum_{j\leq i} x_j\varphi''_j.$$

Applying Lemma 6.4 (6.4) to the left hand side and the triangle inequality (6.2) to the right hand side, we conclude that

$$\min_{j\leq i}(b_j + 2\,\mathrm{ord}_\ell(x_j)) \geq \min_{j\leq i}(v(\varphi''_j) + \mathrm{ord}_\ell(x_j)) \geq \min_{j\leq i}(a_i + 2\,\mathrm{ord}_\ell(x_j)).$$

For the index j for which $\mathrm{ord}_\ell(x_j)$ takes its minimal value we get $a_i \leq b_j \leq b_i$. This proves the lemma. □

References

[C] J. W. S. Cassels – *Rational quadratic forms*, Cambridge University Press, 1978.

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Invent. math.* **112** (1993), p. 225–245.

[S] J.-P. Serre – *Cours d'arithmétique*, Presses Universitaires de France, 1970.

[Y1] T. Yang – Local densities of 2-adic quadratic forms, *J. Number Theory* **108** (2004), p. 287–345.

[Y2] ———, Isotropic or anisotropic, letter to M. Rapoport, March 2004.

I. I. Bouw, Universität Ulm, Institut für reine Mathematik, D-89069 Ulm
E-mail : irene.bouw@uni-ulm.de

Astérisque
312, 2007, p. 139–169

13. DEFORMATIONS OF ISOGENIES OF FORMAL GROUPS

by

Michael Rapoport

Abstract. — Let $(f_1, f_2, f_3) : E \to E'$ be a triple of isogenies between supersingular elliptic curves over $\overline{\mathbb{F}}_p$. We determine when the locus of deformation of (f_1, f_2, f_3) inside the universal deformation space of (E, E') is an Artin scheme, and in this case we give a formula for its length. These results are due to Gross and Keating.

***Résumé* (Déformations d'isogénies de groupes formels).** — Soit $(f_1, f_2, f_3) : E \to E'$ un triplet d'isogénies entre des courbes elliptiques supersingulières sur $\overline{\mathbb{F}}_p$. Nous donnons un critère pour le lieu de déformation de (f_1, f_2, f_3) dans l'espace de déformations universel de (E, E') d'être un schéma artinien, et nous donnons dans ce cas une formule pour sa longueur. Ces résultats sont dûs à Gross et Keating.

Let A and A' be abelian varieties of the same dimension n over $\overline{\mathbb{F}}_p$. The universal deformation space $\mathcal{M}$ of the pair A, A' is the formal spectrum of a power series ring in $2n^2$ variables over $W(\overline{\mathbb{F}}_p)$. Given an isogeny $f : A \to A'$ one may pose the problem of determining the maximal locus inside $\mathcal{M}$, where f can be deformed. More generally, given an r-tuple $f_1, \ldots, f_r$ of isogenies from A to A', one may ask for the maximal locus inside $\mathcal{M}$ where $f_1, \ldots, f_r$ deform. And, one may ask when this maximal locus is the spectrum of a local Artin ring, and if so, to give a formula for its length.

These questions are very difficult and it even seems likely that no systematic answers exist in general. In this chapter we consider the case $n = 1$, *i.e.*, when A and A' are elliptic curves. More precisely, we present the solution due to Gross and Keating [**GK**] to this problem when A and A' are supersingular elliptic curves. Their proof is a clever application of results on quasi-canonical liftings and their endomorphisms. Unfortunately, some parts of their proof are not so easy to implement in the case $p = 2$, which requires special attention. In fact, I only managed to deal with the case $p = 2$ by making use of the classification of quadratic forms over $\mathbb{Z}_2$, comp. [**B**], and

2000 ***Mathematics Subject Classification.*** — 11F32, 11G15, 14L05.
Key words and phrases. — Formal group, quasi-canonical lifting, Kummer congruence, Gross–Keating invariants.

using a case-by-case analysis. Fortunately, S. Wewers afterwards found a uniform argument for this part of the proof which makes use of deeper properties of anisotropic quadratic forms over $\mathbb{Z}_2$. This proof is presented in the next chapter. We decided to present both proofs because the more pedestrian approach here gives insight into the subtleties of the Gross-Keating invariants in the case $p = 2$.

Let us comment on the general problem above in another example, the case of *ordinary* elliptic curves, comp. [**Me2**]. The case when A and A' are ordinary elliptic curves has been known for a long time and is part of the Serre-Tate theory of canonical coordinates, comp. [**Mes**, Appendix]. Let A and A' be ordinary elliptic curves and fix isomorphisms

$$A[p^\infty]^{\mathrm{et}} \cong \mathbb{Q}_p/\mathbb{Z}_p,\ A'[p^\infty]^{\mathrm{et}} \cong \mathbb{Q}_p/\mathbb{Z}_p,$$

which then induce, via the canonical principal polarization, isomorphisms

$$A[p^\infty]^0 = \widehat{\mathbb{G}}_m,\ A'[p^\infty]^0 = \widehat{\mathbb{G}}_m.$$

The isogeny $f : A \to A'$ determines

$$(z_0, z_1) \in \mathbb{Z}_p^2$$

where f is given by multiplication by z_1 on the étale part and by multiplication by z_0 on the connected part of $A[p^\infty]$. On the other hand, we have

$$\mathcal{M} = \mathrm{Spf}\ W(\overline{\mathbb{F}}_p)[\![t, t']\!]$$

(Serre-Tate canonical coordinates). Then setting $q = 1+t$, $q' = 1+t'$, the locus inside $\mathcal{M}$ where f deforms is defined by the equation

$$q^{z_1} = q'^{z_0},$$

cf. [**Mes**, Appendix, 3.3], comp. also [**Me2**, Example 2.3]. On the other hand, it is easy to see that, for any r-tuple of isogenies $f_1, \dots, f_r : A \to A'$, the locus where $f_1, \dots, f_r$ deform is never of finite length, comp. [**Go2**, proof of Prop. 3.2]. These remarks show that already the case $n = 1$ in the above-mentioned general problem defies a uniform solution.

I wish to thank I. Bouw, U. Görtz, Ch. Kaiser, S. Kudla, S. Wewers and Th. Zink for their help in the preparation of this manuscript, and the referee for his remarks.

1. Statement of the result

Let E and E' be supersingular elliptic curves over $\bar{\mathbb{F}}_p$. Denoting by W the ring of Witt vectors of $\bar{\mathbb{F}}_p$, the ring

$$R = W[\![t, t']\!]$$

is the universal deformation ring of the pair E, E'. Let $\mathbb{E}, \mathbb{E}'$ be the universal deformation of E, E' over R. Let $f_1, f_2, f_3 : E \to E'$ be a triple of isogenies. The

locus inside Spf R to which f_1, f_2, f_3 deform is a closed formal subscheme. Let

$I =$ minimal ideal in R such that $f_1, f_2, f_3 \colon E \longrightarrow E'$ lift to isogenies $\mathbb{E} \longrightarrow \mathbb{E}'$ (mod I).

The problem in this chapter is: Determine

$$\alpha(f_1, f_2, f_3) = \lg_W R/I$$

(in particular, determine when this length is finite).

This problem reduces to a problem on formal groups, as follows. Let $\Gamma = \hat{\mathbb{E}}$ resp. $\Gamma' = \hat{\mathbb{E}}'$ be the formal group over R corresponding to $\mathbb{E}$ resp. $\mathbb{E}'$. By the Serre-Tate theorem we have

$I =$ minimal ideal in R such that $\hat{f}_1, \hat{f}_2, \hat{f}_3 \colon \hat{E} \longrightarrow \hat{E}'$ lift to isogenies $\Gamma \longrightarrow \Gamma'$ (mod I).

Now $\hat{E}$ and $\hat{E}'$ can both be identified with the formal group G of dimension 1 and height 2 over $\overline{\mathbb{F}}_p$ (which is unique up to isomorphism). In this way $\hat{f}_1, \hat{f}_2, \hat{f}_3$ become non-zero elements of $\mathrm{End}(G) = \mathcal{O}_D$. Here D denotes the quaternion division algebra over $\mathbb{Q}_p$.

On $\mathrm{Hom}(E, E')$ we have the quadratic form induced by the canonical principal polarization,

$$Q(f) = {}^t f \circ f = \deg f \quad .$$

This $\mathbb{Z}$-valued quadratic form is induced by the $\mathbb{Z}_p$-valued quadratic form

$$Q(x) = x \cdot {}^\iota x$$

under the inclusion $\mathrm{Hom}(E, E') \subset \mathrm{End}(G)$. Here $x \mapsto {}^\iota x$ denotes the main involution on D characterized by (reduced trace)

$$\mathrm{tr}(x) = x + {}^\iota x \quad .$$

We also write $Q(x) = \mathrm{Nm}(x)$ (reduced norm).

Let $L = \mathbb{Z}_p \hat{f}_1 + \mathbb{Z}_p \hat{f}_2 + \mathbb{Z}_p \hat{f}_3$ be the $\mathbb{Z}_p$-submodule of $\mathcal{O}_D$, with the quadratic form Q obtained by restriction. Then

$$I = \text{minimal ideal in } R \text{ such that } L \subset \mathrm{Hom}_{R/I}(\Gamma, \Gamma').$$

Assume that (L, Q) is non-degenerate, *i.e.*, L is of rank 3. Then to (L, Q) are associated integers $0 \leq a_1 \leq a_2 \leq a_3$, the Gross-Keating invariants. Recall ([**B**, section 2]) that if $p \neq 2$ these invariants are characterized by the fact that in a suitable basis e_1, e_2, e_3 of L the matrix $T = \frac{1}{2}((e_i, e_j))_{i,j}$ is equal to

$$T = \mathrm{diag}(u_1 p^{a_1}, u_2 p^{a_2}, u_3 p^{a_3}) \text{ with } u_1, u_2, u_3 \in \mathbb{Z}_p^\times. \tag{1.1}$$

Here $(x, y) = Q(x + y) - Q(x) - Q(y)$ is the bilinear form associated to the quadratic form Q.

Theorem 1.1. — *The length of R/I is finite if and only if (L,Q) is non-degenerate. In this case, $\lg_W R/I$ only depends on the Gross-Keating invariants (a_1,a_2,a_3) and equals $\alpha(Q)$ where*

$$\alpha(Q) = \sum_{i=0}^{a_1-1}(i+1)(a_1+a_2+a_3-3i)p^i + \sum_{i=a_1}^{(a_1+a_2-2)/2}(a_1+1)(2a_1+a_2+a_3-4i)p^i + \frac{a_1+1}{2}(a_3-a_2+1)p^{(a_1+a_2)/2}, \text{ if } a_1 \equiv a_2 \pmod 2$$

$$\alpha(Q) = \sum_{i=0}^{a_1-1}(i+1)(a_1+a_2+a_3-3i)p^i + \sum_{i=a_1}^{(a_1+a_2-1)/2}(a_1+1)(2a_1+a_2+a_3-4i)p^i, \text{ if } a_1 \not\equiv a_2 \pmod 2$$

Remark 1.2. — Recall from [**B**, Lemma 5.3] that, since (L,Q) is anisotropic, not all a_1,a_2,a_3 have the same parity. Hence the RHS of the formulas above is an integer in all cases.

Remark 1.3. — The formulas above imply that the length of R/I only depends on the isomorphism class of the quadratic module L. This can be seen in an *a priori* way as follows.

First of all, there is an action of $(D^\times)^2$ on the universal deformation ring R, given by changing the identification of the special fibers of Γ,Γ' with G,G by a pair of automorphisms of G. More precisely, an element $d \in D^\times$ defines a quasi-isogeny of G, as the composition $\mathrm{Frob}^{-v}\circ d$. Here Frob denotes the Frobenius endomorphism and $v = v(d)$ is the valuation of d. Since this is a quasi-isogeny of height 0, it is an automorphism of G. Note however, that this is only a semi-linear automorphism, and therefore also the induced automorphism by $(d_1,d_2) \in (D^\times)^2$ on R is only semi-linear.

It follows that for $(d_1,d_2) \in (D^\times)^2$ with $v(d_1) = v(d_2)$, the length of the deformation ring R/I for $L = \mathbb{Z}_p\hat{f}_1 + \mathbb{Z}_p\hat{f}_2 + \mathbb{Z}_p\hat{f}_3$ is equal to the length of the deformation ring R/I' for $L' = \mathbb{Z}_p\hat{f}'_1 + \mathbb{Z}_p\hat{f}'_2 + \mathbb{Z}_p\hat{f}'_3$, where $\hat{f}'_i = d_1\hat{f}_i d_2^{-1}$. Hence it suffices to show that for any two isometric ternary lattices L and L' in $\mathcal{O}_D$, there exists $(d_1,d_2) \in (D^\times)^2$ with $v(d_1) = v(d_2)$ and $L' = d_1 L d_2^{-1}$.

Fix a nondegenerate ternary form Q over $\mathbb{Z}_p$. We want to show that for any two isometries σ,σ' from Q to $\mathcal{O}_D$, there exists $(d_1,d_2) \in (D^\times)^2$ as above with $L' = d_1 L d_2^{-1}$, where L resp. L' denotes the image of σ, resp. σ'. By [**Wd1**, Lemma 1.6], we may identify $\mathrm{SO}(D,\mathrm{Nm})$ with the group

$$\{(d_1,d_2) \in (D^\times)^2 \mid \mathrm{Nm}(d_1) = \mathrm{Nm}(d_2)\}/\mathbb{Q}_p^\times.$$

By [**Wd2**, 1.3], the group $\mathrm{SO}(D,\mathrm{Nm})$ acts simply transitively on the set of isometries σ, hence there exists a unique $(d_1,d_2) \in \mathrm{SO}(D,\mathrm{Nm})$ with $\sigma' = d_1\sigma d_2^{-1}$. The pair (d_1,d_2) has the required properties.

To start the proof of Theorem 1.1, we first recall the following proposition.

Proposition 1.4. — *Let $\psi \in \mathrm{End}(G)$ be an isogeny,* i.e., *$\psi \neq 0$. Let J be the minimal ideal in $R = W[\![t, t']\!]$ such that ψ lifts to an isogeny $\Gamma \to \Gamma' \pmod J$. Then the closed formal subscheme $\mathcal{T}$ of $\mathcal{S} = \mathrm{Spf}\ R$ is a relative divisor over $\mathrm{Spf}\ W$. In other words, J is generated by an element which is neither a unit nor divisible by p.*

Proof. — This is the special case of [**Ww1**, Prop. 5.1], where (in the notation used there) $K = \mathbb{Q}_p$. A different proof that $\mathcal{T}$ is a divisor is (at least implicitly) contained in [**Z**, section 2.5]. □

Let us prove the first statement of Theorem 1.1. If (L, Q) is degenerate, then L is generated by two elements. Hence the deformation locus is by Proposition 1.4 the intersection of two divisors on a regular 3-dimensional formal scheme and therefore cannot be of finite length. Now assume that (L, Q) is non-degenerate. Now $\mathrm{Hom}(E, E') \otimes \mathbb{Z}_p = \mathrm{End}(G)$, so we find isogenies $f_1, f_2, f_3 : E \to E'$ with $\mathbb{Z}_p$-span equal to L. Let $T = \mathrm{Spec}\, W[\![t, t']\!]/J$. Then f_1, f_2, f_3 deform to isogenies from $\mathbb{E}_T$ to $\mathbb{E}'_T$. Hence at any point t of T we have $\mathrm{rg}\ \mathrm{Hom}(\mathbb{E}_t, \mathbb{E}'_t) > 2$, hence the elliptic curves $\mathbb{E}_t$ and $\mathbb{E}'_t$ are supersingular. Since supersingular points are isolated in the moduli scheme, it follows that T is an Artin scheme, as was to be shown.

From now on we assume that (L, Q) is non-degenerate. Let ψ_1, ψ_2, ψ_3 be an optimal basis of L. If $p \neq 2$, this means that the matrix of the bilinear form Q in terms of this basis is diagonal as in (1.1).

Corollary 1.5. — *Let $\mathcal{T}_i \subset \mathcal{S}$ be the locus, defined by the ideal I_i in R, where ψ_i lifts to an isogeny $\Gamma \to \Gamma' \pmod{I_i}$. Then*

$$\lg_W R/I = (\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{T}_3)_{\mathcal{S}} \quad .$$

Here on the RHS there appears the intersection product of divisors on a regular scheme, defined by the Samuel multiplicity or via the Koszul complex of the equations g_i of I_i,

$$\chi((g_1, g_2, g_3)) = \sum (-1)^i \lg(H_i(K_\bullet(g_1, g_2, g_3)))$$

(comp. [**F**, Ex. 7.1.2]).

Proof. — By our non-degeneracy assumption, the g_i form a regular sequence in a regular local ring. □

The corollary allows us to apply the intersection calculus of divisors on a regular scheme. In particular, the RHS is multilinear in all three entries.

Theorem 1.1 will be proved by induction on $a_1 + a_2 + a_3$. It will follow from the following three propositions.

Proposition 1.6. — *Let $a_3 \leq 1$. Then*

$$\alpha(Q) = \begin{cases} 1 & a_2 = 0 \\ 2 & a_2 = 1. \end{cases}$$

Hence Theorem 1.1 holds true in this case.

Proposition 1.7. — *Let $\psi_3 = p \cdot \psi_3'$ with $\psi_3' \in \mathrm{End}(G)$. Then*

$$(\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{T}_3)_{\mathcal{S}} = (\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{T}_3')_{\mathcal{S}} + (\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{S}_{(p)})_{\mathcal{S}} \quad .$$

Here $\mathcal{T}_i$ $(i = 1, 2, 3)$ resp. $\mathcal{T}_3'$ denotes the deformation locus for ψ_i resp. ψ_3' and $\mathcal{S}_{(p)} = \mathcal{S} \times_{\mathrm{Spf}\ W} \mathrm{Spf}\ \bar{\mathbb{F}}_p$ is the special fiber of $\mathcal{S}$.

Proposition 1.8. — *If $a_1 \equiv a_2 (\mathrm{mod}\ 2)$ then*

$$(\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{S}_{(p)})_{\mathcal{S}} = \sum_{i=0}^{a_1 - 1} 2(i+1)p^i + \sum_{i=a_1}^{(a_1+a_2-2)/2} 2(a_1+1)p^i + (a_1+1)p^{(a_1+a_2)/2} \quad .$$

If $a_1 \not\equiv a_2 (\mathrm{mod}\ 2)$ then

$$(\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{S}_{(p)})_{\mathcal{S}} = \sum_{i=0}^{a_1 - 1} 2(i+1)p^i + \sum_{i=a_1}^{(a_1+a_2-1)/2} 2(a_1+1)p^i \quad .$$

These propositions indeed imply Theorem 1.1. For this recall ([**B**, Cor. 5.8]) that we can (and do) choose ψ_3 such that $v(\psi_3) = a_3$. Here, as elsewhere, we denote by v the valuation function on D. Now, if $a_3 > 1$, then there exists $\psi_3' \in \mathrm{End}(G)$ with $\psi_3 = p\psi_3'$.

Lemma 1.9. — *Let (ψ_1, ψ_2, ψ_3) be an optimal basis of the lattice L. Let $\psi_3 = p\psi_3'$ with $\psi_3' \in L$ and denote by L' the lattice generated by ψ_1, ψ_2, ψ_3'. Then the invariants of L' are given in terms of the invariants (a_1, a_2, a_3) of L by*

$$(a_1, a_2, a_3 - 2)$$

(in some order so that they form a weakly increasing sequence).

This is obvious for $p \neq 2$ from the characterization in (1.1). For $p = 2$, the proof is given in the appendix, using the classification of quadratic forms over $\mathbb{Z}_2$. An alternative, more conceptual proof can be found in [**B**, Cor. 6.7].

Using this lemma, the above propositions give an inductive procedure for calculating $(\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{T}_3)_{\mathcal{S}}$. The formula in Theorem 1.1 follows from this calculation.

We now devote one section each to the proof of these three propositions. For Propositions 1.6 and 1.7 the case $p = 2$ presents additional problems. In order not to obscure the argument, the problems arising for $p = 2$ are relegated to the appendix to this chapter. In the chapter following this one, a variant of the proofs of Propositions 1.6 and 1.7 is given which avoids any case-by-case considerations.

2. The induction start: Proposition 1.5

Since not all a_i have the same parity, we have $a_1 = 0$. Hence ψ_1 is an automorphism of G. Since Γ' is a universal deformation of G, the ideal I_1 in $W[\![t, t']\!]$ defining the deformation locus of ψ_1 is of the form $I_1 = (t' - h(t))$, for some $h \in W[\![t]\!]$. For $I \supset I_1$,

it follows that ψ_i lifts to an isogeny $\Gamma \to \Gamma'$ (mod I) if and only if ${}^\iota\psi_1 \circ \psi_i$ lifts to an endomorphism of Γ (mod $I \cap W[\![t]\!]$). Let

$$\varphi_2 = {}^\iota\psi_1 \circ \psi_2 \ , \ \varphi_3 = {}^\iota\psi_1 \circ \psi_3 \ \text{ in } \ \mathrm{End}(G) \ .$$

We see that

$$\mathcal{T}_1 \cap \mathcal{T}_2 \cap \mathcal{T}_3 = \text{locus in Spf } W[\![t]\!] \text{ where } \varphi_2 \text{ and } \varphi_3 \text{ lift to endomorphisms of } \Gamma.$$

More precisely, for $i = 2$ or $i = 3$, let J_i be the minimal ideal in $W[\![t]\!]$ such that φ_i lifts to an endomorphism of Γ(mod J_i). Then $\mathcal{T}_1 \cap \mathcal{T}_2 \cap \mathcal{T}_3$ is isomorphic to the closed formal subscheme of Spf $W[\![t]\!]$ defined by $J_2 + J_3$.

Now let $p \neq 2$. Then we have from the definition of an optimal basis

$$\begin{aligned} {}^\iota\varphi_i &= -\varphi_i \text{ and } \mathrm{Nm}(\varphi_i) = u_1 u_i p^{a_i} \quad , \quad i = 2, 3 \ . \\ \varphi_2\varphi_3 &= -\varphi_3\varphi_2 \ . \end{aligned} \tag{2.1}$$

Let $K = \mathbb{Q}_p(\sqrt{-u_1u_2p^{a_2}})$. Since $a_2 \leq 1$, we deduce from (2.1) that φ_2 generates the ring of integers $\mathcal{O}_K$. Hence Γ(mod J_2) is the canonical lifting of G relative to the quadratic extension K of $\mathbb{Q}_p$, comp. [**Ww1**, Def. 3.1]. Applying the following lemma, we obtain

$$\varphi_3 \in \Pi^{a_3}\mathcal{O}_D \setminus (\mathcal{O}_K + \Pi^{a_3+1}\mathcal{O}_D) \ ,$$

with $a_3 = 1$. Now applying [**Ww1**, Thm. 1.4], or [**Vl**, Thm. 2.1], we have

$$\lg \ W[\![t]\!]/(J_2 + J_3) = \begin{cases} \frac{a_3+1}{2} = 1 & \text{if } a_2 = 0 \\ a_3 + 1 = 2 & \text{if } a_2 = 1. \end{cases} \quad \square$$

Remark 2.1. — The proof shows more generally Theorem 1.1 in the case where $p \neq 2$ and $a_1 = 0$: one appeals to [**Vl**, Thm. 2.1].

Lemma 2.2. — *We allow $p = 2$. Let K be a quadratic extension of $\mathbb{Q}_p$ contained in D, which is unramified or tamely ramified. Let $x \in \mathcal{O}_D$ which anticommutes with K,* i.e., *such that conjugation by x induces on K the non-trivial automorphism of K. Let $r = v(x)$. Then*

$$x \in \Pi^r\mathcal{O}_D \setminus (\mathcal{O}_K + \Pi^{r+1}\mathcal{O}_D) \ .$$

Here Π denotes a uniformizer of $\mathcal{O}_D$.

Proof. — We distinguish cases.

Case $K/\mathbb{Q}_p$ unramified. — In this case we can choose a uniformizer Π of $\mathcal{O}_D$ with $\Pi^2 = p$ and anticommuting with K. Then

$$\mathcal{O}_D = \mathcal{O}_K \oplus \mathcal{O}_K \cdot \Pi$$

where the first summand commutes with K, and the second summand anticommutes with K. Then

$$\mathcal{O}_K + \Pi^s\mathcal{O}_D = \mathcal{O}_K \oplus p^{\lceil \frac{s}{2} \rceil}\mathcal{O}_K \cdot \Pi \ .$$

Now if x anticommutes with K, then $r = v(x) = 2t+1$ is odd and $x \notin \mathcal{O}_K + \Pi^{r+1}\mathcal{O}_D = \mathcal{O}_K \oplus p^{t+1}\mathcal{O}_K \cdot \Pi$.

Case $K/\mathbb{Q}_p$ tamely ramified. — In this case we can write $\mathcal{O}_K = \mathbb{Z}_p[\pi]$ with $\pi^2 = u \cdot p$, for $u \in \mathbb{Z}_p^\times$. Then

$$\mathcal{O}_D = \mathcal{O}_K \oplus \mathcal{O}_K \cdot j \quad , \quad j^2 = u' \in \mathbb{Z}_p^\times \setminus \mathbb{Z}_p^{\times,2} \quad ,$$

where the first summand commutes with K and the second summand anticommutes with K. Then

$$\mathcal{O}_K + \Pi^s \mathcal{O}_D = \mathcal{O}_K \oplus \pi^s \mathcal{O}_K \cdot j \quad .$$

If x anticommutes with K, it lies in $\pi^r \mathcal{O}_K \cdot j$ but not in $\pi^{r+1}\mathcal{O}_K \cdot j$, hence $x \notin \mathcal{O}_K + \Pi^{r+1}\mathcal{O}_D = \mathcal{O}_K \oplus \pi^{r+1}\mathcal{O}_K \cdot j$. □

Remark 2.3. — In the case of wild ramification ($p = 2$) it can happen that x can be corrected by an element of $\mathcal{O}_K$ to have higher valuation than $r = v(x)$.

3. The induction step: Proposition 1.6.

It suffices to prove

$$(\mathcal{C} \cdot \mathcal{T}_3)_{\mathcal{S}} = (\mathcal{C} \cdot \mathcal{T}_3')_{\mathcal{S}} + (\mathcal{C} \cdot \mathcal{S}_{(p)})_{\mathcal{S}} \quad ,$$

for every irreducible component $\mathcal{C}$ of $\mathcal{T}_1 \cap \mathcal{T}_2$. Let

$J =$ minimal ideal in $W[\![t]\!]$ such that ${}^\iota\psi_1 \circ \psi_2$ lifts to an isogeny $\Gamma \longrightarrow \Gamma \pmod J$

$J' =$ minimal ideal in $W[\![t']\!]$ such that $\psi_2 \circ {}^\iota\psi_1$ lifts to an isogeny $\Gamma' \longrightarrow \Gamma' \pmod{J'}$.

We have an obvious inclusion

$$\mathcal{T}_1 \cap \mathcal{T}_2 \hookrightarrow \mathcal{X} \underset{\text{Df.}}{=} \operatorname{Spf} \ (W[\![t]\!]/J)\hat{\otimes}_W(W[\![t']\!]/J') \quad .$$

The proof of [**Ww1**, Prop. 5.1] shows that J is generated by one element. Now ${}^\iota\psi_1 \circ \psi_2$ is not scalar. Hence the generator of J is not divisible by p, because otherwise ${}^\iota\psi_1 \circ \psi_2$ would extend to the universal deformation of G over $\bar{\mathbb{F}}_p[\![t]\!]$, contradicting [**Vi**, Thm. 1.1]. The same argument applies to J' instead of J. Hence all irreducible components of $\mathcal{X}$ have dimension 1, and each irreducible component of $\mathcal{T}_1 \cap \mathcal{T}_2$ is also an irreducible component of $\mathcal{X}$. We now determine the irreducible components of $\mathcal{X}$.

The endomorphisms $\varphi = {}^\iota\psi_1 \circ \psi_2$ and $\varphi' = \psi_2 \circ {}^\iota\psi_1$ generate quadratic extensions $K = \mathbb{Q}_p(\varphi)$ resp. $K' = \mathbb{Q}_p(\varphi')$ which are conjugate inside D.

Lemma 3.1. — *The order $\mathbb{Z}_p[\varphi]$ in K has conductor $[(a_1 + a_2)/2]$.*

Proof for $p \neq 2$. — In this case the fact that the ψ_i form an optimal basis, *i.e.*, diagonalize the bilinear form as in (1.1), implies that

$$\operatorname{tr}(\varphi) = 0 \quad , \quad \varphi^2 = -u_1 u_2 p^{a_1+a_2} \quad .$$

Hence $\mathbb{Z}_p[\varphi] = \mathbb{Z}_p + p^r\mathcal{O}_K$, with $r = [(a_1 + a_2)/2]$. □

We therefore obtain an equality of divisors on Spf $W[\![t]\!]$,

$$\text{Spf } W[\![t]\!]/J = \sum_{s=0}^{[(a_1+a_2)/2]} \mathcal{W}_s(\varphi) \quad .$$

Here $\mathcal{W}_s(\varphi)$ is the quasicanonical locus of level s, with respect to the embedding of K in D defined by φ. Hence $\mathcal{W}_s(\varphi)$ is a reduced irreducible regular divisor such that the pullback of Γ to $\mathcal{W}_s(\varphi)$ has as its endomorphism algebra the order $\mathcal{O}_s = \mathbb{Z}_p + p^s\mathcal{O}_K$ of conductor[(1)] s in K. We may choose an identification

$$\mathcal{W}_s(\varphi) = \text{Spf } W_s \quad ,$$

where W_s is the ring of integers in the ray class field extension M_s of the completion M of the maximal unramified extension of K with norm group $\mathcal{O}_s^\times$.

