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 $f_1, \ldots, f_r : A \to A'$, the locus where $f_1, \ldots, f_r$ 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 $\bar{\mathbb{F}}_p$ (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*

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

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 $\Gamma \to \Gamma'$ $(\mathrm{mod}\ J)$. Then the closed formal subscheme $\mathcal{T}$ of $\mathcal{S} = \mathrm{Spf}\ R$ is a relative divisor over* 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 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 $\Gamma \to \Gamma'(\mathrm{mod}\ I_i)$. Then*

$$\mathrm{lg}_W\, R/I = (\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{T}_3)_{\mathcal{S}} \quad .$$

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,

$$\chi((g_1,g_2,g_3)) = \sum (-1)^i \, \mathrm{lg}(H_i(K_\bullet(g_1,g_2,g_3)))$$

(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

$$\varphi_2 = {}^\iota\psi_1 \circ \psi_2 \ , \ \varphi_3 = {}^\iota\psi_1 \circ \psi_3 \ \text{ in } \operatorname{End}(G) \ .$$

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 $\Gamma(\text{mod } J_i)$. 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

$$\begin{aligned} {}^\iota\varphi_i &= -\,\varphi_i \text{ and } \operatorname{Nm}(\varphi_i) = u_1 u_i p^{a_i} \quad , \quad i = 2,3 \ . \\ \varphi_2\varphi_3 &= -\,\varphi_3\varphi_2 \ . \end{aligned} \tag{2.1}$$

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 $\Gamma(\text{mod } J_2)$ 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

$$\lg \ W[[t]]/(J_2 + J_3) = \begin{cases} \frac{a_3+1}{2} = 1 & \text{if } a_2 = 0 \\ a_3 + 1 = 2 & \text{if } a_2 = 1. \quad \square \end{cases}$$

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

$$\mathcal{O}_K + \Pi^s\mathcal{O}_D = \mathcal{O}_K \oplus p^{\lfloor \frac{s}{2} \rfloor}\mathcal{O}_K \cdot \Pi \ .$$

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

$$\operatorname{tr}(\varphi) = 0 \quad , \quad \varphi^2 = -u_1u_2p^{a_1+a_2} \quad .$$

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 $W[[t]]$,

$$\mathrm{Spf}\ W[[t]]/J = \sum_{s=0}^{[(a_1+a_2)/2]} \mathcal{W}_s(\varphi) \ .$$

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

$$\mathcal{W}_s(\varphi) = \mathrm{Spf}\ W_s \ ,$$

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

$$\mathrm{Spf}\ W[[t']]/J' = \sum_{s=0}^{[(a_1+a_2)/2]} \mathcal{W}_s(\varphi') \ .$$

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 $\tau|M =$ *id*, let Γ_τ be the graph of the corresponding morphism* $\mathrm{Spec}\,\mathcal{O}_L \to \mathrm{Spec}\,\mathcal{O}_K$. *Then*

$$\mathrm{Spec}\,\mathcal{O}_K \otimes_{\mathcal{O}_M} \mathcal{O}_L = \bigcup_\tau \Gamma_\tau \ .$$

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

$$\varphi \circ \varphi_i = \varphi_i \circ \varphi \quad , \quad i = 1, 2 \quad .$$

□

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*

$$\pi(X) = \pi_1 X + \pi_2 X^2 + \dots \quad , \quad \pi_i \in \mathcal{O} \quad .$$

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 $F_r \to F_s$ (mod $I(r,s)$). Let $I(r,s+1)$ be the minimal ideal in $\mathcal{O}$, such that $\pi \circ \psi$ lifts to an isogeny $F_r \to F_{s+1}$ (mod $I(r,s+1)$). 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 $\mathcal{M}_{a,b}$,

$$\begin{tikzcd}
\mathcal{M} \times \mathcal{M} \arrow[r] & \mathcal{M} \times \mathcal{M} \\
\mathcal{M}_{a,b} \arrow[r] \arrow[u] & \mathcal{M} \arrow[u, "\Delta"']
\end{tikzcd}$$

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 $E \longrightarrow E'$ 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

$$E \xrightarrow{F^a} E^{(p^a)} \xrightarrow[\alpha]{\sim} E'^{(p^b)} \xrightarrow{{}^tF^b} E' \quad .$$

