Torsion points on Elliptic Curves and the Jackson Space

Daniel Larsson

Abstract

In this paper we will use a particular non-commutative scheme to, among other things, study the ramification properties of the field of p-torsion points on an elliptic curve and its reduction properties. Also, we show that this non-commutative space also allow us to use the p-torsion points to "parametrise" classes in the p-torsion of the Brauer group of the base field.

1 Introduction

Let K be a local field with ring of integers $\mathfrak{o}_K$ and $E_{/K}$ an elliptic curve over K with minimal regular model $\mathscr{E}_{/\mathfrak{o}_K}$. Arithmetically it is interesting to study the specialisation (reduction) of E to the special fibre of $\mathscr{E}$. In this paper we will use a non-commutative deformation theory (see [Lau02] or [ELS17]) and non-commutative algebraic geometry to do exactly that.

A natural question is what non-commutative deformation theory and non-commutative algebraic geometry can bring to the table in this context. As deformation theory is the local study of an object in the moduli space of all such objects, deformation theory can give information connected to the reduction of these objects to characteristic p. Extension to non-commutative base rings as versal deformation spaces, allows us to study the reduction properties of a family of objects *at the same time*. In other words, how the objects deform (reduce) together as a family. This simultaneous deformations are measured by the size of certain Ext^1-groups. In our case the family of objects are rational points on non-commutative spaces constructed by using p-torsion points on E.

The starting point in the present approach is the following. Let p be a prime. We will assume through most of the paper that $p \geq 3$, but this is not necessary at this point. Under the assumption that the p-torsion group $E[p]$ has a K-rational point, the field $K(E[p])$ generated by the coefficients of all p-torsion points is known to fit in the following tower of fields

$$K \text{ ——— } K(\zeta_p) \text{ ——— } K(E[p]),$$

where ζ_p is primitive p-th root of unity. In fact, $K(E[p])/K(\zeta_p)$ is a Kummer extension (this is well-known but see [Yas13] for one reference)

$$K(E[p]) = K(\zeta_p)[\sqrt[p]{x}] = K(\zeta_p)[T]/(T^p - x), \qquad x \in K.$$

e-mail: daniel.larsson@usn.no

Put $F := K(E[p])$. Clearly, F encodes interesting arithmetic properties associated with E and its p-torsion points. From the field F we will construct two non-commutative algebras $\mathcal{J}_x$ and $\mathscr{F}_\xi$ (the description of ξ comes below), with associated non-commutative schemes, $\mathfrak{X}_{\mathcal{J}_x}$ and $\mathfrak{X}_{\mathscr{F}_\xi}$, respectively, using non-commutative deformation theory. Using these noncommutive algebras/schemes we will study the specialisation of E to the special fibre. For simplicity we will, in this introduction denote either of $\mathfrak{X}_{\mathcal{J}_x}$ and $\mathfrak{X}_{\mathscr{F}_\xi}$, by $\mathfrak{X}$. In this paper we will use a "soft" approach to non-commutative algebraic geometry, more meant to be suggestive than actually essential in this particular instance. For a more comprehensive discussion see [Lar23b] and the references therein.

Let me indicate the construction of $\mathcal{J}_x$ since this is slightly more simple. This algebra is associated with the reduction modulo a prime $\ell \neq p$. The algebra $\mathscr{F}_x$ is used for the reduction modulo p itself.

Suppose $\mathfrak{o}_K \to B \to A$ is a general cyclic extension of an $\mathfrak{o}_K$-algebra B and let G be its automorphism group. Take an element $\sigma \in G$. The operator $\Delta := a(\mathrm{id} - \sigma)$ for $a \in A$ acts on A and satisfies the generalised Leibniz rule $\Delta(bc) = \Delta(b)c + \sigma(b)\Delta(c)$. Form the left A-module $A \cdot \Delta$. This can be endowed with a nonassociatve algebraic structure turning it into a generalised Lie algebra called a hom-Lie algebra (see section 2 for more details). Akin to the enveloping algebra of a Lie algebra, so can one construct an associative "enveloping" algebra of a hom-Lie algebra. The algebra $\mathcal{J}_x$ is then defined as the subalgebra of the "enveloping" algebra of the hom-Lie algebra $A \cdot \Delta$. In fact, $\mathcal{J}_x$ is a "q-deformation" of the enveloping algebra of $\mathfrak{sl}_2$ (see [LS07]).

Remark 1.1. Notice that $A \cdot \Delta$ captures information of the group action of G on A. This transfers to naturally to $\mathcal{J}_x$.

It turns out that $\mathcal{J}_x$ (and $\mathscr{F}_\xi$) satisfies some desirable ring-theoretic and homological properties. For instance, the algebra (or its associated non-commutative scheme) is noetherian, normal, Auslander-regular, and Cohen–Macaulay (CM). The definition of "Auslander-regularity" is not necessary here beyond it including a condition of finite global dimension. Hence this is indeed a generalisation of regularity in the commutative context. However, rings can be Auslander-regular and still behave "singular" in the non-commutative realm. Indeed, as we will see an Auslander-regular ring can have a singular centre. Similarly, a non-commutative ring can be CM, but have a centre which is not. On the other hand, the algebras we will consider here, will have CM centres. I refer to the literature for the definition of Auslander-regular and Cohen–Macaulay in the non-commutative case (a definition can be found in [Lar23a], for instance).

The paper is organised as follows. Section 2 is preliminary and contains, for the reader's benefit, the constructions of algebras related to twisted derivations. In particular, it includes the construction of an "infinitesimal enveloping algebra", $\mathbf{I}_q$, that will crucially be used later. This section overlaps, by necessity, some discussions from [Lar23a]. However, there are some differences in presentation.

Section 2.3 introduces the so-called Kummer–Witt algebra $\mathbf{W}_x^{1/n}$. This is defined to be the "enveloping algebra" of the hom-Lie algebra $A \cdot \Delta$ where A is a Kummer extension of B. This section also lists a number of ring-theoretic properties satisfied by $\mathbf{W}_x^{1/n}$ and $\mathbf{I}_q$.

Section 3 introduces the notion of non-commutative algebraic space that we will use. Included is also a definition of rational points on such a space. The

section following section 3 contains a recollection of polynomial identity algebras and the definition of $\mathcal{J}_x$ and a description of its centre and some of the ring-theoretic properties it enjoys. We also describe the non-commutative space $\mathfrak{X}_{\mathcal{J}_x}$ and its set of one-dimensional rational points together with their infinitesimal structure.

In section 5 we discuss ramification in cyclic extensions and its connection to $\mathcal{J}_x$. Then in section 6, which is the main part of the paper, we consider the reduction properties of elliptic curves and relate these to properties of $\mathcal{J}_x$ and $\mathscr{J}_\xi$ and their associated spaces. In the case where $F = K(E[\ell])$ and $\ell \neq p$ we use $\mathcal{J}_x$. However, $\mathcal{J}_x$ does not give enough information in the case $\ell = p$ and this is where $\mathscr{J}_x$ comes in. Let f be the conductor of E and d the number of irreducible components of the special fibre $\bar{E}$ which are defined over k (the residue class field of K). We now take $\xi = \zeta_{f+d}$ and $\mathscr{J}_{\zeta_{f+d}}$. This choice might seem ad hoc at first glance but it turns out to be a very fruitful choice.

The reduction properties of E in the case where $\ell = p$ are studied via a family of one-dimensional rational points on $\mathfrak{X}_{\mathscr{J}_{\zeta_{f+d}}}$. We pay particular attention to additive reduction. It turns out that the only possible values for p in the case where K is absolutely unramified are $2, 3, 5$ and 7. En route to the construction of the one-dimensional points alluded to above, we introduce a set of elements $\theta_i \in F = K(E[p])$. These are used in the last section to construct hyperplane arrangements in $\mathfrak{X}_{\mathscr{J}_x}$ and Brauer-classes in $\mathrm{Br}(K)$.

It is not an understatement to say that the study of K-rational p-torsion points and their associated p-torsion fields $K(E[p])$ is an active field of study. For instance, the recent paper [FK18] by Freitas and Kraus gives a complete description of the degree $[\mathbb{Q}_\ell(E[p]) : \mathbb{Q}_\ell]$ when $\ell \neq p \geq 3$; in [BP16] Bandini and Paladino studies the generators of $K(E[p])$ where K is any field of characteristic not equal to 2 or 3. The latter paper also indicate the complexity of the p-torsion field with several examples. It is my hope that the present paper could also be used to study the fields $K([p])$ as well as the p-torsion points themselves.

Acknowledgements

Notation

We will adhere to the following notation throughout.

- All associative rings are unital. Unless otherwise stated all rings A, B, k e.t.c., are associative.

- All modules are *left* modules unless otherwise explicitly specified. The groupoid of (left) A-modules up to isomorphism is denoted $\mathsf{Mod}(A)$.

- The notation $\mathrm{Max}(A)$ denotes the *set* of maximal ideals, while $\mathrm{Specm}(A)$ denotes the maximal spectrum of A, i.e., $\mathrm{Max}(A)$ together with the Zariski topology.

- $\mathfrak{Z}(A)$ denotes the centre of A.

- For $\mathfrak{p}$ a prime in A, $k(\mathfrak{p})$ denotes the residue class field of $\mathfrak{p}$.

2 Algebras related to twisted derivations

We should probably say a few things about the construction of the family of algebras $\mathcal{J}_x(r)$, otherwise what follows will feel completely pulled from the mist. Since the construction is spelled out in detail in [Lar23a] we will deliberately be as brief as possible.

Throughout $\mathfrak{o}$ is a commutative ring and A commutative $\mathfrak{o}$-algebra.

2.1 hom-Lie algebras

Suppose then that σ is a $\mathfrak{o}$-algebra endomorphism on A. Then a *twisted $\mathfrak{o}-derivation* (or *σ-derivation*) on A is an operator

$$\Delta(ab) = \Delta(a)b + \sigma(a)\Delta(b), \quad a, b \in A.$$

Example 2.1. The canonical example of a σ-derivation is a map $A \to A$ on the form

$$\Delta := a(\mathrm{id} - \sigma) : \ A \to A, \quad a \in A.$$

In fact, for many algebras these types of maps are the only σ-derivations available.

Under certain conditions (which are satisfied in our case) one can prove the following theorem (see [HLS06]).

Theorem 2.1. The A-module $A \cdot \Delta$ can be endowed with a $\mathfrak{o}$-linear product

$$\langle\!\langle a \cdot \Delta, b \cdot \Delta \rangle\!\rangle := \sigma(a) \cdot \Delta(b \cdot \Delta) - \sigma(b) \cdot \Delta(a \cdot \Delta), \quad a, b \in A$$

satisfying

(i) $\langle\!\langle a \cdot \Delta, b \cdot \Delta \rangle\!\rangle = (\sigma(a)\Delta(b) - \sigma(b)\Delta(a)) \cdot \Delta$;

(ii) $\langle\!\langle a \cdot \Delta, a \cdot \Delta \rangle\!\rangle = 0$;

(iii) $\circlearrowleft_{a,b,c} \left(\langle\!\langle \sigma(a) \cdot \Delta, \langle\!\langle b \cdot \Delta, c \cdot \Delta \rangle\!\rangle \rangle\!\rangle + q \cdot \langle\!\langle a \cdot \Delta, \langle\!\langle b \cdot \Delta, c \cdot \Delta \rangle\!\rangle \rangle\!\rangle \right) = 0$,

where $a, b, c \in A$. The product is in particular non-associative.

Definition 2.1. A *hom-Lie algebra* is an A-module M together with a $\mathfrak{o}$-bilinear product $\langle\!\langle \cdot, \cdot \rangle\!\rangle$ on M such that

(hL1.) $\langle\!\langle a, a \rangle\!\rangle = 0$, for all $a \in M$;

(hL2.) there is a $q \in A$ such that the identity

$$\circlearrowleft_{a,b,c} \left\{ \langle\!\langle \sigma(a), \langle\!\langle b, c \rangle\!\rangle \rangle\!\rangle + q \cdot \langle\!\langle a, \langle\!\langle b, c \rangle\!\rangle \rangle\!\rangle \right\} = 0,$$

holds for all $a, b, c \in M$.

If we let σ vary in a group G, we get a collection of hom-Lie algebras, called an *equivariant hom-Lie algebra*. Notice that an equivariant hom-Lie algebra includes a Lie algebra (which might certainly be abelian) since this is what we get when σ is the unit element in G. We can thus view the equivariant structure as a deformation of a Lie algebra, parametrised by the elements in G.

Example 2.2. The obvious example is the left A-module $A \cdot \Delta$ with product defined by theorem 2.1.

Some reasons why σ-derivations are important (and actually prevalent in abundance) in arithmetic and geometry, can be found in [Lar17] and the references therein. In short, σ-derivations and their associated hom-Lie algebras encodes the Galois structure (or more generally, the automorphism-structure) of the underlying algebra.

2.2 Infinitesimal hom-Lie algebras

We give a brief illustration of the above constructions that will be of some importance later.

Let $\mathfrak{o}$ be a commutative algebra and put $\mathfrak{o}^! := \mathfrak{o}[t]/t^n$, for some $n \geq 2$. Then $\mathfrak{o}^!$ is an *infinitesimal thickening* of $\mathfrak{o}$. Put $\Delta := a(\mathrm{id} - \sigma)$, where $a \in \mathfrak{o}$ and where $\sigma(t) = qt$, for some $q \in \mathfrak{o}^\times$. Then $(\mathfrak{o}^! \cdot \Delta, \langle\!\langle \, , \, \rangle\!\rangle)$ is *infinitesimal hom-Lie algebra* on $\mathfrak{o}^!$. The elements $\boldsymbol{e}_i := t^i \Delta$, $0 \leq i \leq n-1$, forms a basis for $\mathfrak{o}^! \cdot \Delta$ as an $\mathfrak{o}^!$-module.

Now, put $\Delta := a(\mathrm{id} - \sigma)$. Then $\Delta(t^i) = a(1 - q^i)t^i$. Using Theorem 2.1 (i) a small computation gives that

$$\langle\!\langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle\!\rangle = a(q^i - q^j)\boldsymbol{e}_{i+j}.$$

Observe that when $i + j \geq n$, then $\langle\!\langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle\!\rangle = 0$ since in that case $t^{i+j} = 0$. In addition, $\langle\!\langle \boldsymbol{e}_0, \boldsymbol{e}_i \rangle\!\rangle = a(1 - q^i)\boldsymbol{e}_i$, for all i.

Example 2.3. When $n = 3$, we get the (a, q)-parametric family of solvable $\mathfrak{o}$-Lie algebras:

$$\langle\!\langle \boldsymbol{e}_0, \boldsymbol{e}_1 \rangle\!\rangle = a(1 - q)\boldsymbol{e}_1, \qquad \langle\!\langle \boldsymbol{e}_0, \boldsymbol{e}_2 \rangle\!\rangle = a(1 - q^2)\boldsymbol{e}_2, \qquad \langle\!\langle \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle\!\rangle = 0.$$

One would be tempted to conjecture that infinitesimal hom-Lie algebras are Lie algebras for all n. However, this is not true in general.

Associated to $(\mathfrak{o}^! \cdot \Delta, \langle\!\langle \, , \, \rangle\!\rangle)$ is an associative "enveloping algebra", defined by

$$\mathbf{I}_q := \frac{\mathfrak{o}\{\boldsymbol{e}_0, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{n-1}\}}{\left(\boldsymbol{e}_i \boldsymbol{e}_j - q^{j-i}\boldsymbol{e}_j \boldsymbol{e}_i - (1 - q^{j-i})\boldsymbol{e}_{i+j} \right)}.$$

See [Lar23a] for its construction.