Analogously we have

$$\text{Spf } W[\![t']\!]/J' = \sum_{s=0}^{[(a_1+a_2)/2]} \mathcal{W}_s(\varphi') \quad .$$

We apply the following simple observation.

Lemma 3.2. — *Let M be a discretely valued field. Let $M \subset K \subset L$ be finite field extensions such that $K \otimes_M L = L^{|K:M|}$ (*e.g. *K/M Galois). For each field embedding $\tau : K \to L$ with $\tau|M = \text{id}$, let Γ_τ be the graph of the corresponding morphism* $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$. *Then*

$$\operatorname{Spec} \mathcal{O}_K \otimes_{\mathcal{O}_M} \mathcal{O}_L = \bigcup_\tau \Gamma_\tau \quad .$$

Proof. — Obviously, the RHS is a closed subscheme of the LHS with identical generic fibers. But the LHS is flat over $\mathcal{O}_M$, hence is the closure of its generic fiber. □

Note that $W_r \subset W_s$ whenever $r \leq s$. The lemma implies that each irreducible component of $\mathcal{W}_r(\varphi) \cap \mathcal{W}_s(\varphi')$ is isomorphic to Spf W_m, where $m = \max\{r, s\}$. Hence each irreducible component of $\mathcal{T}_1 \cap \mathcal{T}_2$ is isomorphic to Spf W_s for some s with $0 \leq s \leq [(a_1 + a_2)/2]$.

Proposition 3.3. — *Let F_r, F_s be quasi-canonical liftings of G of level r, s (with respect to the quadratic extension K of $\mathbb{Q}_p$) defined over the ring of integers $\mathcal{O}$ of a finite extension of* Frac W. *Assume that ψ_1, ψ_2 lift to isogenies $F_r \to F_s$ over $\mathcal{O}$. Let I resp. I' be the minimal ideal in $\mathcal{O}$ such that $\psi_3 = p\psi_3'$, resp. ψ_3' lifts to an isogeny $F_r \to F_s(\bmod I)$ resp. $F_r \to F_s(\bmod I')$. Then $I = pI'$.*

(1) It is more traditional to attribute the conductor p^s to this order.

Proof. — Perhaps replacing the isogenies by their duals, we may assume $r \leq s$. First assume $r = s$. All quasi-canonical liftings of level r are conjugate under $\mathrm{Gal}(M_r/M)$. By [**Ww1**, Remark 3.3], there exists an isomorphism of the underlying formal groups

$$\gamma : F_s \longrightarrow F_r$$

such that

$$\varphi \circ \gamma = \gamma \circ \varphi' \quad .$$

However, γ is in general not an isomorphism of deformations of G, since γ conjugates the subfield $K = \mathbb{Q}_p(\varphi)$ of D into the subfield $K' = \mathbb{Q}_p(\varphi')$, hence γ may be a non-central element of D. Let

$$u = \mathrm{Nm}(\gamma) \in \mathbb{Z}_p^\times \quad . \tag{3.1}$$

We set

$$\varphi_i = \gamma \circ \psi_i \in \mathrm{End}(F_r) \quad , \quad i = 1, 2, 3 \quad .$$

Then

$$\varphi \circ \varphi_i = \varphi_i \circ \varphi \quad , \quad i = 1, 2 \quad . \qquad \square$$

Lemma 3.4. — *We have* $2r \leq a_2$ *and* $2r < a_3$.

Proof for $p \neq 2$. — Since F_r is a quasi-canonical lifting of level r, it suffices for the first statement to show that the conductor of one of the orders $\mathbb{Z}_p[\varphi_1]$ resp. $\mathbb{Z}_p[\varphi_2]$ is at most $a_2/2$. Now $v(\varphi_i) = a_i$. But φ_i is not traceless. Set

$$\varphi_i^0 = \varphi_i - \frac{1}{2}\,\mathrm{tr}(\varphi_i) \quad , \quad i = 1, 2 \quad .$$

Then φ_i^0 is traceless and hence the conductor of $\mathbb{Z}_p[\varphi_i] = \mathbb{Z}_p[\varphi_i^0]$ is equal to $[v(\varphi_i^0)/2]$. Hence it suffices to show

$$v(\varphi_i^0) \leq a_2 \text{ for } i = 1 \text{ or } i = 2 \quad . \tag{3.2}$$

We distinguish cases.

Case $K/\mathbb{Q}_p$ *unramified.* — Then a_1 and a_2 are even and

$$\varphi_i = \lambda_i p^{a_i/2} \quad , \quad \lambda_i \in \mathcal{O}_K^\times \quad , \quad i = 1, 2 \quad .$$

Then $\mathrm{tr}(\varphi_i) = (\lambda_i + {}^\iota\lambda_i)p^{a_i/2}$ and

$$\varphi_i^0 = \frac{1}{2}(\lambda_i - {}^\iota\lambda_i) \cdot p^{a_i/2} \quad .$$

Hence $v(\varphi_i^0) = a_i$ unless the residue class $[\lambda_i]$ of λ_i lies in $\mathbb{F}_p$. But since the ψ_i diagonalize the bilinear form, we have

$${}^\iota\varphi_1 \circ \varphi_2 = -{}^\iota\varphi_2 \circ \varphi_1 \quad . \tag{3.3}$$

Hence not both $[\lambda_1]$ and $[\lambda_2]$ can lie in $\mathbb{F}_p$ whence the claim (3.2). Now if $a_3 = 2r$, then $2r = a_2 = a_3$. Hence a_1 would have to be odd, which is impossible.

Case $K/\mathbb{Q}_p$ ramified. — Let $\pi \in \mathcal{O}_K$ be a uniformizer with ${}^\iota\pi = -\pi$. Let

$$\varphi_i = \lambda_i \pi^{a_i} \quad , \quad \lambda_i \in \mathcal{O}_K^\times \quad , \quad i = 1, 2 \quad .$$

Then

$$\varphi_i^0 = \frac{1}{2}(\lambda_i - (-1)^{a_i} \cdot {}^\iota\lambda_i) \cdot \pi^{a_i} \quad .$$

Hence $v(\varphi_i^0) = a_i$ if a_i is odd. Now the identity (3.3) implies

$$(-1)^{a_1} \cdot {}^\iota\lambda_1 \lambda_2 = -(-1)^{a_2} \cdot \lambda_1 {}^\iota\lambda_2 \quad .$$

Hence a_1 and a_2 have to have different parities which shows (3.2) in this case. Now if $a_3 = 2r$, then $a_1 < 2r$ would have to be odd which contradicts $2r \leq v(\varphi_1^0) = a_1$. □

Lemma 3.5. — *We have $\varphi_3 \in \Pi^{a_3}\mathcal{O}_D \setminus (\mathcal{O}_K + \Pi^{a_3+1}\mathcal{O}_D)$.*

Proof for $p \neq 2$. — Again using that the ψ_i diagonalize the bilinear form, we have

$$\varphi_3 \varphi = {}^\iota\varphi \varphi_3 \quad .$$

Since $v(\varphi_3) = a_3$, an application of Lemma 2.2 gives the result. □

We now apply [**Vl**, Thm. 2.1]. Since $a_3 \geq 2r - 1$, we are in the "stable range" of that result. Hence I is the n-th power of the maximal ideal of $\mathcal{O}$, where

$$n = 2 \cdot \frac{p^r - 1}{p - 1} \cdot |\mathcal{O} : W_r| + \left(\frac{a_3 + 1}{2} - r \right) \cdot |\mathcal{O} : W| \quad . \tag{3.4}$$

Now $v(\varphi_3') = a_3 - 2$. Since $a_3 - 2 \geq 2r - 1$, we are again in the stable range and the ideal I' is the n'-th power of the maximal ideal of $\mathcal{O}$, where n' is given by (3.4) with a_3 replaced by $a_3 - 2$. Hence $n - n' = |\mathcal{O} : W|$. This proves the proposition in the case $r = s$.

To prove the general case, we use the following lemma. For the proof we refer to [**Ww1**, Cor. 5.3]. Note that the element π_1 appearing in the statement below has the same valuation as a uniformizer of W_{s+1}, by [**Ww1**, Cor. 4.8].

Lemma 3.6. — *Let $r \leq s$ and let F_r, F_s and F_{s+1} be quasi-canonical liftings of level r, s, and $s+1$, all defined over $\mathcal{O}$. Let $\pi : F_s \to F_{s+1}$ be an isogeny of degree p defined over $\mathcal{O}$ and write π in terms of a formal parameter*

$$\pi(X) = \pi_1 X + \pi_2 X^2 + \ldots \quad , \quad \pi_i \in \mathcal{O} \quad .$$

Let $\psi \in \mathrm{End}(G) \setminus \{0\}$ and let $I(r, s)$ be the minimal ideal in $\mathcal{O}$, such that ψ lifts to an isogeny $F_r \to F_s \pmod{I(r, s)}$. Let $I(r, s+1)$ be the minimal ideal in $\mathcal{O}$, such that $\pi \circ \psi$ lifts to an isogeny $F_r \to F_{s+1} \pmod{I(r, s+1)}$. Then

$$I(r, s+1) = \pi_1 I(r, s) \quad .$$

□

The lemma shows that if the assertion of Proposition 3.3 holds for $\psi_1, \psi_2, \psi_3, \psi_3' : F_r \to F_s$, it holds for $\pi \circ \psi_1, \pi \circ \psi_2, \pi \circ \psi_3, \pi \circ \psi_3' : F_r \to F_{s+1}$ as well (note that (ψ_1, ψ_2, ψ_3) is an optimal basis of their $\mathbb{Z}_p$-span if and only if $(\pi \circ \psi_1, \pi \circ \psi_2, \pi \circ \psi_3)$ is an optimal basis of their $\mathbb{Z}_p$-span). We note the following lemma.

Lemma 3.7. — *Let $r \leq s$ and let F_r, F_{s+1} be quasi-canonical liftings of level $r, s+1$ defined over $\mathcal{O}$. Then all isogenies $\psi : F_r \to F_{s+1}$ factor through an isogeny $F_s \to F_{s+1}$ of degree p, where F_s is a quasi-canonical lifting of level s.*

Proof. — This follows from the proof of Prop. 1.1 in [**Ww2**]. After choosing suitable isogenies from the canonical lifting to F_r and to F_{s+1}, we may assume that the Tate modules of F_r and F_{s+1} are of the form

$$T_r = (\mathbb{Z}_p \cdot p^{-r} + \mathcal{O}_K) \cdot t, \quad T_{s+1} = (\mathbb{Z}_p \cdot p^{-(s+1)} + \mathcal{O}_K) \cdot t.$$

Let F_s be defined by $T_s = (\mathbb{Z}_p \cdot p^{-s} + \mathcal{O}_K) \cdot t$. Then (loc. cit.),

$$\begin{aligned} \mathrm{Hom}(F_r, F_{s+1}) &= \{\ \alpha \in \mathcal{O}_K \mid \alpha T_r \subset T_{s+1}\} \\ &= \{\ \alpha \in \mathcal{O}_K \mid \alpha T_r \subset T_r\ \} \\ &= \{\ \alpha \in \mathcal{O}_K \mid \alpha T_r \subset T_s\ \}\ . \end{aligned}$$

Therefore all isogenies $F_r \to F_{s+1}$ factor through $F_r \to F_s$. □

Using the previous two lemmas we now prove Proposition 3.3 by induction on the difference $s - r$. Indeed, the induction step from (r, s) to $(r, s+1)$ is obvious, except in the case [(2)] when the result $\tilde{\psi}_3 : F_r \longrightarrow F_s$ of dividing $\psi_3 : F_r \longrightarrow F_{s+1}$ by π is not of the form $\tilde{\psi}_3 = p\tilde{\psi}_3'$, for a suitable $\tilde{\psi}_3' : F_r \longrightarrow F_s$. However, in this case we have $a_3 = v(\psi_3) = 2$ and hence $r = s = 0$ and $v(\psi_3') = 0$. In this case the ideal I' describes the locus where the quasi-canonical lifting F_1 is isomorphic to the canonical lifting F_0. By [**Ww1**, Cor. 4.7], the ideal I' is equal to the n-th power of the maximal ideal of $\mathcal{O}$, where $n = e/e_1$ with e the absolute ramification index of $\mathcal{O}$, and e_1 the absolute ramification index of W_1. By [**Vl**, Thm. 2.1], the ideal $I(0,0)$ is equal to the e-th power of the maximal ideal of $\mathcal{O}$. On the other hand, the element π_1 occurring in Lemma 3.5 has valuation e/e_1 in $\mathcal{O}$, cf. [**Ww1**, Cor. 4.8]. Hence $I(0,1) = pI'$, as required.

4. Intersection with $\mathcal{S}_{(p)}$: Proposition 1.7.

For the proof of Proposition 1.8 we will make use of the Kummer congruence ([**KM**, 13.4.6]). We first recall the statement.

(2) I thank S. Wewers for pointing out this possibility, which I had overlooked.

We denote by $\mathcal{M}$ the moduli stack of elliptic curves over Spec $\mathbb{F}_p$. For integers a, b with $a \geq 0$, $b \geq 0$ and $a + b = n$, we form the fiber product stack $\mathcal{M}_{a,b}$,

$$\begin{array}{ccc} \mathcal{M} \times \mathcal{M} & \longrightarrow & \mathcal{M} \times \mathcal{M} \\ \uparrow & & \uparrow \Delta \\ \mathcal{M}_{a,b} & \longrightarrow & \mathcal{M} \end{array}$$

Here Δ denotes the diagonal morphism and the upper horizontal morphism sends (E, E') to $(E^{(p^a)}, E'^{(p^b)})$. Here we denoted by $E^{(p^a)}$ the pullback of E under the a^{th} power of the Frobenius morphism. Then $\mathcal{M}_{a,b}$ classifies pairs (E, E') with an isomorphism $\alpha : E^{(p^a)} \xrightarrow{\sim} E'^{(p^b)}$.

We consider the moduli stack $\mathcal{M}_{(p^n)}$ over Spec $\mathbb{F}_p$ classifying isogenies $E \to E'$ of degree p^n (in [**Go2**], this stack is denoted by $\mathcal{T}_{p^n, \mathbb{F}_p}$). We obtain a morphism

$$\varphi_{a,b} : \mathcal{M}_{a,b} \longrightarrow \mathcal{M}_{(p^n)} \quad .$$

It sends (E, E', α) to the composition isogeny

$$E \xrightarrow{F^a} E^{(p^a)} \underset{\alpha}{\xrightarrow{\sim}} E'^{(p^b)} \xrightarrow{{}^tF^b} E' \quad .$$

Letting a, b vary we obtain a morphism

$$\varphi : \coprod_{\substack{a+b=n \\ a \geq 0, b \geq 0}} \mathcal{M}_{a,b} \longrightarrow \mathcal{M}_{(p^n)} \quad .$$

Theorem 4.1 **([KM**, 13.4.6]). —** *The morphism φ is an isomorphism outside the supersingular locus. The inverse image of a supersingular geometric point $x \in \mathcal{M}(\bar{\mathbb{F}}_p)$ in $\mathcal{M}_{(p^n)}(\bar{\mathbb{F}}_p)$ consists of precisely one point $\tilde{x}$ and the completed local ring of $\tilde{x}$ is isomorphic to*

$$\bar{\mathbb{F}}_p[\![X, Y]\!] \ / \prod_{\substack{a+b=n \\ a \geq 0, b \geq 0}} (X^{p^a} - Y^{p^b})$$

in such a way that $\mathcal{M}_{a,b}$ is defined by the equation $X^{p^a} - Y^{p^b} = 0$. □

Recall the ideal I_i in $W[\![t]\!]$ defining the divisors $\mathcal{T}_i$, for $i = 1, 2$. By the Kummer congruence there exist for $i = 1$ and 2 uniformizers t_i of $\bar{\mathbb{F}}_p[\![t]\!]$ and t'_i of $\bar{\mathbb{F}}_p[\![t']\!]$ and generators g_i of I_i such that

$$g_i \equiv (t_i - (t'_i)^{p^{a_i}}) \cdot (t_i^p - (t'_i)^{p^{a_i - 1}}) \cdot \ldots \cdot (t_i^{p^{a_i}} - t'_i) \pmod{p} \quad .$$

Hence $\mathcal{T}_i \cap \mathcal{S}_{(p)}$ is the union of irreducible components $\mathcal{V}_{i\mu}$ $(\mu = 0, 1, \ldots, a_i)$, where $\mathcal{V}_{i\mu}$ is the divisor in $\mathcal{S}_{(p)} = \text{Spf } \bar{\mathbb{F}}_p[\![t, t']\!]$ defined by $t_i^{p^\mu} - (t'_i)^{p^{a_i - \mu}}$. Hence

$$(\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{S}_{(p)})_{\mathcal{S}} = \sum_{\mu=0}^{a_1} \sum_{\nu=0}^{a_2} (\mathcal{V}_{1\mu} \cdot \mathcal{V}_{2\nu})_{\mathcal{S}} \quad . \tag{4.1}$$

We write

$$t_2 = u \cdot t_1 \quad , \quad u \in \bar{\mathbb{F}}_p[\![t]\!]^\times$$
$$t'_2 = u' \cdot t'_1 \quad , \quad u' \in \bar{\mathbb{F}}_p[\![t']\!]^\times \quad .$$

Lemma 4.2. — *Let* $a_1 \equiv a_2 (\mathrm{mod}\ 2)$. *Then* $u(0), u'(0) \in \mathbb{F}_{p^2}$ *and* $u(0) \neq u'(0)^{p^{a_2}}$.

Lemma 4.3. — *We have*

$$(\mathcal{V}_{1\mu} \cdot \mathcal{V}_{2\nu}) = p^n \quad ,$$

with $n = \min\{a_1 - \mu + \nu, a_2 - \nu + \mu\}$.

It is an elementary matter to use Lemma 4.3 to calculate the sum on the RHS of (4.1). The result is Proposition 1.8.

Proof of Lemma 4.3 (assuming Lemma 4.2). — We must show

$$\lg\ \bar{\mathbb{F}}_p[\![t,t']\!]/(t^{p^\mu} - (t')^{p^{a_1-\mu}}, (ut)^{p^\nu} - (u' \cdot t')^{p^{a_2-\nu}}) = p^n \quad . \tag{4.2}$$

By symmetry it suffices to consider the following two cases.
Case 1: $\mu \leq a_1 - \mu$, $\nu \leq a_2 - \nu$
Case 2: $\mu \leq a_1 - \mu$, $a_2 - \nu \leq \nu$.

In case 1 the LHS of (4.2) is equal to

$$\lg\ \bar{\mathbb{F}}_p[\![t,t']\!]/(t - t'^{p^{a_1-2\mu}})^{p^\mu}, (ut - (u't')^{p^{a_2-2\nu}})^{p^\nu} \overset{(1)}{=}$$
$$p^{\mu+\nu} \cdot \lg\ \bar{\mathbb{F}}_p[\![t']\!]/(u \cdot t'^{p^{a_1-2\mu}} - (u't')^{p^{a_2-2\nu}}) \overset{(2)}{=} p^{\mu+\nu+\min\{a_1-2\mu, a_2-2\nu\}} = p^n.$$

Here in (1) we used the formula ([**Go2**, Lemma 4.2])

$$\lg_A B/x_1 \dots x_n = \sum_i \lg_A B/x_i \quad ,$$

valid for any A-algebra B and non zero divisors $x_1, \dots, x_n$ in B. In (2) we used Lemma 4.2 which implies that if $a_1 - 2\mu = a_2 - 2\nu$, then $u(0) \neq u'(0)^{p^{a_2-2\nu}} = u'(0)^{p^{a_2}}$.

In case 2, the LHS of (4.2) is equal to

$$\lg\ \bar{\mathbb{F}}_p[\![t,t']\!]/((t - t'^{p^{a_1-2\mu}})^{p^\mu}, (u't' - (ut)^{p^{2\nu-a_2}})^{p^{a_2-\nu}}) =$$
$$p^\mu \cdot p^{a_2-\nu} \cdot \lg\ \mathbb{F}_p[\![t,t']\!]/(t - t'^{p^{a_1-2\mu}}, u't' - (ut)^{p^{2\nu-a_2}}) =$$
$$p^{a_2-\nu+\mu} \cdot \lg\ \bar{\mathbb{F}}_p[\![t']\!]/(u't' - u^{p^{2\nu-a_2}} \cdot t'^{p^{a_1-2\mu+2\nu-a_2}}) \overset{(3)}{=} p^{a_2-\nu+\mu} = p^n.$$

Here in (3) we used Lemma 4.2: if $a_1 - 2\mu + 2\nu - a_2 = 0$, then $a_1 = 2\mu$ and $a_2 = 2\nu$ are both even and $u'(0) \neq u(0)^{p^{2\nu-a_2}} = u(0)$. □

Proof of Lemma 4.2. — Let $\ell = (a_2 - a_1)/2$. Let

$$I_1' = \text{minimal ideal in } W[\![t,t']\!] \text{ such that } p^\ell \psi_1 \text{ lifts to an isogeny } \Gamma \longrightarrow \Gamma' (\text{mod } I_1').$$

By the Kummer congruence we can choose uniformizers t_1 of $\bar{\mathbb{F}}_p[\![t]\!]$ and t_1' of $\bar{\mathbb{F}}_p[\![t']\!]$ and a generator g_1' of I_1' with

$$g_1' \equiv (t_1 - t_1'^{p^{a_2}}) \cdot (t_1^p - t_1'^{p^{a_2-1}}) \cdot \ldots \cdot (t_1^{p^{a_2}} - t_1') (\text{mod } p) \quad .$$

Now $\psi_2 = \alpha \circ (p^\ell \psi_1)$, where $\alpha \in \text{Aut}(G)$. By the universal property of Γ there exists a unique W-algebra homomorphism $h : W[\![t]\!] \to W[\![t]\!]$ such that α lifts to an isomorphism

$$\tilde{\alpha} : \Gamma \longrightarrow h_*(\Gamma) \quad .$$

Hence I_2 is generated by g_2' with

$$g_2' \equiv (h(t_1) - t_1'^{p^{a_2}}) \cdot (h(t_1)^p - t_1'^{p^{a_2-1}}) \cdot \ldots \cdot (h(t_1)^{p^{a_2}} - t_1') (\text{mod } p) \quad . \tag{4.3}$$

The two elements g_2' and g_2 differ by a unit and

$$g_2 \equiv (ut_1 - (u't_1')^{p^{a_2}}) \cdot ((u \cdot t_1)^p - (u't_1')^{p^{a_2-1}}) \cdot \ldots \cdot ((ut_1)^{p^{a_2}} - u't_1') (\text{mod } p) \quad . \tag{4.4}$$

The first factor on the RHS of (4.4) is irreducible and can only divide the first factor of the RHS of (4.3). Hence the first factors differ by a unit. Let

$$h(t_1) \equiv v \cdot t_1 \ (\text{mod } p) \ \text{ with } \ v \in \bar{\mathbb{F}}_p[\![t_1]\!]^\times \quad , \tag{4.5}$$

and put $c = v(0)$. Comparing coefficients we obtain

$$c = u(0)/u'(0)^{p^{a_2}} \quad .$$

The remaining factors on the RHS of (4.4) are not irreducible: $(ut_1)^{p^\mu} - (u't_1')^{p^{a_2-\mu}}$ is the p^ν-th power of an irreducible element, where $\nu = \min\{\mu, a_2 - \mu\}$. An analogous comparison of coefficients gives

$$c = u(0)/u'(0)^{p^{a_2-2\mu}} \quad , \quad \mu = 0, \ldots, a_2 \quad .$$

It follows that $u'(0) \in \mathbb{F}_{p^2}$ and by symmetry $u(0) \in \mathbb{F}_{p^2}$. It remains to show $c \neq 1$. Now c is the induced action of α on the tangent space of the universal deformation of G over $\bar{\mathbb{F}}_p$. And α is given in terms of the formal group law by

$$\alpha(X) = \alpha_1 X + \alpha_2 X^2 + \ldots \quad , \quad \alpha_i \in \bar{\mathbb{F}}_p \quad .$$

Then $\alpha_1 \in \mathbb{F}_{p^2} = \mathcal{O}_D/\Pi\mathcal{O}_D$ is the residue class of α. By the lemma below, the action of α on the tangent space of the universal deformation space is by multiplication by $\alpha_1/\bar{\alpha}_1$. Hence $c = \alpha_1/\bar{\alpha}_1$. But $\alpha_1 \notin \mathbb{F}_p$ and hence $c \neq 1$. Indeed, otherwise for any $a \in \mathbb{Z}_p$ with residue class α_1 modulo p, we would have

$$v(\psi_2 - ap^\ell \psi_1) > v(\psi_2) \quad . \tag{4.6}$$

But the optimal basis ψ_1, ψ_2, ψ_3 may be chosen so that ψ_2 has *maximal* valuation in its residue class modulo $\mathbb{Z}_p \psi_1$. Indeed, if $p \neq 2$, any optimal basis has this property (otherwise an easy application of Hensel's lemma would imply that L is isotropic).

If $p = 2$, we take the optimal basis constructed in table 1 of the appendix. By assumption $a_1 \equiv a_2 (\mathrm{mod}\ 2)$. Going through all cases in table 1, we see that this can only happen in cases A2 and B3 a). In the case A2, we have $v(\psi_1) > v(\psi_2)$ which contradicts (4.6). In the case B3 a), we get

$$(\psi_2 - ap^\ell \psi_1, \psi_2 - ap^\ell \psi_1) = 2^{\beta_2}\ (u_1 + u_2 + 4\ (a^2 - a)\ u_1),$$

which has valuation $a_2 = v(\psi_2) = \beta_2 + 2$, since in this case $u_1 + u_2 \equiv 4 (\mathrm{mod}\ 8)$. □

Remark 4.4. — In fact, even for $p = 2$, it is true that *any* optimal basis has the property that ψ_2 has maximal valuation in its residue class modulo $\mathbb{Z}_p \psi_1$. This follows from [**B**, Prop. 6.9].

Lemma 4.5. — *Let $\alpha \in \mathcal{O}_D^\times = \mathrm{Aut}(G)$, with action on* Lie G *given by (multiplication by) $\alpha_1 \in \mathbb{F}_{p^2}$. The induced action of α on the tangent space of the universal deformation space of G over $\bar{\mathbb{F}}_p$ is by multiplication by $\alpha_1/\bar{\alpha}_1$.*

Here we denote by $x \mapsto \bar{x}$ the non-trivial automorphism of $\mathbb{F}_{p^2}$.

Proof (comp. [**Z**, Lemma 78]*).* — The tangent space can be canonically identified with

$$\mathrm{Hom}(\mathrm{Lie}\ {}^tG,\ \mathrm{Lie}\ G)\quad .$$

For $\varphi \in \mathrm{Hom}(\mathrm{Lie}\ {}^tG,\ \mathrm{Lie}\ G)$ we have

$$\alpha_*(\varphi) = \alpha_1 \circ \varphi \circ {}^t\alpha_1^{-1}\quad .$$

Identifying ${}^tG$ with G replaces ${}^t\alpha_1$ by the residue class of ${}^\iota\alpha$, *i.e.*, by $\bar{\alpha}_1$. □

A. Appendix: The case $p = 2$

In sections 2 and 3 we made the assumption $p > 2$. In this appendix we treat the case $p = 2$. In this case one has to take into account the delicate theory of quadratic forms over $\mathbb{Z}_2$. We will proceed according to the following table. The table gives

- the normal form of the quadratic space (L, Q) in terms of a suitable basis e_1, e_2, e_3 (we give the matrix $T = (\frac{1}{2}(e_i, e_j))$),
- an optimal basis ψ_1, ψ_2, ψ_3,
- the Gross-Keating invariants (a_1, a_2, a_3) of (L, Q).

We go through all cases of *anisotropic* ternary lattices, according to the table in [**Y1**, appendix B], comp. also [**B**, Thm. 5.7].

Table 1

A) $T = \operatorname{diag}\left(u_1 2^\alpha, 2^\beta \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)\right)$, $\alpha \geq 0, \beta \geq -1$, $\alpha \equiv \beta \bmod 2$
(the condition $\alpha \equiv \beta \bmod 2$ is due to the anisotropy of T, comp. [**B**, section 5]).

1) $\alpha \leq \beta + 1$. Then $\psi_1 = e_1, \psi_2 = e_2, \psi_3 = e_3$ and

$$GK(T) = (\alpha, \beta + 1, \beta + 1)$$

2) $\alpha > \beta + 1$. Then $\psi_1 = e_2, \psi_2 = e_3, \psi_3 = e_1$ and

$$GK(T) = (\beta + 1, \beta + 1, \alpha)$$

B) $T = \operatorname{diag}(u_1 2^{\beta_1}, u_2 2^{\beta_2}, u_3 2^{\beta_3})$ with $0 \leq \beta_1 \leq \beta_2 \leq \beta_3$
This matrix is anisotropic if and only if

$$(-1, u_2 u_3) = (u_1 u_2, u_1 u_3) \cdot (2, u_1 u_2)^{\beta_1 + \beta_3} \cdot (2, u_1 u_3)^{\beta_1 + \beta_2} \quad ,$$

cf. [**Y2**], or [**B**, section 5].