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*

$$\bar{\mathbb{F}}_p[[X, Y]] \ \Big/ \prod_{\substack{a+b=n \\ a \geq 0, b \geq 0}} (X^{p^a} - Y^{p^b})$$

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 $\mathcal{S}_{(p)} = \operatorname{Spf} \bar{\mathbb{F}}_p[[t, t']]$ 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

$$\begin{aligned} t_2 &= u \cdot t_1 \quad , \quad u \in \bar{\mathbb{F}}_p[[t]]^\times \\ t_2' &= u' \cdot t_1' \quad , \quad u' \in \bar{\mathbb{F}}_p[[t']]^\times \quad . \end{aligned}$$

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

$$\mathrm{lg}\ \bar{\mathbb{F}}_p[[t,t']]/(t^{p^\mu} - (t')^{p^{a_1-\mu}}, (ut)^{p^\nu} - (u' \cdot t')^{p^{a_2-\nu}}) = p^n \quad . \tag{4.2}$$

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

$$\begin{aligned} &\mathrm{lg}\ \bar{\mathbb{F}}_p[[t,t']]/(t - t'^{p^{a_1-2\mu}})^{p^\mu}, (ut - (u't')^{p^{a_2-2\nu}})^{p^\nu} \overset{(1)}{=} \\ &\qquad p^{\mu+\nu} \cdot \mathrm{lg}\ \bar{\mathbb{F}}_p[[t']]/(u \cdot t'^{p^{a_1-2\mu}} - (u't')^{p^{a_2-2\nu}}) \overset{(2)}{=} p^{\mu+\nu+\min\{a_1-2\mu, a_2-2\nu\}} = p^n. \end{aligned}$$

Here in (1) we used the formula ([**Go2**, Lemma 4.2])

$$\mathrm{lg}_A\, B/x_1 \ldots x_n = \sum_i \mathrm{lg}_A\, B/x_i \quad ,$$

valid for any A-algebra B and non zero divisors $x_1, \ldots, x_n$ 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

$$\begin{aligned} &\mathrm{lg}\ \bar{\mathbb{F}}_p[[t,t']]/((t - t'^{p^{a_1-2\mu}})^{p^\mu}, (u't' - (ut)^{p^{2\nu-a_2}})^{p^{a_2-\nu}}) = \\ &p^\mu \cdot p^{a_2-\nu} \cdot \mathrm{lg}\ \mathbb{F}_p[[t,t']]/(t - t'^{p^{a_1-2\mu}}, u't' - (ut)^{p^{2\nu-a_2}}) = \\ &\quad p^{a_2-\nu+\mu} \cdot \mathrm{lg}\ \bar{\mathbb{F}}_p[[t']]/(u't' - u^{p^{2\nu-a_2}} \cdot t'^{p^{a_1-2\mu+2\nu-a_2}}) \overset{(3)}{=} p^{a_2-\nu+\mu} = p^n. \end{aligned}$$

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 $\alpha \in \mathrm{Aut}(G)$. 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) $T = \operatorname{diag}\big(u_1 2^\alpha, 2^\beta \left(\begin{smallmatrix}2&1\\1&2\end{smallmatrix}\right)\big)$, $\alpha \geq 0, \beta \geq -1$, $\alpha \equiv \beta \bmod 2$
(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.

- $$T = \operatorname{diag}\left(u_1 2, 2^{-1}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\right), \quad \text{hence } GK(T) = (0,0,1) \quad .$$

Then $\varphi_2 = {}^\iota\psi_1 \circ \psi_2 = {}^\iota e_2 \circ e_3$ and

$$\operatorname{tr}(\varphi_2) = (e_2, e_3) = 1 \quad \text{and} \quad \operatorname{Nm}(\varphi_2) = 1 \quad .$$

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 $\Gamma(\text{mod } J_2)$ is a canonical lifting relative to K.

Now $\varphi_3 = {}^\iota\psi_1 \circ \psi_3 = {}^\iota e_2 \circ e_1$ and

$$\operatorname{tr}(\varphi_3) = 0 \quad \text{and} \quad \operatorname{Nm}(\varphi_3) = u_1 \cdot 2 \quad .$$

Furthermore

$$\operatorname{tr}(\varphi_2 \circ {}^\iota\varphi_3) = \operatorname{tr}({}^\iota e_3 \circ e_2 \circ {}^\iota e_2 \circ e_1) = Q(e_2) \cdot \operatorname{tr}({}^\iota e_3 \circ e_1) = (e_1, e_3) = 0 \quad .$$

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.