Example 2.4. For the algebra in example 2.3 we find (after change of basis $\boldsymbol{e}_0 \mapsto \boldsymbol{e}_0 + 1$) we get the algebra

$$\mathbf{Q}^3_{\mathfrak{o},q} := \frac{\mathfrak{o}\{\boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2\}}{\left(\boldsymbol{e}_0\boldsymbol{e}_1 - q\boldsymbol{e}_1\boldsymbol{e}_0, \ \boldsymbol{e}_0\boldsymbol{e}_2 - q^2\boldsymbol{e}_2\boldsymbol{e}_0, \ \boldsymbol{e}_1\boldsymbol{e}_2 - q\boldsymbol{e}_2\boldsymbol{e}_1 \right)}. \tag{2.1}$$

The space $\mathsf{Mod}\big(\mathbf{Q}^3_{\mathfrak{o},q}\big)$ is a *quantum affine three-space*.

2.3 Kummer–Witt hom-Lie algebras and their "enveloping algebras"

We keep the notation from above and further denote the algebra structure on A by

$$y_i y_j = \sum_{k=0}^{n} a_{ij}^k y_k, \quad a_{ij}^k \in \mathfrak{o},$$

where the y_i are the algebra generators of A. Let σ be the $\mathfrak{o}$-linear algebra morphism on A defined by $\sigma(y_i) = q_i y_i$, $q_i \in \mathfrak{o}^\times$ and let $\Delta = a(\mathrm{id} - \sigma)$ be the σ-derivation from the previous section. Put $\boldsymbol{e}_i := y_i \cdot \Delta$. Then, from Theorem 2.1, the pair

$$W_A^\sigma := (A \cdot \Delta, \langle\!\langle\, ,\, \rangle\!\rangle), \qquad \langle\!\langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle\!\rangle = a \sum_{k=0}^{n} (q_i - q_j) a_{ij}^k \boldsymbol{e}_k \tag{2.2}$$

defines a hom-Lie algebra structure on $A \cdot \Delta$. We call W_A^σ the *Witt hom-Lie algebra* over X attached to A and σ.

Remark 2.1. The construction just given is obviously not dependent on the particular choice $\sigma(y_i) = q_i y_i$. Any other automorphism can be used. However, the result will, of course, be more complicated and harder to write out.

From now on we assume that the n-th roots of unity are included in $\mathfrak{o}$. Fix a primitive such root $\zeta = \zeta_n$ and let A be the Kummer extension

$$A = \mathfrak{o}[\sqrt[n]{x}] = \mathfrak{o}[t]/(t^n - x), \quad x \in \mathfrak{o}.$$

Fix an $r \in \mathbb{Z}$ and let σ be the automorphism $\sigma(t) = \zeta^r t$.

The hom-Lie algebra of σ-twisted derivations on A is called the *Kummer–Witt hom-Lie algebra of level r* (see [Lar23a]) and its enveloping algebra is the *Kummer–Witt algebra of level r*:

$$\mathbf{W}_x^{1/n}(r) = \frac{\mathfrak{o}\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \dots, \boldsymbol{e}_{n-1} \rangle}{\left(\boldsymbol{e}_i \boldsymbol{e}_j - \zeta^{r(j-i)} \boldsymbol{e}_j \boldsymbol{e}_i - (1 - \zeta^{r(j-i)}) x^\circlearrowleft \, \boldsymbol{e}_{\{i+j \ (\mathrm{mod}\, n)\}} \right)}. \tag{2.3}$$

The notation $x^\circlearrowleft$ means that x is included when $i + j \geq n$.

Remark 2.2. The same game can clearly be played with Artin–Schreier extensions. We invite the reader to write out the corresponding relations for him/herself.

Remark 2.3. The above construction will be used with the following remark. The element $x \in \mathfrak{o}$ is the *A-ramification divisor*. This element determines a canonical subscheme in the ramification locus of a non-commutative space attached to A. The element x is a ramification invariant in two senses: (1) as the divisor in $\mathfrak{o}$ over which A is ramified (i.e., $\mathfrak{p} \mid x \Rightarrow \mathfrak{p}$ ramified); and (2) as an element giving a subscheme of the ramification locus in a certain non-commutative space (which we will construct later).

2.3.1 Fibres of $\mathbf{W}_x^{1/n}(r)$

Let $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{o})$ be a prime. Observe that the reduction of ζ modulo $\mathfrak{p}$ (i.e., the image of ζ in $k(\mathfrak{p})$), $\bar{\zeta}$, is non-zero, since $\zeta \in \mathfrak{o}^\times$. Then

$$\mathbf{W}_x^{1/n}(r)_{/\mathfrak{p}} = \frac{k(\mathfrak{p})\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{n-1}\rangle}{\left(\boldsymbol{e}_i\boldsymbol{e}_j - \bar{\zeta}^{r(j-i)}\boldsymbol{e}_j\boldsymbol{e}_i - (1 - \bar{\zeta}^{r(j-i)})x^{\circlearrowleft}\ \boldsymbol{e}_{\{i+j\ (\mathrm{mod}\,n)\}}\right)}. \qquad (2.4)$$

We record the following for easy reference.

Proposition 2.2. There are the following three possibilities when reducing modulo a prime $\mathfrak{p}$:

(1) $\bar{\zeta} = 1$, in which case we get

$$\mathbf{W}_x^{1/n}(r)_{/\mathfrak{p}} = \frac{k(\mathfrak{p})\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{n-1}\rangle}{(\boldsymbol{e}_i\boldsymbol{e}_j - \boldsymbol{e}_j\boldsymbol{e}_i)} = k(\mathfrak{p})[\boldsymbol{e}_0, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{n-1}],$$

the commutative polynomial algebra;

(2) $\bar{x} = 0$, in which case we get

$$\mathbf{W}_x^{1/n}(r)_{/\mathfrak{p}} = \frac{k(\mathfrak{p})\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{n-1}\rangle}{\left(\boldsymbol{e}_i\boldsymbol{e}_j - \bar{\zeta}^{r(j-i)}\boldsymbol{e}_j\boldsymbol{e}_i\right)},$$

a *quantum affine space*;

(3) and the *generic case* (2.4) with relations unchanged.

It is important to note that in all three cases, the reduced algebra is a domain.

Proof. Obvious. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Some ring-theoretic properties of $\mathbf{W}_x^{1/n}(r)$ are summarised in the following theorem. Here will use notions that will not be defined in this paper. For more details see [Lar23a]. It is not essential to understand all words in the theorem in order to appreciate the rest of the paper.

Theorem 2.3. The algebra $\mathbf{W}_x^{1/n}(r)$ satisfies the following:

(i) it is an Auslander-regular, noetherian PI-domain, finite over its centre;

(ii)
$$\mathrm{Kdim}(\mathbf{W}_x^{1/n}(r)) = \mathrm{gl.dim}(\mathbf{W}_x^{1/n}(r)) = n + \mathrm{Kdim}(\mathfrak{o}),$$

where Kdim is the Krull dimension and gl.dim the global dimension;

(iii) it is fibre-wise Cohen–Macaulay with

$$\mathrm{GKdim}\big(\mathbf{W}_x^{1/n}(r)_{/\mathfrak{p}}\big) = \mathrm{tr.deg}\big(\mathbf{W}_x^{1/n}(r)_{/\mathfrak{p}}\big) = n,$$

where GKdim denotes the Gelfand–Kirillov dimension;

(iv) it is fibre-wise a maximal order in its fibre-wise division rings of fractions;

Remark 2.4. The Auslander-regularity is a natural generalisations of regularity for non-commutative algebras. The same applies to Cohen–Macaulay-ness.

3 Non-commutative algebraic spaces

In this section we will very briefly introduce the concept of non-commutative algebraic spaces in the sense of [Lar23b]. We refer to this paper for all details.

Let k be a field, A be a k-algebra and $\mathsf{M} := \{M_1, M_2, \ldots, M_s\}$ be a finite family of finite-dimensional (over k) A-modules with structure morphisms ξ_i. Then there is a non-commutative ring $\hat{\mathcal{O}}_{\mathsf{M}}$ and a map $\boldsymbol{\xi} : A \to \hat{\mathcal{O}}_{\mathsf{M}}$, encoding the *simultaneous* deformations of the modules M_i. In fact, $\boldsymbol{\xi}$ is a versal family of M.

The ring object $\hat{\mathcal{O}}_{\mathsf{M}}$ is constructed as follows (details can be found in [ELS17] or [Lar23b]). Associated to M is a deformation functor having a matric pro-representing hull $(\hat{H}_{ij})$. The diagonal consists of quotients of non-commutative formal power series rings, and the entries off-diagonal are bimodules over the diagonal. Then $\mathcal{O}_{\mathsf{M}}$ is defined as the matrix ring

$$\hat{\mathcal{O}}_{\mathsf{M}} := \big(\operatorname{Hom}_k(M_i, M_j) \otimes_k \hat{H}_{ij} \big).$$

The ring $\hat{\mathcal{O}}_{\mathsf{M}}$ is to be thought of as the completion of the local ring at M in the moduli space $\mathsf{Mod}(A)$ of A-modules up to isomorphism. In all cases that I'm aware of this has a natural algebraisation $\mathcal{O}_{\mathsf{M}}$, which should be viewed as the local ring itself.

Taking the projective limit over all finite families M, we define a ring object $\mathcal{O}$ on $\mathsf{Mod}(A)$.

Definition 3.1. The *non-commutative algebraic space* of A, is the pair

$$\mathfrak{X}_A := \big(\mathsf{Mod}(A), \mathcal{O} \big),$$

where $\mathcal{O}$ is the *structure object* of $\mathfrak{X}_A$. The *tangent space* of $\mathfrak{X}_A$ at M is the matrix $T_{\mathsf{M}} := (\operatorname{Ext}^1_A(M_i, M_j)_{ij})$. We say that $\mathfrak{X}_A$ has property **P** if $\operatorname{Spec}(\mathfrak{Z}(A))$ has this property.

Remark 3.1. (i) Note that $\mathcal{O}$ is not a sheaf.

- (ii) Since $\mathcal{O}$ is constructed by deformation theory, the structure object is only defined fibre-by-fibre over $\mathfrak{o}$. The construction *can* be made in a formal sense without referring to any special type of base but this is not very useful in practice. In fact:

- (iii) The ring $(\hat{H}_{ij})$ is constructed in the same way as in the commutative case (although it is more complicated): successively lifting the tangent structure (defined over a field) and killing obstructions to further liftings.

The following is definition 2.8 in [Lar23b].

Definition 3.2. Let k be a field and let A and S be k-algebras.

- (a) An *étale S-rational point* on $\mathfrak{X}_A$ is an algebra morphism

$$\boldsymbol{\xi} : A \to S$$

  such that

$$A/\ker\boldsymbol{\xi} = A/\mathfrak{m}_1 \times A/\mathfrak{m}_2 \times \cdots \times A/\mathfrak{m}_s$$

  is a direct product of prime rings. If the $A/\mathfrak{m}_i$ are artinian, being prime is equivalent to being simple so the $\mathfrak{m}_i$ are maximal ideals. This applies in particular to the case when S is artinian.

(b) The *underlying étale point* of $\boldsymbol{\xi}$ is the set of algebras $\bar{\xi}_i := A/\mathfrak{m}_i$.

(c) If all $\bar{\xi}_i$ are simple, the point is *closed*, otherwise it is *non-closed*. The point is *open* if all the $\bar{\xi}_i$ are non-simple.

(d) If $s = 1$, the map $\boldsymbol{\xi}$ is an *S-rational point*, which we write in non-boldface: ξ; the algebra $\bar{\xi} = A/\mathfrak{m}$ is then the (unique) underlying point of ξ.

(e) If $S = \operatorname{End}_L(M)$ for some field L and M finite-dimensional over L, we say that ξ is an *L-rational point*.

(f) $\boldsymbol{\xi}$ is a *geometric étale point* if it is closed and $\mathfrak{Z}(\bar{\xi}_i) = k^{\mathrm{al}}$ for all i.

As usual we denote the S-rational points on $\mathfrak{X} = \underline{\mathsf{Mod}}(A)$ as

$$\mathfrak{X}(S) = \underline{\mathsf{Mod}}(A)(S).$$

4 The Jackson space

4.1 Polynomial identity algebras

Let R be a commutative ring and let $\mathbb{Z}\langle\mathbf{x}\rangle = \mathbb{Z}\langle x_1, x_2, \ldots, x_n\rangle$ be the free $\mathbb{Z}$-algebra on n generators. An R-algebra A is a *polynomial identity algebra* (*PI-algebra*) if there is an n and a $P(\mathbf{x}) \in \mathbb{Z}\langle\mathbf{x}\rangle$ such that $P(a_1, a_2, \ldots, a_n) = 0$ for all n-tuples $(a_1, a_2, \ldots, a_n) \in A^n$.

Examples abound: all commutative algebras, Azumaya algebras (and so matrix algebras and central simple algebras) and algebras that are finite modules over their centres, are arguably the most important ones.

Let A be a PI-algebra with centre $\mathfrak{Z}(A)$. Then every ideal in A intersects $\mathfrak{Z}(A)$ non-trivially. Furthermore, there is a dense open subscheme $\mathtt{azu}(A) \subset \operatorname{Specm}(\mathfrak{Z}(A))$ such that for all $\mathfrak{m} \in \mathtt{azu}(A)$ the extension of $\mathfrak{m}$ to A is also a maximal ideal. The subscheme $\mathtt{azu}(A)$ is called the *Azumaya locus* of A. The complement,
$$\mathtt{ram}(A) := \operatorname{Specm}(\mathfrak{Z}(A)) \setminus \mathtt{azu}(A),$$
is the support of a Cartier divisor and is called the *ramification locus*. We will be a bit sloppy and refer to $\mathtt{azu}(A)$ and $\mathtt{ram}(A)$ both as subsets of $\mathfrak{Z}(A)$ and as subschemes of $\operatorname{Spec}(A)$.

We will routinely identify an A-module M with its annihilator $\mathfrak{a} := \operatorname{Ann}_A(M)$. If M is a simple A-module, its annihilator is a primitive ideal. In the case of PI-algebras, an ideal being primitive is equivalent to it being maximal so we identify simple modules and maximal ideals via this correspondence.

The following theorem is central in the theory of algebras finite over their centres.

Theorem 4.1 (Müller's theorem)**.** Let A be an affine PI-algebra over a field k and let M and N be simple finite-dimensional A-modules. Then

$$\operatorname{Ext}_A^1(M, N) \neq \emptyset \quad \Longleftrightarrow \quad \operatorname{Ann}(M) \cap \mathfrak{Z}(A) = \operatorname{Ann}(N) \cap \mathfrak{Z}(A).$$

(The annihilators are *left* ideals.) The statement can be rephrased as the equivalence

$$\operatorname{Ext}_A^1(M, N) \neq \emptyset \quad \Longleftrightarrow \quad \operatorname{Ann}(M) \cap \mathfrak{Z}(A) = \operatorname{Ann}(N) \cap \mathfrak{Z}(A) \in \mathtt{ram}(A),$$

since $\mathrm{Ann}(M)$, $\mathrm{Ann}(N)$ are maximal, and so also their intersections with the centre.

Every simple module of a PI-algebra over a field is finite-dimensional over the ground field.

We denote by Ψ the map $\mathrm{Spec}(A) \to \mathrm{Spec}(\mathfrak{Z}(A))$ defined by ideal contraction. When A is finite over $\mathfrak{Z}(A)$ this is a finite morphism in the sense that $\#\Psi^{-1}(\mathfrak{p}) < \infty$ for all $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{Z}(A))$.

4.2 The Jackson algebra

Now, to summarise the constructions made so far bullet-wise:

- We have taken a Kummer extension $A = \mathfrak{o}[\sqrt[n]{x}]$, $x \in \mathfrak{o}$, of degree n;

- On this extension we have chosen a ζ_n^r-derivation;

- From ζ_n^r-derivation we constructed the associated hom-Lie algebra (which is an infinitesimal structure for twisted derivations, analogously to Lie algebras for ordinary derivations) and its "enveloping algebra", $\mathbf{W}_x^{1/n}(r)$.