1) $\beta_2 \not\equiv \beta_1 \bmod 2$. Then $\psi_1 = e_1, \psi_2 = e_2, \psi_3 = c_1 e_1 + c_2 e_2 + e_3$ for suitable $c_1, c_2 \in \mathbb{Z}_2$, and

$$GK(T) = (\beta_1, \beta_2, \beta_3 + 2)$$

2) $\beta_2 \equiv \beta_1 \bmod 2$ and $\beta_3 \leq \beta_2 + 1$.

a) $\beta_3 = \beta_2$. Then $\psi_1 = e_1, \psi_2 = 2^{\frac{\beta_2 - \beta_1}{2}} \cdot e_1 + e_2, \psi_3 = 2^{\frac{\beta_2 - \beta_1}{2}} \cdot e_1 + e_3$ and

$$GK(T) = (\beta_1, \beta_2 + 1, \beta_3 + 1)$$

b) $\beta_3 = \beta_2 + 1$ and $u_1 \equiv u_2 \bmod 4$. Then $\psi_1 = e_1, \psi_2 = 2^{\frac{\beta_2 - \beta_1}{2}} \cdot e_1 + e_2$, $\psi_3 = 2^{\frac{\beta_2 - \beta_1}{2}} \cdot e_1 + e_2 + e_3$ and

$$GK(T) = (\beta_1, \beta_2 + 1, \beta_3 + 1)$$

c) $\beta_3 = \beta_2 + 1$ and $u_1 \equiv -u_2 \bmod 4$. Then $\psi_1 = e_1$, $\psi_2 = 2^{\frac{\beta_2 - \beta_1}{2}} \cdot e_1 + e_2 + e_3$, $\psi_3 = 2^{\frac{\beta_2 - \beta_1}{2}} \cdot e_1 + e_2 + 2e_3$ and

$$GK(T) = (\beta_1, \beta_2 + 1, \beta_3 + 1)$$

3) $\beta_2 \equiv \beta_1 \bmod 2$ and $\beta_3 \geq \beta_2 + 2$.

a) $u_1 \equiv -u_2 \bmod 4$. Then $\psi_1 = e_1$, $\psi_2 = 2^{\frac{\beta_2 - \beta_1}{2}} \cdot e_1 + e_2$, $\psi_3 = e_3$ and

$$GK(T) = (\beta_1, \beta_2 + 2, \beta_3)$$

b) $u_1 \equiv u_2 \bmod 4$. Then $\psi_1 = e_1, \psi_2 = 2^{\frac{\beta_2 - \beta_1}{2}} \cdot e_1 + e_2, \psi_3 c_1 e_1 + c_2 e_2 + e_3$ for suitable $c_1, c_2 \in \mathbb{Z}_2$, and

$$GK(T) = (\beta_1, \beta_2 + 1, \beta_3 + 1) \quad .$$

A.1. The induction start. — Let $a_3 \leq 1$, *i.e.*, $a_1 = 0$ and $a_3 = 1$. We follow the proof of Proposition 1.6 in each of the following cases.

- $$T = \mathrm{diag}\left(u_1 2, 2^{-1}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\right), \quad \text{hence } GK(T) = (0,0,1) \quad .$$

Then $\varphi_2 = {}^\iota\psi_1 \circ \psi_2 = {}^\iota e_2 \circ e_3$ and

$$\mathrm{tr}(\varphi_2) = (e_2, e_3) = 1 \quad \text{and} \quad \mathrm{Nm}(\varphi_2) = 1 \quad .$$

Hence $K = \mathbb{Q}_2(\varphi_2) = \mathbb{Q}_2[X]/(X^2 - X + 1)$ is an unramified extension of $\mathbb{Q}_2$, and $\mathcal{O}_K = \mathbb{Z}_2[\varphi_2]$. Therefore $\Gamma(\mathrm{mod}\ J_2)$ is a canonical lifting relative to K.

Now $\varphi_3 = {}^\iota\psi_1 \circ \psi_3 = {}^\iota e_2 \circ e_1$ and

$$\mathrm{tr}(\varphi_3) = 0 \quad \text{and} \quad \mathrm{Nm}(\varphi_3) = u_1 \cdot 2 \quad .$$

Furthermore

$$\mathrm{tr}(\varphi_2 \circ {}^\iota\varphi_3) = \mathrm{tr}({}^\iota e_3 \circ e_2 \circ {}^\iota e_2 \circ e_1) = Q(e_2) \cdot \mathrm{tr}({}^\iota e_3 \circ e_1) = (e_1, e_3) = 0 \quad .$$

Hence $-\varphi_2 \circ \varphi_3 + \varphi_3 \circ {}^\iota\varphi_2 = 0$, *i.e.*, φ_3 anticommutes with K. Since $K/\mathbb{Q}_2$ is unramified, an application of Lemma 2.2 gives

$$\varphi_3 \in \Pi\mathcal{O}_D \setminus (\mathcal{O}_K + \Pi^2\mathcal{O}_D) \quad .$$

Hence, applying [**Ww1**, Thm. 1.4],

$$\lg\ W[\![t]\!]/(J_2 + J_3) = \frac{1+1}{2} = 1 = \frac{a_3 + 1}{2} \quad ,$$

which proves the claim in this case.

- $$T = \mathrm{diag}\left(u_1, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\right) \quad , \quad \text{hence } GK = (0,1,1) \quad .$$

Then $\varphi_2 = {}^\iota\psi_1 \circ \psi_2 = {}^\iota e_1 \circ e_2$ and

$$\mathrm{tr}(\varphi_2) = (e_1, e_2) = 0 \quad \text{and} \quad \mathrm{Nm}(\varphi_2) = u_1 \cdot 2 \quad .$$

Hence $K = \mathbb{Q}_2(\varphi_2) = \mathbb{Q}_2[X]/(X^2 + u_1 2)$ is a ramified extension of $\mathbb{Q}_2$, and $\mathcal{O}_K = \mathbb{Z}_2[\varphi_2]$. Therefore $\Gamma(\mathrm{mod}\ J_2)$ is a canonical lifting relative to K.

Now $\varphi_3 = {}^\iota\psi_1 \circ \psi_3 = {}^\iota e_1 \circ e_3$ and

$$\mathrm{tr}(\varphi_3) = 0 \quad \text{and} \quad \mathrm{Nm}(\varphi_3) = u_1 \cdot 2 \quad .$$

Furthermore

$$\mathrm{tr}(\varphi_2 \circ {}^\iota\varphi_3) = \mathrm{tr}({}^\iota e_2 \circ e_1 \circ {}^\iota e_1 \circ e_3) = u_1 \cdot (e_2, e_3) = u_1 \cdot 2 \quad .$$

Hence

$$\varphi_2 \circ \varphi_3 + \varphi_3 \circ \varphi_2 = -u_1 \cdot 2 \quad . \tag{A.1.1}$$

We use the presentation of D resp. $\mathcal{O}_D$ from [**G**, Prop. 4.3]. Namely, assume that the different $\mathcal{D}$ of $K/\mathbb{Q}_2$ has valuation equal to e. Then

$$D = K \oplus K \cdot j \quad , \tag{A.1.2}$$

where j anticommutes with K and where $j^2 \in \mathbb{Z}_2^\times$ satisfies $v(j^2-1) = 2(e-1)$. Let π be a uniformizer in K. Then $\alpha := \pi^{-2}(1+j) \in \mathcal{O}_D^\times$ and

$$\mathcal{O}_D = \mathcal{O}_K \oplus \mathcal{O}_K \cdot \alpha \quad . \tag{A.1.3}$$

In the case at hand the extension $K/\mathbb{Q}_2$ is wildly ramified, with different $\mathcal{D}$ of valuation $e = 3$. Hence $v(j^2-1) = 4$. As uniformizer π we take φ_2.

Write $\varphi_3 = a + b\alpha$. Then

$$\begin{aligned}\varphi_2 \circ \varphi_3 + \varphi_3 \circ \varphi_2 &= (a\pi + b\pi\alpha) + (a\pi + b\alpha\pi) \\ &= (a\pi + b\pi^{-1} + b\pi^{-1}j) + (a\pi + b\pi^{-1} - b\pi^{-1}j) \\ &= 2 \cdot (a\pi + b\pi^{-1}) \quad .\end{aligned}$$

Comparing with (A.1.1) we get

$$a\pi + b\pi^{-1} = -u_1 \quad .$$

Hence $v(b) = 1$, *i.e.*, $\varphi_3 \in \Pi\mathcal{O}_D \setminus (\mathcal{O}_K + \Pi^2\mathcal{O}_D)$. Applying [**Ww1**, Thm. 1.4], we obtain

$$\lg\ W[\![t]\!]\,/(J_2 + J_3) = 1 + 1 = 2 = a_2 + a_3 \quad ,$$

which proves the claim in this case.

- $$T = \operatorname{diag}(u_1, u_2, u_3) \quad , \quad \text{hence } GK(T) = (0,1,1) \quad .$$

Then $\varphi_2 = {}^\iota\psi_1 \circ \psi_2 = {}^\iota e_1 \circ (e_1 + e_2) = {}^\iota e_1 \circ e_2 + u_1 \cdot 1$, hence

$$\operatorname{tr}(\varphi_2) = u_1 \cdot 2 \quad , \quad \operatorname{Nm}(\varphi_2) = u_1 \cdot (u_2 + u_1) \quad .$$

Hence $K = \mathbb{Q}_2(\varphi_2) = \mathbb{Q}_2[X]/(X^2 - 2u_1X + u_1 \cdot (u_2 + u_1))$. Since T is anisotropic we have $u_2 + u_1 \equiv 2 \bmod 4$. Hence we are dealing with an Eisenstein polynomial and $\mathcal{O}_K = \mathbb{Z}_2[\varphi_2]$.

Now $\varphi_3 = {}^\iota\psi_1 \circ \psi_3 = {}^\iota e_1 \circ (e_1 + e_3) = {}^\iota e_1 \circ e_3 + u_1 \cdot 1$. At this point it is advantageous to consider instead of φ_3 the endomorphism $\varphi_3' = {}^\iota e_1 \circ e_3$. It is obvious that the locus where φ_2 and φ_3 deform is the same as the locus where φ_2 and φ_3' deform. Now

$$\operatorname{tr}(\varphi_3') = (e_1, e_3) = 0 \quad \text{and} \quad \operatorname{Nm}(\varphi_3') = u_1u_3 \quad .$$

Furthermore

$$\begin{aligned}\operatorname{tr}({}^\iota\varphi_2 \circ \varphi_3') &= \operatorname{tr}({}^\iota(e_1 + e_2) \circ e_1 \circ {}^\iota e_1 \circ e_3) \\ &= u_1 \cdot ((e_1, e_3) + (e_2, e_3)) \\ &= 0 \quad .\end{aligned}$$

Hence

$${}^\iota\varphi_2 \circ \varphi_3' - \varphi_3' \circ \varphi_2 = 0 \quad .$$

Hence φ_3' anticommutes with K. Writing, as in the previous case, $D = K \oplus K \cdot j$ we have

$$\mathcal{O}_D = \mathcal{O}_K \oplus \mathcal{O}_K \cdot \alpha$$

Here $\alpha = \pi^{-1}(1+j) \in \mathcal{O}_D$. Indeed, $\pi = \varphi_2$ is a uniformizer for K and the different $\mathcal{D}$ has valuation $e = 2$. Writing $\varphi_3' = a + b\alpha$ we get

$$a + b\alpha = (a + b\pi^{-1}) + b\pi^{-1} \cdot j \quad .$$

Hence $a + b\pi^{-1} = 0$. Since $\varphi_3' \in \mathcal{O}_D^\times$ it follows that the valuation of b is equal to 1, hence

$$\varphi_3' \in \Pi\mathcal{O}_D \setminus (\mathcal{O}_K + \Pi^2\mathcal{O}_D) \quad .$$

Applying now [**Ww1**, Thm. 1.4], we get

$$\lg\ W[\![t]\!]/(J_2 + J_3) = 1 + 1 = a_2 + a_3 \quad ,$$

which proves the claim in this case. The induction start is now complete.

A.2. The induction step: Lemma 3.1. — In this section we prove Lemma 3.1. We go through all cases of the table.

Case A1: Here $\mathrm{tr}(\varphi) = 0$ and $\mathrm{Nm}(\varphi) = u_1 \cdot 2^{\alpha+\beta+1}$.

Since $\alpha + \beta + 1$ is odd, we get $K = \mathbb{Q}_2(\sqrt{-u_1 2})$ and $\mathcal{O}_K = \mathbb{Z}_2[\sqrt{-u_1 2}]$ and, since $\varphi = 2^{\frac{\alpha+\beta}{2}} \cdot \pi$, where $\pi = \sqrt{-u_1 2}$ is a uniformizer, $\mathbb{Z}_2[\varphi]\mathbb{Z}_2 + 2^{\frac{\alpha+\beta}{2}} \cdot \mathcal{O}_K$. Hence the conductor of $\mathbb{Z}_2[\varphi]$ is equal to $\frac{\alpha+\beta}{2} = \left[\frac{\alpha+(\beta+1)}{2}\right] = \left[\frac{a_1+a_2}{2}\right]$.

Case A2: Here $\mathrm{tr}(\varphi) = 2^{\beta+1}$ and $\mathrm{Nm}(\varphi) = 2^{2(\beta+1)}$.

Hence $K = \mathbb{Q}_2[X]/(X^2 - X + 1)$ is an unramified extension and $\mathcal{O}_K = \mathbb{Z}_2[\xi]$, where ξ is the residue class of X. Then $\varphi = 2^{\beta+1} \cdot \xi$ and $\mathbb{Z}_2[\varphi] = \mathbb{Z}_2 + 2^{\beta+1} \cdot \mathcal{O}_K$ has conductor $\beta + 1 = \left[\frac{(\beta+1)+(\beta+1)}{2}\right] \left[\frac{a_1+a_2}{2}\right]$.

Case B1: Here $\mathrm{tr}(\varphi) = 0$ and $\mathrm{Nm}(\varphi) = u_1 u_2 \cdot 2^{\beta_1+\beta_2}$.

Since $\beta_1 + \beta_2$ is odd, we have $K = \mathbb{Q}_2(\sqrt{-u_1 u_2 2})$ and $\mathcal{O}_K = \mathbb{Z}_2[\sqrt{-u_1 u_2 2}]$. Now $\mathbb{Z}_2[\varphi] = \mathbb{Z}_2 + 2^{\frac{\beta_1+\beta_2-1}{2}} \cdot \mathcal{O}_K$ has conductor $\frac{\beta_1+\beta_2-1}{2} = \left[\frac{\beta_1+\beta_2}{2}\right] = \left[\frac{a_1+a_2}{2}\right]$.

Case B2 a): Here $\mathrm{tr}(\varphi) = u_1 \cdot 2^{\frac{\beta_1+\beta_2}{2}+1}$ and $\mathrm{Nm}(\varphi) u_1 \cdot 2^{\beta_1+\beta_2}(u_1 + u_2)$.

Now by the anisotropy condition on T we have $u_1 + u_2 \equiv 2 \bmod 4$, hence $K = \mathbb{Q}_2[X]/(X^2 - 2u_1 X + u_1(u_1 + u_2))$ is defined by an Eisenstein polynomial and $\mathcal{O}_K = \mathbb{Z}_2[\pi]$, where π denotes the residue class of X. Then $\varphi 2^{\frac{\beta_1+\beta_2}{2}} \cdot \pi$ and $\mathbb{Z}_2[\varphi] = \mathbb{Z}_2 + 2^{\frac{\beta_1+\beta_2}{2}} \cdot \mathcal{O}_K$ has conductor $\frac{\beta_1+\beta_2}{2} = \left[\frac{\beta_1+(\beta_2+1)}{2}\right] = \left[\frac{a_1+a_2}{2}\right]$.

Case B2 b): This is identical with the previous case.

Case B2 c): Here $\mathrm{tr}(\varphi) = u_1 \cdot 2^{\frac{\beta_1+\beta_2}{2}+1}$ and $\mathrm{Nm}(\varphi)u_1^2 \cdot 2^{\beta_1+\beta_2} + u_1u_2 \cdot 2^{\beta_1+\beta_2} + u_1u_3 \cdot 2^{\beta_1+\beta_3}u_1 2^{\beta_1+\beta_2}(2u_3 + u_2 + u_1)$.

Hence $K = \mathbb{Q}_2[X]/(X^2 - 2u_1X + u_1 \cdot (2u_3 + u_2 + u_1))$, which is defined by an Eisenstein equation since $u_1 + u_2 \equiv 0 \bmod 4$. Hence $\mathcal{O}_K = \mathbb{Z}_2[\pi]$, where π is the residue class of X and $\varphi = 2^{\frac{\beta_1+\beta_2}{2}} \cdot \pi$ and $\mathbb{Z}_2[\varphi] = \mathbb{Z}_2 + 2^{\frac{\beta_1+\beta_2}{2}} \cdot \mathcal{O}_K$ has conductor $\frac{\beta_1+\beta_2}{2}\left[\frac{\beta_1+\beta_2+1}{2}\right] = \left[\frac{a_1+a_2}{2}\right]$.

Case B3 a): Here $\mathrm{tr}(\varphi) = 2^{\frac{\beta_1+\beta_2}{2}+1} \cdot u_1$ and $\mathrm{Nm}\,\varphi = 2^{\beta_1+\beta_2} \cdot u_1(u_1 + u_2)$.

Hence $K = \mathbb{Q}_2[X]/(X^2 - 2u_1X + u_1 \cdot (u_1 + u_2))$. Now since T is anisotropic, it follows that $u_1 + u_2 \equiv 4 \bmod 8$. Hence writing $u_1 + u_2 = 4\eta$ with $\eta \in \mathbb{Z}_2^\times$, we have $K = \mathbb{Q}_2[X_1]/(X_1^2 - u_1X_1 + u_1\eta)$. Hence $K/\mathbb{Q}_2$ is unramified and $\mathcal{O}_K = \mathbb{Z}_2[\xi]$, where ξ denotes the residue class of X_1. Now $\varphi = 2^{\frac{\beta_1+\beta_2}{2}+1} \cdot \xi$ and $\mathbb{Z}_2[\varphi] = \mathbb{Z}_2 + 2^{\frac{\beta_1+\beta_2}{2}+1} \cdot \mathcal{O}_K$ has conductor $\frac{\beta_1+\beta_2}{2} + 1\frac{\beta_1+(\beta_2+2)}{2} = \left[\frac{a_1+a_2}{2}\right]$.

Case B3 b): Here the trace and norm are as in the previous case, but this time $K = \mathbb{Q}_2[X]/(X^2 - 2u_1X + u_1 \cdot (u_1 + u_2))$ is defined by an Eisenstein polynomial. Hence $\mathcal{O}_K = \mathbb{Z}_2[\pi]$ where π is the residue class of X and $\varphi = 2^{\frac{\beta_1+\beta_2}{2}} \cdot \pi$ and $\mathbb{Z}_2[\varphi] = \mathbb{Z}_2 + 2^{\frac{\beta_1+\beta_2}{2}} \cdot \mathcal{O}_K$ has conductor $\frac{\beta_1+\beta_2}{2}\frac{\beta_1+(\beta_2+1)}{2} = \left[\frac{a_1+a_2}{2}\right]$.

This proves the assertion in all cases. □

By symmetry we also obtain that $\varphi' = \psi_2 \circ {}^\iota\psi_1$ generates an order of conductor $\left[\frac{a_1+a_2}{2}\right]$ in K'.

A.3. The induction step: Lemmas 3.4 and 3.5. — We first prove Lemma 3.4. We go through all cases, making use of the results in section A.2. Again we wish to bound the conductors of the orders $\mathbb{Z}_2[\varphi_1]$ resp. $\mathbb{Z}_2[\varphi_2]$.

Case A1: Here $K = \mathbb{Q}_2(\sqrt{-u_1 2})$ and $\mathcal{O}_K = \mathbb{Z}_2[\pi]$ with $\pi = \sqrt{-u_1 2}$. Then ${}^\iota\pi = -\pi$ and thereby this case is like the ramified case for $p \neq 2$. We have

$$\mathcal{O}_K = \mathbb{Z}_2 \oplus \mathbb{Z}_2\pi \quad ,$$

the decomposition into traceful and traceless elements. In particular, $\mathrm{tr}(\mathcal{O}_K) \subset 2 \cdot \mathbb{Z}_2$. Let

$$\varphi_i^\circ = \varphi_i - \frac{1}{2}\mathrm{tr}(\varphi_i) \quad , \quad i = 1, 2 \quad .$$

Then $\mathbb{Z}_2[\varphi_i] = \mathbb{Z}_2[\varphi_i^\circ]$ has conductor $\frac{1}{2}(v(\varphi_i^\circ) - 1)$. Let

$$\varphi_i = \lambda_i \cdot \pi^{a_i} \quad , \quad \lambda_i \in \mathcal{O}_K^\times \quad .$$

Then

$$\varphi_i^\circ = \frac{1}{2}(\lambda_i - (-1)^{a_i} \cdot {}^\iota\lambda_i) \cdot \pi^{a_i} \quad , \quad i = 1, 2 \quad .$$

Writing $\lambda_i = a + b\pi$ we have $a \in \mathbb{Z}_p^\times$ and

$$\lambda_i + {}^\iota\lambda_i = 2a$$
$$\lambda_i - {}^\iota\lambda_i = 2b\pi \quad .$$

Hence $v(\varphi_i^\circ) = a_i$ if a_i is odd and $v(\varphi_i^\circ) > a_i$ if a_i is even. Now according to our table, a_1 and a_2 have different parity which implies that $r \leq (a_2 - 1)/2$. This shows the result in this case.

Case A2: Here $K = \mathbb{Q}_2[X]/(X^2 - X + 1)$ and $\mathcal{O}_K\mathbb{Z}_2[\xi]$, where ξ is the residue class of X. In this case, $\mathbb{Z}_2[\varphi_i] = \mathcal{O}_K$ or $\mathrm{tr}(\varphi_i) \in 2\mathbb{Z}_2$. In the first case $r = 0$ and the claim is obvious. Now let $\mathrm{tr}(\varphi_i) \in 2\mathbb{Z}_2$ for $i = 1$ and $i = 2$, and consider

$$\varphi_i^\circ = \varphi_i - \frac{1}{2}\,\mathrm{tr}(\varphi_i) \quad .$$

Then writing $\varphi_i^\circ = a + b\xi$ we have $0 = \mathrm{tr}(\varphi_i^\circ) = 2a + b$. Hence $\varphi_i^\circ = a \cdot (1 - 2\xi)$ and $v(\varphi_i^\circ) = v(a) = v(b) - 2$. The conductor of $\mathbb{Z}_2[\varphi_i] = \mathbb{Z}_2[\varphi_i^\circ]$ is equal to $\frac{1}{2}v(b) = \frac{1}{2}v(\varphi_i^\circ) + 1$. Now

$$\varphi_i = \lambda_i \cdot 2^{a_i/2} \quad , \quad \lambda_i \in \mathcal{O}_K^\times \quad .$$
$$\varphi_i^\circ = \frac{1}{2}(\lambda_i - {}^\iota\lambda_i) \cdot 2^{a_i/2} \quad .$$

Hence $v(\varphi_i^\circ) = a_i - 2$ if the residue class $[\lambda_i]$ of λ_i lies in $\mathbb{F}_4 \setminus \mathbb{F}_2$, and is larger otherwise. Hence if $[\lambda_i] \in \mathbb{F}_4 \setminus \mathbb{F}_2$, then $r \leq \frac{a_i}{2}$, hence $2r \leq a_2$.

But not both $[\lambda_1], [\lambda_2]$ can lie in $\mathbb{F}_2$. Indeed,

$$\varphi_1 \circ \varphi_2 = {}^\iota\lambda_1 \cdot \lambda_2 \cdot 2^{(a_1+a_2)/2} = {}^\iota\lambda_1\lambda_2 \cdot 2^{\beta+1} \quad .$$

On the other hand ${}^\iota\varphi_1 \circ \varphi_2 = u \cdot \varphi$, where $u \in \mathbb{Z}_2^\times$ is as in (3.1), and where φ is as in the previous section. Now $\varphi = 2^{\beta+1}\xi$. Taking the residues modulo $2^{\beta+1}$, we prove the claim.

Now assume $2r = a_2 = a_3$. Then $a_1 < 2r$ has to be odd, which contradicts the fact that $a_1 = a_2 = \beta + 1$.

Case B1: Here $K = \mathbb{Q}_2(\sqrt{-u_1u_2 2})$ and $\mathcal{O}_K = \mathbb{Z}_2[\pi]$, with $\pi = \sqrt{-u_1u_2 2}$. This case is completely analogous to case A1.

Case B2 a): Here $K = \mathbb{Q}_2[X]/(X^2 - 2u_1X + u_1 \cdot (u_1 + u_2))$ and $\mathcal{O}_K = \mathbb{Z}_2[\pi]$ where π denotes the residue class of X. Then π is a uniformizer satisfying an Eisenstein equation. Hence $\mathrm{tr}(\mathcal{O}_K) \subset 2\mathbb{Z}_2$. We again consider $\varphi_i^\circ = \varphi_i - \frac{1}{2}\,\mathrm{tr}(\varphi_i)$. Then writing $\varphi_i^\circ = a + b\pi$ we have $0 = \mathrm{tr}(\varphi_i^\circ) = 2a + 2bu_1 = 2(a + bu_1)$. Hence $\varphi_i^\circ = b \cdot (-u_1 + \pi)$ and $v(\varphi_i^\circ) = v(b)$. The conductor of $\mathbb{Z}_2[\varphi_i] = \mathbb{Z}_2[\varphi_i^\circ]$ is equal to $\frac{1}{2}v(b) = \frac{1}{2}v(\varphi_i^\circ)$. Now

$$\varphi_i = \lambda_i \cdot \pi^{a_i} \quad , \quad \lambda_i \in \mathcal{O}_K^\times \quad .$$

Let us write

$$2u_1 - \pi = \eta \cdot \pi \quad , \quad \eta \in \mathcal{O}_K^\times \quad .$$

Then $\eta = 1 + \eta_1 \cdot \pi$ with $\eta_1 \in \mathcal{O}_K^\times$. We have

$$\begin{aligned}\operatorname{tr}(\varphi_i) &= \lambda_i \cdot \pi^{a_i} + {}^\iota\lambda_i \cdot (\eta\pi)^{a_i} \\ &= (\lambda_i + {}^\iota\lambda_i \eta^{a_i}) \cdot \pi^{a_i} \quad .\end{aligned}$$

Hence

$$\varphi_i^\circ = \frac{1}{2} \cdot (\lambda_i - {}^\iota\lambda_i \eta^{a_i}) \cdot \pi^{a_i} \quad .$$

Let $\lambda_i \equiv 1 + [\lambda_i] \cdot \pi \pmod{\pi^2}$. Then ${}^\iota\lambda_i \equiv 1 - [\lambda_i]\pi \pmod{\pi^2}$. If a_i is odd, we get

$$\begin{aligned}\lambda_i - {}^\iota\lambda_i \eta^{a_i} &\equiv (1 + [\lambda_i]\pi) - (1 - [\lambda_i]\pi) \cdot (1 + \eta_1\pi) (\operatorname{mod} \pi^2) \\ &\equiv \eta_1 \cdot \pi \pmod{\pi^2} \quad .\end{aligned}$$

Hence in this case $v(\varphi_i^\circ) = a_i - 1$. We get $r \leq \frac{1}{2}(a_i - 1)$. Since a_1 or a_2 are odd, we obtain the assertion.

Cases B2 b) and c): These cases are identical to the previous one.

Case B3 a): In this case $K = \mathbb{Q}_2[X]/(X^2 - u_1 X + u_1\eta)$, for some $\eta \in \mathbb{Z}_2^\times$. Hence $K/\mathbb{Q}_2$ is unramified and $\mathcal{O}_K = \mathbb{Z}_2[\xi]$, where ξ is the residue class of X. This case is similar and almost identical to case A2). If $\operatorname{tr}(\varphi_i) \notin 2\mathbb{Z}_2$, then $\mathbb{Z}_2[\varphi_i] = \mathcal{O}_K$ and $r = 0$ and the claim is obvious. If $\operatorname{tr}(\varphi_i) \in 2\mathbb{Z}_2$ for $i = 1$ and $i = 2$, we consider again $\varphi_i^\circ = \varphi_i - \frac{1}{2}\operatorname{tr}(\varphi_i)$. Writing $\varphi_i^\circ = a + b\xi$ we get $0 = \operatorname{tr}(\varphi_i^\circ) = 2a + bu_1$. Hence $\varphi_i^\circ = a(1 - 2u_i^{-1}\xi)$ and $v(\varphi_i^\circ) = v(a) = v(b) - 2$. The conductor of $\mathbb{Z}_2[\varphi_i] = \mathbb{Z}_2[\varphi_i^\circ]$ is equal to $\frac{1}{2}v(b) = \frac{1}{2}v(\varphi_i^\circ) + 1$. Now

$$\begin{aligned}\varphi_i &= \lambda_i \cdot 2^{a_i/2} \quad , \quad \lambda_i \in \mathcal{O}_K^\times \\ \varphi_i^\circ &= \frac{1}{2}(\lambda_i - {}^\iota\lambda_i) \cdot 2^{a_i/2} \quad .\end{aligned}$$

Hence $v(\varphi_i^\circ) = a_i - 2$ if the residue class $[\lambda_i]$ of λ_i lies in $\mathbb{F}_4 \setminus \mathbb{F}_2$, and is larger otherwise. If $[\lambda_i] \in \mathbb{F}_4 \setminus \mathbb{F}_2$, then $r \leq a_i/2$, hence $2r \leq a_2$. But not both $[\lambda_1], [\lambda_2]$ can lie in $\mathbb{F}_2$. Indeed,

$${}^\iota\varphi_1 \circ \varphi_2 = {}^\iota\lambda_1\lambda_2 \cdot 2^{(a_1+a_2)/2} = {}^\iota\lambda_1\lambda_2 \cdot 2^{\frac{\beta_1+\beta_2}{2}+1} = u \cdot \varphi_2 = u \cdot 2^{\frac{\beta_1+\beta_2}{2}+1} \cdot \xi \quad .$$

Taking the residue modulo $2^{\frac{\beta_1+\beta_2}{2}+1}$, we get the claim.

Now assume $2r = a_2 = a_3$. Then $a_1 < 2r$ has to be odd which contradicts the condition that $a_1 = \beta_1$ has to have the same parity as $\beta_2 + 2 = a_2 = 2r$.

Case B3 b): This is again identical to cases B2 a)–c).