- $$T = \operatorname{diag}\left(u_1, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\right) \quad , \quad \text{hence } GK = (0,1,1) \quad .$$

Then $\varphi_2 = {}^\iota\psi_1 \circ \psi_2 = {}^\iota e_1 \circ e_2$ and

$$\operatorname{tr}(\varphi_2) = (e_1, e_2) = 0 \quad \text{and} \quad \operatorname{Nm}(\varphi_2) = u_1 \cdot 2 \quad .$$

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 $\Gamma(\text{mod } J_2)$ is a canonical lifting relative to K.

Now $\varphi_3 = {}^\iota\psi_1 \circ \psi_3 = {}^\iota e_1 \circ e_3$ and

$$\operatorname{tr}(\varphi_3) = 0 \quad \text{and} \quad \operatorname{Nm}(\varphi_3) = u_1 \cdot 2 \quad .$$

Furthermore

$$\operatorname{tr}(\varphi_2 \circ {}^\iota\varphi_3) = \operatorname{tr}({}^\iota e_2 \circ e_1 \circ {}^\iota e_1 \circ e_3) = u_1 \cdot (e_2, e_3) = u_1 \cdot 2 \quad .$$

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

$$\text{(A.1.3)} \qquad \mathcal{O}_D = \mathcal{O}_K \oplus \mathcal{O}_K \cdot \alpha \quad .$$

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

$$\operatorname{tr}(\varphi_3') = (e_1, e_3) = 0 \quad \text{and} \quad \operatorname{Nm}(\varphi_3') = u_1 u_3 \quad .$$

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 $\mathrm{Nm}(\varphi) = u_1u_2 \cdot 2^{\beta_1+\beta_2}$.

Since $\beta_1 + \beta_2$ is odd, we have $K = \mathbb{Q}_2(\sqrt{-u_1u_2 2})$ and $\mathcal{O}_K = \mathbb{Z}_2[\sqrt{-u_1u_2 2}]$. 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 $K = \mathbb{Q}_2[X]/(X^2 - 2u_1X + u_1(u_1 + u_2))$ 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 $\operatorname{tr}(\varphi) = u_1 \cdot 2^{\frac{\beta_1+\beta_2}{2}+1}$ and $\operatorname{Nm}(\varphi) u_1^2 \cdot 2^{\beta_1+\beta_2} + u_1 u_2 \cdot 2^{\beta_1+\beta_2} + u_1 u_3 \cdot 2^{\beta_1+\beta_3} u_1 2^{\beta_1+\beta_2}(2u_3 + u_2 + u_1)$.

Hence $K = \mathbb{Q}_2[X]/(X^2 - 2u_1 X + u_1 \cdot (2u_3 + u_2 + u_1))$, 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 $\operatorname{tr}(\varphi) = 2^{\frac{\beta_1+\beta_2}{2}+1} \cdot u_1$ and $\operatorname{Nm}\varphi = 2^{\beta_1+\beta_2} \cdot u_1(u_1 + u_2)$.

Hence $K = \mathbb{Q}_2[X]/(X^2 - 2u_1 X + u_1 \cdot (u_1 + u_2))$. 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 $K = \mathbb{Q}_2[X_1]/(X_1^2 - u_1 X_1 + u_1 \eta)$. 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 $K = \mathbb{Q}_2[X]/(X^2 - 2u_1 X + u_1 \cdot (u_1 + u_2))$ 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, $\operatorname{tr}(\mathcal{O}_K) \subset 2 \cdot \mathbb{Z}_2$. Let

$$\varphi_i^\circ = \varphi_i - \frac{1}{2}\operatorname{tr}(\varphi_i) \quad , \quad i = 1, 2 \quad .$$

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

$$\begin{aligned} \lambda_i + {}^\iota\lambda_i &= 2a \\ \lambda_i - {}^\iota\lambda_i &= 2b\pi \quad . \end{aligned}$$

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 $\mathbb{F}_4 \backslash \mathbb{F}_2$, 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 $K = \mathbb{Q}_2(\sqrt{-u_1 u_2 2})$ and $\mathcal{O}_K = \mathbb{Z}_2[\pi]$, with $\pi = \sqrt{-u_1 u_2 2}$. This case is completely analogous to case A1.