Hence, $\mathbf{W}_x^{1/n}(r)$ captures the ζ_n^r-infinitesimal structure of $\mathfrak{o}[\sqrt[n]{x}]$.

Clearly, $\mathbf{W}_x^{1/n}(r)$ is quite complicated in general and so is not so easy to work with. Fortunately there is a subalgebra inside $\mathbf{W}_x^{1/n}(r)$ that has some remarkable ring-theoretic, geometric and arithmetic properties, some of which $\mathbf{W}_x^{1/n}(r)$ itself does not enjoy. This subalgebra is isomorphic to a "ζ_n^r-deformation" of the enveloping algebra of the Lie algebra $\mathfrak{sl}_2$. We will now describe this algebra.

Put, in order to simplify notation a bit, $\omega := (1 - \zeta^{2r})$. Recall that $\zeta = \zeta_n$ is assumed to be primitive. Since $\zeta^{-(n-1)} = \zeta$ and $\zeta^{-(n-2)} = \zeta^2$, the algebra

$$S := \mathfrak{o}\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_{n-1}\rangle \big/ I,$$

with

$$I := \Big(\boldsymbol{e}_0\boldsymbol{e}_1 - \zeta^r\boldsymbol{e}_1\boldsymbol{e}_0 - (1 - \zeta^r)\boldsymbol{e}_1,\ \boldsymbol{e}_{n-1}\boldsymbol{e}_0 - \zeta^r\boldsymbol{e}_0\boldsymbol{e}_{n-1} - (1 - \zeta^r)\boldsymbol{e}_{n-1},$$
$$\boldsymbol{e}_{n-1}\boldsymbol{e}_1 - \zeta^{2r}\boldsymbol{e}_1\boldsymbol{e}_{n-1} - x\omega\boldsymbol{e}_0\Big)$$

is easily seen to be a subalgebra of $\mathbf{W}_x^{1/n}(r)$. Now, define the algebra

$$\mathcal{J}_x(r) := \mathfrak{o}\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2\rangle \big/ J, \qquad r \in \mathbb{Z}, \tag{4.1}$$

where J is the ideal

$$J := \Big(\boldsymbol{e}_0\boldsymbol{e}_1 - \zeta^r\boldsymbol{e}_1\boldsymbol{e}_0, \quad \boldsymbol{e}_2\boldsymbol{e}_0 - \zeta^r\boldsymbol{e}_0\boldsymbol{e}_2, \quad \boldsymbol{e}_2\boldsymbol{e}_1 - \zeta^{2r}\boldsymbol{e}_1\boldsymbol{e}_2 - x\boldsymbol{e}_0 - x\omega\Big).$$

Proposition 4.2. The algebras S and $\mathcal{J}_x(r)$ are isomorphic over $\mathfrak{o}\left[\omega^{-1}\right]$, and in particular fibre-wise. Furthermore, $\mathcal{J}_x(r)$ (and hence also S) is an iterated Ore extension (skew polynomial ring). The generator $\boldsymbol{e}_{n-1}$ in S becomes the generator $\boldsymbol{e}_2$ in $\mathcal{J}_x(r)$.

If n is composite with at least two different prime factors, such that ζ^{2r} is primitive, then ω is invertible in $\mathfrak{o}$. Hence, in that case, S and $\mathcal{J}_x(r)$ are isomorphic already over $\mathfrak{o}$.

Definition 4.1. The algebra $\mathcal{J}_x(r)$ is called the *Jackson algebra of level r*. Let w be the Teichmüller character defined by $\sigma(\zeta) = \zeta^{\mathsf{w}(\sigma)}$. The family of algebras

$$\mathcal{J}_x^{\mathrm{tot}} := \left\{ \mathcal{J}_x(\mathsf{w}(\sigma)) \mid \sigma \in \mathbb{Z}/n \right\},$$

is called the *total Jackson algebra*. This is a $\mathbb{Z}/n$-torsor.

We have already indicated the following remark, but it is important enough to repeat.

Remark 4.1. The algebras $\mathcal{J}_x$, $\mathcal{J}_x^{\mathrm{tot}}$ and $\mathbf{W}_x^{1/n}(r)$, encode the Galois structure of $\mathfrak{o}[\sqrt[n]{x}]$ through its ζ^r-derivations, even though we have reduced the number of generators from n to 3.

Remark 4.2. (i) The name "Jackson algebra" is in honour of F.H. Jackson (1870–1960) and his work on q-derivations. Indeed, $\mathcal{J}_x(r)$ is isomorphic to the (enveloping algebra of the) "Jackson-$\mathfrak{sl}_2$", a q-deformed version of the three-dimensional Lie algebra $\mathfrak{sl}_2$, deformed using q-derivations. See [LS07] for the details.

(ii) When $\zeta^{2r} = 1$, the algebra $\mathcal{J}_x(r)$ is either isomorphic to the commutative polynomial algebra $\mathfrak{o}[t_1, t_2, t_3]$ (when $\zeta = 1$) or to the $\mathfrak{o}$-algebra on generators $\boldsymbol{e}_0$, $\boldsymbol{e}_1$, $\boldsymbol{e}_2$ and with relations

$$\boldsymbol{e}_0\boldsymbol{e}_1 + \boldsymbol{e}_1\boldsymbol{e}_0 = 0, \quad \boldsymbol{e}_2\boldsymbol{e}_0 + \boldsymbol{e}_0\boldsymbol{e}_2 = 0, \quad \boldsymbol{e}_2\boldsymbol{e}_1 - \boldsymbol{e}_1\boldsymbol{e}_2 = x\boldsymbol{e}_0.$$

4.3 The centre $\mathfrak{Z}(\mathcal{J}_x(r))$

To simplify notation we will from now on often omit the dependence on r in the notation $\mathcal{J}_x(r)$ and simply write $\mathcal{J}_x$.

As before, we put
$$A_{/\mathfrak{p}} := A \otimes_{\mathfrak{o}} k(\mathfrak{p})$$

for any $\mathfrak{o}$-algebra A.

See [Lar23a] for the proofs of the following theorem and its corollary.

Theorem 4.3. Assume that ζ^r is a primitive n-th root of unity. Then the following holds.

(i) For $x = 0$:

$$\mathfrak{Z}(\mathcal{J}_0)_{/\mathfrak{p}} = k(\mathfrak{p})\Big[\boldsymbol{e}_0^a \boldsymbol{e}_1^b \boldsymbol{e}_2^c \ \Big| \ r(a+2b) \text{ and } r(b-c) \equiv 0 \bmod n\Big].$$

Observe that $k(\mathfrak{p})[\boldsymbol{e}_0^l, \boldsymbol{e}_1^l, \boldsymbol{e}_2^l] \subseteq \mathfrak{Z}(\mathcal{J}_0)_{/\mathfrak{p}}$.

(ii) For $x \neq 0$:
$$k(\mathfrak{p})[\boldsymbol{e}_0^l, \boldsymbol{e}_1^l, \boldsymbol{e}_2^l] \subseteq \mathfrak{Z}(\mathcal{J}_x)_{/\mathfrak{p}}$$

where $l \in \mathbb{N}$ is such that lr is the least multiple of n.

11

In both cases we have

(iii) $\mathcal{J}_x$ is an Auslander-regular, homologically homogeneous[1], noetherian, fibre-wise Cohen–Macaulay domain, finite as a module over its centre and hence a polynomial identity ring (PI) of $\mathrm{pideg}(\mathcal{J}_x) = n$;

(iv) $\mathcal{J}_x$ is a maximal order in its division ring of fractions;

(v) $\mathrm{Spec}(\mathfrak{Z}(\mathcal{J}_x))$ is a normal, irreducible scheme of dimension three.

(vi) $\mathrm{Spec}(\mathfrak{Z}(\mathcal{J}_0))$ is in addition *fibre-wise Cohen–Macaulay* in the commutative sense, i.e.,
$$\mathrm{Spec}\big(\mathfrak{Z}(\mathcal{J}_x)_{/\mathfrak{p}}\big) = \mathrm{Spec}\big(\mathfrak{Z}(\mathcal{J}_0) \otimes_{\mathfrak{o}} k(\mathfrak{p})\big)$$
is a Cohen–Macaulay scheme for all $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{o})$.

In fact, in [Lar23a], the centre in case (ii) is computed explicitly, but we won't be needing this in this paper.

We immediately get the following corollary.

Corollary 4.4. With the notation as above:

(i) The algebra $(\mathcal{J}_x)_{/\mathfrak{p}}$ is finite as a module over $k(\mathfrak{p})\big[e_0^l, e_1^l, e_2^l\big]$.

(ii) Hence, the ring extension $k(\mathfrak{p})\big[e_0^l, e_1^l, e_2^l\big] \subseteq \mathfrak{Z}(\mathcal{J}_x)$ is finite, and consequently the morphism
$$\psi: \ \mathrm{Spec}\big(\mathfrak{Z}(\mathcal{J}_x)\big) \to \mathbb{A}_{(l)}^3 := \mathrm{Spec}\Big(k(\mathfrak{p})\big[e_0^l, e_1^l, e_2^l\big]\Big)$$
is finite as a morphism of schemes. We put l in the notation to indicate that we have a weighted version of the affine three-space.

(iii) In the other direction, any maximal $\mathfrak{m}$ in $\mathfrak{Z}(\mathcal{J}_x)$ splits into i maximal ideals in $\mathcal{J}_x$, where $1 \le i \le m$, and where m is the rank of $\mathcal{J}_x$ as a module over $\mathfrak{Z}(\mathcal{J}_x)$. In other words,
$$\Psi^{-1}(\mathfrak{m}) = \Big\{\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_i \ \Big| \ \text{for some } 1 \le i \le m\Big\}.$$
Recall that Ψ is the contraction map on ideals.

(iv) Also, any maximal $\mathfrak{m}$ in $k(\mathfrak{p})\big[e_0^l, e_1^l, e_2^l\big]$ splits into j maximal ideals in $\mathcal{J}_x(r)$, where $1 \le j \le n$, and where n is the rank of $\mathcal{J}_x$ as a module over $k(\mathfrak{p})\big[e_0^l, e_1^l, e_2^l\big]$. In other words,
$$\big(\psi \circ \Psi\big)^{-1}(\mathfrak{m}) = \Big\{\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_j \ \Big| \ \text{for some } 1 \le j \le n\Big\}.$$

I conjectured in [Lar23a] that $\mathrm{Spec}(\mathfrak{Z}(\mathcal{J}_0))$ is singular for all n, and that it might also be rational. In fact, I could prove the following theorem.

Theorem 4.5. Let K be a field of characteristic zero and let $\mathcal{J}_x^{\mathrm{a}}$ be the base change $(\mathcal{J}_x)_{/K} \otimes_K K^{\mathrm{a}}$ of $(\mathcal{J}_x)_{/K}$ to the algebraic closure K^{al}. Then

(i) $\mathrm{Spec}\big(\mathfrak{Z}(\mathcal{J}_x^{\mathrm{a}})\big)$ has rational singularities;

(ii) both $\mathrm{Spec}\big(\mathfrak{Z}(\mathcal{J}_x^{\mathrm{a}})\big)$ and $\mathrm{Spec}\big(\mathfrak{Z}((\mathcal{J}_x)_{/K})\big)$ are Cohen–Macaulay.

The question I couldn't, and still can't, answer in [Lar23a] is whether this also implies that $\mathrm{Spec}\big(\mathfrak{Z}((\mathcal{J}_x)_{/K})\big)$ itself has rational singularities.

---

[1]This is another regularity property, which I won't define, of non-commutative rings, generalising the commutative counterpart.

4.4 The non-commutative space $\mathfrak{X}_{\mathcal{J}_x}$

4.4.1 Properties of $\mathfrak{X}_{\mathcal{J}_x}$

Since $\mathcal{J}_x$ is finite as a module over its centre, we can directly infer the following result from the previous discussions.

Corollary 4.6. The space $\mathfrak{X}_{\mathcal{J}_x}$ satisfies the following properties.

(i) It is Auslander-regular, homologically homogeneous, noetherian and irreducible.

(ii) It is fibre-wise Cohen–Macaulay of dimension 3.

(iii) It is fibre-wise *rational* in the sense that it is a maximal order in its division ring of fractions.

(iv) It has fibre-wise (at worst) *geometric* rational singularities in that its base change to the algebraic closure has rational singularities.

(v) Contraction of ideals defines a finite morphism $\mathfrak{X}_{\mathcal{J}_x} \to \mathrm{Spec}(\mathfrak{Z}(\mathcal{J}_x))$ which is one-to-one over $\mathtt{azu}(A)$, and j-to-one, for some $1 \le j \le n$, over $\mathtt{ram}(A)$. We view $\mathfrak{X}_{\mathcal{J}_x}$ as fibred over $\mathrm{Spec}(\mathfrak{Z}(A))$.

Note that $\mathfrak{X}_{\mathcal{J}_x}$ satisfies regularity properties generalising the commutative regularity condition even though the centre might have singularities.

We put

$$\mathfrak{X}_{\mathcal{J}_x}^{\mathrm{tot}} := \bigsqcup_{\sigma \in \mathbb{Z}/n} \mathfrak{X}_{\mathcal{J}_x(\mathsf{w}(\sigma))},$$

the *total Jackson space*. This is a $\mathbb{Z}/n$-torsor via the $\mathbb{Z}/n$-action on $\mathcal{J}_x^{\mathrm{tot}}$. We can partition $\mathfrak{X}_{\mathcal{J}_x}^{\mathrm{tot}}$ with respect to subgroups of $\mathbb{Z}/n$ into sets (not disjoint of course).

4.4.2 The locus of one-dimensional points and its infinitesimal structure

For illustration we will now study the rational one-dimensional points. Thus, for this section we let k be *any* field with a primitive n-th root of unity $\zeta := \zeta_n$. Furthermore, we identify 1-dimensional points, 1-dimensional modules and their annihilator ideals. These points are maximal since 1-dimensional (over k) modules are simple.

Note first that any 1-dimensional $\mathcal{J}_x$-module must lie on the ramification locus. Indeed, any module in $\mathtt{azu}(A)$ corresponds to a central simple algebra of dimension n^2.

Assume $\zeta^{2r} \ne 1$. Then the relations reduce to

$$(1 - \zeta^r)\boldsymbol{e}_0 \boldsymbol{e}_1 = 0$$
$$(1 - \zeta^r)\boldsymbol{e}_0 \boldsymbol{e}_2 = 0$$
$$(1 - \zeta^{2r})\boldsymbol{e}_1 \boldsymbol{e}_2 = x\boldsymbol{e}_0 + x(1 - \zeta^{2r}).$$

This implies that $x(\boldsymbol{e}_0 + (1 - \zeta^{2r})) = 0$ so, if $x \ne 0$, we have that $(\zeta^{2r} - 1, 0, 0)$ is a one-dimensional module. In addition, the conic (hyperbola) C_x given by $\boldsymbol{e}_1 \boldsymbol{e}_2 = x$ in the plane $\boldsymbol{e}_0 = 0$ consists entirely of commutative points (i.e., one-dimensional modules). When $x = 0$, we find that the one-dimensional modules lie on the union of the coordinate planes.