The Lemma 3.4 is proved. □

We now turn to the proof of Lemma 3.5. Again we inspect the various cases.

Case A1: We write $D = K \oplus K \cdot j$ as in (A.1.2) in section A.1, where j anticommutes with K and where $j^2 \in \mathbb{Z}_2^\times$ satisfies $v(j^2 - 1) = 2(e - 1)$, where the different $\mathcal{D}$ has

valuation e. Then $\mathcal{O}_D = \mathcal{O}_K \oplus \mathcal{O}_K \cdot \delta\alpha$, where $\alpha = \pi^{-(e-1)} \cdot (1+j) \in \mathcal{O}_D^\times$, cf. (A.1.3). In the case at hand $e = 3$, hence $\alpha = \pi^{-2}(1+j)$. Now

$$\varphi \circ {}^\iota\varphi_3 + {}^\iota\varphi_3 \circ \varphi 2^{\beta+1} \cdot {}^\iota\tilde{e}_1 \quad , \tag{A.3.1}$$

where $\tilde{e}_1 = \gamma \circ e_1$. This follows from $\varphi = {}^\iota\psi_1 \circ \psi_2$ and the definitions $\psi_1 e_1$, $\psi_2 = e_2$, $\psi_3 = e_3$. Now writing ${}^\iota\varphi_3 = a + b\alpha$ for suitable $a, b \in \mathcal{O}_K$ and writing $\varphi = 2^\delta \cdot \pi$ with $\delta = \frac{1}{2}(\alpha + \beta)$, we get from (A.3.1)

$$2^\delta \cdot \pi(a + b\alpha) + (a + b\alpha) \cdot 2^\delta \pi 2^{\beta+1} \cdot {}^\iota\tilde{e}_1 \quad ,$$

i.e., $2^{\delta+1}(a\pi + b\pi^{-1}) = 2^{\beta+1} \cdot {}^\iota\tilde{e}_1$, hence

$$b = 2^{\frac{\beta-\alpha}{2}} \cdot {}^\iota\tilde{e}_1\pi - a\pi^2 \quad . \tag{A.3.2}$$

Now $v({}^\iota\tilde{e}_1) = \alpha$, hence the first summand of the RHS of (A.3.2) has valuation $\beta + 1$. Since $v(\varphi_3) = \beta + 1$, it follows $v(b) = \beta + 1 = a_3$, which proves the claim in this case.

Case A2: Here we write $\mathcal{O}_D = \mathcal{O}_K \oplus \mathcal{O}_K \cdot \Pi$ where $\Pi^2 = 2$ and where Π anticommutes with K. In this case we have

$$\varphi \circ {}^\iota\varphi_3 + {}^\iota\varphi_3 \circ \varphi 2^{\beta+1} \cdot {}^\iota\tilde{e}_1 \quad .$$

Writing ${}^\iota\varphi_3 = a + b\Pi$ and $\varphi 2^{\beta+1} \cdot \xi$ we obtain

$$2^{\beta+1}(2a\xi + b(\xi + {}^\iota\xi) \cdot \Pi) = 2^{\beta+1} \cdot {}^\iota\tilde{e}_1 \quad ,$$

i.e.,

$$2a\xi + b\Pi = {}^\iota\tilde{e}_1 \quad .$$

Now $v({}^\iota\tilde{e}_1) = v({}^\iota\varphi_3) = \alpha$. This implies $v(b\Pi) = \alpha$, hence $\varphi_3 \in \Pi^{a_3}\mathcal{O}_D \setminus (\mathcal{O}_K + \Pi^{a_3+1}\mathcal{O}_D)$, since $a_3 = \alpha$.

Case B1: This case is similar to case A1, except that the identity (A.3.1) is replaced by

$$\varphi \circ {}^\iota\varphi_3 + {}^\iota\varphi_3 \circ \varphi 2 \cdot {}^\iota\tilde{e}_3 \circ \varphi \quad .$$

Now $\varphi = 2^\delta\pi$ with $\delta = (\beta_1 + \beta_2)/2$. Writing as in case A1) ${}^\iota\varphi_3 = a + b\alpha$, where $\alpha = \pi^{-2}(1+j)$, we get

$$2^{\delta+1} \cdot (a\pi + b\pi^{-1}) = 2^{\delta+1} \cdot {}^\iota\tilde{e}_3 \cdot \pi \quad ,$$

i.e.,

$$b = {}^\iota\tilde{e}_3\pi^2 - a\pi^2 \quad .$$

Now the first summand of the RHS has valuation $\beta_3 + 2$ and $v(\tilde{\psi_3}) = \beta_3 + 2$. Hence $v(b) = \beta_3 + 2$, which proves the claim, since $\beta_3 + 2 = a_3$.

Case B2 a): In this case the valuation of the different is equal to 2 and hence $\alpha = \pi^{-1} \cdot (1+j)$. Now

$$\varphi \circ {}^\iota\varphi_3 - {}^\iota\varphi_3 \circ \varphi 2 \cdot {}^\iota e_2 e_3 {}^\iota\tilde{e}_1 \quad .$$

Writing ${}^\iota\varphi_3 = a + b\alpha$ and $\varphi = 2^\delta\pi$ with $\delta = (\beta_1 + \beta_2)/2$, we get

$$2^\delta(((\pi a + b) + bj) - ((\pi a + b) + b\pi^{-1} \cdot {}^\iota\pi j)) = 2 \cdot {}^\iota e_2 e_3 {}^\iota\tilde{e}_1 \quad . \tag{A.3.3}$$

Therefore, since ${}^\iota\pi = 2u_1 - \pi$,

$$2^{\delta+1} j \cdot b \cdot (1 - u_1\pi^{-1}) = 2 \cdot {}^\iota e_2 e_3 {}^\iota\tilde{e}_1 \quad .$$

Comparing valuations we obtain $v(b) = \beta_3 + 1 = a_3$, which proves the assertion in this case.

Case B2 b): Here again $\alpha = \pi^{-1}(1 + j)$, and the same equation (A.3.3) holds. The case is identical with the previous case.

Case B2 c): The same again.

Case B3 a): This case is similar to case A2. We write $\mathcal{O}_D = \mathcal{O}_K \oplus \mathcal{O}_K \cdot \Pi$ as in that case. Now

$$\varphi \circ {}^\iota\varphi_3 - {}^\iota\varphi_3 \circ \varphi = -2 \cdot {}^\iota e_3 e_2 {}^\iota\tilde{e}_1 \quad .$$

We write ${}^\iota\varphi_3 = a + b\Pi$ and $\varphi = 2^\delta \cdot \xi$ where $\delta = \frac{\beta_1+\beta_2}{2} + 1$ and ξ satisfies $\xi^2 - u_1\xi + u_1\eta = 0$ for some $\eta \in \mathbb{Z}_2^\times$. Then

$$2^\delta \cdot ((a\xi + b\xi\Pi) - (a\xi + b \cdot {}^\iota\xi\Pi)) - 2 \cdot {}^\iota e_3 e_2 {}^\iota\tilde{e}_1 \quad .$$

Now $\xi - {}^\iota\xi = 2\xi - u_1$, hence

$$2^\delta \cdot b \cdot \Pi \cdot (2\xi - u_1) = -2 \cdot {}^\iota e_3 e_2 {}^\iota\tilde{e}_1 \quad .$$

Comparing valuations we get $v(b) = \beta_3 - 1 = a_3 - 1$. Hence $\varphi_3 \in \Pi^{a_3}\mathcal{O}_D \setminus (\mathcal{O}_K + \Pi^{a_3+1}\ \mathcal{O}_D)$, as claimed.

Case B3 b): This case is similar to cases B2 a)–c). Again the valuation of the different is equal to 2 and $\alpha = \pi^{-1}(1 + j)$. Now

$$\varphi \circ {}^\iota\varphi_3 - {}^\iota\varphi_3 \circ \varphi 2 \cdot {}^\iota e_2 e_3 {}^\iota\tilde{e}_1 \quad .$$

Writing ${}^\iota\varphi_3 = a + b\alpha$ and $\varphi 2^\delta \cdot \pi$ with $\delta = (\beta_1 + \beta_2)/2$ as in case B2 a), we get just as in that case

$$2^{\delta+1} \cdot j \cdot b(1 - u_1\pi^{-1}) = 2{}^\iota e_2 e_3 {}^\iota\tilde{e}_1 \quad .$$

Comparing valuations we get $v(b) = \beta_3 + 1 = a_3$, which proves the assertion in this case. □

A.4. Lemma 1.9. — The proof of Lemma 1.9 for $p \neq 2$ was very easy. By contrast, the case $p = 2$ is quite elaborate and uses more information than used so far on the construction of an optimal basis. We go through all cases of the table 1. It turns out that in the passage from the type T of L to the type T' of L' a number of things can happen, as can be read off from the following table.

Table 2

Type T		Type T'
A1	$\alpha \neq \beta$	B1
	$\alpha = \beta$	B2 b)
A2		A2
B1	$\beta_2 \leq \beta_3 - 2$	B1
	$\beta_2 = \beta_3 - 1$	B2 b) or c)
	$\beta_2 = \beta_3$	A1 or B2 a)
B2 a)	$\beta_1 < \beta_2$	B3 b)
	$\beta_1 = \beta_2$	B2 b) or c)
B2 b)	$\beta_1 < \beta_2$	B3 a)
	$\beta_1 = \beta_2$	A2
B2 c)	$\beta_1 < \beta_2$	B3 a)
	$\beta_1 = \beta_2$	A2
B3 a)	$\beta_3 \geq \beta_2 + 4$	B3 a)
	$\beta_3 < \beta_2 + 4$	B2 c)
B3 b)	$\beta_3 \geq \beta_2 + 4$	B3 b)
	$\beta_3 = \beta_2 + 3$	B2 b)
	$\beta_3 = \beta_2 + 2$	B2 a)

The calculations exhibit in fact not only the type of T' but also the precise normal form of T' from which one can then read off the Gross-Keating invariants of T'. In all cases, the assertion of Lemma 1.9 is confirmed.

Since these calculations in the 16 cases are quite tedious, we will sometimes be brief.

Case A1: Here $GK = (\alpha, \beta+1, \beta+1)$, and $(\psi_1, \psi_2, \psi_3) = (e_1, e_2, e_3)$. Hence $\psi_3' \frac{1}{2} e_3$, so

$$T' = \operatorname{diag}\left(u_1 2^\alpha, 2^{\beta-1} \begin{pmatrix} 4 & 1 \\ 1 & 1 \end{pmatrix}\right) \quad .$$

Since

$$2^{\beta-1} \begin{pmatrix} 4 & 1 \\ 1 & 1 \end{pmatrix} \sim \operatorname{diag}(3 \cdot 2^{\beta-1}, 3 \cdot 2^{\beta-1})$$

we obtain

$$T' \sim \begin{cases} \operatorname{diag}(u_1 \cdot 2^\alpha, 3 \cdot 2^{\beta-1}, 3 \cdot 2^{\beta-1}) & \text{if } \alpha \neq \beta \\ \operatorname{diag}(3 \cdot 2^{\alpha-1}, 3 \cdot 2^{\alpha-1}, u_1 \cdot 2^\alpha) & \text{if } \alpha = \beta. \end{cases}$$

Hence if $\alpha \neq \beta$, and since $\alpha \equiv \beta \bmod 2$, then T' is of type B1 and $GK(T') = (\alpha, \beta - 1, \beta+1)$ as asserted. If $\alpha = \beta$, then T' is of type B2 b) and $GK(T') = (\alpha-1, \alpha, \alpha+1)$, as asserted.

The case A2 is entirely similar.

Case B1: In this case $GK(T) = (\beta_1, \beta_2, \beta_3 + 2)$ and $(\psi_1, \psi_2, \psi_3) = (e_1, e_2, c_1 e_1 + c_2 e_2 + e_3)$ for suitable $c_1, c_2 \in \mathbb{Z}_2$. If $\beta_2 < \beta_3$, then by [**Y1**, proof of Lemma B.6], both coefficients c_1 and c_2 are divisible by 2. Hence L' is generated by $(e_1, e_2, \frac{1}{2} e_3)$. Hence the matrix of L' in terms of this basis is

$$T' = \operatorname{diag}(u_1 2^{\beta_1}, u_2 2^{\beta_2}, u_3 2^{\beta_3 - 2}) \quad .$$

So if $\beta_2 \leq \beta_3 - 2$, the type of T' is B1 and $GK(T') = (\beta_1, \beta_2, \beta_3)$ as asserted. If $\beta_2 = \beta_3 - 1$, then T' is of type B2 b) or c) and $GK(T') = (\beta_1, \beta_2, \beta_3)$ as asserted.

If $\beta_2 = \beta_3$, then by [**Y1**, proof of Lemma B.6], we have $2 \mid c_1$. On the other hand, we have $2 \nmid c_2$ in this case, because otherwise the valuation of $\frac{1}{2}(\psi_3, \psi_3)$ would be $\beta_2 < a_3 = \beta_2 + 2$ which is impossible. Hence L' is generated by $e_1, e_2, \frac{1}{2}(e_2 + e_3)$. Consider the matrix defined by the basis $e_2, \frac{1}{2}(e_2 + e_3)$ of the lattice $\tilde{L}'$ of rank 2 generated by e_2 and $\frac{1}{2}(e_2 + e_3)$,

$$\tilde{T}' \begin{pmatrix} u_2 2^{\beta_2} & c_2 u_2 2^{\beta_2 - 1} \\ * & (c_2^2 u_2 + u_3) 2^{\beta_2 - 2} \end{pmatrix} \quad .$$

We determine when $\tilde{T}'$ is diagonalizable by determining the valuations of the ideals in $\mathbb{Z}_2$,

$$s(\tilde{L}') = \frac{1}{2}(\tilde{L}', \tilde{L}'), \text{ resp. } n(\tilde{L}') = (Q(x),\ x \in \tilde{L}') \quad .$$

Now

$$\operatorname{ord}\ s(L) = \min\{\beta_2, \beta_2 - 1,\ \operatorname{ord}(c_2^2 u_2 + u_3) + \beta_2 - 2\} = \beta_2 - 1 \quad .$$

And

$$\begin{aligned}\text{ord } n(L) &= \min\{\beta_2, \beta_2, \text{ord}(c_2^2 u_2 + u_3) + \beta_2 - 2\} \\ &= \begin{cases} \beta_2 - 1 & \text{if } u_2 \equiv u_3 \bmod 4 \\ \beta_2 & \text{if } u_2 \equiv -u_3 \bmod 4. \end{cases}\end{aligned}$$

Hence, by [**Y1**, Prop. B.3],

$$\tilde{T}' \sim \begin{cases} \text{diag}(\eta_1 2^{\beta_2 - 1}, \eta_2 2^{\beta_2 - 1}) & \text{if } u_2 \equiv u_3 \bmod 4 \\ 2^{\beta_2 - 1} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} & \text{if } u_2 \equiv -u_3 \bmod 4. \end{cases}$$

Here $\eta_1, \eta_2 \in \mathbb{Z}^\times$. For the total matrix T' we get that if $u_2 \equiv u_3 \bmod 4$, then $T' \sim \text{diag}(u_1 2^{\beta_1}, \eta_1 2^{\beta_2 - 1}, \eta_2 2^{\beta_2 - 1})$ is of type B2 a) and $GK(T') = (\beta_1, \beta_2, \beta_2)$ as asserted. If $u_2 \equiv -u_3 \bmod 4$, then $T' \sim \text{diag}\left(u_1 2^{\beta_1}, 2^{\beta_2 - 1}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)\right)$ is of type A1 and $GK(T') = (\beta_1, \beta_2, \beta_2)$ as asserted.

Case B2 a): In this case $GK(T) = (\beta_1, \beta_2 + 1, \beta_2 + 1)$ and $(\psi_1, \psi_2, \psi_3) = (e_1, 2^\gamma e_1 + e_2, 2^\gamma e_1 + e_3)$, where $\gamma = \frac{1}{2}(\beta_2 - \beta_1)$.

If $\gamma > 0$, then L' is generated by the elements $e_1, e_2, \frac{1}{2}e_3$ and it follows that $T' = \text{diag}(u_1 2^{\beta_1}, u_3 2^{\beta_2 - 2}, u_2 2^{\beta_2})$. Now by the anisotropy condition we have

$$(-1, u_2 u_3) = (u_1 u_2, u_1 u_3) \quad ,$$

hence $u_1 \equiv u_3 \bmod 4$. Therefore T' is of type B3 b) and $GK(T') = (\beta_1, \beta_2 - 1, \beta_2 + 1)$, as asserted.

If $\gamma = 0$, *i.e.*, $\beta_1 = \beta_2 = \beta_3 =: \beta$, then L' is generated by $e_1, e_2, \frac{1}{2}(e_1 + e_3)$ and has matrix with respect to this basis equal to

$$T' = \begin{pmatrix} u_1 2^\beta & 0 & u_2 2^{\beta - 1} \\ * & u_2 2^\beta & 0 \\ * & * & (u_1 + u_3) 2^{\beta - 2} \end{pmatrix} \quad .$$

Now $u_1 \equiv u_3 \bmod 4$, hence by an argument similar to the one used in the case B1 when $\beta_2 = \beta_3$, the lattice generated by $e_1, \frac{1}{2}(e_1 + e_3)$ is diagonalizable to $\text{diag}(\eta_1 2^{\beta - 1}, \eta_2 2^{\beta - 1})$. Hence $T' \sim \text{diag}(\eta_1 2^{\beta - 1}, \eta_2 2^{\beta - 1}, u_2 2^\beta)$ is of type B2 b) or c) and $GK(T') = (\beta - 1, \beta, \beta + 1)$, as asserted.

Case B2 b): In this case $GK(T) = (\beta_1, \beta_2 + 1, \beta_2 + 2)$ and $(\psi_1, \psi_2, \psi_3) = (e_1, 2^\gamma e_1 + e_2, 2^\gamma e_1 + e_2 + e_3)$, with $\gamma = \frac{1}{2}(\beta_2 - \beta_1)$.

If $\gamma > 0$, then L' is generated by $e_1, e_2, \frac{1}{2}(e_2 + e_3)$, and has matrix with respect to this basis equal to

$$T' = \begin{pmatrix} u_1 2^{\beta_1} & 0 & 0 \\ * & u_2 2^{\beta_2} & u_2 2^{\beta_2 - 1} \\ * & * & (u_2 + 2u_3) 2^{\beta_2 - 2} \end{pmatrix} \quad .$$

By an argument similar to the one used in the case B1 when $\beta_2 = \beta_3$, we see that $T' \sim \mathrm{diag}(u_1 2^{\beta_1}, \eta_1 2^{\beta_2 - 2}, \eta_2 2^{\beta_2 + 1})$, hence T' is of type B3. We claim that T' is of type B3 a), so that $GK(T') = (\beta_1, \beta_2, \beta_2 + 1)$, as asserted. But $\eta_1 \equiv -u_2 \equiv -u_1 \bmod 4$, whence the assertion.

There still remains the case when $\gamma = 0$, *i.e.*, $\beta_1 = \beta_2 =: \beta$ and $\beta_3 = \beta + 1$. Then L' is generated by $e_1, e_2, \frac{1}{2}(e_1 + e_2 + e_3)$. Let $\tilde{L}'$ be the sublattice generated by $f_2 = \frac{1}{2}(e_1 + e_2 + e_3)$ and $f_3 = \frac{1}{2}(e_2 - e_1 + e_3)$. Then

$$\begin{aligned}\frac{1}{2}(f_2, f_2) = \frac{1}{2}(f_3, f_3) &= u_1 2^{\beta-2} + u_2 2^{\beta-2} + u_3 2^{\beta-1} \\ &= (u_1 + u_2 + 2u_3) 2^{\beta-2} \\ &= \eta \cdot 2^{\beta}.\end{aligned}$$

Now $\eta \in \mathbb{Z}^\times$. Indeed, by the anisotropy condition we have

$$(-1, u_1 u_3)(2, u_1 u_2) \quad .$$

It follows that if $u_1 \equiv \pm u_2 \bmod 8$, then $u_1 \equiv u_3 \bmod 4$ and if $u_1 \equiv \pm 3u_2 \bmod 8$, then $u_1 \equiv -u_3 \bmod 4$. In either case $u_1 + u_2 + 2u_3 \not\equiv 0 \bmod 8$. Similarly,

$$\begin{aligned}\frac{1}{2}(f_2, f_3) &= -u_1 2^{\beta-2} + u_2 2^{\beta-2} + u_3 2^{\beta-1} = (u_2 - u_1 + 2u_3) 2^{\beta-2} \\ &= \kappa \cdot 2^{\beta-1} \quad , \quad \text{with } \kappa \in \mathbb{Z}_2^\times \quad .\end{aligned}$$

Now an argument similar to the one used previously shows that the quadratic space $\tilde{L}'$ is equivalent to $2^{\beta-1}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. The orthogonal complement of $\tilde{L}'$ in $L \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$ is the line

$$(\tilde{L}')^\perp = \mathbb{Q}_2 \cdot (-2\frac{u_3}{u_2} e_2 + e_3) \quad .$$

Now L' is generated by $e_1 + e_2$ and f_2 and f_3. Hence one easily calculates that

$$(\tilde{L}')^\perp \cap L' = \mathbb{Z}_2 \cdot f \quad ,$$

where $f = -2\frac{u_3}{u_2} e_2 + e_3$. Now

$$\frac{1}{2}(f, f) = \left(\frac{u_3}{u_2}\right)^2 2^{\beta+2} + u_3 2^{\beta+1} = \lambda \cdot 2^{\beta+1} \quad , \quad \lambda \in \mathbb{Z}_2^\times \quad .$$

Hence $\mathbb{Z}_2 \cdot f + \tilde{L}'$ has valuation $(\beta + 1) + 2(\beta - 1)$, equal to the valuation of L'. Hence $L' = \mathbb{Z}_2 f + \tilde{L}'$ is equivalent to $\mathrm{diag}\left(\lambda \cdot 2^{\beta+1}, 2^{\beta-1}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)\right)$, is of type A2 and $GK(T') = (\beta, \beta, \beta + 1)$, as asserted.

Case B2 c): Here $GK(T) = (\beta_1, \beta_2 + 1, \beta_2 + 2)$ and $(\psi_1, \psi_2, \psi_3) = (e_1, 2^\gamma e_1 + e_2 + e_3, 2^\gamma e_1 + e_2 + 2e_3)$, where $\gamma = \frac{1}{2}(\beta_2 - \beta_1)$.

When $\gamma > 0$, this is similar to previous cases with L' generated by $e_1, \frac{1}{2}e_2, e_3$. In this case $T' = \mathrm{diag}(u_1 2^{\beta_1}, u_2 2^{\beta_2 - 2}, u_3 2^{\beta_2 + 1})$ is of type B3 a) and $GK(T')(\beta_1, \beta_2, \beta_2 + 1)$, as asserted.

When $\gamma = 0$, *i.e.*,$\beta_1 = \beta_2 =: \beta$ and $\beta_3 = \beta + 1$, then L' is generated by $e_1, \frac{1}{2}(e_1 + e_2), e_3$. Now the quadratic space generated by e_1 and $\frac{1}{2}(e_1 + e_2)$ has matrix

$$\tilde{T}' = \begin{pmatrix} u_1 2^{\beta} & u_1 2^{\beta-1} \\ * & (u_1+u_2)2^{\beta-2} \end{pmatrix}$$

Now $(u_1 + u_2)2^{\beta-2} = \eta \cdot 2^{\beta}$ with $\eta \in \mathbb{Z}_2$. By the usual argument $\tilde{T}' \sim 2^{\beta-1}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ and hence $T' \sim \operatorname{diag}\left(u_3 2^{\beta+1}, 2^{\beta-1}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)\right)$ is of type A2 with $GK(T') = (\beta, \beta, \beta + 1)$, as asserted.

Case B3 a): In this case $GK(T) = (\beta_1, \beta_2+2, \beta_3)$ and $(\psi_1, \psi_2, \psi_3) = (e_1, 2^{\gamma}e_1+e_2, e_3)$ with $\gamma = \frac{1}{2}(\beta_2 - \beta_1)$.

Now L' is generated by $e_1, e_2, \frac{1}{2}e_3$ and has matrix $T' = \operatorname{diag}(u_1 2^{\beta_1}, u_2 2^{\beta_2}, u_3 2^{\beta_3-2})$. If $\beta_2 + 2 \leq \beta_3 - 2$, then T' is of type B3 a) and $GK(T') = (\beta_1, \beta_2 + 2, \beta_3 - 2)$, as asserted. Let $\beta_3 - 2 < \beta_2 + 2$. Since not all GK-invariants can have the same parity, we have $\beta_1 \not\equiv \beta_2 \bmod 2$. Hence $\beta_3 = \beta_2 + 3$, and $T' = \operatorname{diag}(u_1 2^{\beta_1}, u_2 2^{\beta_2}, u_3 2^{\beta_2+1})$ is of type B2 c) and $GK(T') = (\beta_1, \beta_2 + 1, \beta_2 + 2)$, as asserted.

Case B3 b): In this case $GK(T) = (\beta_1, \beta_2+1, \beta_3+1)$ and $(\psi_1, \psi_2, \psi_3) = (e_1, 2^{\frac{\beta_2-\beta_1}{2}}e_1+ e_2, c_1e_1 + c_2e_2 + e_3)$ for suitable $c_1, c_2 \in \mathbb{Z}_2$. In this case we need to extract more information about the coefficients c_1, c_2 from [**Y1**, proof of Lemma B.8]. If $\beta_3 \equiv \beta_1 \bmod 2$, then $c_1 = 2^{\frac{\beta_3-\beta_1}{2}}$ and $c_2 = 0$. Hence L' is generated by $e_1, e_2, \frac{1}{2}e_3$, hence its matrix is $T' = \operatorname{diag}(u_1 2^{\beta_1}, u_2 2^{\beta_2}, u_3 2^{\beta_3-2})$. If $\beta_3 - 2 \geq \beta_2 + 2$, then T' is of type B3 b) and $GK(T') = (\beta_1, \beta_2 + 1, \beta_3 - 1)$, as asserted. If $\beta_3 = \beta_2 + 2$, then T' is of type B2 a) and $GK(T') = (\beta_1, \beta_2 + 1, \beta_3 - 1)$, as asserted.

If $\beta_3 \not\equiv \beta_1 \bmod 2$, then by loc. cit., $c_1 = 2^{\frac{\beta_3-\beta_1-1}{2}}$ and $c_2 = 2^{\frac{\beta_3-\beta_2-1}{2}}$. Now $\beta_3 \geq \beta_2 + 3$, hence c_1 and c_2 are divisible by 2. Hence L' is generated by $e_1, e_2, \frac{1}{2}e_3$, and its matrix is $T' = \operatorname{diag}(u_1 2^{\beta_1}, u_2 2^{\beta_2}, u_3 2^{\beta_3-2})$. If $\beta_3 \geq \beta_2 + 4$, then T' is of type B3 b) and $GK(T') = (\beta_1, \beta_2 + 1, \beta_3 - 1)$, as asserted. If $\beta_3 = \beta_2 + 3$, then T' is of type B2 b) and $GK(T') = (\beta_1, \beta_2 + 1, \beta_3 - 1)$, as asserted.

Lemma 1.9 is now proved in all cases. □

References

[B] I. I. Bouw – Invariants of ternary quadratic forms, this volume, p. 113–137.

[F] W. Fulton – *Intersection Theory*, Springer Verlag, 1984.

[G] B. H. Gross – On canonical and quasi-canonical liftings, *Invent. Math.* **84** (1986), p. 321–326.

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Invent. Math.* **112** (1993), p. 225–245.

[Go2] U. Görtz – Arithmetic intersection numbers, this volume, p. 15–24.

[KM] N. Katz & B. Mazur – *Arithmetic Moduli of Elliptic Curves*, Annals of Math. Studies, vol. 108, Princeton University Press, 1985.

[Mes] W. MESSING – *The crystals associated to Barsotti–Tate groups: with applications to abelian schemes*, Lecture Notes in Math., vol. 264, Springer, 1972.

[Me2] V. MEUSERS – Canonical and quasi-canonical liftings in the split case, this volume, p. 87–98.

[Vi] E. VIEHMANN – Lifting endomorphisms of formal $\mathcal{O}_K$-modules, this volume, p. 99–104.

[Vl] I. VOLLAARD – Endomorphisms of quasi-canonical lifts, this volume, p. ???–???

[Wd1] T. WEDHORN – The genus of the endomorphisms of a supersingular elliptic curve, this volume, p. pagesmf04.

[Wd2] ———, Calculation of representation densities, this volume, p. 179–190.

[Ww1] S. WEWERS –Canonical and quasi-canonical liftings, this volume, p. 67–86.

[Ww2] ———, An alternative approach using ideal bases, this volume, p. 171–177.

[Y1] T. YANG –Local densities of 2-adic quadratic forms, *J. Number Theory* **108** (2004), p. 287–345.

[Y2] ———, Isotropic or anisotropic, letter to Rapoport, March 2004.

[Z] T. ZINK – The display of a formal p-divisible group, in *Cohomologies p-adiques et applications arithmétiques (I)*, Astérisque, vol. 278, Soc. Math. France, Paris, 2002, p. 127–248.

M. RAPOPORT, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : rapoport@math.uni-bonn.de

Astérisque
312, 2007, p. 171–177

14. AN ALTERNATIVE APPROACH USING IDEAL BASES

by

Stefan Wewers

***Abstract.* —** We give another approach to the proof of the Gross-Keating intersection formula. This approach is based on the concept of *ideal bases* in the theory of anisotropic quadratic forms over $\mathbb{Z}_p$, and in the case $p = 2$ is drastically simpler than the proof given in the previous chapter.