Case B2 a): Here $K = \mathbb{Q}_2[X]/(X^2 - 2u_1 X + u_1 \cdot (u_1 + u_2))$ 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

$$\begin{aligned}\lambda_i - {}^\iota\lambda_i\eta^{a_i} &\equiv (1 + [\lambda_i]\pi) - (1 - [\lambda_i]\pi) \cdot (1 + \eta_1\pi) (\mathrm{mod}\ \pi^2) \\ &\equiv \eta_1 \cdot \pi \pmod{\pi^2} \quad .\end{aligned}$$

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 $K = \mathbb{Q}_2[X]/(X^2 - u_1X + u_1\eta)$, 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 $\mathbb{F}_4 \backslash \mathbb{F}_2$, 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

(A.3.1) $$\varphi \circ {}^{\iota}\varphi_3 + {}^{\iota}\varphi_3 \circ \varphi 2^{\beta+1} \cdot {}^{\iota}\tilde{e}_1 \quad ,$$

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

(A.3.2) $$b = 2^{\frac{\beta-\alpha}{2}} \cdot {}^{\iota}\tilde{e}_1\pi - a\pi^2 \quad .$$

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

(A.3.3) $$2^{\delta}(((\pi a + b) + bj) - ((\pi a + b) + b\pi^{-1} \cdot {}^{\iota}\pi j)) = 2 \cdot {}^{\iota}e_2 e_3 {}^{\iota}\tilde{e}_1 \quad .$$

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 $\alpha \neq \beta$ $\alpha = \beta$	B1 B2 b)
A2	A2
B1 $\beta_2 \leq \beta_3 - 2$ $\beta_2 = \beta_3 - 1$ $\beta_2 = \beta_3$	B1 B2 b) or c) A1 or B2 a)
B2 a) $\beta_1 < \beta_2$ $\beta_1 = \beta_2$	B3 b) B2 b) or c)
B2 b) $\beta_1 < \beta_2$ $\beta_1 = \beta_2$	B3 a) A2
B2 c) $\beta_1 < \beta_2$ $\beta_1 = \beta_2$	B3 a) A2
B3 a) $\beta_3 \geq \beta_2 + 4$ $\beta_3 < \beta_2 + 4$	B3 a) B2 c)
B3 b) $\beta_3 \geq \beta_2 + 4$ $\beta_3 = \beta_2 + 3$ $\beta_3 = \beta_2 + 2$	B3 b) B2 b) 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

$$T' = \operatorname{diag}\left(u_1 2^{\alpha}, 2^{\beta-1}\begin{pmatrix}4 & 1\\ 1 & 1\end{pmatrix}\right) \ .$$

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 $(\psi_1, \psi_2, \psi_3) = (e_1, e_2, c_1e_1 + c_2e_2 + e_3)$ 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

$$T' = \operatorname{diag}(u_1 2^{\beta_1}, u_2 2^{\beta_2}, u_3 2^{\beta_3-2}) \ .$$

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 $\frac{1}{2}(e_2 + e_3)$,

$$\tilde{T}'\begin{pmatrix}u_2 2^{\beta_2} & c_2u_2 2^{\beta_2-1}\\ * & (c_2^2u_2 + u_3)2^{\beta_2-2}\end{pmatrix} \ .$$

We determine when $\tilde{T}'$ is diagonalizable by determining the valuations of the ideals in $\mathbb{Z}_2$,

$$s(\tilde{L}') = \frac{1}{2}(\tilde{L}', \tilde{L}'), \ \text{resp. } n(\tilde{L}') = (Q(x),\ x \in \tilde{L}') \ .$$

Now

$$\operatorname{ord}\ s(L) = \min\{\beta_2, \beta_2 - 1,\ \operatorname{ord}(c_2^2u_2 + u_3) + \beta_2 - 2\} = \beta_2 - 1 \ .$$

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 $(\psi_1, \psi_2, \psi_3) = (e_1, 2^{\frac{\beta_2 - \beta_1}{2}} e_1 + e_2, c_1 e_1 + c_2 e_2 + e_3)$ 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