Remark 4.3. When $\zeta^{2r} = 1$ we may assume that $\zeta^r = -1$. The relations

$$\boldsymbol{e}_0\boldsymbol{e}_1 + \boldsymbol{e}_1\boldsymbol{e}_0 = 0, \quad \boldsymbol{e}_2\boldsymbol{e}_0 + \boldsymbol{e}_0\boldsymbol{e}_2 = 0, \quad \boldsymbol{e}_2\boldsymbol{e}_1 - \boldsymbol{e}_1\boldsymbol{e}_2 = x\boldsymbol{e}_0$$

imply that

$$2\boldsymbol{e}_0\boldsymbol{e}_1 = 0, \quad 2\boldsymbol{e}_0\boldsymbol{e}_2 = 0, \quad x\boldsymbol{e}_0 = 0.$$

Consider first when $\mathrm{char}(k) \neq 2$. When $x \neq 0$ we get that the plane $\{\boldsymbol{e}_0 = 0\}$ consists entirely of one-dimensional points. On the other hand, when $x = 0$, we get the union of the coordinate planes. Now, if $\mathrm{char}(k) = 2$, we get, when $x \neq 0$, the plane $\{\boldsymbol{e}_0 = 0\}$ and, if $x = 0$, the whole $\mathbb{A}^3$.

We begin by working in $\boldsymbol{e}_0 = 0$. Let $k \subseteq k'$ be a field extension and consider the k'-rational point

$$\xi_{(a,b)} := k' \cdot \boldsymbol{f}, \quad \text{with} \quad \boldsymbol{e}_1 \cdot \boldsymbol{f} = a\boldsymbol{f}, \quad \boldsymbol{e}_2 \cdot \boldsymbol{f} = b\boldsymbol{f}, \quad a, b \in k',$$

and similarly $\xi_{(u,v)}$. Then we have the following results.

Proposition 4.7. Put $\boldsymbol{\xi} := \{\xi_{(a,b)}, \xi_{(u,v)}\}$ be an étale k'-rational point on $\mathfrak{X}_{\mathscr{J}_x}$. Recall that $T_{\boldsymbol{\xi}}$ denotes the tangent space at $\boldsymbol{\xi}$.

(i) Suppose $x \neq 0$ and $\zeta^{2r} \neq 1$. Then,

$$T_{\boldsymbol{\xi}} = \mathrm{Ext}^1_{\mathscr{J}_x}\big(\xi_{(a,b)}, \xi_{(u,v)}\big) = \begin{cases} k, & \text{when } a = \zeta^r u, \text{ and } v = \zeta^r b \\ k', & \text{when } a = \zeta^{2r} u, \text{ and } v = \zeta^{2r} b \\ k', & \text{when } a = u, \text{ and } b = v. \end{cases}$$

In all other cases $\mathrm{Ext}^1_{\mathscr{J}_x}\big(\xi_{(a,b)}, \xi_{(u,v)}\big) = 0$.

(ii) Suppose $x = 0$ and $\zeta^{2r} \neq 1$. Then

$$T_{\boldsymbol{\xi}} = \mathrm{Ext}^1_{\mathscr{J}_x}\big(\xi_{(a,b)}, \xi_{(u,v)}\big) = \begin{cases} k', & \text{when } a = u, \text{ and } b = v \\ k', & \text{when } a = \zeta^{2r} u, \text{ and } v = \zeta^{2r} b \\ (k')^2, & \text{if when } a = b = u = v = 0 \\ 0, & \text{otherwise}. \end{cases}$$

(iii) Suppose $x \neq 0$ and $\zeta^{2r} = 1$. Then

$$T_{\boldsymbol{\xi}} = \mathrm{Ext}^1_{\mathscr{J}_x}\big(\xi_{(a,b)}, \xi_{(u,v)}\big) = \begin{cases} k', & \text{when } a = u, \text{ and } b = v \\ 0, & \text{otherwise}. \end{cases}$$

(iv) Suppose $x = 0$ and $\zeta^{2r} = 1$. Then

$$T_{\boldsymbol{\xi}} = \mathrm{Ext}^1_{\mathscr{J}_x}\big(\xi_{(a,b)}, \xi_{(u,v)}\big) = \begin{cases} k', & \text{when } a = \pm u, \, b = \pm v, \, \mathrm{char}(k) \neq 2 \\ (k')^3 & \text{when } a = u, \, b = v, \, \mathrm{char}(k) = 2. \end{cases}$$

Proof. The proof (which is rather simple) can be found, together with other information, in [Lar23a]. $\square$

From the above, one can construct the ring object $\mathfrak{O}$ over families of 1-dimensional modules. Even though the result will probably be hard to interpret I feel that it can be helpful to see what $\mathfrak{O}$ actually look like in practice.

We only write it out for families of two modules.

Proposition 4.8. Let the notation be as above. Modulo possible obstructions the versal bases for the deformations of $\boldsymbol{\xi}$ are the following.

(i) Suppose $x \neq 0$ and $\zeta^{2r} \neq 1$. Then, for $j = 1, 2$,

$$\hat{\mathfrak{O}}_{\boldsymbol{\xi}} = \begin{pmatrix} \mathrm{End}_{k'}(\xi_{(\zeta^{jr}u,b)}) \otimes k'[[t_{11}]] & \mathrm{Hom}_{k'}(\xi_{(\zeta^{jr}u,b)}, \xi_{(u,\zeta^{jr}b)}) \otimes \langle t_{12} \rangle \\ \mathrm{Hom}_{k'}(\xi_{(u,\zeta^{jr}b)}, \xi_{(\zeta^{jr}u,b)}) \otimes \langle t_{21} \rangle & \mathrm{End}_{k'}(\xi_{(\zeta^{jr}u,b)}) \otimes k'[[t_{22}]] \end{pmatrix},$$

with algebraisation,

$$\mathfrak{O}_{\boldsymbol{\xi}} = \begin{pmatrix} \mathrm{End}_{k'}(\xi_{(\zeta^{jr}u,b)}) \otimes k'[t_{11}] & \mathrm{Hom}_{k'}(\xi_{(\zeta^{jr}u,b)}, \xi_{(u,\zeta^{jr}b)}) \otimes \langle t_{12} \rangle \\ \mathrm{Hom}_{k'}(\xi_{(u,\zeta^{jr}b)}, \xi_{(\zeta^{jr}u,b)}) \otimes \langle t_{21} \rangle & \mathrm{End}_{k'}(\xi_{(\zeta^{jr}u,b)}) \otimes k'[t_{22}] \end{pmatrix},$$

in all non-zero cases. In the other cases

$$\hat{\mathfrak{O}}_{\boldsymbol{\xi}} = \mathfrak{O}_{\boldsymbol{\xi}} = \mathrm{Hom}_{k'}(\xi_{(a,b)}, \xi_{(u,v)}).$$

(ii) Suppose $x = 0$ and $\zeta^{2r} \neq 1$. Then, the first two rows combine to the case in (i), while the second is

$$\hat{\mathfrak{O}}_{\xi_{(0,0)}} = \mathrm{End}_{k'}(\xi_{(0,0)}) \otimes k'\langle\langle t_1, t_2 \rangle\rangle, \quad \mathfrak{O}_{\xi_{(0,0)}} = \mathrm{End}_{k'}(\xi_{(0,0)}) \otimes k'\langle t_1, t_2 \rangle.$$

(iii) Suppose $x \neq 0$ and $\zeta^{2r} = 1$. Then

$$\hat{\mathfrak{O}}_{\xi_{(a,b)}} = \mathrm{End}_{k'}(\xi_{(a,b)}) \otimes k'[[t]], \quad \mathfrak{O}_{\xi_{(a,b)}} = \mathrm{End}_{k'}(\xi_{(a,b)}) \otimes k'[t]$$

and $\hat{\mathfrak{O}}_{\boldsymbol{\xi}} = \mathfrak{O}_{\boldsymbol{\xi}} = \mathrm{Hom}_{k'}(\xi_{(a,b)}, \xi_{(u,v)})$ in all other cases.

(iv) Suppose $x = 0$ and $\zeta^{2r} = 1$ and let $\boldsymbol{\xi}$ be the étale rational point $\boldsymbol{\xi} = \{\xi_{(a,b)}, \xi_{(-a,-b)}\}$. Then, when $\mathrm{char}(k) \neq 2$,

$$\hat{\mathfrak{O}}_{\boldsymbol{\xi}} = \begin{pmatrix} \mathrm{End}_{k'}(\xi_{(a,b)}) \otimes k'[[t_{11}]] & \mathrm{Hom}_{k'}(\xi_{(a,b)}, \xi_{(-a,-b)}) \otimes \langle t_{12} \rangle \\ \mathrm{Hom}_{k'}(\xi_{(-a,-b)}, \xi_{(a,b)}) \otimes \langle t_{21} \rangle & \mathrm{End}_{k'}(\xi_{(-a,-b)}) \otimes k'[[t_{22}]] \end{pmatrix}$$

and when $\mathrm{char}(k) = 2$,

$$\hat{\mathfrak{O}}_{\xi_{(a,b)}} = \mathrm{End}_{k'}(\xi_{(a,b)}) \otimes k'\langle\langle t_1, t_2, t_3 \rangle\rangle,$$

both with obvious algebraisations.

Be sure to notice the situation when $\mathrm{char}(k) = 2$.

5 Ramification

We will separate the discussion into two cases: (1) the geometric case, and (2) the arithmetic case. The geometric case is essentially trivial.

5.1 The geometric case

This is the case when the base $\mathfrak{o}$ is an algebra over a field k, such that $\zeta_n \in k$. The discussion below applies to both $\mathcal{J}_x$ and $\mathbf{W}_x^{1/n}$, but we will only write it out for $\mathcal{J}_x$.

Assume $\mathfrak{o} = k[b_1, b_2, \ldots, b_m]/I$. Hence

$$A = \mathfrak{o}[\sqrt[n]{x}] = \mathfrak{o}[t]/(t^n - x) = k[b_1, b_2, \ldots b_m, t]/(I, t^n - x), \quad x \in \mathfrak{o}.$$

The zero-locus of x is the branch locus, $\texttt{branch}(A_{/\mathfrak{o}})$, of $A_{/\mathfrak{o}}$. Over $\mathfrak{p} \notin \texttt{branch}(A_{/\mathfrak{o}})$ the cover $\mathrm{Spec}(A) \to \mathrm{Spec}(\mathfrak{o})$ is étale (and in particular unramified) and so the fibre over $\mathfrak{p}$ is

$$A \otimes_{\mathfrak{o}} k(\mathfrak{p}) = \prod_{i=1}^{\ell} k_i, \quad 1 \le \ell \le \deg(A_{/\mathfrak{o}}),$$

and where each k_i a finite field extension of $k(p)$. The group $\mathbb{Z}/n$ acts transitively on the points of the fibre. Therefore we can construct the algebras $\mathcal{J}_x$ (and $\mathbf{W}_x^{1/n}$) fibre-wise, but that is not what we are going to do.

Since n is invertible on the base the only interesting case of ramification is when $\mathfrak{p} \mid x$, i.e., when $\mathfrak{p} \in \texttt{branch}(A_{/\mathfrak{o}})$. Therefore,

Proposition 5.1. Let $\mathfrak{o}$ and A be as above. Then

(i) if $\mathfrak{p} \notin \texttt{branch}(A_{/\mathfrak{o}})$, the reduction of $\mathcal{J}_x$ modulo $\mathfrak{p}$ gives a generic (i.e., $x \ne 0$) $\mathcal{J}_{x,/\mathfrak{p}}$;

(ii) if $\mathfrak{p} \in \texttt{branch}(A_{/\mathfrak{o}})$, the reduction of $\mathcal{J}_x$ modulo $\mathfrak{p}$ gives a quantum affine algebra $\mathcal{J}_{0,/\mathfrak{p}}$.

Hence, the ramification properties of $A_{/\mathfrak{o}}$ determines the structure of the algebras $\mathcal{J}_x$ fibre-wise. The converse is also true in the geometric case: the structure of $\mathcal{J}_x$ can be used to read off the ramification properties of $A_{/\mathfrak{o}}$ fibre-wise.

5.2 The arithmetic case

In a sense the geometric case is simple enough, it only comes down to the fact that Kummer extensions have simple properties when n is invertible on all fibres.

The arithmetic case is not so straightforward since the fibres have characteristic that can divide n. Let $\mathfrak{o}_K$ be the ring of integers in a number field K such that $\zeta_n \in \mathfrak{o}_K$.

Consequently, $A = \mathfrak{o}_K[\sqrt[n]{x}]$, $x \in \mathfrak{o}_K$. The branch locus is still the zero-locus of x, but now there are more possible types of ramification. In this paper we will only consider ramification at closed points, so ramification coming from inseparability (or imperfectness) of the residue class rings, will not be an issue.

Assume now that $p \mid n$, say $n = p^k m$. Then, $\zeta^n = 1 \iff (\zeta_n^m - 1)^{p^k} = 0$, implying that $\zeta^m = 1$ for $m < n$. Hence there are no, non-trivial, primitive n-th roots of unity in this case.

Proposition 5.2. Let $A = \mathfrak{o}_K[\sqrt[n]{x}]$, with $x \in \mathfrak{o}_K$, and let $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{o}_K)$.

(i) If $\mathfrak{p} \nmid n$ and $\mathfrak{p} \nmid x$, the extension is unramified and $\mathfrak{X}_{\mathcal{J}_x} \otimes k(\mathfrak{p})$ is generic;

(ii) if $\mathfrak{p} \nmid n$ and $\mathfrak{p} \mid x$, the extension is tamely ramified (total if $\mathfrak{p}^2 \nmid x$) and $\mathfrak{X}_{\mathcal{J}_0} \otimes k(\mathfrak{p})$ is a quantum affine space;

(iii) if $\mathfrak{p} \mid n$ and $\mathfrak{p} \nmid x$, the extension is ramified and

$$\mathfrak{X}_{\mathcal{J}_x} \otimes k(\mathfrak{p}) = \mathfrak{X}_{\mathbf{A}^1_{k(\mathfrak{p})}},$$

where

$$\mathbf{A}^1_{k(\mathfrak{p})} := \frac{k(\mathfrak{p})[u]\langle t, \partial \rangle}{(\partial t - t\partial - u)},$$

is the first Weyl algebra over the affine line, which in characteristic p, is Azumaya, and, finally

(iv) if $\mathfrak{p} \mid n$ and $\mathfrak{p} \mid x$, the extension is ramified and $\mathfrak{X}_{\mathcal{J}_x} \otimes k(\mathfrak{p})$ is the affine three-space.

Observe that we cannot distinguish the ramification types (tame/wild) in (iii) and (iv). On the other hand, the partition of $\mathfrak{X}^{\text{tot}}_{\mathcal{J}_x}$ with respect to subgroups of $\mathbb{Z}/n$ mentioned before can clearly be used with the ramification groups. However, the result will obviously not be visible in the structure of the spaces $\mathfrak{X}_{\mathcal{J}_x}$ themselves. Nevertheless, maybe studying the relation (via non-commutative "morphisms" between the elements in the partitions) might be used in some way.

Proof. If $\mathfrak{p} \nmid n$ and $\mathfrak{p} \nmid x$ the extension is unramified and $\mathcal{J}_{x/\mathfrak{p}}$ is a generic Jackson algebra since all n-the roots of unity are in $k(\mathfrak{p})$. On the other hand, if $\mathfrak{p} \nmid n$ and $\mathfrak{p} \mid x$, the ramification is tame and we end up in the affine quantum algebra case $\mathcal{J}_{0/\mathfrak{p}}$. If, in addition $\mathfrak{p}^2 \nmid x$, the ramification is total. If $\mathfrak{p} \mid n$, then every ζ_n reduces to 1 modulo $\mathfrak{p}$ so get two the cases in (iii) and (iv). $\square$

6 Torsion points and elliptic Jackson spaces

We will now construct the algebra $\mathcal{J}_x$ from the torsion field of elliptic curves with a K-rational torsion point and show that $\mathcal{J}_x$ encodes the reduction properties of the elliptic curve.