***Résumé* (Une approche alternative à l'aide des bases idéales). —** On donne une autre approche à la démonstration de la formule de Gross et Keating. Cette approche est basée sur la notion de *bases idéales* de la théorie des formes quadratiques anisotropes sur $\mathbb{Z}_p$, et est plus simple que la démonstration dans le chapitre précédent pour $p = 2$.

In this note we give an alternative proof of Proposition 1.5 and Proposition 1.6 of [**R**]. This proof uses the concept of *ideal bases* introduced in Section 6 of [**B**] and thus avoids the difficulties encountered in the case $p = 2$. In fact, our arguments work the same way for any p.

1. Homomorphisms between quasi-canonical lifts

1.1. Let p be a prime number and D the quaternion division algebra over $\mathbb{Q}_p$. The reduced norm gives an anisotropic $\mathbb{Q}_p$-valued quadratic form on D which we denote by Q. The function $v : D^\times \to \mathbb{Z}$, $\alpha \mapsto \operatorname{ord}_p Q(\alpha)$, is the standard normalized valuation on D.

Let $\boldsymbol{\psi} = (\psi_1, \dots, \psi_n)$ be an ordered tuple of linearly independent elements of D, and let $L \subset D$ be the $\mathbb{Z}_p$-lattice spanned by $\boldsymbol{\psi}$. The restriction of Q to L gives L the structure of an anisotropic quadratic $\mathbb{Z}_p$-module. We say that $\boldsymbol{\psi}$ is an *ideal basis* of L if

$$v(\psi_i) \leq v(\psi_j) \quad \text{for all } i \leq j$$

2000 ***Mathematics Subject Classification.* —** 14L05, 11F32.
***Key words and phrases.* —** Formal $\mathcal{O}$-modules, quaternion algebras, modular intersection numbers.

and if

$$v\Big(\sum_i x_i\psi_i\Big) = \min_i v(x_i\psi_i)$$

for all $(x_i) \in \mathbb{Z}_p^n$. By [**B**], Lemma 6.4, this is equivalent to Definition 6.3 of *loc. cit.*. In particular, every sublattice $L \subset D$ has an ideal basis.

By [**B**, Proposition 6.6], an ideal basis is also optimal. Moreover, if $\boldsymbol{\psi}$ is ideal then the numbers $a_i := v(\psi_i)$, $i = 1, \dots, n$, are the Gross-Keating invariants of L.

1.2. Let $K \subset D$ be a subfield which is a quadratic extension of $\mathbb{Q}_p$. Then there exists an element $\varphi \in K$ such that

$$\mathcal{O}_K = \mathbb{Z}_p \oplus \mathbb{Z}_p \cdot \varphi$$

and such that φ is a unit (resp. a uniformizer) if $K/\mathbb{Q}_p$ is unramified (resp. if $K/\mathbb{Q}_p$ is ramified). For such an element, we have

$$v(x + y\varphi) = \min\{2\operatorname{ord}_p x, 2\operatorname{ord}_p y + v(\varphi)\}, \tag{1.1}$$

for all $x, y \in \mathbb{Q}_p$. It follows that $(1, p^r\varphi)$ is an ideal basis of

$$\mathcal{O}_r = \mathbb{Z}_p \oplus \mathbb{Z}_p \cdot p^r\varphi,$$

the unique order in $\mathcal{O}_K$ of conductor p^r, for all $r \geq 0$.

1.3. Let G be the unique formal group of height 2 over $k = \bar{\mathbb{F}}_p$. We identify the ring of endomorphisms of G with the maximal order $\mathcal{O}_D$ of D. Note that for $\psi \in \mathcal{O}_D$ the integer $v(\psi)$ is equal to the *height* of the isogeny $\psi : G \to G$.

Fix two positive integers $r, s \geq 0$, and let F_r, F_s be quasi-canonical lifts of G of level r and s, with respect to the subfield $K \subset D$. We assume that F_r, F_s are defined over A, a complete discrete valuation ring which is a finite extension of the ring of Witt vectors over k. We denote by

$$H_{r,s} := \operatorname{Hom}_A(F_r, F_s)$$

the group of homomorphisms of formal groups $F_r \to F_s$. This is a free $\mathbb{Z}_p$-module of rank 2. It is also a right (resp. left) module under the order $\mathcal{O}_r = \operatorname{End}(F_r)$ (resp. the order $\mathcal{O}_s = \operatorname{End}(F_s)$).

Reducing a homomorphism $F_r \to F_s$ to the special fibre yields a $\mathbb{Z}_p$-linear embedding $H_{r,s} \hookrightarrow D$. Via this embedding we may consider $H_{r,s}$ as a quadratic $\mathbb{Z}_p$-module.

Proposition 1.1

1. *As a right $\mathcal{O}_r$-module, $H_{r,s}$ is free of rank 1, generated by a homomorphism $\psi_1 : F_r \to F_s$ of height $|s - r|$.*
2. *The Gross-Keating invariants of $H_{r,s}$ are $(|s - r|, r + s)$ if $K/\mathbb{Q}_p$ is unramified and $(|s - r|, r + s + 1)$ if $K/\mathbb{Q}_p$ is ramified.*

Proof. — Replacing all isogenies by their duals, we may assume that $r \leq s$. Let F/A be the canonical lift of G with respect to the embedding $K \subset D$. By [**Ww1**, §4], we may identify F_r with the quotient of F corresponding to the superlattice $T_r \supset T := \mathcal{O}_K$ defined by

$$T_r := \mathbb{Z}_p \cdot p^{-r} + \mathcal{O}_K$$

(and similarly for F_s). By [**Ww1**, Corollary 2.3], this presentation of F_r, F_s yields an isomorphism of right $\mathcal{O}_r$-modules

$$H_{r,s} \cong \{\alpha \in \mathcal{O}_K \mid \alpha T_r \subset T_s\}.$$

We let $\psi_1 \in H_{r,s}$ denote the element corresponding to 1 under this isomorphism. Clearly, the height of ψ_1 equals the index of T_r in T_s, which is $s - r$. To prove Part 1 of the proposition, it remains to show that $\alpha T_r \subset T_s$ if and only if $\alpha \in \mathcal{O}_r$. One direction is clear. For the other direction, fix $\alpha \in \mathcal{O}_K$ with $\alpha T_r \subset T_s$. In order to show that $\alpha \in \mathcal{O}_r$, we may add any element of $\mathbb{Z}_p$ to α. Hence we may assume that $\alpha = x\varphi$, where $x \in \mathbb{Z}_p$ and φ is as in Section 1.2. Our assumption implies that

$$\alpha p^{-r} = x p^{-r} \varphi \in T_s = \mathbb{Z}_p \cdot p^{-s} \oplus \mathbb{Z}_p \cdot \varphi.$$

We conclude that $p^r | x$ and hence $\alpha \in \mathcal{O}_r$. This proves Part 1.

Set $\psi_2 := p^r \varphi \psi_1$. Clearly, (ψ_1, ψ_2) is the basis of $H_{r,s}$ corresponding to the ideal basis $(1, \varphi)$ of $\mathcal{O}_r$ under the isomorphism $\mathcal{O}_r \cong H_{r,s}$. This isomorphism is not an isometry, but for $\psi = \alpha \cdot \psi_1 \in H_{r,s}$, with $\alpha \in \mathcal{O}_r$, we have

$$v(\psi) = v(\alpha) + (s - r).$$

Therefore, it follows from (1.1) that (ψ_1, ψ_2) is an ideal basis of $H_{r,s}$. By the choice of $\varphi \in K$ in Section 1.2, we get $v(\psi_2) = s + r$ (resp. $v(\psi_2) = s + r + 1$) if $K/\mathbb{Q}_p$ is unramified (resp. ramified). This completes the proof of Part 2 of the proposition. □

1.4. We choose a uniformizer λ of the discrete valuation ring A. For $n \geq 0$ we set $A_n := A/(\lambda^{n+1})$. Let $H_{r,s,n}$ denote the subgroup of $\mathcal{O}_D$ consisting of endomorphisms $\psi : G \to G$ which lift to a homomorphism $F_r \otimes A_n \to F_s \otimes A_n$.

Given an element $\psi \in \mathcal{O}_D - H_{r,s}$, we define two integers,

$$l_{r,s}(\psi) := \max\{v(\psi + \phi) \mid \phi \in H_{r,s}\}$$

and

$$n_{r,s}(\psi) := \max\{m \mid \psi \in H_{r,s,m}\}.$$

We let e denote the absolute ramification index of the discrete valuation ring A.

Proposition 1.2. — *There exists a constant $c_{r,s}$, only depending on (r, s), such that the following holds. If $l_{r,s}(\psi) \geq r + s - 1$ then*

$$n_{r,s}(\psi) = c_{r,s} + \frac{e}{2} \cdot l_{r,s}(\psi).$$

Proof. — First we consider the case $r = s$. Then we may assume that $F_r = F_s$. This is the case studied in [**Vl**]. By ă*loc. cit.*, Proposition 3.1, we have for $l_{r,s}(\psi) \geq 2r - 1$

$$n_{r,s}(\psi) = a(r-1) + p^{r-1} + \Big(\frac{l_{r,s}(\psi)+1}{2} - r\Big)e + 1, \tag{1.2}$$

where $a(k) = (p^k - 1)(p+1)/(p-1)$. Hence the proposition is true for $r = s$.

For the general case, we may again assume that $r \leq s$. By induction on s, we will reduce to the case $r = s$. Suppose that the proposition is proved for some pair (r, s) with $r \leq s$. Let F_r, F_s, F_{s+1} be quasi-canonical lifts of level $r, s, s+1$. We want to prove the proposition for the pair $(r, s+1)$. By Proposition 1.1.1, the group $H_{s,s+1}$ is generated, as a right $\mathcal{O}_s$-module, by a homomorphism $\beta : F_s \to F_{s+1}$ of height one. Moreover, the map $\psi \mapsto \beta\psi$ is an isomorphism of $\mathbb{Z}_p$-modules $H_{r,s} \xrightarrow{\sim} H_{r,s+1}$.

Let $\psi \in \mathcal{O}_D - H_{r,s+1}$ with $l_{r,s+1}(\psi) \geq s+r$. In a first step we will assume in addition that either $r > 0$ or that $l_{r,s+1}(\psi) \geq r + s + 1$. It is no restriction of generality to assume that $v(\psi) = l_{r,s+1}(\psi)$. Then $v(\psi) > 0$ and we can write $\psi = \beta\psi'$, with $\psi' \in \mathcal{O}_D$. It follows from the assertions made in the preceding paragraph that we have

$$l_{r,s+1}(\psi) = l_{r,s}(\psi') + 1. \tag{1.3}$$

In particular, $l_{r,s}(\psi') \geq r + s$. On the other hand, [**Ww1**, Corollary 6.3], says that

$$n_{r,s+1}(\psi) = n_{r,s}(\psi') + e/e_{s+1}, \tag{1.4}$$

where we use the following notation. Let $M = K \cdot W[1/p]$, and let $\mathcal{O}_M$ be its ring of integers. By M_s we denote the ring class field of $O_s^\times \subset \mathcal{O}_K^\times$, by $\mathcal{O}_{M_s}$ its ring of integers, and by e_s its absolute ramification index. Then $\mathcal{O}_{M_s}$ is the minimal subring of A over which F_s can be defined. So for $r > 0$, the proposition follows from (1.3), (1.4) and induction.

Unfortunately, for $r = 0$ the above argument proves the claim only for the weaker bound $l_{r,s} \geq r + s = s$. The problem is that for $s = 1$ and $l = 0$ the element ψ is a unit in $\mathcal{O}_D$, and so we cannot divide by β and reduce to the case $s = 0$. However, the argument can be used to compute the value of the constant $c_{r,s}$. For instance, for $(r, s) = (0, 0)$ we have $c_{0,0} = e/2$ by (1.2), and so by (1.3) and (1.4) we get $c_{0,1} = e/e_1$. Therefore, the proposition is proved if we can show that for $l_{0,1}(\psi) = 0$ we have $n = n_{0,1}(\psi) = e/e_1$.

Since $l_{0,1}(\psi) = 0$, the endomorphism ψ is an automorphism of G. Let F_r^ψ denote the lift of G obtained from F_r by composing the isomorphism $F_r \otimes_A k \xrightarrow{\sim} G$ with ψ. Then ψ lifts to a homomorphism $F_r \to F_s$ modulo λ^n if and only if the two deformations $F_r^\psi \otimes A/(\lambda^n)$ and $F_s \otimes A/(\lambda^n)$ are isomorphic. This, in turn, means that $u(F_r^\psi) \equiv u(F_s) \pmod{\lambda^n}$ (here $u(F) \in A$ denotes the modulus of a lift of G defined over A). By [**Ww1**, Corollary 5.6], the valuation of $u(F_r^\psi)$ (resp. of $u(F_s)$) is equal to e/e_r (resp. equal to e/e_s). Since $e_r = e_0 < e_s = e_1$, the maximal value that n can take is e/e_1. This is what we still had to prove. □

2. The modular intersection number

2.1. Let p be an arbitrary prime and $k = \bar{\mathbb{F}}_p$. Let G be the (unique) formal group of height 2 over k. We identify $\mathrm{End}_k(G)$ with the maximal order $\mathcal{O}_D$ of the quaternion division algebra D over $\mathbb{Q}_p$. Let $W = W(k)$ denote the ring of Witt-vectors over k. Let (Γ, Γ') be the universal deformation of the pair of formal groups (G, G). It is defined over the universal deformation space $\mathcal{S} \cong \mathrm{Spf}\, W[[t, t']]$.

Let $L \subset \mathcal{O}_D$ be a sub-$\mathbb{Z}_p$-module of rank 3. We denote by Q the quadratic form induced on L by the reduced norm on $\mathcal{O}_D$. For $\psi \in L$ we define $v(\psi) := \mathrm{ord}_p\, Q(\psi)$. Choose an ideal basis (ψ_1, ψ_2, ψ_3) of (L, Q), see Section 1.1. Let $a_i := v(\psi_i)$. The numbers a_1, a_2, a_3 are the Gross–Keating invariants of L.

For $i = 1, 2, 3$, let $\mathcal{T}_i$ denote the closed subscheme of $\mathcal{S}$ corresponding to the ideal $I \lhd W[[t, t']]$ which is minimal for the property that ψ_i lifts to a homomorphism $\Gamma \to \Gamma'$ modulo I. The following proposition corresponds to Proposition 1.5 of [**R**].

Proposition 2.1. — *If $a_3 \leq 1$ then $a_3 = 1$ and*

$$(\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{T}_3)_{\mathcal{S}} = \begin{cases} 1, & \text{for } a_2 = 0, \\ 2, & \text{for } a_2 = 1. \end{cases}$$

Proof. — Since Q is anisotropic, the a_i cannot have all the same parity. Therefore, $a_1 \leq a_2 \leq a_3 \leq 1$ implies $a_0 = 0$ and $a_3 = 1$. In particular, ψ_1 is an automorphism of G. It follows that $\mathcal{T}_1 \cong \mathrm{Spf}\, W[[t]]$, and that we may identify $\Gamma|_{\mathcal{T}_1}$ with $\Gamma'|_{\mathcal{T}_1}$ via ψ_1. So for the rest of the proof, we assume that $\psi_1 = 1 \in \mathcal{O}_D$ and consider $\mathcal{T}_2, \mathcal{T}_3$ as closed subschemes of $\mathcal{S}' = \mathrm{Spf}\, W[[t]]$, the universal deformation space of G. For $i = 2, 3$, $\mathcal{T}_i$ is defined by the condition that ψ_i lifts to an endomorphism of Γ.

Let $\mathcal{O} = \mathbb{Z}_p[\psi_2] \subset \mathcal{O}_D$ denote the subring generated by ψ_2. Since $(\psi_1 = 1, \psi_2)$ is an ideal basis of $\mathcal{O}$, we have

$$a_2 = v(\psi_2) = \max\{v(x + \psi_2) \mid x \in \mathbb{Z}_p\}.$$

If $a_2 = 0$, then it follows that $\mathcal{O} = \mathcal{O}_K$ is the maximal order of $K \subset D$, an unramified quadratic extension of $\mathbb{Q}_p$. Therefore, $\mathcal{T}_2 \cong \mathrm{Spf}\, W \subset \mathcal{S}'$ and $F := \Gamma|_{\mathcal{T}_2}$ is the canonical lift corresponding to the subfield $K \subset D$. Moreover, in the notation of §1.4 we have $l = l_{0,0}(\psi_3) = v(\psi_3) = a_3$. It follows from [**Ww1**], Theorem 3.3 (see the proof of Proposition 1.2) that $\mathcal{T}_3 \cap \mathcal{T}_2 \subset \mathcal{T}_2$ corresponds to the ideal $(p^n) \lhd W$, with

$$n = n_{0,0}(\psi_3) = \frac{l+1}{2} e = \frac{a_3 + 1}{2} = 1.$$

This proves the proposition for $a_2 = 0$.

If $a_2 = 1$, then $\mathcal{O} = \mathcal{O}_K$ is also the maximal order of K, but $K/\mathbb{Q}_p$ is ramified. With the same arguments as above, it follows that $\mathcal{T}_2 \cong \mathrm{Spf}\, \mathcal{O}_M \subset \mathcal{S}'$ is the canonical locus corresponding to the subfield $K \subset D$. Applying again [**Ww1**], Theorem 3.3, we get

$$n = n_{0,0}(\psi_3) = \frac{l+1}{2} e = a_3 + 1 = 2.$$

This proves the proposition for $a_2 = 1$. □

2.2. The next proposition corresponds to Proposition 1.6 of [**R**].

Proposition 2.2. — *Suppose that $\psi_3 = p\psi_3'$, for some $\psi_3' \in \mathcal{O}_D$. Let $\mathcal{T}_3' \subset \mathcal{S}$ be the closed formal subscheme corresponding to ψ_3' and $\mathcal{S}_{(p)} \subset \mathcal{S}$ the special fiber. Then*

$$(\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{T}_3)_{\mathcal{S}} = (\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{T}_3')_{\mathcal{S}} + (\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{S}_{(p)})_{\mathcal{S}}.$$

Proof. — Let (F_r, F_s) be a pair of quasi-canonical lifts of G of level r and s, with respect to the same subfield $K \subset D$. The set $H_{r,s} := \mathrm{Hom}(F_r, F_s)$ is a sub-$\mathbb{Z}_p$-module of $\mathcal{O}_D$ of rank two. We consider all pairs (F_r, F_s) such that $\psi_1, \psi_2 \in H_{r,s}$. Note that (ψ_1, ψ_2) is, by construction, an ideal basis of its linear span in $H_{r,s}$. Therefore, Proposition 1.1.1 shows that

$$a_1 \geq |r - s|, \quad a_2 \geq r + s + \epsilon,$$

where $\epsilon = 0$ if $K/\mathbb{Q}_p$ is unramified and $\epsilon = 1$ otherwise. We claim that

$$a_3 = l_{r,s}(\psi_3) := \max\{v(\psi_3 + \varphi) \mid \varphi \in H_{r,s}\} \tag{2.1}$$

(this notation was already used in the previous section). Indeed, since ψ_1, ψ_2, ψ_3 is an ideal basis of L we have

$$a_3 = v(\psi_3) = \max\{v(x_1\psi_1 + x_2\psi_2 + \psi_3) \mid x_1, x_2 \in \mathbb{Z}_p\}. \tag{2.2}$$

Therefore, the inequality '$\leq$' in (2.1) follows from the inclusion $\langle \psi_1, \psi_2 \rangle \subset H_{r,s}$. On the other hand, [**B**, Corollary 6.7], shows that (2.2) still holds if we allow $x_1, x_2 \in \mathbb{Q}_p$. Hence the inequality '$\geq$' follows from the inclusion $H_{r,s} \subset \langle \psi_1, \psi_2 \rangle \otimes \mathbb{Q}_p$, proving the claim. We conclude that $l_{r,s}(\psi_3) = a_3 \geq a_2 \geq r + s + \epsilon$. In fact, we even have

$$l_{r,s}(\psi_3) \geq r + s + 1. \tag{2.3}$$

For if $K/\mathbb{Q}_p$ is unramified, then a_1 and a_2 are even and so a_3 must be odd.

By [**B**], Corollary 6.7, $(\psi_1, \psi_2, \psi_3')$ is again an ideal basis of its linear span (in some order). Therefore, we can apply the same argument to ψ_3'. We get

$$l_{r,s}(\psi_3') = l_{r,s}(\psi_3) - 2 \geq r + s - 1. \tag{2.4}$$

For $\alpha \in \mathcal{O}_D^\times$, let F_r^α denote the deformation of G obtained by composing the identification $F_r \otimes k \xrightarrow{\sim} G$ with α. Define $\mathcal{C}_{r,s} = \mathcal{C}(F_r, F_s) \subset \mathcal{S}$ as the closed subscheme where $\Gamma|_{\mathcal{C}_{r,s}} \cong F_r^\alpha$ and $\Gamma'|_{\mathcal{C}_{r,s}} \cong F_s^\alpha$, for some $\alpha \in \mathcal{O}_D^\times$. It follows from the results of [**Ww1**] that $\mathcal{C}_{r,s} \cong \mathrm{Spf}\, \mathcal{O}_{M_t}$, where $t = \max\{s, r\}$. Moreover,

$$\mathcal{T}_1 \cdot \mathcal{T}_2 = \bigcup_{(F_r, F_s)} \mathcal{C}_{r,s}$$

is the decomposition into irreducible components. To prove the proposition it therefore suffices to show that

$$(\mathcal{C}_{r,s} \cdot \mathcal{T}_3)_{\mathcal{S}} = (\mathcal{C}_{r,s} \cdot \mathcal{T}_3')_{\mathcal{S}} + (\mathcal{C}_{r,s} \cdot \mathcal{S}_{(p)})_{\mathcal{S}} \tag{2.5}$$

for all pairs (F_r, F_s). We also may assume that $r \leq s$. Then $(\mathcal{C}_{r,s} \cdot \mathcal{S}_{(p)})_{\mathcal{S}} = e_s$ is the ramification index of $\mathcal{O}_{M_s}$ over W. Moreover, in the notation of the last subsection, we have

$$(\mathcal{C}_{r,s} \cdot \mathcal{T}_3)_{\mathcal{S}} = n_{r,s}(\psi_3), \quad (\mathcal{C}_{r,s} \cdot \mathcal{T}_3')_{\mathcal{S}} = n_{r,s}(\psi_3'). \tag{2.6}$$

However, by (2.3), (2.4) and Proposition 1.2 we have $n_{r,s}(\psi_3) = n_{r,s}(\psi_3') + e_s$. This proves (2.5) and finishes the proof of the proposition. □

References

[B] I. I. Bouw – Invariants of ternary quadratic forms, this volume, p. 113–137.

[R] M. Rapoport – Deformations of isogenies of formal groups, this volume, p. 139–169.

[Vl] I. Vollaard – Endomorphisms of quasi-canonical lifts, this volume, p. 105–112.

[Ww1] S. Wewers – Canonical and quasi-canonical liftings, this volume, p. 67–86.

S. Wewers, IWR, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
E-mail : stefan.wewers@iwr.uni-heidelberg.de

Astérisque
312, 2007, p. 179–190

15. CALCULATION OF REPRESENTATION DENSITIES

by

Torsten Wedhorn

Abstract. — We calculate for all primes $p \geq 2$ the local representation density of a ternary quadratic form Q over $\mathbb{Z}_p$ in a quadratic space of the form $N \perp H^r$, where N is a quadratic space of rank 4, H is the hyperbolic plane, and $r \geq 0$ is any non-negative integer. Our principal tool is a formula of Katsurada. This defines a rational function $f_{Q,N}$ in p^{-r}. We also determine the derivative of $f_{Q,N}$ and relate it to the arithmetic intersection number of three modular correspondences.

***Résumé* (Calcul de densités de représentation).** — On calcule, pour tous les nombres premiers $p \geq 2$, la densité de représentation locale d'une forme quadratique ternaire Q sur $\mathbb{Z}_p$ dans un espace quadratique de la forme $N \perp H^r$, où N est un espace quadratique de rang 4, H est le plan hyperbolique, et r est un entier ≥ 0. Notre outil principal est une formule de Katsurada. Elle est donnée par une fonction rationnelle $f_{Q,N}$ en p^{-r}. Nous déterminons également la dérivée de $f_{Q,N}$ et nous la relions au nombre d'intersection arithmétique de trois correspondances modulaires.

Introduction

In this note we consider local representation densities of ternary quadratic spaces and derivatives of associated rational functions. These results are used in [**RW**] to relate the arithmetic intersection number of three modular correspondences $(\mathcal{T}_{m_1} \cdot \mathcal{T}_{m_2} \cdot \mathcal{T}_{m_3})$ to a Fourier coefficient of the restriction of the derivative at $s = 0$ of a Siegel–Eisenstein series of genus 3 and weight 2. We also obtain an explicit formula for the integers $\beta_l(Q)$ which occur in [**Go2**].

Let Q and N be quadratic spaces over $\mathbb{Z}_p$ of rank 3 and 4 respectively, and let H be the hyperbolic plane over $\mathbb{Z}_p$. Denote by $\alpha_p(Q, N \perp H^r)$ the local representation density, compare [**Wd1**, 4.3]. This is a rational function $f_{Q,N}(X)$ in $X = p^{-r}$.

2000 ***Mathematics Subject Classification.*** — 11E08, 11E12, 14G35.
Key words and phrases. — Representation density, modular correspondence.

In the first section we consider the case that N is anisotropic and that $r = 0$:

(1) Let D be "the" quaternion division algebra over $\mathbb{Q}_p$ and $N = O_D$ be its maximal order endowed with the reduced norm. Then we compute $\alpha_p(Q, N)$ for any ternary form Q by a direct calculation (Theorem 1.1), following closely [**GK**, section 6].

The value obtained is of course 0 if Q is isotropic, and for anisotropic Q we will see that it does not depend on Q.

In general it is very difficult to compute local representation densities $\alpha_p(Q, N)$, and their computation has a long history. We give only a few references: For $p \neq 2$ a general explicit formula has been given by Hironaka and Sato [**HS**] for arbitrary quadratic spaces Q and N over $\mathbb{Z}_p$. If the rank of Q is 2, Yang has given a formula for $\alpha_p(Q, N)$ in the case of $p = 2$ [**Y1**]. We will use a result of Katsurada [**Ka**] who calculated $\alpha_p(Q, N)$ for arbitrary p and Q in the case that N is an orthogonal sum of copies of the hyperbolic plane H.

In the second section we are interested in the following values:

(2) Let $N = H^2$. Then we specialize Katsurada's formula for $\alpha_p(Q, N \perp H^r) = \alpha_p(Q, H^{r+2})$ to the case where Q is a ternary form and express it in terms of a refinement of the Gross-Keating invariants (see [**B**]) of the ternary form Q. This is done in 2.11.

(3) For Q (ternary and) isotropic we specialize this formula to $r = 0$ and therefore obtain $\alpha_p(Q, H^2)$ (Proposition 2.1) (for Q anisotropic, $\alpha_p(Q, H^2) = 0$).

(4) Finally we calculate for $N = H^2$ and for Q a ternary anisotropic quadratic form the derivative $\frac{\partial}{\partial X} f_{Q,H^2}(X)$ at $X = 1$ (see 2.16).

We remark that the values obtained in (3) and (4) depend only on the Gross-Keating invariants of the ternary form Q although the value in (2) depends on a refinement of these invariants.

Acknowledgements. — I am grateful to T. Yang for spotting a mistake in an earlier version of the manuscript.

1. Calculation of the representation density in the anisotropic case

1.1. We fix a prime number p, let D be "the" quaternion division algebra over $\mathbb{Q}_p$, and denote by $N = O_D$ the maximal order of D which we consider as a quadratic space of rank 4 over $\mathbb{Z}_p$ with respect to the reduced norm. Let Q be any ternary quadratic form over $\mathbb{Z}_p$. In this section we are going to calculate the representation density $\alpha_p(Q, N)$.

As N is an anisotropic quadratic space, Q is represented by N if and only if Q is anisotropic. In this case the result is:

Theorem 1.1. — *Let Q be anisotropic. Then*

$$\alpha_p(Q,N) = 2(p+1)(1+\frac{1}{p}).$$

1.2. For the proof we quote the following lemma from [**Ki**] Theorem 5.6.4(e):

Lemma 1.2. — *For any integer $r \in \mathbb{Z}$ we have*

$$\alpha_p(p^r Q,N) = \alpha_p(Q,N).$$

1.3. Proof of Theorem 1.1. — By Lemma 1.2 we can assume that the underlying $\mathbb{Z}_p$-module of the quadratic space Q is a sublattice Λ in O_D such that $\Lambda \not\subset pO_D$.

Clearly any element of $\mathrm{O}(D,\mathrm{Nrd})$ preserves N and hence $\mathrm{O}(D,\mathrm{Nrd})$ acts on

$$\tilde{A}_{p^r}(Q,N) := \{\, \sigma\colon Q/p^rQ \longrightarrow N/p^rN \mid \mathrm{Nrd}(\sigma(x)) \equiv Q(x) \bmod p^r \,\}$$

for all $r \geq 1$. By definition (see [**Wd1**, 4.3]) we have

$$\alpha_p(Q,N) = (p^r)^{-6}\#\tilde{A}_{p^r}(Q,N)$$

for r sufficiently large.

