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.