Let K be a local field and adjoin ζ_p, a primitive p-th root of unity for p a prime and put $L := K(\zeta_p)$. Let E be an elliptic curve over K with a (non-trivial) K-rational p-torsion point. Then $K(E[p])/L$ is a Kummer extension of degree p or 1, with $K(E[p])$ the field generated by the p-torsion points of E. Hence, $K(E[p]) = L[\sqrt[p]{x}] = L[t]/(t^p - x)$, for some $x \in L$, or $K(E[p]) = L$. See [Yas13], for instance. We can, and will, assume that $x \in \mathfrak{o}_L$. In order to achieve this we might need to multiply x with a unit (clearing denominators).

The criterion of Néron–Ogg–Shafarevich (NOS) gives that if E has good reduction at $\ell \neq p$, $\ell \in \text{Spec}(\mathbb{Z})$, then $K(E[p])/K$ is unramified at ℓ. We will need the following generalisation due to M. Kida. We will denote the reduction types of elliptic curves with the corresponding Kodaira symbols.

Theorem 6.1. Let E be an elliptic curve over a local field K, finite over $\mathbb{Q}_\ell$. Put $n := -v(j(E))$, where v is the valuation of K.

(a) If $p \geq 3$, $K(E[p])/K$ is unramified at the place of K over ℓ, if and only if

$$\text{Type}(E) = \begin{cases} I_0, & \text{or} \\ I_n, & \text{if } p \mid n. \end{cases}$$

In other words, $K(E[p])/K$ is unramified if and only if E has semistable reduction (over K).

(b) If $p = 2$, $K(E[2])/K$ is unramified if and only if

$$\text{Type}(E) = \begin{cases} I_0, & \text{or} \\ I_n, & \text{if } n \text{ even, or} \\ I_0^* \text{ or } I_n^*, & \text{with } n \text{ odd.} \end{cases}$$
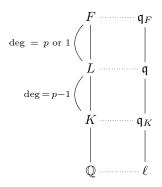
Proof. See [Kid03, Theorem 1.1] $\qquad \square$

The following lemma holds also when K i a number field.

Lemma 6.2. A prime $\mathfrak{p}$ in K is ramified in $L = K(\zeta_p)$ if and only if $\mathfrak{p} \mid p$ and $(p-1) \nmid e(\mathfrak{p})$, where $e(\mathfrak{p})$ is the absolute ramification index of $\mathfrak{p}$. In particular, if $e(\mathfrak{p}) = 1$ and $p \geq 3$, $\mathfrak{p}$ is ramified if and only if $\mathfrak{p} \mid p$. If $p = 2$, $\mathfrak{p}$ is ramified if and only if $\mathfrak{p} \mid p$ (regardless of $e(\mathfrak{p})$).

Proof. See [CDyDO03, Theorem 1.1(1)]. $\qquad \square$

Put $F := K(E[p])$ and consider the following tower of extensions:

Throughout, we put $k := k(\mathfrak{q})$, the residue class field of $\mathfrak{q}$.

Observe that $[F : L] = p$ or $[F : L] = 1$, $[L : K] = p - 1$, so either $[F : K] = p(p-1)$ or $[F : K] = p - 1$.

Remark 6.1. It seems that the case $[F : L] = 1$ is rare. Recall that the roots of the modular equation $\Phi_p(X, j(E)) = 0$ are the j-values of all elliptic curves isogeneous to E with cyclic kernel of degree p. From this follows that any cyclic isogeny is defined over a subfield of $K(E[p])$ and so

$$L \subseteq L \cdot K(\Phi_p(X, j(E))) \subseteq K(E[p]).$$

Therefore a necessary condition for $F = K(E[p])$ to be equal to L is that the modular polynomial $\Phi_p(X, j(E))$ (of degree p) splits completely over L, i.e., that L is a splitting field for $\Phi_p(X, j(E))$. Hence it is necessary that E is represented

18

by an L-rational point on the modular curve $X_0(p)_{/\mathbb{Q}}$. Further evidence of this scarcity can be found in [GJLR16], where it is proved that if $K = \mathbb{Q}$, the only possible values for n where $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$ can happen are $2, 3, 4$ and 5.

Remark 6.2. Assuming the degree of F/L is bigger than one, it is fairly simple to find a generator x such that $F = L[\sqrt[p]{x}]$. See the (sketch of) the proof of [Yas13, Proposition 2.5].

I want to point out that many of the statements made below are well-known. However, I made the decision to prove most of them anyway, probably with more difficult proofs than needed. The main reasons are that I had problem finding suitable references and also that I found some joy in coming up with the proofs, in addition to fresh insights.

We need to separate the following into two cases: $\ell \neq p$, and $\ell = p$.

6.1 Special fibres of elliptic Jackson spaces; the case $\ell \neq p$

By hypotheses here then, $\mathfrak{q} \nmid p$. Then $\mathfrak{q}_K$ is unramified in L by lemma 6.2. Assume $[F : L] \neq 1$.

Lemma 6.3. Let $\mathfrak{q}$ be a prime in L over $\mathfrak{q}_K$. Then $\mathfrak{q}$ is unramified in F/L if and only if $v_{\mathfrak{q}}(x) \equiv 0 \pmod{p}$. In particular, if $\mathfrak{q} \nmid x$, $\mathfrak{q}$ is unramified.

Proof. See [Cas67, Exercise 2.12]. □

Remark 6.3. Notice that $\mathfrak{q}$ can be unramified even if $\mathfrak{q} \mid x$. Namely if

$$x = \mathfrak{a}\mathfrak{q}^{p^t}, \quad t \geq 1 \quad \text{or, equivalently,} \quad v_{\mathfrak{q}}(x) \not\equiv 0 \pmod{p},$$

for some ideal $\mathfrak{a}$ in $\mathfrak{o}_L$, relatively prime to $\mathfrak{q}$. This is seen by a change of divisor x to an isomorphic, unramified extension (see [Cas67, Exercise 2.12]). In other words, we can change x to an element $y \in L$ such that

$$F = L[\sqrt[p]{x}] \simeq L[\sqrt[p]{y}], \quad \text{with } \mathfrak{q} \nmid y.$$

Now since $\mathfrak{q}_K$ is unramified in L, $\mathfrak{q}$ is unramified in F if and only if $v_{\mathfrak{q}}(x) \equiv 0 \pmod{p}$. Also, since $\ell \neq p$, $\zeta_p \not\equiv 1 \pmod{\ell}$. Note that

$$e(\mathfrak{q}_F|\mathfrak{q}_K) = e(\mathfrak{q}_F|\mathfrak{q})e(\mathfrak{q}|\mathfrak{q}_K). \tag{6.1}$$

Theorem 6.4. Suppose $\ell \neq p$. Then E has semistable reduction at $\mathfrak{q}_K \mid \ell$ if and only if, possibly after a change of generator x, $\mathcal{J}_x \otimes_L k$ is generic, or, equivalently, that $\mathfrak{X}_{\mathcal{J}_x} \otimes_L k$ is a generic Jackson space.

The claim is independent of r since ζ^r is primitive for all $1 \leq r \leq p - 1$. However, the resulting spaces are non-isomorphic in general.

Proof. Assume first that E is semistable. This is, by Kida's theorem 6.1, equivalent to $\mathfrak{q}_K$ unramified in F/K. Since the left-hand-side of (6.1) is then 1, we see that $\mathfrak{q}$ is unramified in F/L. By lemma 6.3 this is equivalent to $v_{\mathfrak{q}}(x) \equiv 0 \pmod{p}$. Therefore, either $\mathfrak{q} \nmid x$ and the reduction becomes generic; or $x = \mathfrak{a}\mathfrak{q}^s$, with $p \mid s$, in which case remark 6.3 implies that we can change generator $x \to y$ so that $F = L[\sqrt[p]{y}]$ and $\mathfrak{q} \nmid y$, and therefore the reduction is still generic (after change to y).

Conversely, suppose $\mathcal{J}_x \otimes_L k$ is generic. Then $x \not\equiv 0 \pmod{\mathfrak{q}}$. Hence $v_{\mathfrak{q}}(x) \equiv 0 \pmod{p}$, implying that $\mathfrak{q}$ is unramified in F by lemma 6.3. From (6.1) we thus find that $e(\mathfrak{q}_F | \mathfrak{q}_K) = e(\mathfrak{q} | \mathfrak{q}_K)$. Since $\mathfrak{q}_K \nmid p$, lemma 6.2 implies that $e(\mathfrak{q} | \mathfrak{q}_K) = 1$ and so $\mathfrak{q}_K$ is unramified in F. Kida's theorem then gives that E is semistable. The proof is complete. $\qquad\square$

Theorem 6.5. Suppose $\ell \neq p$. If E has non-semistable reduction at $\mathfrak{q}_K \mid \ell$, then $\mathfrak{X}_{\mathcal{J}_x} \otimes_L k$ is a (possible trivial, depending on the roots of unity in k) quantum affine space.

Suppose, conversely, that $\mathfrak{X}_{\mathcal{J}_x} \otimes_L k$ is a quantum affine space, implying that $x = \mathfrak{a}\mathfrak{q}^s$.

(i) If $p \nmid s$, then E has non-semistable reduction;

(ii) if $p \mid s$, then E has semistable reduction.

Proof. Since $\mathfrak{q}_K \nmid p$, lemma 6.2 implies that $\mathfrak{q}_K$ is unramified in L. From (6.1) we find that $e(\mathfrak{q}_F | \mathfrak{q}_K) = e(\mathfrak{q}_F | \mathfrak{q}_K)$ and so if $\mathfrak{q}$ ramifies in F, $\mathfrak{q}$ must also ramify in F. Therefore, lemma 6.3 implies that $v_{\mathfrak{q}}(x) \not\equiv 0 \pmod{p}$. Hence $x = 0$ in $\mathcal{J}_x \otimes_L k$.

Conversely, assume $x = \mathfrak{a}\mathfrak{q}^s$. If $p \nmid s$ then lemma 6.3 gives that $\mathfrak{q}$ is ramified in F, implying that $\mathfrak{q}_K$ is also ramified in F. Kida's theorem then implies that E has non-semistable reduction. On the other hand, if $p \mid s$, then $\mathfrak{q}$ is unramified in F (after a change of generator). Equation (6.1) gives $e(\mathfrak{q}_F | \mathfrak{q}_K) = e(\mathfrak{q} | \mathfrak{q}_K)$, implying that $\mathfrak{q}$ is unramified in F, since $e(\mathfrak{q} | \mathfrak{q}_K) = 1$ when $\mathfrak{q}_K \nmid p$ by lemma 6.2. Therefore, Kida's theorem implies that E has semistable reduction. $\qquad\square$

Clearly, we didn't need to prove theorem 6.5 since it is a consequence of theorem 6.4. However, I feel that the above proof gives me some interesting insights.

Remark 6.4. It is interesting to note that, by [Sil94, Theorem IV.10.3(b)], E has good reduction over $K(E[\ell])$.

6.2 Special fibres of elliptic Jackson spaces; the case $\ell = p$

Since $\mathfrak{q} \mid p$, we have that $\zeta_p \equiv 1 \pmod{p}$ unless $(p-1) \mid e(\mathfrak{q})$. We assume from now on that $e(\mathfrak{q}) = 1$, and so we can observe that $\bar{\zeta}_p = 1 \in k$. The case $e(\mathfrak{q}) \geq 2$ is probably considerably harder. As always, the case $p = 2$, presents additional difficulties so we assume for simplicity that $p > 2$.

Theorem 6.6. Let $E_{/K}$ be an elliptic curve with a K-rational p-torsion point. Assume that $[F : L] \geq 2$ (i.e., that not all p-torsion points are K-rational) and that $e(\mathfrak{q}) = 1$.

(i) Let $E_{/K}$ be an elliptic curve with a K-rational p-torsion point and let $\mathfrak{q}_K$ be a prime of K over p. Then E cannot have good supersingular reduction at $\mathfrak{q}_K$; in addition,

(ii) the case of non-split multiplicative reduction cannot happen.

(iii) If $E_{/K}$ has good ordinary, split multiplicative, or additive, reduction at $\mathfrak{q}_K$, then

$$\mathfrak{X}_{\mathcal{J}_x} \otimes_L k = \begin{cases} \mathfrak{X}_{\mathbf{A}_k^1}, & \text{if } \mathfrak{q} \nmid x \\ \mathbb{A}_k^3, & \text{if } \mathfrak{q} \mid x. \end{cases}$$

20

Recall that $\mathbf{A}_k^1$ denotes the first Weyl algebra over the affine k-line.

Parts of the above theorem are almost certainly known but I haven't found precise references so I supply complete proofs of all statements. There are almost certainly easier and shorter arguments than presented.

Proof. Assume that $E_{/K}$ has good supersingular reduction at $\mathfrak{q}_K \mid p$. Since E has a K-rational p-torsion point, we know that F/L is either trivial or cyclic of degree p. In the first case there is nothing to prove, so assume that the degree of the extension is p. This means that $[F : K] = p(p - 1)$. By the assumption that E has good supersingular reduction, [Ser72, Proposition 12, 1.11] implies that the inertia group of $\mathrm{Gal}(F/K)$ has degree $p^2 - 1$, which is then clearly not possible for an extension of degree $p(p - 1)$.

Suppose that $E_{/K}$ has multiplicative reduction over p. Let E_q be the associated Tate curve, with $v_{\mathfrak{q}}(q) < 0$ (see [Sil94, Theorem V.5.3] for details). Then E has a K-rational p-torsion point if and only if E has split multiplicative reduction and the Tate period q is a p-th power. Now, from [Sil94, Theorem V.5.3(b)]) we have that E is split multiplicative if and only if $E \simeq E_q$ over K, in particular $E[p] \simeq E_q[p]$ (over K). On the other hand, if E has non-split multiplicative reduction there are no K-rational p-torsion points. The reason for this is that we need to base change E to an unramified quadratic extension of K to get an isomorphism between E and E_q. The details can be found in [Sil94, Section V.5].

Since $\mathfrak{q} \mid [F : L]$, proposition 5.2 (iii) shows that, F/L is ramified and $\mathfrak{X}_{\mathcal{J}_x} \otimes_L k$ is either $\mathfrak{X}_{\mathbf{A}_{k(\mathfrak{p})}^1}$ or $\mathbb{A}_k^3$, depending on whether $\mathfrak{q} \mid x$ or not. $\qquad\square$

The above theorem suggests that $\mathcal{J}_x$ might not be the best algebra to use to study the case $\ell = p$. Therefore we will turn to the infinitesimal algebras from section **??**. We remark that the infinitesimal algebras $\mathbf{I}_q$ enjoy the same ring-theoretic and homological properties as $\mathcal{J}_x$ as given in theorem 4.3 and corollary 4.4.

Assume that K is a local field, unramified over $\mathbb{Q}_p$ (so $e = 1$). We can (and will) choose p as the uniformiser of $\mathfrak{o}_K$. Put $k := \mathfrak{o}_K/p$. Because K is unramified over $\mathbb{Q}_p$ we can write

$$K = \mathbb{Q}_p(\zeta_m), \quad m = p^n - 1, \quad n = [K : \mathbb{Q}_p]$$

where ζ_m is a primitive m-th root of unity. Hence $k = \mathbb{F}_{p^n}$ and $\bar{\zeta}_m \in k$.

Let $E_{/K}$ be an elliptic curve over K and $\mathscr{E} := \mathscr{E}_{/\mathfrak{o}_K}$ its minimal regular model. The extension $F/L = K(E[p])/K(\zeta_p)$ is a separable extension with ring of integers $\mathfrak{o}_L[\sqrt[p]{x}] = \mathfrak{o}_K[\zeta_p][\sqrt[p]{x}]$. Therefore, we can find a $\beta \in F$ such that $F/L = K(\zeta_p)(\beta)/K(\zeta_p)$ and $\mathfrak{o}_F := \mathfrak{o}_L[\beta]$.