The dual lattice of $N = O_D$ with respect to the pairing associated to the quadratic form is $N^\vee = \mathfrak{m}^{-1} \subset D$ where $\mathfrak{m}$ is the maximal ideal of O_D. We claim that the induced action of $\mathrm{SO}(D,\mathrm{Nrd})$ on

$$\tilde{B}_{p^r}(Q,N) := \{\, \sigma\colon \mathbb{Z}_p^3 \longrightarrow N/p^r\mathfrak{m}^{-1}N \mid \mathrm{Nrd}(\sigma(x)) \equiv Q(x) \bmod p^r \,\}$$

is transitive for $r \geq 1$. For this it suffices to show that $\mathrm{SO}(D,\mathrm{Nrd})$ acts transitively on the set M of all isometries $\tilde{\sigma}\colon Q \to N$. But by Witt's lemma, $\mathrm{O}(D,\mathrm{Nrd})$ acts transitively on M. For every such $\tilde{\sigma}$ the stabilizer in $\mathrm{O}(D,\mathrm{Nrd})$ is nothing but the orthogonal group of the orthogonal complement of the quadratic $\mathbb{Q}_p$-space generated by $\tilde{\sigma}(Q)$. As this complement is a one-dimensional space, we see that $\mathrm{SO}(D,\mathrm{Nrd})$ acts in fact simply transitively on M.

Using [**Wd1**, Lemma 1.6] we identify $\mathrm{SO}(D,\mathrm{Nrd})$ with

$$\{\, (d,d') \in D^\times \times D^\times \mid \mathrm{Nrd}(d) = \mathrm{Nrd}(d') \,\}/\mathbb{Q}_p^\times.$$

This group contains the subgroup of index 2

$$G = \{\, (d,d') \in O_D^\times \times O_D^\times \mid \mathrm{Nrd}(d) = \mathrm{Nrd}(d') \,\}/\mathbb{Z}_p^\times.$$

Therefore G acts with two orbits on $\tilde{B}_{p^r}(Q,N)$. Let $\bar{G}$ be the quotient of G by the subgroup generated by

$$\{\, (d,d') \in G \mid d \equiv d' \equiv 1 \pmod{p^rN^\vee} \,\}$$

and by $1 + p^{r-1}O_{D_p}$ diagonally embedded in G. Then $\bar{G}$ acts faithfully with 2 orbits on $\tilde{B}_{p^r}(Q,N)$. As

$$\#\tilde{A}_{p^r}(Q,N) = (\#\tilde{B}_{p^r}(Q,N)) \cdot (\#(\mathfrak{m}^{-1}/O_D))^3,$$

we see that

$$\#\tilde{A}_{p^r}(Q,N) = 2(\#\bar{G})(\#(\mathfrak{m}^{-1}/O_D))^3 = 2(p+1)^2 p^{6r-7} p^6.$$

It follows that

$$\alpha_p(Q,N) = p^{-6r} 2(p+1)^2 p^{6r-1} = 2(p+1)(1+\frac{1}{p}).$$

2. Calculation of the representation density in the hyperbolic case

2.1. Again we fix a prime number p. For any element $a \in \mathbb{Q}_p^\times$ we write $\mathrm{ord}(a) \in \mathbb{Z}$ for the p-adic valuation of a.

We denote by H the quadratic space over $\mathbb{Z}_p$ whose underlying module is $\mathbb{Z}_p^2$ and whose matrix with respect to the standard basis is $\left(\begin{smallmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{smallmatrix}\right)$. This means that the quadratic form is given by $\mathbb{Z}_p^2 \ni (x,y) \mapsto xy$.

Note that $H^2 \cong (M_2(\mathbb{Z}_p), \det)$.

Let (M,Q) be any quadratic space over $\mathbb{Z}_p$ of rank 3. In this section we will compute the representation density $\alpha_p(M, H^{r+2})$. In fact, there is a polynomial $f_M(X) \in \mathbb{Q}[X]$ such that $f_M(p^{-r}) = \alpha_p(M, H^{2+r})$ ([**Ka**]). We are interested in

$$f_M(1) = \alpha_p(M, H^2) \tag{2.1}$$

and, for (M,Q) anisotropic, in

$$\frac{\partial}{\partial X} f_M(X)_{|X=1}. \tag{2.2}$$

The first value is given in 2.12 and the second in 2.16.

2.2. We use the formulas by Katsurada [**Ka**] but we express them in terms of the Gross-Keating invariants (cf. [**B**]) of the ternary space (M,Q), an invariant $\tilde{\xi} = \tilde{\xi}(M) \in \{-1,0,1\}$, and an invariant $\eta = \eta(M) \in \{\pm 1\}$.

The invariant η is equal to $+1$ if (M,Q) is isotropic and equal to -1 if (M,Q) is anisotropic.

The Gross-Keating invariants consist of a tuple of integers $GK(M) = (a_1, a_2, a_3)$ such that $0 \leq a_1 \leq a_2 \leq a_3$. In addition, if $a_1 \equiv a_2 \bmod 2$ and $a_2 < a_3$ there is a further invariant $\epsilon_{GK}(M) \in \{\pm 1\}$.

In fact, we will not need the invariant $\epsilon_{GK}(M)$ directly in the sequel, as $\tilde{\xi}(T)$ is a refinement. But we remark that the final expressions for (2.1) and (2.2) depend only on $\eta(M)$ (that is, whether (M,Q) is isotropic or not) and on the Gross-Keating invariants $GK(M)$ and $\epsilon_{GK}(M)$.

If T is the matrix associated to (M,Q) and a $\mathbb{Z}_p$-base of M, we also write $\eta(T)$, $GK(T)$, $\epsilon_{GK}(T)$, and $\tilde{\xi}(T)$.

2.3. Recall the Hilbert symbol $(a,b)_p \in \{\pm 1\}$ for $a,b \in \mathbb{Q}_p^\times$. It is uniquely determined by the following properties (where $a,b,b' \in \mathbb{Q}_p^\times$, $u,v \in \mathbb{Z}_p^\times$):

$$\begin{aligned}(a,b)_p &= (b,a)_p,\\ (a,bb')_p &= (a,b)_p(a,b')_p,\\ (p,p)_p &= (-1,p)_p\end{aligned}$$

and, for p odd, by

$$\begin{aligned}(u,p)_p &= \left(\frac{u}{p}\right),\\ (u,v)_p &= 1,\end{aligned}$$

and, for $p=2$, by

$$(u,2)_2 = \begin{cases}+1, & \text{if } u \equiv \pm 1 \bmod 8,\\ -1, & \text{otherwise,}\end{cases}$$

$$(u,v)_2 = \begin{cases}+1, & \text{if } u \text{ or } v \equiv 1 \bmod 4,\\ -1, & \text{otherwise.}\end{cases}$$

2.4. For any symmetric matrix $T \in \mathrm{Sym}_m(\mathbb{Q}_p)$ we denote by $h(T) = h_p(T)$ the Hasse invariant of the associated quadratic space (M,Q). We use the normalization in [**Ki**]. For $m=3$ we have

$$h(T) = \begin{cases}(-1)^{\delta_{2p}}, & \text{if } (M,Q) \text{ is isotropic;}\\ -(-1)^{\delta_{2p}}, & \text{if } (M,Q) \text{ is anisotropic}\end{cases}$$

by [**Ki**, 3.5.1]. Here δ_{2p} is the Kronecker delta.

2.5. In the next sections we recall some results from [**B**] (cf. also [**Y1**]). We start with the case $p>2$. In that case there exists a basis (e_i) of M such that the matrix $T=(t_{ij})$ associated to Q with respect to this basis (*i.e.*, $t_{ij} = \frac{1}{2}(Q(e_i+e_j) - Q(e_i) - Q(e_j))$) is a diagonal matrix. If we write $t_{ii} = u_i p^{a_i}$ for $a_i \in \mathbb{Z}$ and $u_i \in \mathbb{Z}_p^\times$, we can assume that $a_1 \le a_2 \le a_3$. Moreover, if $a_i = a_{i+1}$ we can assume that $u_{i+1} = 1$. Then the Gross-Keating invariants are given as follows. We have

$$GK(T) = (a_1, a_2, a_3).$$

If $a_1 \equiv a_2 \bmod 2$ and $a_2 < a_3$, we have

$$\epsilon_{GK}(T) = \left(\frac{-u_1u_2}{p}\right).$$

We set

$$\tilde{\xi}(T) = \begin{cases}\left(\frac{-u_1u_2}{p}\right), & \text{if } a_1 \equiv a_2 \bmod 2;\\ 0, & \text{if } a_1 \not\equiv a_2 \bmod 2.\end{cases}$$

Finally, let $i, j \in \{1,2,3\}$ with $i \neq j$ and $a_i \equiv a_j \bmod 2$ and define $k \in \{1,2,3\}$ by $\{1,2,3\} \setminus \{i,j\} = \{k\}$. Then T is isotropic if and only if $(-u_i u_j, p)_p = 1$ or $a_k \equiv a_j \bmod 2$.

2.6. Now assume that $p = 2$. In the sequel K will denote one of the matrices

$$H = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} \qquad \text{or} \qquad Y := \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$$

There exists a basis $\mathcal{B}$ of M such that the matrix T associated to Q with respect to $\mathcal{B}$ is of one of the following forms.

Either Q is not diagonalizable (case A). Then we distinguish two subcases:

(A1) $T = \operatorname{diag}(u2^\alpha, 2^\beta K)$ where $\alpha \leq \beta$ are integers and $u \in \mathbb{Z}_2^\times$. Then

$$GK(T) = (\alpha, \beta, \beta).$$

We set

$$\tilde{\xi}(T) = \begin{cases} 1, & \text{if } a_1 \equiv a_2 \bmod 2; \\ 0, & \text{if } a_1 \not\equiv a_2 \bmod 2. \end{cases}$$

(A2) $T = \operatorname{diag}(2^\alpha K, u2^\beta)$ where $\alpha < \beta$ are integers and $u \in \mathbb{Z}_2^\times$. Then

$$GK(T) = (\alpha, \alpha, \beta).$$

In this case $\epsilon_{GK}(T)$ is defined and we have

$$\epsilon_{GK}(T) = \begin{cases} +1 & \text{if } K = H; \\ -1 & \text{if } K = Y. \end{cases}$$

We set $\tilde{\xi}(T) := \epsilon_{GK}(T)$.

In the nondiagonalizable case A, T is isotropic if and only if $K = H$ or $\alpha \equiv \beta \bmod 2$.

Now assume that T is diagonalizable over $\mathbb{Z}_2$ (case B), *i.e.*, there exists a basis such that $T = \operatorname{diag}(u_1 2^{\beta_1}, u_2 2^{\beta_2}, u_3 2^{\beta_3})$ where $0 \leq \beta_1 \leq \beta_2 \leq \beta_3$ are integers and $u_i \in \mathbb{Z}_2^\times$. Then there are four subcases (here our subdivision of cases is different from [**R**]):

(B1) $\beta_1 \not\equiv \beta_2 \bmod 2$. Then

$$GK(T) = (\beta_1, \beta_2, \beta_3 + 2).$$

We set $\tilde{\xi}(T) := 0$.

(B2) $\beta_1 \equiv \beta_2 \bmod 2$ and ($u_1 u_2 \equiv 1 \bmod 4$ or $\beta_3 = \beta_2$)). Then

$$GK(T) = (\beta_1, \beta_2 + 1, \beta_3 + 1).$$

We set $\tilde{\xi}(T) := 0$.

(B3) $\beta_1 \equiv \beta_2 \bmod 2$, $\beta_3 = \beta_2 + 1$, and $u_1 u_2 \equiv -1 \bmod 4$. Then

$$GK(T) = (\beta_1, \beta_2 + 1, \beta_3 + 1).$$

We set $\tilde{\xi}(T) := (-u_1 u_2, 2)_2$ where $(\ ,\ )_2$ denotes the Hilbert symbol.

(B4) $\beta_1 \equiv \beta_2 \bmod 2$, $\beta_3 > \beta_2 + 1$, and $u_1u_2 \equiv -1 \bmod 4$. Then

$$GK(T) = (\beta_1, \beta_2 + 2, \beta_3).$$

In this case $\epsilon_{GK}(T)$ is defined and we have

$$\epsilon_{GK}(T) = (-u_1u_2, 2)_2.$$

We set $\tilde{\xi}(T) := \epsilon_{GK}(T)$.

Finally, let $i, j \in \{1, 2, 3\}$ with $i \neq j$ and $\beta_i \equiv \beta_j \bmod 2$ and define $k \in \{1, 2, 3\}$ by $\{1, 2, 3\} \setminus \{i, j\} = \{k\}$. Then T is isotropic if and only if

$$(-u_ku_j, -u_iu_j)_2 = (-u_iu_j, 2)_2^{\beta_k+\beta_j}.$$

2.7. Going through the cases in 2.5 and 2.6 we see that there are the following possibilities for the value of $\tilde{\xi}$ if T is anisotropic:

- If $a_1 \not\equiv a_2 \bmod 2$, we either have $\tilde{\xi} = 0$ or we have $\tilde{\xi} = -1$ and $a_3 = a_2 + 1$.
- If $a_1 \equiv a_2 \bmod 2$, we always have $a_2 \not\equiv a_3 \bmod 2$ and $\tilde{\xi} = -1$.

If T is isotropic, the possibilities for the value of $\tilde{\xi}$ are the following:

- If $a_1 \not\equiv a_2 \bmod 2$, we either have $\tilde{\xi} = 0$ or we have $\tilde{\xi} = 1$ and $a_3 = a_2 + 1$.
- If $a_1 \equiv a_2 \bmod 2$, we either have $\tilde{\xi} = 1$ or we have $\tilde{\xi} = -1$ and $a_2 \equiv a_3 \bmod 2$.

2.8. By [**Ka**] there exists a polynomial $f_M(X) = f_T(X) \in \mathbb{Q}[X]$ such that $f_T(p^{-r}) = \alpha_p(M, H^{2+r})$. We use the formulas from [**Ka**] to compute f_T. Indeed, by *loc. cit.* p. 417 and p. 428 we have

$$f_T(X) = \tilde{\gamma}_p(T; X)\tilde{F}_p(T; X)$$

with $\tilde{\gamma}_p(T; X) = \gamma_p(T; p^{-2}X)$ and $\tilde{F}_p(T; X) = F_p(T; p^{-2}X)$ where $\gamma_p(T; X)$ and $F_p(T; X)$ are the rational functions defined in *loc. cit.* p. 417 and p. 451 respectively. Thus

$$\tilde{\gamma}_p(T; X) = (1 - p^{-2}X)(1 - p^{-2}X^2).$$

The function $\tilde{F}_p(T; X)$ is more complicated. We will express it in the next sections using the Gross-Keating invariants $GK(T)$ and the invariant $\tilde{\xi}(T)$.

2.9. By [**Ka**] we have

$$\begin{aligned}\tilde{F}_p(T; X) = &\sum_{i=0}^{\hat{\delta}} \sum_{j=0}^{\tilde{\delta}'/2-i-1} p^{i+j}X^{i+2j} \\ &+ \eta p^{(\tilde{\delta}'-2)/2}X^{\delta-\tilde{\delta}'+2} \sum_{i=0}^{\hat{\delta}} \sum_{j=0}^{\tilde{\delta}'/2-i-1} p^{-j}X^{i+2j} \\ &+ \tilde{\xi}^2 p^{\tilde{\delta}'/2}X^{\tilde{\delta}'-\hat{\delta}} \sum_{i=0}^{\hat{\delta}} \sum_{j=0}^{\delta-2\tilde{\delta}'+\hat{\delta}} \tilde{\xi}^j X^{i+j}\end{aligned} \tag{2.3}$$

where η, δ, $\hat{\delta}$, and $\tilde{\delta}'$ are the invariants defined on p. 450 of *loc. cit.* (note that in *loc. cit.* the definitions of $\tilde{\delta}$ and $\hat{\delta}$ have to be interchanged).

2.10. Going through all the cases in 2.5 and 2.6 one sees that η, δ, $\hat{\delta}$, and $\tilde{\delta}'$ can be expressed as follows (where $GK(T) = (a_1, a_2, a_3)$ are the Gross-Keating invariants):

$$\eta = \begin{cases} +1 & \text{if } T \text{ is isotropic,} \\ -1 & \text{if } T \text{ is anisotropic,} \end{cases} \tag{2.4}$$

$$\delta = a_1 + a_2 + a_3, \tag{2.5}$$

$$\hat{\delta} = a_1, \tag{2.6}$$

$$\tilde{\delta}' = \begin{cases} a_1 + a_2, & \text{if } a_1 \equiv a_2 \bmod 2, \\ a_1 + a_2 + 1, & \text{if } a_1 \not\equiv a_2 \bmod 2, \end{cases} \tag{2.7}$$

2.11. If we set

$$\sigma := \begin{cases} 2, & \text{if } a_1 \equiv a_2 \bmod 2, \\ 1, & \text{if } a_1 \not\equiv a_2 \bmod 2, \end{cases}$$

we can rewrite (2.3) using the invariants η, (a_1, a_2, a_3), and $\tilde{\xi}$:

$$\begin{aligned} \tilde{F}_p(T, X) = &\sum_{i=0}^{a_1} \sum_{j=0}^{(a_1+a_2-\sigma)/2-i} p^{i+j} X^{i+2j} \\ &+ \eta \sum_{i=0}^{a_1} \sum_{j=0}^{(a_1+a_2-\sigma)/2-i} p^{(a_1+a_2-\sigma)/2-j} X^{a_3+\sigma+i+2j} \\ &+ \tilde{\xi}^2 p^{(a_1+a_2-\sigma+2)/2} \sum_{i=0}^{a_1} \sum_{j=0}^{a_3-a_2+2\sigma-4} \tilde{\xi}^j X^{a_2-\sigma+2+i+j}. \end{aligned} \tag{2.8}$$

2.12. We now specialize to $r = 0$, *i.e.*, $X = 1$. In that case we have

$$\alpha_p(T, H^2) = f_T(1) = (1 - p^{-2})^2 \tilde{F}_p(T, 1).$$

If we set $\beta_p(T) := \tilde{F}_p(T, 1)$, it follows from (2.8) that

$$\begin{aligned} \beta_p(T) = (1 + \eta)\Big(&\sum_{i=0}^{a_1-1} (i+1) p^i + \sum_{i=a_1}^{(a_1+a_2-\sigma)/2} (a_1 + 1) p^i \Big) \\ &+ p^{(a_1+a_2-\sigma+2)/2} (a_1 + 1) R_{\tilde{\xi}} \end{aligned} \tag{2.9}$$

where

$$R_{\tilde{\xi}} = \begin{cases} 0, & \text{if } \tilde{\xi} = 0 \\ 0, & \text{if } \tilde{\xi} = -1 \text{ and } a_3 \not\equiv a_2 \bmod 2; \\ a_3 - a_2 + 2\sigma - 3, & \text{if } \tilde{\xi} = 1; \\ 1, & \text{if } \tilde{\xi} = -1 \text{ and } a_3 \equiv a_2 \bmod 2. \end{cases}$$

2.13. If T is anisotropic we have $\alpha_p(T, H^2) = \beta_p(T) = 0$, as a three dimensional anisotropic space cannot be represented by a four-dimensional hyperbolic space. Alternatively this follows also from (2.9): By (2.4) we have $\eta = -1$ and hence it suffices to show that $R_{\tilde{\xi}} = 0$ if T is anisotropic. By 2.7 we are in one of the following two cases:

(a) $\tilde{\xi} = 0$;

(b) $\tilde{\xi} = -1$ and $a_2 \not\equiv a_3 \bmod 2$.

In both cases we have $R_{\tilde{\xi}} = 0$ by definition.

2.14. If T is isotropic, (2.9) gives Proposition 6.25 of [**GK**]:

Proposition 2.1. — *Let T be isotropic. Then:*

(1) *If $a_1 \not\equiv a_2 \bmod 2$, we have*

$$\beta_p(T) = 2\Big(\sum_{i=0}^{a_1-1}(i+1)p^i + \sum_{i=a_1}^{(a_1+a_2-\sigma)/2}(a_1+1)p^i\Big).$$

(2) *If $a_1 \equiv a_2 \bmod 2$ and $\tilde{\xi} = 1$, we have*

$$\beta_p(T) = 2\Big(\sum_{i=0}^{a_1-1}(i+1)p^i + \sum_{i=a_1}^{(a_1+a_2-\sigma)/2}(a_1+1)p^i\Big) + (a_1+1)(a_3-a_2+1)p^{(a_1+a_2)/2}.$$

(3) *If $a_1 \equiv a_2 \bmod 2$ and $\tilde{\xi} = -1$, we have*

$$\beta_p(T) = 2\Big(\sum_{i=0}^{a_1-1}(i+1)p^i + \sum_{i=a_1}^{(a_1+a_2-\sigma)/2}(a_1+1)p^i\Big) + (a_1+1)p^{(a_1+a_2)/2}.$$

Proof. — We have $\eta = 1$, and by 2.7 we are in one of the following cases:

(a) $a_1 \not\equiv a_2 \bmod 2$ and $\tilde{\xi} = 0$;

(b) $a_1 \not\equiv a_2 \bmod 2$, $\tilde{\xi} = 1$, and $a_3 = a_2 + 1$;

(c) $a_1 \equiv a_2 \bmod 2$ and $\tilde{\xi} = 1$;

(d) $a_1 \equiv a_2 \bmod 2$, $\tilde{\xi} = -1$, and $a_2 \equiv a_3 \bmod 2$.

In case (a), we have $R_{\tilde{\xi}} = 0$ by definition, and in case (b) we also have $R_{\tilde{\xi}} = a_3 - a_2 + 2\sigma - 3 = 0$. This proves (1).

In case (c), we have $R_{\tilde{\xi}} = a_3 - a_2 + 1$ and therefore (2).

In case (d), we have $R_{\tilde{\xi}} = 1$ which implies (3) □

Corollary 2.2. — *Set $\Delta(T) = \frac{1}{2}\det(2T) = 4\det(T)$ and assume that T is isotropic. Then $\beta_p(T) = 1$ if $\operatorname{ord}_p(\Delta(T)) = 0$.*

Proof. — For $p > 2$ the equality $\mathrm{ord}_p(\Delta(T)) = 0$ is equivalent to $a_1 = a_2 = a_3 = 0$ by definition of the Gross–Keating invariants (see 2.5). For $p = 2$ the condition $\mathrm{ord}_p(\Delta) = 0$ implies that we are in case (A1) of 2.6 with $\alpha = \beta = 0$ and $K = H$. Therefore we have again $a_1 = a_2 = a_3 = 0$. Hence the corollary follows for all p from Proposition 2.1. □

2.15. From now on we assume that T is anisotropic. We are going to calculate

$$f'_T(1) = \frac{\partial}{\partial X} f_T(X)_{|X=1}.$$

As T is anisotropic we have $\tilde{F}_p(T;1) = 0$ and therefore

$$f'_T(1) = \tilde{\gamma}_p(T,1)\frac{\partial}{\partial X}\tilde{F}_p(T;X)_{|X=1} \tag{2.10}$$

$$= (1-p^{-2})^2\frac{\partial}{\partial X}\tilde{F}_p(T;X)_{|X=1}. \tag{2.11}$$

Using (2.8) we see that

$$\frac{\partial}{\partial X}\tilde{F}_p(T;X)_{|X=1} = F_1 + F_2 + F_3.$$

Here

$$\begin{aligned} F_1 &= \sum_{i=0}^{a_1}\sum_{j=0}^{(a_1+a_2-\sigma)/2-i}(i+2j)p^{i+j} \\ &= \sum_{l=0}^{a_1-1}\frac{3}{2}(l+1)lp^l + \sum_{l=a_1}^{(a_1+a_2-\sigma)/2}(a_1+1)(2l-\frac{a_1}{2})p^l, \end{aligned}$$

and

$$\begin{aligned} F_2 &= -\sum_{i=0}^{a_1}\sum_{j=0}^{(a_1+a_2-\sigma)/2-i}(a_3+\sigma+i+2j)p^{(a_1+a_2-\sigma)/2-j} \\ &= -\sum_{i=0}^{a_1}\sum_{j=i}^{(a_1+a_2-\sigma)/2}(a_1+a_2+a_3+i-2j)p^j \\ &= -\sum_{l=0}^{a_1-1}(l+1)(a_1+a_2+a_3-\frac{3}{2}l)p^l \\ &\quad -\sum_{l=a_1}^{(a_1+a_2-\sigma)/2}(a_1+1)(\frac{3}{2}a_1+a_2+a_3-3l)p^l \end{aligned}$$

and hence

$$F_1 + F_2 = \sum_{l=0}^{a_1-1} (l+1)(3l - a_1 - a_2 - a_3)p^l + \sum_{l=a_1}^{(a_1+a_2-\sigma)/2} (a_1+1)(4l - 2a_1 - a_2 - a_3)p^l,$$

and

$$F_3 = p^{(a_1+a_2-\sigma+2)/2} \frac{a_1+1}{2} A_{\tilde{\xi}}$$

with

$$A_{\tilde{\xi}} = \begin{cases} 0, & \text{if } \tilde{\xi} = 0; \\ (a_3 - a_2 + 2\sigma - 3)(a_1 + a_2 + a_3), & \text{if } \tilde{\xi} = 1; \\ a_2 - a_3 - 2\sigma + 3, & \text{if } \tilde{\xi} = -1,\ a_2 \not\equiv a_3 \bmod 2; \\ 3a_3 - a_2 + a_1 + 4\sigma - 8, & \text{if } \tilde{\xi} = -1,\ a_2 \equiv a_3 \bmod 2. \end{cases}$$

2.16. We distinguish two cases. The first case is $a_1 \not\equiv a_2 \bmod 2$, *i.e.*, $\sigma = 1$. By 2.7 we either have $\tilde{\xi} = 0$ and hence $A_{\tilde{\xi}} = 0$ or we have $\tilde{\xi} = -1$ and $a_3 = a_2 + 1$ and hence again $A_{\tilde{\xi}} = 0$. Therefore we see that for $a_1 \not\equiv a_2 \bmod 2$ we have

$$\frac{\partial}{\partial X} \tilde{F}_p(T;X)_{|X=1} = \sum_{l=0}^{a_1-1} (l+1)(3l - a_1 - a_2 - a_3)p^l + \sum_{l=a_1}^{(a_1+a_2-1)/2} (a_1+1)(4l - 2a_1 - a_2 - a_3)p^l. \tag{2.12}$$

The second case is $a_1 \equiv a_2 \bmod 2$, *i.e.*, $\sigma = 2$. Then we have $a_3 \not\equiv a_2 \bmod 2$ and hence

$$\frac{\partial}{\partial X} \tilde{F}_p(T;X)_{|X=1} = \sum_{l=0}^{a_1-1} (l+1)(3l - a_1 - a_2 - a_3)p^l + \sum_{l=a_1}^{(a_1+a_2-2)/2} (a_1+1)(4l - 2a_1 - a_2 - a_3)p^l + p^{(a_1+a_2)/2} \frac{a_1+1}{2}(a_2 - a_3 - 1). \tag{2.13}$$

Therefore we see by [**R**, Theorem 1.1] that in either case

$$\frac{\partial}{\partial X} \tilde{F}_p(T;X)_{|X=1} = -\lg(\mathcal{O}_{\mathcal{T}_T,\xi}).$$

References

[B] I. I. Bouw – Invariants of ternary quadratic forms, this volume, p. 113–137.

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Inventiones Math.* **112** (1993), p. 225–245.

[Go2] U. Görtz – Arithmetic intersection numbers, this volume, p. 15–24.

[HS] Y. Hironaka & F. Sato – Local densities of representations of quadratic forms over p-adic integers (the non-dyadic case), *J. Number Theory* **83** (2000), no. 1, p. 106–136.

[Ka] H. Katsurada – An explicit formula for Siegel series, *Amer. J. Math.* **121** (1999), no. 2, p. 415–452.

[Ki] Y. Kitaoka – *Arithmetic of quadratic forms*, Cambridge University Press, 1993.

[R] M. Rapoport – Deformations of isogenies of formal groups, this volume, p. 139–169.

[RW] M. Rapoport & T. Wedhorn – The connection to Eisenstein series, this volume, p. 191–208.

[Wd1] T. Wedhorn – The genus of the endomorphisms of a supersingular elliptic curve, this volume, p. 25–47.

[Y1] T. Yang – Local densities of 2-adic quadratic forms, *J. Number Theory* **108** (2004), no. 2, p. 287–345.

T. Wedhorn, Institut für Mathematik der Universität Paderborn, Warburger Straße 100, 33098 Paderborn, Germany • *E-mail :* wedhorn@math.uni-paderborn.de
Url : www2.math.uni-paderborn.de/people/torsten-wedhorn.html

Astérisque
312, 2007, p. 191–208

16. THE CONNECTION TO EISENSTEIN SERIES

by

Michael Rapoport & Torsten Wedhorn

Abstract. — We consider the non-singular Fourier coefficients of the special value of the derivative of a Siegel-Eisenstein series of genus 3 and weight 2. We identify these coefficients with the arithmetic degrees of non-degenerate intersections of arithmetic modular correspondences.

***Résumé* (Relation avec les séries d'Eisenstein).** — Nous identifions les coefficients de Fourier non-dégénerés d'une valeur spéciale de la dérivée d'une série de Siegel-Eisenstein de genre 3 et de poids 2 avec les degrés arithmétiques des intersections de correspondances modulaires arithmétiques.

Introduction

In a previous chapter [**Go2**] an expression was obtained for the arithmetic intersection number of three modular correspondences $(\mathcal{T}_{m_1} \cdot \mathcal{T}_{m_2} \cdot \mathcal{T}_{m_3})$, when their intersection is of dimension 0. This expression is quite complicated, and involves certain local representation densities $\beta_\ell(Q)$ of quadratic forms and a local intersection multiplicity $\alpha_p(Q)$. It is this expression that is the main result of [**GK**]. However, already in the introduction to their paper, Gross and Keating mention that computations of S. Kudla and D. Zagier strongly suggest that the arithmetic intersection number $(\mathcal{T}_{m_1} \cdot \mathcal{T}_{m_2} \cdot \mathcal{T}_{m_3})$ agrees (up to a constant) with a Fourier coefficient of the restriction of the derivative at $s = 0$ of a Siegel-Eisenstein series of genus 3 and weight 2.