We can choose x as $x = \sum_{i=0}^{p-1} \zeta_p^i \tau^i(\beta)$, where we have chosen a generator τ for $\mathrm{Gal}(F/L)$. The extension $K(E[p])/K(\zeta_p) = L(\beta)/L$ is totally (and wildly) ramified since reducing modulo the maximal ideal $\mathfrak{m} = (p) \subset \mathfrak{o}_K$ we have

$$\mathfrak{o}_L[\sqrt[p]{x}] = \mathfrak{o}_K[\zeta_p][\sqrt[p]{x}] \twoheadrightarrow k[T]/(T - \bar{x})^p.$$

In addition, $\bar{x}$ is identically zero since

$$\bar{x} = \sum_{i=0}^{p-1} \bar{\zeta}_p^i \bar{\tau}^i(\bar{\beta}) = p\bar{\beta} = 0.$$

21

Recall that, since the extension is ramified, $\bar{\tau} = \mathrm{id}$. Since $K(E[p])/K(\zeta_p)$ is a totally ramified Kummer extension it is, a priori, clear that x must be a unit times a uniformiser (which in this case is p).

The choice of $\mathtt{P} \in E[p](K)$ allows us to choose a $\mathtt{Q} \in E[p]$ such that $\{\mathtt{P},\mathtt{Q}\}$ is a $\mathbb{Z}$-basis for $E[p]$. The lifting $\{\hat{\mathtt{P}},\hat{\mathtt{Q}}\}$ becomes a $\mathbb{Z}$-basis on $\mathscr{E}$, but its specialisation to the closed fibre need not be a basis. Since $\mathtt{P} \in E[p](K)$ the specialisation $\bar{\mathtt{P}}$ to the closed fibre can be viewed as an element in the special fibre $\bar{\mathscr{E}}(k)$.

Recall that $\mathfrak{o}_L^! = \mathfrak{o}_L[T]/(T^p)$ and consider the polynomial ring $\mathfrak{o}_L^![y] = \mathfrak{o}_L[T,y]/(T^p)$. There are two natural morphisms $\mathfrak{o}_L^![y] \to L^![y]$ and $\mathfrak{o}_L^![y] \to k^![y]$. On $\mathfrak{o}_L^![y]$ we introduce the $\mathfrak{o}_L[y]$-linear automorphism $\sigma(T) := yT$. This naturally extends to the generic fibre $L^![y]$ and the special fibre $k^![y]$.

Evaluation $y \to \lambda \in K^{\mathrm{al}}$ defines an $\mathfrak{o}_L^![\lambda]$-rational point on $\mathrm{Spec}(\mathfrak{o}_L^![y])$. We now construct the algebra

$$\mathbf{I}_\lambda := \mathbf{E}\Big(\mathfrak{o}_L[\lambda]^! \cdot (\mathrm{id} - \sigma)\Big) = \frac{\mathfrak{o}_L[\lambda]\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{p-1}\rangle}{\Big(\boldsymbol{e}_i\boldsymbol{e}_j - \lambda^{j-i}\boldsymbol{e}_j\boldsymbol{e}_i - (1 - \lambda^{j-i})\boldsymbol{e}_{i+j}\Big)},$$

over $\mathfrak{o}_L[\lambda]$. Remember that we take $i+j$ modulo p.

There is a natural subalgebra of $\mathbf{I}_\lambda$, namely,

$$\mathscr{I}_\lambda := \mathfrak{o}_L[\lambda]\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_{p-1}\rangle \Big/ \begin{pmatrix} \boldsymbol{e}_0\boldsymbol{e}_1 - \lambda\boldsymbol{e}_1\boldsymbol{e}_0 - (1-\lambda)\boldsymbol{e}_1 \\ \boldsymbol{e}_0\boldsymbol{e}_{p-1} - \lambda^{p-1}\boldsymbol{e}_{p-1}\boldsymbol{e}_0 - (1-\lambda^{p-1})\boldsymbol{e}_{p-1} \\ \boldsymbol{e}_1\boldsymbol{e}_{p-1} - \lambda^{p-2}\boldsymbol{e}_{p-1}\boldsymbol{e}_1 \end{pmatrix}.$$

For simplicity, we put $\boldsymbol{e}_2 := \boldsymbol{e}_{p-1}$. If we want to make the prime explicit in the notation we write $\mathscr{I}_\lambda^{(p)}$.

Making the substitution $\boldsymbol{e}_0 \mapsto \boldsymbol{e}_0 + 1$ and some re-arranging yields the isomorphic algebra (which we also denote $\mathscr{I}_\lambda$):

$$\mathscr{I}_\lambda = \mathfrak{o}_L[\lambda]\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2\rangle \Big/ \begin{pmatrix} \boldsymbol{e}_0\boldsymbol{e}_1 - \lambda\boldsymbol{e}_1\boldsymbol{e}_0 \\ \boldsymbol{e}_2\boldsymbol{e}_0 - \lambda^{1-p}\boldsymbol{e}_0\boldsymbol{e}_2 \\ \boldsymbol{e}_2\boldsymbol{e}_1 - \lambda^{2-p}\boldsymbol{e}_1\boldsymbol{e}_2 \end{pmatrix}.$$

Remark 6.5. The algebra $\mathscr{I}_\lambda$ can be viewed as the glueing of three (in general) distinct quantum planes.

6.2.1 The special fibre of $\mathscr{I}$

We will now reduce modulo the maximal ideal (p) and the generic point. The following diagram summarises the situation:

$$\bar{\mathscr{E}} \xleftarrow{\ \mathrm{red}\ } \mathscr{E} \longrightarrow E_{/K}$$

$$\mathscr{I}_\lambda \otimes_{\mathfrak{o}_K} k \xleftarrow{\ \mathrm{red}\ } \mathscr{I}_\lambda \longrightarrow \mathscr{I}_\lambda \otimes_{\mathfrak{o}_K} K.$$

Put $\overline{\mathscr{I}}_\lambda = \mathscr{I}_\lambda \otimes_{\mathfrak{o}_K} k$, the *special fibre* of $\mathscr{I}_\lambda$. We call $\mathscr{I}_\lambda \otimes_{\mathfrak{o}_K} K$, the *generic fibre* (of course).

We will continue working with the minimal regular model $\mathscr{E}$ of $E_{/K}$. Recall that $E(K) = \mathscr{E}(\mathfrak{o}_K)$, and thus $E(K)[p] = \mathscr{E}(\mathfrak{o}_K)[p]$. The set of non-singular

k-points on $\bar{E}$ is isomorphic to the identity component of the special fibre $\bar{\mathscr{E}}^0(k)$ (see [Sil94, Corollary IV.9.2(c)]).

Fix $a, b \in \mathbb{Z}$ and let

$$\boldsymbol{\theta}_{(a,b);S} := S([a]\mathsf{P} + [b]\mathsf{Q}) \in F = K(E[p]),$$

where S is a function in the coordinates of $[a]\mathsf{P} + [b]\mathsf{Q}$. Normally we will consider a, b and S as fixed and so we simply write $\boldsymbol{\theta}$ for $\boldsymbol{\theta}_{(a,b);S}$ unless confusion can arise. We write $\boldsymbol{\theta} = \sum_{i=0}^{p-1} \theta_i \beta^i$, with $\theta_i \in L$.

From now on we let d be the number of irreducible components of $\bar{\mathscr{E}}(k)$, counted without multiplicities, and f the conductor of E. Put $w := f + d$ and evaluate λ at ζ_w, where $\zeta_w \in \mu_w$ is primitive. We choose $\zeta = \zeta_w$ such that $\bar{\zeta}$ is also primitive. In addition, we set $\mathscr{F}_w := \mathscr{F}_\zeta$. Ogg's formula (see [Sil94, IV.11.1]) shows that $w = v_p(\Delta_E^{\min}) + 1$, where $\Delta_E^{\min}$ is the minimal discriminant of $E_{/K}$.

Remark 6.6. Note that we make three successive evaluations: $y \to \lambda \to \zeta_w$. We could certainly do the evaluation $y \to \zeta_w$ directly, but I feel that this misses the point in the sense that the value ζ_w for λ is a specific *choice*.

When $w = f + d$ is irrelevant we sometimes write ζ instead of ζ_w. Put $k_w := k(\zeta_w)$ and let $\mathbf{z} := (z_0, z_1, \ldots, z_{p-1})^T$ be a vector in $\mathfrak{o}_L[\zeta]^p$. Recall that $\boldsymbol{\theta} := \boldsymbol{\theta}_{(a,b);S}$ is fixed. Define the étale L-rational point $\mathfrak{N}_{\boldsymbol{\theta},\mathbf{z}}$ to be the family of one-dimensional $\mathscr{F}_w$-modules $\mathfrak{N}_j := \mathfrak{o}_L[\zeta] \cdot \mathbf{y}$ defined by

$$\boldsymbol{e}_0 \cdot \mathbf{y} := \Delta_E \mathbf{y}, \quad \boldsymbol{e}_1 \cdot \mathbf{y} := z_j \mathbf{y}, \quad \boldsymbol{e}_2 \cdot \mathbf{y} := \theta_j \mathbf{y},$$

where Δ_E is the discriminant of E and θ_j is the j-th coefficient of $\boldsymbol{\theta}$. To be explicit we will sometimes write $\mathfrak{N}_j$ as a triplet $(\Delta_E, z_j, \theta_j)$ and the étale point $\mathfrak{N}_{\boldsymbol{\theta},\mathbf{z}} = (\Delta_E, \mathbf{z}, \boldsymbol{\theta})$.

In order for $\mathfrak{N}_j$ to be an $\mathscr{F}_w$-module it is necessary and sufficient that

$$(1 - \zeta)\Delta_E z_j = 0, \qquad (1 - \zeta^{1-p})\Delta_E \theta_j = 0, \quad \text{and} \quad (1 - \zeta^{2-p})z_j \theta_j = 0.$$

Clearly, the special fibre, which we denote $\overline{\mathscr{F}}_w$, is

$$(1 - \bar{\zeta})\bar{\Delta}_E \bar{z}_j = 0, \qquad (1 - \bar{\zeta}^{1-p})\bar{\Delta}_E \bar{\theta}_j = 0, \quad \text{and} \quad (1 - \bar{\zeta}^{2-p})\bar{z}_j \bar{\theta}_j = 0.$$

If $z_j \neq 0$ for all j the étale rational point $\mathfrak{N}_{\boldsymbol{\theta},\mathbf{z}}$ is clearly empty since the element $\boldsymbol{\theta}$ is fixed.

A computation shows the following theorem.

Theorem 6.7. Let $\bar{\mathfrak{N}}_1$ and $\bar{\mathfrak{N}}_2$ be $(\bar{\Delta}_E, \bar{z}_1, \bar{\theta}_1)$ and $(\bar{\Delta}_E, \bar{z}_2, \bar{\theta}_2)$, respectively. Then

$$T_{\mathsf{N}} = \mathrm{Ext}^1_{\overline{\mathscr{F}}_\zeta}(\bar{\mathfrak{N}}_1, \bar{\mathfrak{N}}_2) = \begin{cases} k_w, & \text{if } \bar{\Delta}_E = 0 \text{ and } \bar{z}_1 = \bar{z}_2 = 0 \text{ and } \bar{\theta}_2 = \bar{\zeta}^{2-p}\bar{\theta}_1 \\ k_w, & \text{if } \bar{\Delta}_E = 0 \text{ and } \bar{\theta}_1 = \bar{\theta}_2 = 0 \text{ and } \bar{z}_1 = \bar{\zeta}^{2-p}\bar{z}_2 \\ 0, & \text{otherwise.} \end{cases}$$

From this follows that

$$\hat{\mathfrak{o}}_{\mathsf{N}} = \begin{pmatrix} \mathrm{End}_{k_w}(\bar{\mathfrak{N}}_1) \otimes k_w[[t_{11}]] & \mathrm{Hom}_{k_w}(\bar{\mathfrak{N}}_1, \bar{\mathfrak{N}}_2) \otimes \langle t_{12} \rangle \\ \mathrm{Hom}_{k_w}(\bar{\mathfrak{N}}_2, \bar{\mathfrak{N}}_1) \otimes \langle t_{21} \rangle & \mathrm{End}_{k_w}(\bar{\mathfrak{N}}_2) \otimes k_w[[t_{22}]] \end{pmatrix}$$

where $\mathsf{N} = \{\bar{\mathfrak{N}}_1, \bar{\mathfrak{N}}_2\}$.

Remark 6.7. The theorem applies also to the case $1 - \bar{\zeta}^{2-p} = 0$. Unless $z_1 = z_2 = 0$ or $\theta_1 = \theta_2 = 0$, we always end up in the third case.

Assume $\bar{z}_j = 0$ and let $\bar{\mathfrak{N}}_j$ be $(0, 0, \bar{\theta}_j)$. Then the *mirror* of $\bar{\mathfrak{N}}_j$ is the module $\bar{\mathfrak{N}}_j^{\perp}$ such that $\bar{\mathfrak{N}}_j^{\perp} = (0, 0, \bar{\zeta}^{2-p}\bar{\theta}_j)$. Theorem 6.7 the shows that there is a tangent between $\bar{\mathfrak{N}}_j$ and $\bar{\mathfrak{N}}_j^{\perp}$, visually $\bar{\mathfrak{N}}_j \to \bar{\mathfrak{N}}_j^{\perp}$. Note that $(\bar{\mathfrak{N}}_j^{\perp})^{\perp}$ is not necessarily $\bar{\mathfrak{N}}_j$. However, identifying the modules $\bar{\mathfrak{N}}_j = (0, 0, \bar{\zeta}^{2-p}\bar{\theta}_j)$ and $\bar{\mathfrak{N}}_j' = (0, 0, \bar{\zeta}^{p-2}\bar{\theta}_j)$, sets up a symmetry and so with this we can claim the implication $\bar{\mathfrak{N}}_j \to \bar{\mathfrak{N}}_j^{\perp} \implies \bar{\mathfrak{N}}_j^{\perp} \to \bar{\mathfrak{N}}_j$.

The *mirror* of the étale k_w-rational point $\bar{\mathfrak{N}}_{\boldsymbol{\theta}, \mathbf{z}}$ is naturally the family of modules

$$\bar{\mathfrak{N}}_{\boldsymbol{\theta}, \mathbf{z}}^{\perp} := \bar{\zeta}^{2-p} \bar{\mathfrak{N}}_{\boldsymbol{\theta}, \mathbf{z}}.$$

We say that $\mathfrak{N}_{\boldsymbol{\theta}, \mathbf{z}}^{\perp}$ is *a* mirror of $\mathfrak{N}_{\boldsymbol{\theta}, \mathbf{z}}$ if $\bar{\mathfrak{N}}_{\boldsymbol{\theta}, \mathbf{z}}^{\perp}$ is the mirror of $\bar{\mathfrak{N}}_{\boldsymbol{\theta}, \mathbf{z}}$. Any mirror of $\mathfrak{N}_{\boldsymbol{\theta}, \mathbf{z}}$ defines an element in F, namely $\boldsymbol{\theta}^{\perp} := \zeta^{2-p}\boldsymbol{\theta}$, hence also in $\mathbf{I}_\zeta$, and by restriction, in $\mathscr{F}_w$.

6.2.2 $p \neq 3$

For $p \geq 5$ we have

$$f = \begin{cases} 0, & \text{if } E \text{ has good reduction,} \\ 1, & \text{if } E \text{ has multiplicative reduction, and} \\ 2, & \text{if } E \text{ has additive reduction.} \end{cases}$$

We can directly note that, in the case of good reduction, $\overline{\mathscr{F}}_0^{(p)} = k_0[\boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2]$.

In the case of multiplicative reduction, i.e., $f = 1$, the relations are

$$\overline{\mathscr{F}}_{d+1}^{(p)}: \quad \boldsymbol{e}_0\boldsymbol{e}_1 - \bar{\zeta}_{d+1}\boldsymbol{e}_1\boldsymbol{e}_0, \quad \boldsymbol{e}_2\boldsymbol{e}_0 - \bar{\zeta}_{d+1}^{1-p}\boldsymbol{e}_0\boldsymbol{e}_2, \quad \boldsymbol{e}_2\boldsymbol{e}_1 - \bar{\zeta}_{d+1}^{2-p}\boldsymbol{e}_1\boldsymbol{e}_2,$$

where $d = -v_p(j_E)$. Hence the reduction is a quantum affine space.

When the reduction is additive we find the relations

$$\overline{\mathscr{F}}_{d+2}^{(p)}: \quad \boldsymbol{e}_0\boldsymbol{e}_1 - \bar{\zeta}_{d+2}\boldsymbol{e}_1\boldsymbol{e}_0, \quad \boldsymbol{e}_2\boldsymbol{e}_0 - \bar{\zeta}_{d+2}^{1-p}\boldsymbol{e}_0\boldsymbol{e}_2, \quad \boldsymbol{e}_2\boldsymbol{e}_1 - \bar{\zeta}_{d+2}^{2-p}\boldsymbol{e}_1\boldsymbol{e}_2.$$

The possible values for d in the additive case are

$$d = 1, 2, 3, 5, 5 - v_p(j_E), 7, 8, 9.$$

However, it will turn out that not all these are possible when the curve has a K-rational p-torsion point.

6.2.3 $p = 3$

Due to possible wild ramification when $p = 3$, the results are more subtle. Theorem IV.10.4 in [Sil94] gives the bound $2 \leq f \leq 5$, with each value possible. When $f > 2$, [Sil94, Table IV.4.1], shows that, when $p = 3$, d has the possibilities $d = 1, 3, 7, 9$, corresponding to Kodaira types II, IV, IV* and II*, respectively.

We refrain from writing out all possible algebras, simply writing $\overline{\mathscr{F}}_{f+d}^{(3)}$ as given by the relations

$$\boldsymbol{e}_0\boldsymbol{e}_1 - \bar{\zeta}_{f+d}\boldsymbol{e}_1\boldsymbol{e}_0, \quad \boldsymbol{e}_2\boldsymbol{e}_0 - \bar{\zeta}_{f+d}^{-2}\boldsymbol{e}_0\boldsymbol{e}_2, \quad \boldsymbol{e}_2\boldsymbol{e}_1 - \bar{\zeta}_{f+d}^{-1}\boldsymbol{e}_1\boldsymbol{e}_2,$$

with $3 \leq f \leq 5$ and $d \in \{1, 3, 7, 9\}$. The case $f = 2$ was treated above.

6.2.4 Multiplicative reduction

Now, when the reduction is multiplicative the number of components is $d = -v_p(j(E)) > 1$, corresponding to the Kodaira type I_d.

For the two examples below we fix S and (a, b) and write $\boldsymbol{\theta} = \boldsymbol{\theta}_{(a,b);S} = \sum_0^{p-1} \theta_i \beta^i$, with $\theta_i \in L$. I tried to find explicit curves with K-rational points so that some choice of $\boldsymbol{\theta}$ would be manageable, i.e., would be possible to write down in a reasonable way, but did not succeed.

Example 6.1. Suppose that E has Kodaira type I_2. Then

$$\overline{\mathscr{F}}_{I_2} := \frac{k(\bar{\zeta}_3)\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle}{\left(\boldsymbol{e}_0\boldsymbol{e}_1 - \bar{\zeta}_3\boldsymbol{e}_1\boldsymbol{e}_0, \; \boldsymbol{e}_2\boldsymbol{e}_0 - \bar{\zeta}_3^{1-p}\boldsymbol{e}_0\boldsymbol{e}_2, \; \boldsymbol{e}_2\boldsymbol{e}_1 - \bar{\zeta}_3^{2-p}\boldsymbol{e}_1\boldsymbol{e}_2 \right)}.$$

The centre $\mathfrak{Z}(\overline{\mathscr{F}}_{I_2})$ includes the algebra $k(\bar{\zeta}_3)[\boldsymbol{e}_0^3, \boldsymbol{e}_1^3, \boldsymbol{e}_2^3]$, so $\mathrm{Spec}\big(\mathfrak{Z}(\overline{\mathscr{F}}_{I_2})\big)$, and by convention, $\mathfrak{X}_{\overline{\mathscr{F}}_{I_2}}$, can be seen as an $\mathbb{A}^3$-fibration.

Assume given a $\mathbf{z}$ such that $\bar{\theta}_i$ is not zero. Put $\bar{\mathfrak{N}}_i = (0, 0, \bar{\theta}_i)$. From theorem 6.7 we see that

$$T_{\mathsf{N}_i} = \mathrm{Ext}^1_{\overline{\mathscr{F}}_{I_2}}(\bar{\mathfrak{N}}_i, \bar{\mathfrak{N}}') = \begin{cases} k & \text{if } \bar{\theta}' = \bar{\zeta}_3^{2-p}\bar{\theta}_i, \\ 0, & \text{otherwise,} \end{cases},$$

where, of course, $\bar{\mathfrak{N}}' = (0, 0, \bar{\boldsymbol{\theta}}')$ and $\mathsf{N}_i := \{\bar{\mathfrak{N}}_i, \bar{\mathfrak{N}}'\}$. Hence $\bar{\mathfrak{N}}' = \bar{\mathfrak{N}}_i^{\perp}$. Notice that if $p = 3$, $\bar{\zeta}_3 = 1$ so $\overline{\mathscr{F}}_{I_2}^{(3)} = \mathbb{A}^3$.

Example 6.2. For E of Kodaira type I_5, we find

$$\overline{\mathscr{F}}_{I_5} = \frac{k(\bar{\zeta}_6)\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle}{\left(\boldsymbol{e}_0\boldsymbol{e}_1 - \bar{\zeta}_6\boldsymbol{e}_1\boldsymbol{e}_0, \; \boldsymbol{e}_2\boldsymbol{e}_0 - \bar{\zeta}_3^{1-p}\boldsymbol{e}_0\boldsymbol{e}_2, \; \boldsymbol{e}_2\boldsymbol{e}_1 + \bar{\zeta}_3^{2-p}\boldsymbol{e}_1\boldsymbol{e}_2 \right)}.$$

The slightly different relations here follow from p being an odd prime and $\bar{\zeta}_6 = \bar{\zeta}_2\bar{\zeta}_3$.

In this case the centre is quite complicated but it certainly includes the algebra $k(\bar{\zeta}_6)[\boldsymbol{e}_0^6, \boldsymbol{e}_1^6, \boldsymbol{e}_2^6]$ (hence $\mathrm{Spec}\big(\mathfrak{Z}(\overline{\mathscr{F}}_{I_2})\big)$ and $\mathfrak{X}_{\overline{\mathscr{F}}_{I_2}}$ can be seen as $\mathbb{A}^3$-fibrations in this case also). With the same notation as in the previous example we find

$$T_{\mathsf{N}_i} = \mathrm{Ext}^1_{\overline{\mathscr{F}}_{I_5}}(\bar{\mathfrak{N}}_i, \bar{\mathfrak{N}}') = \begin{cases} k & \text{if } \bar{\theta}' = -\bar{\zeta}_3^{2-p}\bar{\theta}_i \\ 0, & \text{otherwise,} \end{cases}$$

following from theorem 6.7.

The case of additive reduction is more subtle as was alluded to above. The possible number of components are $1 \le d \le 9$ but it will turn out that not all of these are possible.

6.2.5 Additive reduction

We will look at bit deeper into the case of additive reduction. The following theorem is [KP17, Theorem 12].

Theorem 6.8. Let $E_{/K}$ be an elliptic curve with additive reduction at $\mathfrak{q}_K \mid p$. Then

(i) $E_0(K) \simeq \widehat{E}(\mathfrak{o}_K)$ as (topological) groups, and

(ii) if $6e(\mathfrak{q}) < p - 1$, then $E_0(K) \simeq \mathbb{Z}_p^n$, as $\mathbb{Z}_p$-modules. When $6e(\mathfrak{q}) \geq p - 1$, we have $E_0(K) \simeq \mathbb{Z}_p^n \times \mathbb{Z}/p$.

Here n is the degree of $K/\mathbb{Q}_p$.

Theorem 6.9. Let $E_{/K}$ be an elliptic curve with a K-rational p-torsion point and $e(\mathfrak{q}) = 1$. Then $E_{/K}$ cannot have additive reduction at $\mathfrak{q}_K$, unless $p = 2, 3, 5$ or 7.

Proof. By theorem 6.8 (ii), if $e(\mathfrak{q}) = 1$, then $E_0(K) \simeq \mathbb{Z}_p^n$ when $p \geq 11$. Hence the only possibilities to have p-torsion in the additive reduction case are when $p = 2, 3, 5, 7$. $\qquad\square$

Let $E_{/K}$ be an elliptic curve with additive reduction at $\mathfrak{q}_K$ and with Weierstrass equation

$$E_{/K}: \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{6.2}$$

In fact, [KP17, Lemma 9] shows that the coefficients can be chosen so that they are all in the maximal ideal $\mathfrak{m} \subset \mathfrak{o}_K$.

Recall that, for an elliptic curve $E_{/K}$, there is an exact sequence

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \xrightarrow{\text{red}} \bar{E}_{\text{sm}}(k) \longrightarrow 0 ,$$

where $E_0(K)$ is the set of K-rational points on E reducing to the smooth locus $\bar{E}_{\text{sm}}$ on the reduced curve $\bar{E}$ and where $E_1(K)$ is the kernel of reduction. Also, $E_1(K) \simeq \widehat{E}(\mathfrak{o}_K)$, where $\widehat{E}$ is the formal group of E. See [Sil86, Propositions 2.1 and 2.2, chapter VII] for details. Let $E_{/K}$ have additive reduction and let $\mathscr{E}_{/\mathfrak{o}_K}$ be its minimal regular model. Then

$$\bar{\mathscr{E}}^0(k) \simeq \bar{E}_{\text{sm}}(k),$$

where $\bar{\mathscr{E}}^0$ is the connected component of the identity in the closed fibre, by [Sil94, IV.9.2(c)]. Also, there is an exact sequence of group schemes

$$0 \longrightarrow \mathscr{E}^0 \longrightarrow \mathscr{E} \longrightarrow \Phi. \tag{6.3}$$

From this sequence and [Sil94, IV.9.2(a,b)] follows the exact sequences

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathscr{E}^0(\mathfrak{o}_K) & \longrightarrow & \mathscr{E}(\mathfrak{o}_K) & \longrightarrow & \Phi(\mathfrak{o}_K) & \longrightarrow & 0 \\
& & \| & & \| & & \| & & \\
0 & \longrightarrow & E_0(K) & \longrightarrow & E(K) & \longrightarrow & \Phi(K) & \longrightarrow & 0 \\
& & & & & & \| & & \\
& & & & & & E(K)/E_0(K) & &
\end{array}
$$

26

and

$$0 \longrightarrow \mathscr{E}^0(\mathfrak{o}_K)[p^\infty] \longrightarrow \mathscr{E}(\mathfrak{o}_K)[p^\infty] \longrightarrow \Phi(\mathfrak{o}_K)[p^\infty]$$

$$0 \longrightarrow E_0(K)[p^\infty] \longrightarrow E(K)[p^\infty] \longrightarrow \Phi(K)[p^\infty] =\!=\!= \big(E(K)/E_0(K)\big)[p^\infty].$$

In addition, [Sil94, IV.9.2(b)] gives that

$$\Phi(K) = E(K)/E_0(K) \simeq \bar{\mathscr{E}}^0(k) = \Phi(k).$$

The group $\Phi(k)$ is the group of components of $\bar{\mathscr{E}}$.

Now, table [Sil94, Table IV.4.1] shows that $\Phi(k)[p] = \{0\}$ if $p > 3$ and hence $E_0(K)[p] \simeq E(K)[p]$. Therefore, all K-rational p-torsion points must reduce to non-singular points on $\bar{E}(k) = \bar{\mathscr{E}}(k)$. Theorem 6.8 now implies that, if $p > 7$, $E_0(K)$ is p-torsion-free, and hence also $E(K)$.

Let us begin by looking at the cases $p = 5$ or 7. Since $E(K)[p] \simeq E_0(K)[p]$, the discussion in section 3.3.1 in [KP17] implies that

$$E(K)[p] \simeq \mathbb{Z}_p^n \times \mathbb{Z}/p, \qquad (\text{with } n = [K : \mathbb{Q}_p])$$

if and only if $f(T) := T - aT^p$ has a non-trivial solution in k, where $a = 3a_4/5 \pmod{\mathfrak{q}}$ when $p = 5$ and $a = 4a_6/7 \pmod{\mathfrak{q}}$, when $p = 7$, and where a_4, a_6 are the coefficients given by the Weierstrass model (6.2). See [KP17, Section 3.3.1] for the details. It is important to be aware that these congruences refer *only* to the Weierstrass model (6.2) where the coefficients are in $\mathfrak{m}$. Incidentally, the polynomial $f(T)$ is the reduction of the power series $[p](T)$ in the formal group of $E_{/K}$.

If a solution to the these congruences does not exist, $E(K)[p] = \mathbb{Z}_p^n$ and hence there are no non-trivial K-rational p-torsion points. The above comment indicates that the number of curves with additive reduction with a K-rational p-torsion point is quite rare for $p = 5$ and rarer still for $p = 7$. In fact, the first curve where the curve has additive reduction with a non-trivial $\mathbb{Q}_7$-rational point is **294b2** in Cremona's table [Cre15]. The next curve after this is the curve **490k2**.

The following two examples show that existence and non-existence of rational p-torsion points can occur for both $p = 5$ and $p = 7$ in the additive reduction case. The computations are done with Sage [Sag20].

Example 6.3. Let $E_{/\mathbb{Q}_5}$ be the elliptic curve given by the Weierstrass equation

$$y^2 + xy + y = x^3 + x^2 + 22x - 9. \tag{50b2}$$

This curve has bad additive reduction (of type II) and is **50b2** in Cremona's table [Cre15]. The $\mathbb{Q}_5$-rational 5-torsion points are

$$\Big\{\infty, (1 : -5 : 1), (1 : 3 : 1), (9 : -37 : 1), (9 : 27 : 1)\Big\}$$

and so $E(\mathbb{Q}_5)[5] = E(\mathbb{Q})[5] \simeq \mathbb{Z}/5$. All these have non-singular reduction. On the other hand, the curve **50a4** also has bad additive reduction (of type IV^*). However, this time the only rational 5-torsion point is $\{\infty\} = \{[0 : 1 : 0]\}$.

Example 6.4. Now, let $E_{/\mathbb{Q}_7}$ be the elliptic curve **49a3** given by the Weierstrass equation

$$y^2 + xy = x^3 - x^2 - 107x + 552. \tag{49a3}$$

This curve has bad additive reduction of type III*. The only $\mathbb{Q}_7$-rational 7-torsion points is $\{\infty\} = \{[0:1:0]\}$. Looking now at the curve $E'_{/\mathbb{Q}_7}$

$$y^2 + xy + y = x^3 - x^2 + 918x + 5289 \tag{490k2}$$

of bad additive Kodaira type II, one finds that

$$E'(\mathbb{Q}_7)[7] = E'(\mathbb{Q})[7] = \Big\{\infty, (-3:-49:1), (-3:51:1), (17:-169:1),$$
$$(17:151:1), (97:-1049:1), (97:951:1)\Big\},$$

all of non-singular reduction.