In the intervening years since the publication of [**GK**], Kudla has vastly advanced this idea and has in particular proved the analogue of this statement for the intersection of two Hecke correspondences on Shimura curves [**Ku3**]. In fact, Kudla has proposed a whole program which postulates a relation between special values of

2000 ***Mathematics Subject Classification.*** — 11E08, 11F30, 11F32, 11G18.
Key words and phrases. — Eisenstein series, local Whittaker functions, Siegel-Weil formula, local representation densities.

derivatives of Siegel-Eisenstein series and arithmetic intersection numbers of special cycles on Shimura varieties for orthogonal groups, comp. [**Ku4**].

The purpose of the present chapter is to sketch these ideas of Kudla and to derive from Kudla's various papers on the subject the statement alluded to in the introduction of [**GK**]. We stress that what we have done here is simply a task of compilation, since we do not (and cannot) claim to have mastered the automorphic side of the statement in question. We use the results of Katsurada [**Ka**] on local representation densities of quadratic forms, valid even for $p = 2$, to relate the local intersection multiplicities to the derivatives of certain local Whittaker functions, comp. [**Wd2**]. For $p \neq 2$ the corresponding calculations of representation densities are much older and are based on results of Kitaoka [**Kit**].

We thank S. Kudla for his help with this chapter.

1. Decomposition of the intersections of modular correspondences

1.1. To $m \in \mathbb{Z}_{>0}$ we have associated the Deligne-Mumford stack which parametrizes the category of isogenies of degree m between elliptic curves,

$$\mathcal{T}_m(S) = \{\, f\colon E \longrightarrow E' \mid \deg(f) = m \,\}.$$

Here E and E' are elliptic curves over S. Then $\mathcal{T}_m$ maps by a finite unramified morphism to the stack $\mathcal{M}^{(2)} = \mathcal{M} \times_{\operatorname{Spec}\mathbb{Z}} \mathcal{M}$ parametrizing pairs (E, E') of elliptic curves.

Let now $m_1, m_2, m_3 \in \mathbb{Z}_{>0}$ and consider

$$\mathcal{T}(m_1, m_2, m_3) = \{\, \mathbf{f} = (f_1, f_2, f_3) \mid f_i\colon E \longrightarrow E',\ \deg f_i = m_i \,\},$$

the fiber product of $\mathcal{T}_{m_1}, \mathcal{T}_{m_2}, \mathcal{T}_{m_3}$ over $\mathcal{M}^{(2)}$. Denoting by Q the degree quadratic form on $\operatorname{Hom}(E, E')$, we obtain a disjoint sum decomposition,

$$\mathcal{T}(m_1, m_2, m_3) = \coprod_T \mathcal{T}_T. \tag{1.1}$$

Here

$$\mathcal{T}_T(S) = \{\, \mathbf{f} \in \operatorname{Hom}_S(E, E')^3 \mid \frac{1}{2}(\mathbf{f}, \mathbf{f}) = T \,\},$$

where $(\mathbf{f}, \mathbf{f})$ denotes the matrix (a_{ij}) with $a_{ij} = (f_i, f_j) = Q(f_i + f_j) - Q(f_i) - Q(f_j)$. Note that, due to the positive definiteness of Q, the index set in (1.1) is $\operatorname{Sym}_3(\mathbb{Z})^\vee_{\geq 0}$, the set of positive semi-definite half-integral matrices.

Lemma 1.1. — *Let $T \in \operatorname{Sym}_3(\mathbb{Z})^\vee_{>0}$, i.e., T is positive definite. Then there exists a unique prime number p such that $\mathcal{T}_T$ is a finite scheme with support lying over the supersingular locus of $\mathcal{M}^{(2)}_p = \mathcal{M}^{(2)} \otimes_{\mathbb{Z}} \mathbb{F}_p$.*

Proof. — Let $(E, E') \in \mathcal{M}^{(2)}$ be in the image of $\mathcal{T}_T$. Since $\operatorname{Hom}(E, E')$ has rank at least 3, it follows that (E, E') has to be a pair of supersingular elliptic curves in some positive characteristic p. To see that p is uniquely determined by T, note that T is

represented by the quadratic space over $\mathbb{Q}$ corresponding to the definite quaternion algebra ramified in p. However, by [**Ku3**, Prop. 1.3], there is only one quadratic space with fixed discriminant which represents T. □

1.2. In this chapter we consider, for $T \in \mathrm{Sym}_3(\mathbb{Z})^\vee_{>0}$, the number

$$\widehat{\deg}(\mathcal{T}_T) = \lg(\mathcal{T}_T) \cdot \log p \ ,$$

where p is the unique prime in the statement of Lemma 1.1, and where

$$\lg(\mathcal{T}_T) = \sum_{\xi \in \mathcal{T}_T(\bar{\mathbb{F}}_p)} e_\xi^{-1} \cdot \lg(\mathcal{O}_{\mathcal{T}_T,\xi}),$$

with $e_\xi = |\operatorname{Aut}(\xi)|$. Our aim is to compare $\widehat{\deg}(\mathcal{T}_T)$ with the T^{th} Fourier coefficient of a certain Siegel-Eisenstein series of genus 3 and weight 2.

We first define a class of Eisenstein series, among which will be the one appearing in our main theorem.

2. Eisenstein series and the main theorem

2.1. Let B be a quaternion algebra over $\mathbb{Q}$. We denote by $V = V_B$ the quadratic space defined by B, *i.e.*, B with its norm form Q. We note that the idèle class character usually associated to a quadratic space, $x \mapsto (x, (-1)^{n(n-1)/2} \det(V))_{\mathbb{Q}}$ is in this case the trivial character χ_0 ($4 \mid n$, and $\det(V)$ is a square). Let $H = \mathrm{O}(V)$ be the associated orthogonal group. Let $W = \mathbb{Q}^6$, with standard symplectic form $\langle\ ,\ \rangle$ whose matrix with respect to the standard basis is given by $\left(\begin{smallmatrix} 0 & I_3 \\ -I_3 & 0 \end{smallmatrix}\right)$. Let $G = \mathrm{Sp}(W) = \mathrm{Sp}_6$, and denote by $P = M.N$ the Siegel parabolic subgroup, with

$$M = \{\, m(a) = \begin{pmatrix} a & 0 \\ 0 & {}^t a^{-1} \end{pmatrix} \mid a \in \mathrm{GL}_3 \,\},$$

$$N = \{\, n(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathrm{Sym}_3 \,\}.$$

Let $K = K_\infty.K_f = \prod_v K_v$ be the maximal compact subgroup of $G(\mathbb{A})$ with

$$K_v = \begin{cases} \mathrm{Sp}_6(\mathbb{Z}_p), & \text{if } v = p < \infty; \\ \{\, \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mid a + ib \in \mathrm{U}_3(\mathbb{R}) \,\}, & \text{if } v = \infty. \end{cases} \tag{2.1}$$

We have the Weil representation ω of $G(\mathbb{A}) \times H(\mathbb{A})$ (for the standard additive character ψ of $\mathbb{A}$ with archimedean component $\psi_\infty(x) = \exp(2\pi i x)$ and of conductor zero at all non-archimedean places) on the Schwartz space $\mathcal{S}(V(\mathbb{A})^3)$ (the action of the elements $P(\mathbb{A}) \times H(\mathbb{A})$ are given by simple formulae [**We**], comp. also (4.1) and (4.2) below). In the local version at a place v, we have a representation ω_v of $G(\mathbb{Q}_v) \times H(\mathbb{Q}_v)$ on $\mathcal{S}(V(\mathbb{Q}_v)^3)$.

We have the Iwasawa decomposition

$$G(\mathbb{A}) = P(\mathbb{A})K = N(\mathbb{A})M(\mathbb{A})K.$$

If $g = nm(a)k \in G(\mathbb{A})$, then

$$|a(g)| = |\det(a)|_{\mathbb{A}}$$

is well-defined. For a character χ of $\mathbb{A}^\times/\mathbb{Q}^\times$, we have the induced representation of $G(\mathbb{A})$, corresponding to $s \in \mathbb{C}$,

$$I(s,\chi) = \{\, \Phi\colon G(\mathbb{A}) \to \mathbb{C} \ K\text{-finite function} \mid \Phi(nm(a)g) = \chi(\det(a)) \cdot |a(g)|^{s+2} \cdot \Phi(g) \,\}.$$

For $\varphi \in \mathcal{S}(V(\mathbb{A})^3)$, we set

$$\Phi(g,s) = (\omega(g)\varphi)(0) \cdot |a(g)|^s.$$

In this way, we obtain an intertwining map

$$\mathcal{S}(V(\mathbb{A})^3) \longrightarrow I(0,\chi_0), \quad \varphi \longmapsto \Phi(g,0)\ . \tag{2.2}$$

Note that $|a(g)|$ is a right K-invariant function on $G(\mathbb{A})$, so $\Phi(g,s)$ is a standard section of the induced representation, *i.e.*, its restriction to K is independent of s. We will also need the local version $I(s,\chi_v)$ of the induced representation at a place v and the $G(\mathbb{Q}_v)$-equivariant map

$$\mathcal{S}(V_v^3) \longrightarrow I(0,\chi_{0,v}). \tag{2.3}$$

2.2. Returning to the global situation, we consider the Eisenstein series associated to $\varphi \in \mathcal{S}(V(\mathbb{A})^3)$,

$$E(g,s,\Phi) = \sum_{\gamma \in P(\mathbb{Q})\backslash G(\mathbb{Q})} \Phi(\gamma g, s).$$

This series is absolutely convergent for $\mathrm{Re}(s) > 2$, and defines an automorphic form. It has a meromorphic continuation and a functional equation with $s = 0$ as its center of symmetry.

We will now make a specific choice of Φ which will define an *incoherent* Eisenstein series. Let $B = \mathrm{M}_2(\mathbb{Q})$ and let $V(\mathbb{Z}_p) = \mathrm{M}_2(\mathbb{Z}_p)$ for any p. We let $\varphi_f = \otimes\varphi_p = \otimes\,\mathrm{char}\, V(\mathbb{Z}_p)$, and let $\Phi_f = \otimes\Phi_p$ be the corresponding factorizable standard section. For Φ_∞ we take the standard section uniquely determined by

$$\Phi_\infty(k,0) = \det(\underline{k})^2,$$

where $k \in K_\infty$ is the image of $\underline{k} \in \mathrm{U}_3(\mathbb{R})$ under the natural identification in (2.1). Then by [**Ku3**, (7.13)], Φ_∞ is the image of the Gaussian φ_∞ under the local map (2.3) for $v = \infty$, where the local quadratic space is V_∞^+, the positive-definite quadratic space corresponding to the Hamilton quaternion algebra over $\mathbb{R}$, and where

$$\varphi_\infty(x) = \exp(-\pi\ \mathrm{tr}(x,x)), \quad x \in (V_\infty^+)^3. \tag{2.4}$$

Since $V_\infty^+ \otimes V(\mathbb{A}_f)$ does not correspond to a quaternion algebra over $\mathbb{Q}$, the standard section $\Phi = \Phi_\infty \otimes \Phi_f$ is *incoherent* in the sense of *loc. cit.*, and hence (*loc. cit.*, Theorem 2.2),

$$E(g, 0, \Phi) \equiv 0.$$

Consider the Fourier expansion of $E(g, s, \Phi)$,

$$E(g, s, \Phi) = \sum_{T \in \mathrm{Sym}_3(\mathbb{Q})} E_T(g, s, \Phi),$$

where

$$E_T(g, s, \Phi) = \int_{N(\mathbb{Q})\backslash N(\mathbb{A})} E(ng, s, \Phi) \cdot \psi_T(n)^{-1} dn,$$

with

$$\psi_T(n(b)) = \psi(\mathrm{tr}(Tb)), \quad b \in \mathrm{Sym}_3(\mathbb{A}). \tag{2.5}$$

For $T \in \mathrm{Sym}_3(\mathbb{Q})$ with $\det(T) \neq 0$, the Fourier coefficient has an explicit expression as a product

$$E_T(g, s, \Phi) = \prod_v W_{T,v}(g_v, s, \Phi_v), \tag{2.6}$$

see [**Ku3**, (4.4)]. Here $W_{T,v}(g_v, s, \Phi_v)$ is the local Whittaker function, cf. section 5. The local Whittaker functions are entire (cf. [**Ku3**, (4.2) and (4.3)]), and the product (2.6) is absolutely convergent and holomorphic in $s = 0$. More precisely, for $\mathrm{Re}(s) > 2$, the identity (2.6) holds and for almost all places p, the local factor at p on the right hand side equals $\zeta_p(s+2)^{-1} \cdot \zeta_p(2s+2)^{-1} = (1 - p^{-s-2}) \cdot (1 - p^{-2s-2})$, and for all places the local factor is an entire function.

2.3. For $T \in \mathrm{Sym}_3(\mathbb{Q})_{>0}$, let

$$\mathrm{Diff}(T, V) = \{\, p \mid T \text{ not represented by } V(\mathbb{Q}_p) \,\}.$$

Then the cardinality $|\mathrm{Diff}(T, V)|$ is odd, cf. [**Ku3**, Cor. 5.2]. Moreover we have $W_{T,p}(g_p, 0, \Phi_p) \equiv 0$ for $p \in \mathrm{Diff}(T, V)$, cf. [**Ku3**, Prop. 1.4]. On the other hand, $W_{T,\infty}(g_\infty, 0, \Phi_\infty) \neq 0$, cf. [**Ku3**, Prop. 9.5]. Hence

$$\operatorname*{ord}_{s=0} E_T(g, s, \Phi) \geq |\mathrm{Diff}(T, V)|.$$

In particular, if $E_T'(g, 0, \Phi) \neq 0$, then $\mathrm{Diff}(T, V) = \{p\}$ for a unique prime number p.

2.4. We may now formulate our main theorem.

Theorem 2.1. — *Let $V = \mathrm{M}_2(\mathbb{Q})$ and let $\Phi = \Phi_\infty \otimes \Phi_f$ be the incoherent standard section as above. Let $T \in \mathrm{Sym}_3(\mathbb{Q})_{>0}$ with $\mathrm{Diff}(T, V) = \{p\}$.*

(i) *If $T \notin \mathrm{Sym}_3(\mathbb{Z})^\vee$, then $\mathcal{T}_T = \varnothing$ and $\widehat{\deg}(\mathcal{T}_T) = 0$ and $E_T'(g, 0, \Phi) \equiv 0$.*

(ii) *Let* $T \in \mathrm{Sym}_3(\mathbb{Z})^\vee$. *Then* $\mathcal{T}_T$ *has support in characteristic* p. *For* $g = (g_\infty, e, e \dots) \in G(\mathbb{A})$ *with*

$$g_\infty = \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} y^{1/2} & \\ & y^{-1/2} \end{pmatrix}, \qquad x, y \in \mathrm{Sym}_3(\mathbb{R}), y > 0,$$

let $\tau = g_\infty \cdot i1_3 = x + iy \in \mathfrak{H}_3$. *Then*

$$\det(y)\, \widehat{\deg}(\mathcal{T}_T) \cdot q^T = \kappa \cdot E_T'(g, 0, \Phi),$$

where $q^T = \exp(2\pi i \operatorname{tr}(T\tau))$ *and where the negative constant* κ *is independent of* T.

Here $\mathfrak{H}_3 = \{ \tau \in \mathrm{Sym}_3(\mathbb{C}) \mid \mathrm{Im}(\tau) > 0 \}$ is the Siegel upper half space.

The proof of the theorem consists in calculating explicitly both sides of the identity. The first assertion of (i) is obvious and the second is a consequence of section 5 below, where the local Whittaker functions are related to local representation densities (see Proposition 5.2 below). The proof of (ii) will be reduced in section 3 to a statement about local Whittaker functions which will be taken up in sections 4 and 5.

2.5. In the rest of this section we relate the adelic Eisenstein series to the classical Siegel-Eisenstein series, following [**Ku1**, section IV.2]. By strong approximation,

$$G(\mathbb{A}) = G(\mathbb{Q})G(\mathbb{R})K.$$

By our choice of Φ, which is right K_f-invariant, the Eisenstein series $E(g, s, \Phi)$ is determined by its restriction to $G(\mathbb{R})$ (embedded *via* $g_\infty \mapsto (g_\infty, e, e \dots)$ in $G(\mathbb{A})$).

We have

$$G(\mathbb{Z}) = G(\mathbb{Q}) \cap (G(\mathbb{R}).K_f).$$

Also, $P(\mathbb{Q})\backslash G(\mathbb{Q}) = P(\mathbb{Z})\backslash G(\mathbb{Z})$, hence for $g = g_\infty$,

$$\begin{aligned} E(g, s, \Phi) &= \sum_{\gamma \in P(\mathbb{Q})\backslash G(\mathbb{Q})} \Phi_\infty(\gamma g_\infty, s) \cdot \Phi_f(\gamma, s) \\ &= \sum_{\gamma \in P(\mathbb{Z})\backslash G(\mathbb{Z})} \Phi_\infty(\gamma g_\infty, s). \end{aligned} \tag{2.7}$$

For our choice of Φ_∞ and of $g_\infty = \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} y^{1/2} & \\ & y^{-1/2} \end{pmatrix}$, we have

$$\Phi_\infty(\gamma g_\infty, s) = \det(y)^{\frac{s}{2}+1} \cdot \det(c\tau + d)^{-2} \cdot |\det(c\tau + d)|^{-s},$$

where

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_6(\mathbb{Z}).$$

Inserting this expression into the sum (2.7), one obtains from [**Ku1**, IV.2.23], (for $\ell = \rho_n = 2$),

$$E(g, s, \Phi) = \det(y) \cdot E_{\mathrm{class}}(\tau, s), \tag{2.8}$$

where

$$E_{\text{class}}(\tau, s) = \det(y)^{s/2} \sum_{(c,d)} \det(c\tau + d)^{-2} \cdot |\det(c\tau + d)|^{-s}$$

is the classical Siegel Eisenstein series (the sum here ranges over a complete set of representatives of the equivalence classes of pairs of co-prime symmetric integer matrices).

2.6. Using the comparison (2.8) between the adelic and the classical Eisenstein series, we obtain from Theorem 2.1 the following statement. We consider the Fourier expansion of the classical Eisenstein series,

$$E_{\text{class}}(\tau, s) = \sum_{T \in \text{Sym}_3(\mathbb{Z})^\vee} c(T, y, s)\, q^T.$$

Here $\tau = x + iy \in \mathfrak{H}_3$ and $q^T = \exp(2\pi i \ \text{tr}(T\tau))$.

Theorem 2.2. — *Let $T \in \text{Sym}_3(\mathbb{Z})^\vee_{>0}$.*
(1) *Then $c'(T) = (\frac{\partial}{\partial s} c(T, y, s))_{|s=0}$ is independent of y.*
(2) *If $\text{Diff}(T, V) = \{p\}$, then $\mathcal{T}_T$ has support in characteristic p and*

$$\widehat{\deg}(\mathcal{T}_T) = \kappa \cdot c'(T)$$

for a negative constant κ independent of T.

Corollary 2.3. — *Assume that there is no positive definite binary quadratic form over $\mathbb{Z}$ which represents m_1, m_2 and m_3, so that the divisors $\mathcal{T}_{m_1}$, $\mathcal{T}_{m_2}$, and $\mathcal{T}_{m_3}$ intersect in dimension 0, cf.* [**Go2**, Prop. 3.2]. *Then there exists a constant κ independent of (m_1, m_2, m_3) such that*

$$(\mathcal{T}_{m_1} \cdot \mathcal{T}_{m_2} \cdot \mathcal{T}_{m_3}) = \kappa \cdot \sum_{\substack{T \in \text{Sym}_3(\mathbb{Z})^\vee_{>0} \\ \text{diag}(T) = (m_1, m_2, m_3)}} c'(T)$$

Proof. — The hypothesis implies that in the disjoint sum (1.1) only positive definite $T \in \text{Sym}_3(\mathbb{Z})^\vee$ occur as indices, comp. [**Go2**, Prop. 3.5]. Therefore the assertion follows from Theorem 2.2. □

3. Use of the Siegel-Weil formula

3.1. Let $\tilde{V}$ be the quadratic space associated to a quaternion algebra $\tilde{B}$ over $\mathbb{Q}$. For $\tilde{\varphi} \in \mathcal{S}(\tilde{V}(\mathbb{A})^3)$, there is the theta series

$$\theta(g, h; \tilde{\varphi}) = \sum_{x \in \tilde{V}(\mathbb{Q})^3} (\omega(g)\tilde{\varphi})(h^{-1}x),$$

and the corresponding theta integral over the orthogonal group $\tilde{H} = \mathrm{O}(\tilde{V})$ associated to $\tilde{V}$,

$$I(g;\tilde{\varphi}) = \int_{\tilde{H}(\mathbb{Q})\backslash\tilde{H}(\mathbb{A})} \theta(g,h;\tilde{\varphi})\,dh.$$

Here the Haar measure dh is normalized so that

$$\mathrm{vol}(\tilde{H}(\mathbb{Q})\backslash\tilde{H}(\mathbb{A})) = 1.$$

We will only consider the case in which the quadratic space $\tilde{V}$ is anisotropic. If $\tilde{\varphi}$ is K-finite, then $I(g;\tilde{\varphi})$ is an automorphic form on $G(\mathbb{A})$. The Siegel-Weil formula [**KR**] states that, if $\tilde{\varphi}$ gives rise to $\tilde{\Phi}$ *via* the map (2.2), then

$$E(g,0,\tilde{\Phi}) = 2\cdot I(g;\tilde{\varphi}). \tag{3.1}$$

Let $T \in \mathrm{Sym}_3(\mathbb{Q})$ with $\det(T) \neq 0$. Then the T^{th}-Fourier coefficient of $I(g;\tilde{\varphi})$ is equal to ([**KR**, (6.21)])

$$I_T(g;\tilde{\varphi}) = \int_{\tilde{H}(\mathbb{Q})\backslash\tilde{H}(\mathbb{A})} \sum_{x\in\tilde{V}(\mathbb{Q})^3_T} (\omega(g)\tilde{\varphi})(h^{-1}x)\,dh$$

where

$$\tilde{V}(\mathbb{Q})^3_T = \{\, x\in\tilde{V}(\mathbb{Q})^3 \mid \frac{1}{2}(x,x) = T \,\}.$$

3.2. We now return to the situation considered in Theorem 2.1. Let $V = \mathrm{M}_2(\mathbb{Q})$ and let Φ be the standard section defined in the previous section. We also fix $T \in \mathrm{Sym}_3(\mathbb{Q})_{>0}$ with $\mathrm{Diff}(T,V) = \{p\}$. Let $\tilde{V}$ be the quadratic space associated to the definite quaternion algebra $\tilde{B} = B^{(p)}$ ramified at p, and unramified at all other finite primes. Note that $\tilde{V}(\mathbb{R}) = V^+_\infty$. We consider the standard section $\tilde{\Phi}$ which is the image of $\tilde{\varphi} = \tilde{\varphi}_\infty \otimes \tilde{\varphi}^p_f \otimes \tilde{\varphi}_p$ under

$$\mathcal{S}(\tilde{V}(\mathbb{A})^3) \longrightarrow I(0,\chi_0),$$

where $\tilde{\varphi}^p_f = \varphi^p_f$, where $\tilde{\varphi}_\infty = \varphi_\infty$ is the Gaussian (2.4) and where $\tilde{\varphi}_p = \mathrm{char}\,\tilde{V}(\mathbb{Z}_p)^3$, with $\tilde{V}(\mathbb{Z}_p)$ the maximal order of the division algebra $B^{(p)}\otimes\mathbb{Q}_p$. Hence $\tilde{\Phi}_\infty = \Phi_\infty$, $\tilde{\Phi}^p_f = \Phi^p_f$ and $\tilde{\Phi}$ is a *coherent* standard section. Comparing the expressions (2.6) for the Fourier coefficients of $E(g,s,\Phi)$ and $E(g,s,\tilde{\Phi})$, we can write, for $g = g_\infty \in G(\mathbb{R})$,

$$E'_T(g,0,\Phi) = \frac{W'_{T,p}(e,0,\Phi_p)}{W_{T,p}(e,0,\tilde{\Phi}_p)}\cdot E_T(g,0,\tilde{\Phi}).$$

We refer to Corollary 5.3 below for a proof of the fact that the denominator here is nonzero. Using the Siegel-Weil formula (3.1) for the anisotropic quadratic space $\tilde{V}$, we can rewrite this as

$$E'_T(g,0,\Phi) = 2\cdot\frac{W'_{T,p}(e,0,\Phi_p)}{W_{T,p}(e,0,\tilde{\Phi}_p)}\cdot I_T(g;\tilde{\varphi}). \tag{3.2}$$

Now the function $\tilde{\varphi}_\infty$ is invariant under $\tilde{H}(\mathbb{R})$. For

$$g_\infty = \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} y^{1/2} & \\ & y^{-1/2} \end{pmatrix}, \qquad x, y \in \mathrm{Sym}_3(\mathbb{R}), y > 0,$$

the value of $\omega(g_\infty)\tilde{\varphi}_\infty$ at $t \in \tilde{V}(\mathbb{R})^3$ with $\frac{1}{2}(t,t) = T$ is equal to

$$(\omega(g_\infty)\tilde{\varphi}_\infty)(t) = \exp(2\pi i \operatorname{tr}(T\tau)) \det(y).$$

Since $\tilde{H}(\mathbb{R}) = \mathrm{O}(\tilde{V}(\mathbb{R}))$ is compact, we may write using the product measure $dh = d_\infty h \times d_f h$,

$$2 \cdot I_T(g; \tilde{\varphi}) = 2 \det(y) \cdot q^T \cdot \mathrm{vol}(\tilde{H}(\mathbb{R}), d_\infty h) \cdot I_T(\tilde{\varphi}_f), \tag{3.3}$$

where

$$I_T(\tilde{\varphi}_f) = \int\limits_{\tilde{H}(\mathbb{Q})\backslash \tilde{H}(\mathbb{A}_f)} \sum_{x \in \tilde{V}(\mathbb{Q})^3_T} \tilde{\varphi}_f(h^{-1}x)\, d_f h.$$

3.3. Let

$$\tilde{H}' = \{\, \tilde{g} = (g, g') \in \tilde{B}^\times \times \tilde{B}^\times \mid \mathrm{Nm}(g) = \mathrm{Nm}(g') \,\}.$$

Then $\tilde{H}'$ acts on $\tilde{V}$ *via*

$$\tilde{g} \cdot x = (g, g') \cdot x = g' x g^{-1}.$$

This induces an exact sequence, where $\mathbb{G}_m$ lies in the center of $\tilde{H}'$, cf. [**Wd1**, Lemma 1.6],

$$1 \to \mathbb{G}_m \to \tilde{H}' \xrightarrow{\mathrm{pr}} \mathrm{SO}(\tilde{V}) \to 1. \tag{3.4}$$

We fix the Haar measure on $\tilde{H}'(\mathbb{A})$ such that the measure induced by the exact sequence (3.4) on $\mathrm{SO}(\tilde{V})(\mathbb{A})$ is the Tamagawa measure, and with the standard Haar measure on the central idele group $\mathbb{A}^\times$ which is the product of the local measures $\lambda_\ell \frac{dx_\ell}{|x_\ell|}$ with convergence factors $\lambda_\ell = 1 - \ell^{-1}$, so that $\mathrm{vol}(\hat{\mathbb{Z}}^\times) = 1$. Let

$$\tilde{K}' = \tilde{H}'(\mathbb{A}_f) \cap ((O_{\tilde{B}} \otimes \hat{\mathbb{Z}})^\times \times (O_{\tilde{B}} \otimes \hat{\mathbb{Z}})^\times).$$

Proposition 3.1. — *Let*

$$|\mathcal{T}_T| = \sum_{\xi \in \mathcal{T}_T(\mathbb{F}_p)} e_\xi^{-1}$$

with $e_\xi = |\operatorname{Aut}(\xi)|$. *Then*

$$|\mathcal{T}_T| = \kappa_1 \cdot I_T(\tilde{\varphi}_f),$$

where $\kappa_1 = 2\ \mathrm{vol}(\tilde{K}')^{-1}$.