When $p = 5$ or 7, the conductor is $f = 2$ for type II and III. In the case $p = 7$ the only possibility is $d = 1$ (Kodaira symbol II) and so, since all 3-rd roots of unity are in $\mathbb{F}_7$,

$$\overline{\mathscr{F}}_{\mathrm{II}}^{(7)} = \frac{k\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle}{\Big(\boldsymbol{e}_0\boldsymbol{e}_1 - \bar{\zeta}_3\boldsymbol{e}_1\boldsymbol{e}_0, \ \boldsymbol{e}_2\boldsymbol{e}_0 - \boldsymbol{e}_0\boldsymbol{e}_2, \ \boldsymbol{e}_2\boldsymbol{e}_1 - \bar{\zeta}_3^{-2}\boldsymbol{e}_1\boldsymbol{e}_2 \Big)}.$$

When $p = 5$ we find the algebras

$$\overline{\mathscr{F}}_{\mathrm{III}}^{(5)} = \frac{k\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle}{\Big(\boldsymbol{e}_0\boldsymbol{e}_1 - \bar{\zeta}_4\boldsymbol{e}_1\boldsymbol{e}_0, \ \boldsymbol{e}_2\boldsymbol{e}_0 - \boldsymbol{e}_0\boldsymbol{e}_2, \ \boldsymbol{e}_2\boldsymbol{e}_1 + \bar{\zeta}_4\boldsymbol{e}_1\boldsymbol{e}_2 \Big)},$$

where $\bar{\zeta}_4 \in \mathbb{F}_5$, and

$$\overline{\mathscr{F}}_{\mathrm{II}}^{(5)} = \frac{k(\bar{\zeta}_3)\langle \boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle}{\Big(\boldsymbol{e}_0\boldsymbol{e}_1 - \bar{\zeta}_3\boldsymbol{e}_1\boldsymbol{e}_0, \ \boldsymbol{e}_2\boldsymbol{e}_0 - \bar{\zeta}_3^{-1}\boldsymbol{e}_0\boldsymbol{e}_2, \ \boldsymbol{e}_2\boldsymbol{e}_1 - \boldsymbol{e}_1\boldsymbol{e}_2 \Big)}.$$

Note that, depending on the degree of $k/\mathbb{F}_5$, $\bar{\zeta}_3$ may or may not be in k already. The degree $[k(\bar{\zeta}_3):k]$ is either 1 or 2.

In the case $p = 3$, the group $\Phi(k) = \Phi(K)$ is not necessarily trivial. Therefore, we cannot conclude from (6.3) that

$$E_0(K)[3] \simeq E(K)[3].$$

In fact, this is false in general. Thanks to Chris Wuthrich for indicating the following examples. Computations once again courtesy of Sage [Sag20].

Example 6.5. Let $E_{/\mathbb{Q}_3}$ be the elliptic curve

$$y^2 + y = x^3 - 7 \tag{27a1}$$

over $\mathbb{Q}_3$. Then

$$E(\mathbb{Q}_3)[3^\infty] \simeq \mathbb{Z}/3$$

and only $\{\infty\} = \{[0:1:0]\}$ has good reduction. In fact, $E(\mathbb{Q})[3] = E(\mathbb{Q}_3)[3] = E(\mathbb{Q}_3)[3^\infty]$. This curve has Kodaira type IV*.

Example 6.6. Now, let $E_{/\mathbb{Q}_3}$ be Cremona's curve **54b3**:

$$y^2 + xy + y = x^3 - x^2 - 14x + 29. \tag{54b3}$$

In this example

$$E(\mathbb{Q}_3)[3^\infty] \simeq \mathbb{Z}/9$$

and three $\mathbb{Q}_3$-rational points have good reduction (incidentally, these are the points of $E(\mathbb{Q})[3]$). The Kodaira symbol for **54b3** is IV.

The possibility for the p-torsion points to reduce into the singular locus is measured by $\Phi(k) = \Phi(K) = E(K)/E_0(K)$ and when $p = 3$ the only possibility is $\Phi(K) = \mathbb{Z}/3$, which corresponds to the Kodaira symbols IV and IV*. The reason for this is that $E(K)[3]/E_0(K)[3]$ is a subgroup of $\Phi(K)$ of order 3. Hence 3 must be a divisor of the order of $\Phi(K)$. According to [Sil94, Table IV.4.1] this corresponds to $E(K)[3]/E_0(K)[3] = E(K)/E_0(K) = \mathbb{Z}/3$ and the Kodaira symbols IV and IV*.

Another possibility is that $E(K)[3]/E_0(K)[3]$ is trivial while $E(K)/E_0(K) = (0)$ or $E(K)/E_0(K) = \mathbb{Z}/2$. In this case we get the symbols II and III. This happens for instance for **54b1** (which is of type II) and **90b2** (which is of type III). Note that $E(K)[3]/E_0(K)[3]$ and $E(K)/E_0(K) = (0)$ can both be trivial without E having good reduction (when $\bar{E}$ is a cusp with only one component).

On the other hand, the Kodaira symbols I have found for the 3-torsion reducing to the smooth locus, for curves over $\mathbb{Q}_3$, are II, III, IV, I$_0^*$, I$_1^*$, I$_2^*$, I$_3^*$ and I$_4^*$. At the moment I'm not sure whether I$_n^*$ can appear for $n \geq 5$ or not (and, in that case, if there is an upper bound). This shouldn't be too difficult to prove or disprove.

Remark 6.8. It is important to remember that all the above claims are made under the assumption that E has a K-*rational* 3-torsion point.

Summarising the additive case when $p = 3$:

Theorem 6.10. Suppose $E_{/\mathbb{Q}_3}$ has additive reduction. The relations for $\overline{\mathscr{F}}_{f+d}^{(3)}$ are

$$\boldsymbol{e}_0\boldsymbol{e}_1 - \bar{\zeta}_{f+d}\boldsymbol{e}_1\boldsymbol{e}_0, \quad \boldsymbol{e}_2\boldsymbol{e}_0 - \bar{\zeta}_{f+d}^{-2}\boldsymbol{e}_0\boldsymbol{e}_2, \quad \boldsymbol{e}_2\boldsymbol{e}_1 - \bar{\zeta}_{f+d}^{-1}\boldsymbol{e}_1\boldsymbol{e}_2$$

and the possibilities for d and f are (remember, $2 \leq f \leq 5$):

II: $d = 1$, $f > 2$;

III: $d = 2$, $f = 2$;

IV: $d = 3$, $f > 2$;

I$_n^*$: $d = 5 + n$, $f = 2$, and

IV*: $d = 7$, $f > 2$.

Depending on d, f and $[k : \mathbb{F}_3]$, $\bar{\zeta}_{f+d}$ may, or may not, be in k already.

7 The $\boldsymbol{\theta}$-elements

Now, fix S. We then get a function

$$\boldsymbol{\theta}_{-;S} : \ E[p] \longrightarrow F, \quad [a]\mathtt{P} + [b]\mathtt{Q} \ \longmapsto \ \boldsymbol{\theta} = \boldsymbol{\theta}_{(a,b);S} = \sum_{i=0}^{p-1} \theta_i \beta^i. \qquad (7.1)$$

This defines a one-dimensional étale L-rational point of order $p-1$,

$$\mathfrak{N}_{\boldsymbol{\theta},\mathbf{0}} = \Big\{ \mathfrak{N}_j \mid 0 \le j \le p-1 \Big\}, \quad \mathfrak{N}_j = (0,0,\theta_j),$$

on $\mathfrak{X}_{\mathscr{I}_{f+d}}$. We can define a mirror family $\mathfrak{N}_{\boldsymbol{\theta},\mathbf{0}}^{\perp}$ such that $\bar{\mathfrak{N}}_{\boldsymbol{\theta},\mathbf{0}}^{\perp} = \zeta^{2-p} \bar{\mathfrak{N}}_{\boldsymbol{\theta},\mathbf{0}}$.
   Hence,

Proposition 7.1. The association (7.1) sets up a correspondence between $E[p]$ and one-dimensional étale L-rational points of order in $\mathfrak{X}_{\mathscr{I}_{f+d}}$. Each such étale L-rational point $\mathfrak{N}_{\boldsymbol{\theta},\mathbf{0}}$ defines a unique mirror $\bar{\mathfrak{N}}_{\boldsymbol{\theta},\mathbf{0}}^{\perp}$ on the special fibre $\mathfrak{X}_{\mathscr{I}_{f+d}} \otimes k_w$.

   There is another way to use the correspondence (7.1). It is natural to say that the $\mathscr{I}_{f+d}$-module $\mathfrak{H} := \mathscr{I}_{f+d}/(H)$, where $H := a_0 \boldsymbol{e}_0 + a_1 \boldsymbol{e}_1 + a_2 \boldsymbol{e}_2 \in \mathscr{I}_{f+d}$, is a *hyperplane* in $\mathfrak{X}_{\mathscr{I}_{f+d}}$.

Proposition 7.2. The association $\boldsymbol{\theta}_{-;S}^{\mathfrak{H}} : \ E[p] \longrightarrow \mathscr{I}_{f+d}$,

$$[a]\mathtt{P} + [b]\mathtt{Q} \ \longmapsto \ \sum_{i=0}^{p-1} \theta_i \beta^i \ \longmapsto \ H := \theta_0 \boldsymbol{e}_0 + \theta_1 \boldsymbol{e}_1 + \theta_{p-1} \boldsymbol{e}_2. \qquad (7.2)$$

(recall $\boldsymbol{e}_2$ is actually $\boldsymbol{e}_{p-1}$) sets up a correspondence between $E[p]$ and hyperplanes in $\mathfrak{X}_{\mathscr{I}_{f+d}}$. Hence the function $\boldsymbol{\theta}_{-;S}^{\mathfrak{H}}$ is a *hyperplane arrangement* in $\mathfrak{X}_{\mathscr{I}_{f+d}}$ defined by $E[p]$.

   Note that the restriction of $\boldsymbol{\theta}_{E[p];S}^{\mathfrak{H}}$ to the central subscheme defines an actual hyperplane arrangement in $\mathrm{Spec}(\mathfrak{Z}(\mathscr{I}_{f+d}))$.

Remark 7.1. The above constructions are obviously not restricted to the particular choice $w = f + d$.

   As a third, and final, construction involving the $\boldsymbol{\theta}$-elements we present a way to construct elements in the Brauer group of $L[\zeta_{f+d}]$.
   As mentioned in remark (6.5) we can view $\mathscr{I}_w$ as the glueing of three quantum planes

$$\mathbf{Q}_{i,j} := \mathfrak{o}_L[\zeta_{f+d}]\langle \boldsymbol{e}_i, \boldsymbol{e}_j \rangle \Big/ (\boldsymbol{e}_i \boldsymbol{e}_j - \zeta_{f+d}^a \boldsymbol{e}_j \boldsymbol{e}_i), \quad 0 \le i < j \le 2,$$

where $a = 1$, $p-1$ or $p-2$.
   Given a hyperplane $\mathfrak{H} = \theta_0 \boldsymbol{e}_0 + \theta_1 \boldsymbol{e}_1 + \theta_{p-1} \boldsymbol{e}_2$ we can form the following quotients

$$\mathbf{Q}_{i,j}^{\boldsymbol{\theta}} := \frac{\mathbf{Q}_{i,j}}{\Big(\boldsymbol{e}_i^{f+d} = \theta_i, \ \boldsymbol{e}_j^{f+d} = \theta_j \Big)}, \quad 0 \le i < j \le 2.$$

If $\theta_i \theta_j \ne 0$, $\mathbf{Q}_{i,j}^{\boldsymbol{\theta}}$ defines an Azumaya algebra over $\mathfrak{o}_L[\zeta_{f+d}]$, defining an element in $\mathrm{Br}(\mathfrak{o}_L[\zeta_{f+d}])$. Consequently the generic fibre is a central simple algebra and hence defines an element in $\mathrm{Br}(L[\zeta_{f+d}])$. By the functoriality of Br there is a natural morphism $\mathrm{Br}(\mathfrak{o}_L[\zeta_{f+d}]) \to \mathrm{Br}(L[\zeta_{f+d}])$.

Proposition 7.3. The association $\boldsymbol{\theta}^{\mathrm{Br}}_{-;S} : \ E[p] \longrightarrow \mathrm{Br}(L[\zeta_{f+d}])$,

$$[a]\mathtt{P} + [b]\mathtt{Q} \ \longmapsto \ \sum_{l=0}^{p-1} \theta_l \beta^l \ \longmapsto \ \mathbf{Q}^{\boldsymbol{\theta}}_{i,j}, \quad 0 \le i < j \le 2, \quad \theta_i \theta_j \ne 0, \qquad (7.3)$$

sets up a correspondence between $E[p]$ and elements in $\mathrm{Br}(L[\zeta_{f+d}])$, and by restriction to a (possibly trivial) element in $\mathrm{Br}(L)$.

The above correspondences (7.1), (7.2) and (7.3) might deserve some further study.

Remark 7.2. If $f + d = 2$ the algebras $\mathbf{Q}^{\boldsymbol{\theta}}_{i,j}$, under the condition $\theta_i \theta_j \ne 0$, are all quaternion algebras. This can only happen when E has Kodaira symbol I_1, i.e., when $\bar{\mathscr{E}} = \mathbb{P}^1$.

References

[BP16] Andrea Bandini and Laura Paladino. Fields generated by torsion points of elliptic curves. *J. Number Theory*, 169:103–133, 2016.

[Cas67] *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

[CDyDO03] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Cyclotomic extensions of number fields. *Indag. Math. (N.S.)*, 14(2):183–196, 2003.

[Cre15] J. Cremona. Elliptic curve data for conductors up to 350000, 2015.

[ELS17] Eivind Eriksen, Olav Arnfinn Laudal, and Arvid Siqveland. *Noncommutative deformation theory*. Monographs and Research Notes in Mathematics. CRC Press, Boca Raton, FL, 2017.

[FK18] Nuno Freitas and Alain Kraus. On the degree of the p-torsion field of elliptic curves over $\mathbb{Q}_\ell$ for $\ell \ne p$, 2018.

[GJLR16] Enrique González-Jiménez and Álvaro Lozano-Robledo. Elliptic curves with abelian division fields. *Math. Z.*, 283(3-4):835–859, 2016.

[HLS06] Jonas T. Hartwig, Daniel Larsson, and Sergei D. Silvestrov. Deformations of Lie algebras using σ-derivations. *J. Algebra*, 295(2):314–361, 2006.

[Kid03] M. Kida. Ramification in the division fields of an elliptic curve. *Abh. Math. Sem. Univ. Hamburg*, 73:195–207, 2003.

[KP17]   Michiel Kosters and René Pannekoek. On the structure of ellip-
          tic curves over finite extensions of $\mathbb{Q}_p$ with additive reduction.
          arXiv:1703.07888, Mar 2017.

[Lar17]   Daniel Larsson. Equivariant hom-Lie algebras and twisted deriva-
          tions on (arithmetic) schemes. *J. Number Theory*, 176:249–278,
          2017.

[Lar23a] Daniel Larsson. Kummer–Witt–Jackson algebras. *Preprint*, Au-
          gust 2023. Available at http://www.numberlab.se.

[Lar23b] Daniel Larsson. Arithmetic Geometry of Algebras with Large Cen-
          tres. *Preprint*, June 2023. Available at http://www.numberlab.se.

[Lau02]   O. A. Laudal. Noncommutative deformations of modules. *Ho-
          mology Homotopy Appl.*, 4(2, part 2):357–396, 2002. The Roos
          Festschrift volume, 2.

[LS07]   Daniel Larsson and Sergei D. Silvestrov. Quasi-deformations of
          $\mathfrak{sl}_2(\mathbb{F})$ using twisted derivations. *Comm. Algebra*, 35(12):4303–
          4318, 2007.

[Sag20]   Sage Developers, The. *SageMath, the Sage Mathematics Software
          System (Version 9.0)*, 2020. https://www.sagemath.org.

[Ser72]   Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini
          des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Sil86]   Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106
          of *Graduate Texts in Mathematics*. Springer-Verlag, New York,
          1986.

[Sil94]   Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic
          curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-
          Verlag, New York, 1994.

[Yas13]   Masaya Yasuda. Kummer generators and torsion points of elliptic
          curves with bad reduction at some primes. *Int. J. Number Theory*,
          9(7):1743–1752, 2013.