Proof. — We choose a finite set of double coset representatives $h_j \in \tilde{H}'(\mathbb{A}_f)$ such that

$$\tilde{H}'(\mathbb{A}_f) = \coprod_j \tilde{H}'(\mathbb{Q}) h_j \tilde{K}'.$$

Since each double coset $\tilde{H}'(\mathbb{Q})h_j\tilde{K}'$ is stable under $\widehat{\mathbb{Z}}^\times\mathbb{Q}^\times = \mathbb{A}_f^\times$, we obtain a disjoint decomposition,

$$\mathrm{SO}(\tilde{V})(\mathbb{A}_f) = \coprod_j \mathrm{SO}(\tilde{V})(\mathbb{Q})\mathrm{pr}(h_j)\mathrm{pr}(\tilde{K}').$$

Let

$$\tilde{\Gamma}'_j = \tilde{H}'(\mathbb{Q}) \cap h_j\tilde{K}'h_j^{-1}.$$

Note that $\mathrm{vol}(\mathrm{SO}(\tilde{V})(\mathbb{Q})\backslash\mathrm{SO}(\tilde{V})(\mathbb{A})) = 2$. We have

$$\tilde{H}(\mathbb{A}_f) = \mathrm{SO}(\tilde{V})(\mathbb{A}_f) \rtimes \mu_2(\mathbb{A}_f).$$

Hence

$$\begin{aligned}
1 &= \mathrm{vol}(\mathrm{O}(\tilde{V})(\mathbb{Q})\backslash\mathrm{O}(\tilde{V})(\mathbb{A})) \\
&= \frac{1}{2}\mathrm{vol}(\mathrm{SO}(\tilde{V})(\mathbb{Q})\backslash\mathrm{O}(\tilde{V})(\mathbb{A})) \\
&= \frac{1}{2}\mathrm{vol}(\mathrm{SO}(\tilde{V})(\mathbb{Q})\backslash\mathrm{SO}(\tilde{V})(\mathbb{A}))\,\mathrm{vol}(\mu_2(\mathbb{A})) \\
&= \mathrm{vol}(\mu_2(\mathbb{A}))
\end{aligned}$$

and therefore

$$\mathrm{vol}(\mu_2(\mathbb{Q})\backslash\mu_2(\mathbb{A})) = \frac{1}{2}.$$

Let us normalize the Haar measure on $\mu_2(\mathbb{R})$ by $\mathrm{vol}(\mu_2(\mathbb{R})) = 1$. Then we get $\mathrm{vol}(\mu_2(\mathbb{Q})\backslash\mu_2(\mathbb{A}_f)) = \frac{1}{2}$. Then we obtain as in [**Ku3**, (7.28)],

$$\begin{aligned}
I_T(\tilde{\varphi}_f) &= \int_{\mathrm{SO}(\tilde{V})(\mathbb{Q})\backslash\mathrm{SO}(\tilde{V})(\mathbb{A}_f)} \int_{\mu_2(\mathbb{Q})\backslash\mu_2(\mathbb{A}_f)} \sum_{x\in\tilde{V}(\mathbb{Q})_T^3} \tilde{\varphi}_f(h^{-1}cx)\,d_fh\,dc \\
&= \frac{1}{2}\int_{\mathrm{SO}(\tilde{V})(\mathbb{Q})\backslash\ \mathrm{SO}(\tilde{V})(\mathbb{A}_f)} \sum_{x\in\tilde{V}(\mathbb{Q})_T^3} \tilde{\varphi}_f(h^{-1}x)\,d_fh \\
&= \frac{1}{2}\sum_j \int_{\mathrm{SO}(\tilde{V})(\mathbb{Q})\backslash\mathrm{SO}(\tilde{V})(\mathbb{Q})\mathrm{pr}(h_j)\mathrm{pr}(\tilde{K}')} \sum_{x\in\tilde{V}(\mathbb{Q})_T^3} \tilde{\varphi}_f(h^{-1}x)\,d_fh \\
&= \frac{1}{2}\cdot\mathrm{vol}(\mathrm{pr}(\tilde{K}'))\cdot\sum_j \sum_{x\in\tilde{V}(\mathbb{Q})_T^3} \frac{1}{|\tilde{\Gamma}_{j,x}|}\cdot\tilde{\varphi}_f(h_j^{-1}x).
\end{aligned}$$

Here $\tilde{\Gamma}_{j,x}$ is the image of $\tilde{\Gamma}'_{j,x}$ in $\mathbb{Q}^\times\backslash\tilde{H}'(\mathbb{Q}) = \mathrm{SO}(\tilde{V})(\mathbb{Q})$. Therefore we have $|\tilde{\Gamma}_{j,x}| = \frac{1}{2}\cdot|\tilde{\Gamma}'_{j,x}|$. Note that $\tilde{\Gamma}_{j,x}$ is trivial since x spans a three-dimensional subspace of the 4-dimensional space $\tilde{V}$.

To make the connection with $\mathcal{T}_T$, note that the supersingular locus of $\mathcal{M}_p^{(2)}$ can be written as a double coset space (cf. [**Mi**, 6]),

$$(\mathcal{M}^{(2)})^{ss} = \tilde{H}'(\mathbb{Q})\backslash\tilde{H}'(\mathbb{A}_f)/\tilde{K}'.$$

Here we chose (E_0, E_0) as a base point, such that $\tilde{K}'$ is the stabilizer of the Tate module $\hat{T}(E_0) \times \hat{T}(E_0)$ (completed by the Dieudonné module at p). To $\tilde{g} = (g, g') \in \tilde{H}'(\mathbb{A}_f)$ corresponds $E_g \times E_{g'}$ with the diagonal isogeny,

$$(g, g') \colon E_0 \times E_0 \longrightarrow E_g \times E_{g'}.$$

The lattice $\mathrm{Hom}(E_g, E_{g'})$ in $\tilde{V}(\mathbb{Q}) = \mathrm{Hom}(E_0, E_0) \otimes \mathbb{Q}$ is given by

$$\begin{aligned}\mathrm{Hom}(E_g, E_{g'}) &= \{\, y \in \tilde{B} \mid yg(\hat{T}(E_0)) \subset g'\hat{T}(E_0) \,\} \\ &= \{\, y \in \tilde{B} \mid g'^{-1}yg \in \tilde{V}(\hat{\mathbb{Z}}) \,\} \\ &= \{\, y \in \tilde{B} \mid \tilde{g}^{-1}y \in \tilde{V}(\hat{\mathbb{Z}}) \,\}.\end{aligned}$$

Hence we obtain

$$\begin{aligned}|\mathcal{T}_T| &= \sum_{[y,\tilde{g}] \in \tilde{H}'(\mathbb{Q}) \backslash (\tilde{V}^3(\mathbb{Q})_T \times \tilde{H}'(\mathbb{A}_f)/\tilde{K})} \tilde{\varphi}_f(\tilde{g}^{-1} \cdot y) \\ &= \sum_j \sum_{x \in \tilde{V}^3(\mathbb{Q})_T} \tilde{\varphi}_f(h_j^{-1} \cdot x) \\ &= 2 \cdot \mathrm{vol}(\mathrm{pr}(\tilde{K}'))^{-1} \cdot I_T(\tilde{\varphi}_f).\end{aligned}$$

Since $\mathrm{vol}(\tilde{K}') = \mathrm{vol}(\mathrm{pr}(\tilde{K}'))$, the result follows. □

3.4. The next result will be proved in section 5.6.

Theorem 3.2. — *The lengths of the local rings $\mathcal{O}_{\mathcal{T}_{T,\xi}}$ at all points $\xi \in \mathcal{T}_T(\bar{\mathbb{F}}_p)$ are all equal to*

$$\lg(\mathcal{O}_{\mathcal{T}_{T,\xi}}) = -\frac{2}{(p-1)^2} \cdot \frac{W'_{T,p}(e, 0, \Phi_p)}{W_{T,p}(e, 0, \tilde{\Phi}_p)} \cdot (\log p)^{-1}.$$

3.5. We will now prove Theorem 2.1 using Theorem 3.2. Let

$$\begin{aligned}H' &= \{\tilde{g} = (g, g') \in \mathrm{GL}_2 \times \mathrm{GL}_2 \mid \det(g) = \det(g')\}, \\ K' &= H'(\mathbb{A}_f) \cap (\mathrm{GL}_2(\hat{\mathbb{Z}}) \otimes \mathrm{GL}_2(\hat{\mathbb{Z}})).\end{aligned}$$

Then $\tilde{H}'$ is an inner form of H'.

We now fix Haar measures on $\tilde{H}'(\mathbb{A})$ and on $H'(\mathbb{A})$ following [**Ku3**, p. 573]. More precisely, in *loc. cit.* Kudla defines for any quaternion algebra B over $\mathbb{Q}$ a Haar measure on $(B \otimes \mathbb{A})^\times$ which is decomposed, *i.e.*, the explicit product of local Haar measures on $(B \otimes \mathbb{Q}_v)^\times$ for all places v. By our fixed choice of Haar measure on $\mathbb{A}^\times$, we therefore also obtain a decomposed Haar measure on $H(B)'(\mathbb{A})$, where

$$H(B)' = \{\tilde{g} = (g, g') \in B^\times \times B^\times \mid \mathrm{Nm}(g) = \mathrm{Nm}(g')\}.$$

By *loc. cit.*, the induced Haar measure on $SO(V(B))(\mathbb{A})$ is the Tamagawa measure, as required above.

We apply this construction to $B = \mathrm{M}_2(\mathbb{Q})$ and to $B = \tilde{B} = B^{(p)}$, the definite quaternion algebra, ramified at p and unramified at all other finite places. Then we have for these Haar measures (comp. [**Ku3**, Lemma 14.10]),

$$\frac{\mathrm{vol}(K'_p)}{\mathrm{vol}(\tilde{K}'_p)} = (p-1)^2$$

and

$$\frac{\mathrm{vol}(K')}{\mathrm{vol}(\tilde{K}')} = (p-1)^2.$$

Hence

$$\begin{aligned} q^T \cdot \widehat{\deg}(\mathcal{T}_T) &= q^T \ \lg(\mathcal{O}_{\mathcal{T}_T}) \cdot \log p \\ &= q^T \ \lg(\mathcal{O}_{\mathcal{T}_{T,\xi}}) \cdot |\mathcal{T}_T| \cdot \log p \\ &= -\frac{2}{(p-1)^2 \cdot \mathrm{vol}(\tilde{K}')} \cdot 2 \cdot \frac{W'_{T,p}(e,0,\Phi_p)}{W_{T,p}(e,0,\tilde{\Phi}_p)} \cdot q^T \cdot I_T(\tilde{\varphi}_f) \\ &= -\frac{2}{\mathrm{vol}(K')} \cdot E'_T(g,0,\Phi) \det(y)^{-1} \ v^{-1}, \end{aligned}$$

where we used (3.2) and (3.3) in the last step, and where $v = \mathrm{vol}(\tilde{H}(\mathbb{R}), d_\infty h)$. This proves the main theorem with the negative constant $\kappa = -\frac{2}{\mathrm{vol}(K')} \cdot v^{-1}$.

4. The Weil representation

4.1. The remainder of this chapter is devoted to the proof of Theorem 3.2. This is a purely local statement.

We fix a prime number p and change our notation: We replace V by $V \otimes \mathbb{Q}_p$, G by $G \otimes \mathbb{Q}_p$, ψ by its localization ψ_p (of conductor zero), etc. At the same time we consider a more general situation.

4.2. Instead of the quadratic space associated to a quaternion algebra, we now let V be any $\mathbb{Q}_p$-vector space and $(\ ,\ )$ a symmetric nondegenerate bilinear form on V. Then $Q(x) = \frac{1}{2}(x,x)$ is a quadratic form on V.

We assume that $n := \dim(V)$ is even. In fact, we will only need the case $V = B \perp H^r$ where B is a quaternion algebra over $\mathbb{Q}_p$ endowed with the reduced norm, and where H^r is the orthogonal sum of r copies of the hyperbolic plane H.

We denote by $\det(V)$ the image in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ of the determinant of the matrix $((v_i,v_j))_{ij}$ where $(v_1,\dots,v_n)$ is some basis of V. As in 2.1 we have the quadratic character χ_V of $\mathbb{Q}_p^\times$ associated to V given by

$$\chi_V(x) = (x, (-1)^{n(n-1)/2} \det(V))_p = (x, (-1)^{n/2} \det((v_i,v_j))_{ij})_p,$$

where $(\ ,\ )_p$ denotes the Hilbert symbol.

4.3. Let $(W, \langle\ ,\ \rangle)$ be the space $\mathbb{Q}_p^{2m}$ endowed with the standard symplectic form whose matrix with respect to the standard basis is given by $\left(\begin{smallmatrix} 0 & I_m \\ -I_m & 0 \end{smallmatrix}\right)$. We consider W as vector space of row vectors, in particular the canonical GL_{2m}-action is from the right. To prove Theorem 3.2 we will need only the case $m = 3$.

As in 2.1 we denote by $P = MN$ the Siegel parabolic subgroup of $G = \mathrm{Sp}_{2m}(\mathbb{Q}_p)$ over $\mathbb{Q}_p$ where

$$M = \{\, m(a) = \begin{pmatrix} a & 0 \\ 0 & {}^t a^{-1} \end{pmatrix} \mid a \in \mathrm{GL}_m(\mathbb{Q}_p) \,\},$$

$$N = \{\, n(b) = \begin{pmatrix} I_m & b \\ 0 & I_m \end{pmatrix} \mid b \in \mathrm{Sym}_m(\mathbb{Q}_p) \,\}.$$

Let $K = \mathrm{Sp}_{2m}(\mathbb{Z}_p) \subset G$ the standard maximal compact subgroup and set

$$w := \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix} \in G.$$

4.4. In the sequel we let $a \in \mathrm{GL}_m$ act on $V^m = V \otimes \mathbb{Q}_p^m$ via right multiplication, which we denote by $x \mapsto xa$.

Moreover for $x, y \in V^m$ we set

$$(x, y) := ((x_i, y_j))_{ij} \in \mathrm{Sym}_m(\mathbb{Q}_p).$$

4.5. Associated to the quadratic space V and the fixed additive character ψ there is a Weil representation ω_V of G on the vector space $\mathcal{S}(V^m)$ of Schwartz functions on V^m. For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, $\varphi \in \mathcal{S}(V^m)$, and $x \in V^m$ we have by [**Ku2**, Prop. 4.3] (cf. also [**Rao**, Lemma 3.2], and [**We**]),

$$(\omega_V(g)(\varphi))(x) = \gamma(V, \psi, g) \cdot \int_{V^m/\mathrm{Ker}(c)} \psi(\mathrm{tr}(\frac{1}{2}(xa, xb) + (xb, yc) + \frac{1}{2}(yc, yd)))\, \varphi(xa + yc)\, d_g y$$

where $\gamma(V, \psi, g)$ is a certain 8^{th} root of unity depending on V, ψ, and g such that $\gamma(V, \psi, e) = 1$ and where $d_g y$ is a suitable Haar measure. We make this more explicit in three special cases:

$$(\omega_V(m(a))\varphi)(x) = \chi_V(\det a)|\det a|^{n/2}\varphi(xa), \tag{4.1}$$

$$(\omega_V(n(b))\varphi)(x) = \psi(\frac{1}{2}\,\mathrm{tr}((x, x)b))\varphi(x), \tag{4.2}$$

$$(\omega_V(w^{-1}))\varphi)(x) = \gamma(V) \int_{V^m} \psi(-\,\mathrm{tr}((x, y)))\, \varphi(y)\, dy \tag{4.3}$$

where in (4.3) dy is the Haar measure on V^m which is self dual for Fourier transform and where $\gamma(V) = \gamma(V, \psi, w^{-1})$ is the 8^{th} root of unity explicitly given in [**Ku3**, A.4].

5. Local Whittaker functions and representation densities

5.1. We keep the notation of section 4 and assume from now on that $m = 3$ and hence $G = \mathrm{Sp}_6(\mathbb{Q}_p)$, and $n = 4$.

For $s \in \mathbb{C}$ let $I(s, \chi_V)$ be the degenerate principal series representation of G induced from P, *i.e.*, $I(s, \chi_V)$ consists of K-finite functions $\Phi(\cdot, s)\colon G \to \mathbb{C}$ such that

$$\Phi(nm(a)g, s) = \chi_V(\det a)|\det a|^{s+2}\Phi(g, s)$$

for all $n \in N$, $a \in \mathrm{GL}_3(\mathbb{Q}_p)$, and $g \in G$.

We also set for $T \in \mathrm{Sym}_3(\mathbb{Q}_p)$, as in (2.5),

$$\psi_T\colon N \longrightarrow \mathbb{C}^\times, \qquad \psi_T(n(b)) = \psi(\mathrm{tr}(Tb)).$$

5.2. For $s \in \mathbb{C}$, $\Phi \in I(s, \chi_V)$, $T \in \mathrm{Sym}_3(\mathbb{Q}_p)$ with $\det(T) \neq 0$, and $g \in G$ we define the local Whittaker function by

$$W_T(g, s, \Phi) = \int_N \Phi(w^{-1}n(b)g, s)\,\psi_T(n(b))^{-1}\,db$$

where db is the Haar measure on $\mathrm{Sym}_3(\mathbb{Q}_p)$ which is selfdual with respect to the pairing

$$\psi_N\colon \mathrm{Sym}_3(\mathbb{Q}_p) \times \mathrm{Sym}_3(\mathbb{Q}_p) \longrightarrow \mathbb{C}, \qquad (b, b') \longmapsto \psi(\mathrm{tr}(bb')).$$

As the conductor of ψ is zero, we have

$$\{\, b \in \mathrm{Sym}_3(\mathbb{Q}_p) \mid \psi_N(b, b') = 1 \text{ for all } b' \in \mathrm{Sym}_3(\mathbb{Z}_p) \,\} = \mathrm{Sym}_3(\mathbb{Z}_p)^\vee. \tag{5.1}$$

Therefore

$$\mathrm{vol}_{db}(\mathrm{Sym}_3(\mathbb{Z}_p))\mathrm{vol}_{db}(\mathrm{Sym}_3(\mathbb{Z}_p)^\vee) = 1.$$

As the index of $\mathrm{Sym}_3(\mathbb{Z}_p)$ in $\mathrm{Sym}_3(\mathbb{Z}_p)^\vee$ is $2^{3\delta_{2p}}$, we obtain

$$\mathrm{vol}_{db}(\mathrm{Sym}_3(\mathbb{Z}_p)) = 2^{-(3/2)\delta_{2p}}. \tag{5.2}$$

It is known that $W_T(g, s, \Phi)$ converges for $\mathrm{Re}(s) > 2$ and admits a holomorphic continuation to the entire complex plane, if Φ is standard, *i.e.*, if its restriction to K is independent of s [**Ku3**, Prop. 1.4]. Moreover, we will see in Proposition 5.2 below that $W_T(e, s, \Phi)$ is a polynomial in p^{-s}.

5.3. For $\varphi \in \mathcal{S}(V^3)$ we set

$$\Phi(g,s) = (\omega(g)\varphi)(0) \cdot |a(g)|^s.$$

It follows from (4.1) and (4.2) that $\Phi(g,s) \in I(s,\chi_V)$. In this way, we obtain a G-equivariant map similar to (2.2),

$$\mathcal{S}(V^3) \longrightarrow I(0,\chi_V), \qquad \varphi \longmapsto \Phi(g,0).$$

5.4. For $r \geq 0$ we denote by the H_r the quadratic space $\mathbb{Q}_p^{2r}$ whose associated bilinear form has the matrix $\frac{1}{2}\left(\begin{smallmatrix} 0 & I_r \\ I_r & 0 \end{smallmatrix}\right)$ with respect to the standard basis, and set

$$V_r = V \perp H_r.$$

It is known [**Ku3**, Lemma A.2] that $\omega_{V_r} = \omega_V \otimes \omega_{H_r}$ as representations of G on $\mathcal{S}(V_r^3) = \mathcal{S}(V^3) \otimes \mathcal{S}(H_r^3)$.

We also recall Lemma A.3 from [**Ku3**] (see also [**Ral**, Remark II.3.2]):

Lemma 5.1. — *Let $\varphi_r^0 \in \mathcal{S}(H_r^3)$ be the characteristic function of $\mathrm{M}_{2r,3}(\mathbb{Z}_p)$ and $\varphi \in \mathcal{S}(V^3)$ with associated $\Phi(g,s) \in I(s,\chi_V)$. Set $\varphi^{[r]} = \varphi \otimes \varphi_r^0 \in \mathcal{S}(V_r^3) = \mathcal{S}(V^3) \otimes \mathcal{S}(H_r^3)$. Then we have for all $g \in G$ and $r \geq 0$*

$$\Phi(g,r) = (\omega_{V_r}(g)\varphi^{[r]})(0).$$

5.5. We fix a $\mathbb{Z}_p$-lattice L of V such that $(\ ,\ )$ is integral on L. Choose a $\mathbb{Z}_p$-basis of L and let S_r be the matrix associated to the quadratic form on $V_r = V \oplus H_r$ with respect to the chosen basis of L and the standard basis of H_r. In particular, the matrix of the bilinear form $(\ ,\ )$ with respect to the chosen base of L equals $2S_0$.

Let $\varphi \in \mathcal{S}(V^3)$ be the characteristic function of L^3 with associated $\Phi = \Phi(g,s) \in I(s,\chi_V)$. Then the local Whittaker function $W_T(e,s,\Phi)$ interpolates the local representation densities:

Proposition 5.2. — *For all integers $r \geq 0$ we have*

$$W_T(e,r,\Phi) = 2^{-(15/2)\delta_{2p}} |\det S_0|^{3/2} \gamma(V) \alpha_p(T,S_r),$$

where we denote by $\alpha_p(\ ,\ )$ the local representation density as normalized in [**Wd1**, (4.4)]. *In particular, $W_T(e,s,\Phi)$ is a polynomial in $X = p^{-s}$.*

Proof. — The right hand side is a polynomial in $X = p^{-r}$ [**Kit**] and the left hand side is an entire function in r. Hence it suffices to show the identity for $r > 2$. Now we have

$$\begin{aligned}
W_T(e,r,\Phi) &= \int_{\mathrm{Sym}_3(\mathbb{Q}_p)} \Phi\big(w^{-1}n(b),r\big)\psi\big(-\operatorname{tr}(Tb)\big)\,db \\
&\overset{(5.1)}{=} \int_{\mathrm{Sym}_3(\mathbb{Q}_p)} \big(\omega_{V_r}(w^{-1}n(b))\varphi^{[r]}\big)(0)\psi\big(-\operatorname{tr}(Tb)\big)\,db \\
&\overset{(4.3)}{=} \int_{\mathrm{Sym}_3(\mathbb{Q}_p)} \gamma(V)\int_{V_r^3}\psi\big(\frac{1}{2}\operatorname{tr}(b(y,y))\big)\cdot\varphi^{[r]}(y)\,dy\,\psi\big(-\operatorname{tr}(Tb)\big)\,db \\
&= \gamma(V)\lim_{t\to\infty}\int_{p^{-t}\,\mathrm{Sym}_3(\mathbb{Z}_p)}\int_{V_r^3}\psi\big(\operatorname{tr}(b(\frac{1}{2}(y,y)-T))\big)\cdot\varphi^{[r]}(y)\,dy\,db \\
&\overset{(5.1)}{=} \gamma(V)\lim_{t\to\infty}\operatorname{vol}_{db}(p^{-t}\,\mathrm{Sym}_3(\mathbb{Z}_p))\cdot \int_{\substack{y\in V_r^3\\ \frac{1}{2}(y,y)-T\in p^t\,\mathrm{Sym}_3(\mathbb{Z}_p)^\vee}}\varphi^{[r]}(y)\,dy \\
&\overset{(5.2)}{=} \gamma(V)\lim_{t\to\infty}2^{-(3/2)\delta_{2p}}p^{6t}\int_{\substack{y\in \mathrm{M}_{2r+4,3}(\mathbb{Z}_p)\\ {}^tyS_ry-T\in p^t\,\mathrm{Sym}_3(\mathbb{Z}_p)^\vee}} dy.
\end{aligned}$$

Now $\{\, y\in \mathrm{M}_{2r+4,3}(\mathbb{Z}_p) \mid {}^tyS_ry-T\in p^t\,\mathrm{Sym}_3(\mathbb{Z}_p)^\vee \,\}$ is a union of

$$\tilde{A}_{p^t}(T,S_r) := \#\{\, y\in \mathrm{M}_{2r+4,3}(\mathbb{Z}_p/2p^t\mathbb{Z}_p) \mid {}^tyS_ry-T\in p^t\,\mathrm{Sym}_3(\mathbb{Z}_p)^\vee \,\}$$

cosets for $2p^t\mathrm{M}_{2r+4,3}(\mathbb{Z}_p)$. Moreover, by the definition of dy (4.3) we have

$$\begin{aligned}
\operatorname{vol}_{dy}(\mathrm{M}_{2r+4,3}(\mathbb{Z}_p)) &= |\det 2S_r|^{3/2} \\
&= |\det 2S_0|^{3/2} \\
&= 2^{-6\delta_{2p}}|\det S_0|^{3/2},
\end{aligned}$$

and hence

$$\operatorname{vol}_{dy}(2p^t\mathrm{M}_{2r+4,3}(\mathbb{Z}_p)) = 2^{-6\delta_{2p}}|\det S_0|^{3/2}2^{-3(4+2r)\delta_{2p}}p^{-t3(4+2r)}.$$

Therefore $W_T(e,r,\Phi)$ is equal to

$$\gamma(V)2^{-6\delta_{2p}}|\det S_0|^{3/2}2^{(-(3/2)-3(4+2r))\delta_{2p}}\lim_{t\to\infty}p^{6t-t3(4+2r)}\tilde{A}_{p^t}(T,S_r).$$

Now we have

$$\tilde{A}_{p^t}(T,S_r) = 2^{3(4+2r)\delta_{2p}}A_{p^t}(T,S_r)$$

with

$$A_{p^t}(T,S_r) = \#\{\, y\in \mathrm{M}_{2r+4,3}(\mathbb{Z}_p/p^t\mathbb{Z}_p) \mid {}^tyS_ry-T\in p^t\,\mathrm{Sym}_3(\mathbb{Z}_p)^\vee \,\}.$$

By definition we have

$$\alpha_p(T, S_r) = \lim_{t\to\infty} p^{6t-t3(4+2r)} A_{p^t}(T, S_r)$$

and this proves the proposition. □

Corollary 5.3. — *For Φ as in Proposition 5.2, $W_T(e, 0, \Phi) \neq 0$ if and only if T is represented by S_0.*

5.6. We will now prove Theorem 3.2.

As $\alpha_p(T, S_r)$ is a rational function in $X = p^{-r}$, it follows from Proposition 5.2 that

$$W'_T(e, 0, \Phi) = -\log(p) 2^{-(15/2)\delta_{2p}} |\det S_0|^{3/2} \gamma(V) \frac{\partial}{\partial X} \alpha_p(T, S_r)_{|X=1}. \tag{5.3}$$

Let D be the division quaternion algebra over $\mathbb{Q}_p$ and denote by $\mathcal{O}_D$ its maximal order. We denote by $S = S_0$ (resp. $\tilde{S} = \tilde{S}_0$) the matrix associated to the quadratic space $V = \mathrm{M}_2(\mathbb{Z}_p)$ (resp. $\tilde{V} = \mathcal{O}_D$) endowed with the reduced Norm. Then we have (see *e.g.*, [**Wd1**, (4.5) and (4.6)])

$$|\det(S_0)| = 2^{4\delta_{2p}},$$
$$|\det(\tilde{S}_0)| = 2^{4\delta_{2p}} p^{-2}.$$

Moreover we have by the explicit formulas in the Appendix of [**Ku3**]

$$\gamma(V) = -\gamma(\tilde{V}).$$

Using the notation of Theorem 3.2, we therefore have by Proposition 5.2 and (5.3)

$$\frac{W'_{T,p}(e, 0, \Phi_p)}{W_{T,p}(e, 0, \tilde{\Phi}_p)} (\log p)^{-1} = p^3 \frac{\frac{\partial}{\partial X} \alpha_p(T, S_r)_{|X=1}}{\alpha_p(T, \tilde{S}_0)}. \tag{5.4}$$

But now by [**Wd2**, Theorem 1.1 and 2.16] we have

$$\alpha_p(T, \tilde{S}_0) = 2(p+1)^2 p^{-1} \tag{5.5}$$

and

$$\frac{\partial}{\partial X} \alpha_p(T, S_r)_{|X=1} = -p^{-4}(p^2-1)^2 \mathrm{lg}(\mathcal{O}_{\mathcal{T}_T, \xi}). \tag{5.6}$$

Therefore we have

$$\mathrm{lg}(\mathcal{O}_{\mathcal{T}_T,\xi}) \log(p) \overset{(5.5)}{\underset{(5.6)}{=}} -\frac{p^4}{(p^2-1)^2} \frac{2(p+1)^2}{p} \frac{\frac{\partial}{\partial X} \alpha_p(T, S_r)_{|X=1}}{\alpha_p(T, \tilde{S}_0)}$$
$$\overset{(5.4)}{=} -\frac{2}{(p-1)^2} \frac{W'_T(e, 0, \Phi_p)}{W_T(e, 0, \tilde{\Phi}_p)}$$

which proves the theorem.

References

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Inventiones Math.* **112** (1993), p. 225–245.

[Go2] U. Görtz – Arithmetic intersection numbers, this volume, p. 15–24.

[Ka] H. Katsurada – An explicit formula for Siegel series, *Amer. J. Math.* **121** (1999), no. 2, p. 415–452.

[Kit] Y. Kitaoka – A note on local densities of quadratic forms, *Nagoya Math. J.* **92** (1983), p. 145–152.

[KR] S. Kudla & M. Rallis – On the Weil-Siegel formula, *J. Reine Angew. Math.* **387** (1988), p. 1–68.

[Ku1] S. Kudla – Some extensions of the Siegel Weil formula, preprint 1992, available at `http://www.math.umd.edu/~ssk/ssk.research.html`.

[Ku2] ———, Notes on the local theta correspondence, preprint 1996, available at `http://www.math.umd.edu/~ssk/ssk.research.html`.

[Ku3] ———, Central derivatives of Eisenstein series and height pairings, *Ann. of Math. (2)* **146** (1997), no. 3, p. 545–646.

[Ku4] S. Kudla – Derivatives of Eisenstein series and arithmetic geometry, in *Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002)*, Higher Ed. Press, Beijing, 2002, p. 173–183.

[Mi] J. Milne – Points on Shimura varieties mod p, in *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, 1977), Part 2*, p. 165–184.

[Ral] S. Rallis – On the Howe duality conjecture, *Comp. Math.* **51** (1984), p. 333–399.

[Rao] R. Rao – On some explicit formulas in the theory of the Weil representation, *Pacific J. Math.* **157** (1993), p. 335–371.

[Wd1] T. Wedhorn –The genus of the endomorphisms of a supersingular elliptic curve, this volume, p. 25–47.

[Wd2] ———, Calculation of representation densities, this volume, p. 179–190.

[We] A. Weil – Sur certains groupes d'opérateurs unitaires, *Acta Math.* **111** (1964), p. 143–211.

M. Rapoport, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : `rapoport@math.uni-bonn.de`

T. Wedhorn, Institut für Mathematik der Universität Paderborn, Warburger Straße 100, 33098 Paderborn, Germany • *E-mail :* `wedhorn@math.uni-paderborn.de`
Url : `www2.math.uni-paderborn.de/people/torsten-wedhorn.html`

INDEX