EXPLICIT n-DESCENT ON ELLIPTIC CURVES II. GEOMETRY

J.E. CREMONA, T.A. FISHER, C. O'NEIL, D. SIMON, AND M. STOLL

Abstract. This is the second in a series of papers in which we study the n-Selmer group of an elliptic curve. In this paper, we show how to realize elements of the n-Selmer group explicitly as curves of degree n embedded in $\mathbb{P}^{n-1}$. The main tool we use is a comparison between an easily obtained embedding into $\mathbb{P}^{n^2-1}$ and another map into $\mathbb{P}^{n^2-1}$ that factors through the Segre embedding $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1} \to \mathbb{P}^{n^2-1}$. The comparison relies on an explicit version of the local-to-global principle for the n-torsion of the Brauer group of the base field.

1. Introduction

This paper is the second in a series of papers discussing 'Explicit n-descent on elliptic curves.' Let E be an elliptic curve over a number field K, and let $n \geq 3$. The elements of the n-Selmer group of E may be viewed as isomorphism classes of n-coverings $C \to E$. For us, to do an 'explicit n-descent' means to represent each such isomorphism class by giving equations for C as a curve of degree n in $\mathbb{P}^{n-1}$.

It is well known that computing the n-Selmer group as an abstract group gives partial information about both the Mordell-Weil group $E(K)$ and the Tate-Shafarevich group $Ш(K, E)$. There are likewise several motivations for computing the n-Selmer group in the explicit sense described above. Firstly, it is known that a point in $E(K)$ of x-coordinate height h lifts to a point of height approximately $h/(2n)$ on one of the Selmer n-coverings (see Theorem B.3.2 in [6]). Thus explicit n-descent enables us to find generators for the Mordell-Weil group more easily, and hence sometimes to show that the n-torsion of the Tate-Shafarevich group is trivial. Secondly, if we have already computed the Mordell-Weil group, for instance using descent at some other n', then we can use explicit n-descent to exhibit concrete examples of non-trivial n-torsion elements of $Ш(K, E)$. Our work is also likely to form a

Date: 20th November 2006.

useful starting point for performing higher descents, and for computing the Cassels-Tate pairing.

The first paper in this series [3] gives more background on the theory of descent. In particular we explain a number of different interpretations of the elements of the group $H^1(K, E[n])$, which contains the Selmer group as a subgroup. One of these interpretations, and the one which is relevant to this paper, is as 'Brauer-Severi diagrams' $[C \to S]$; such a diagram consists of a morphism that is a twist of the embedding $E \to \mathbb{P}^{n-1}$ associated to the complete linear system $|n(\mathcal{O})|$, where $\mathcal{O}$ is the origin of E. In particular C is a torsor under E and S is a Brauer-Severi variety of dimension $n-1$. If C has points everywhere locally, then so does S, hence (by Global Class Field Theory) S is isomorphic to $\mathbb{P}^{n-1}$. Our goal in this paper is to explain how one can obtain equations for the image of C in $S \cong \mathbb{P}^{n-1}$ in this case.

In brief, we compare two different embeddings of C into $\mathbb{P}^{n^2-1}$. The first comes from the fact that, even without assuming C has points everywhere locally, the cohomology map $H^1(K, E[n]) \to H^1(K, E[n^2])$ sends the Brauer-Severi diagram $[C \to S]$ to a diagram $[C \to S']$ with $S' \cong \mathbb{P}^{n^2-1}$. The second map is more abstract: starting with the diagram $C \to S$ we form a dual map $C \to S^\vee$ and thus $C \to S \times S^\vee$. We then compose with the (generalised) Segre embedding to obtain

$$C \to S \times S^\vee \to \mathbb{P}^{n^2-1}.$$

Equations for the image of the first map to $\mathbb{P}^{n^2-1}$ are given in Section 3. By a suitable change of coordinates on $\mathbb{P}^{n^2-1}$ followed by projection to a hyperplane, we obtain equations for the image of the second map. Finally, we pull back to $C \to S$ and, when we start with a Selmer group element, obtain equations for $C \to \mathbb{P}^{n-1}$. For obvious reasons we refer to this as the Segre embedding method.

We will not be concerned in this paper with the details of implementation; these will be discussed in the third paper of the series [4]. However, we would like to mention that the Segre embedding method, as well as two more methods discussed in [3], have been implemented for $n = 3$ and $K = \mathbb{Q}$ and are available as part of the MAGMA computer algebra system [7] (version 2.13 or later).

All three methods rely for their practical implementation on a 'Black Box' that computes, for a given central simple K-algebra A of dimension n^2 that is known to be isomorphic to the matrix algebra $\mathrm{Mat}_n(K)$, an explicit isomorphism $A \to \mathrm{Mat}_n(K)$. Algorithms for this when $K = \mathbb{Q}$ will be described in [4].

2. Background and overview

Unless stated otherwise, K will denote a number field, with absolute Galois group G_K, and E will be an elliptic curve over K with origin $\mathcal{O}$. Let n be a positive integer. Recall the definition of the *n-Selmer group* of E: the short exact sequence of K-group schemes

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow 0$$

gives rise to the following commutative diagram with exact rows.

$$\begin{array}{ccccc} E(K) & \xrightarrow{\delta} & H^1(K, E[n]) & \longrightarrow & H^1(K, E) \\ \downarrow & & \downarrow & \overset{\alpha}{\searrow} & \downarrow \\ \prod_v E(K_v) & \xrightarrow{\delta} & \prod_v H^1(K_v, E[n]) & \longrightarrow & \prod_v H^1(K_v, E) \end{array}$$

Here, v runs through all places of K. The n-Selmer group $\mathrm{Sel}^{(n)}(K, E)$ is then defined to be the kernel of α.

The following notation and facts can be found in [3].

We assume that $n \geq 3$. Then there is an embedding $f : E \to \mathbb{P}^{n-1}$ associated to the complete linear system $|n(\mathcal{O})|$. In fact, if $n = 2$ one would work with a double cover, in which case our algorithm still works with minor changes. Indeed it reduces to the classical number field method for 2-descent (see for example [2], Lecture 15).

We can view an element of $H^1(K, E[n])$ as a twist of the diagram $f : E \to \mathbb{P}^{n-1}$, i.e., as a diagram of the form $[C \to S]$, where C is a torsor under E and S is a Brauer-Severi variety of dimension $n-1$. We call such a diagram a *Brauer-Severi diagram.* In this interpretation, a diagram $[C \to S]$ corresponds to an element of the n-Selmer group if and only if C has points everywhere locally.

The *period-index obstruction map*, defined in [9], is a quadratic map

$$\mathrm{Ob}_n : H^1(K, E[n]) \longrightarrow \mathrm{Br}(K)[n].$$

It sends the diagram $[C \to S]$ to the class of S in $\mathrm{Br}(K)[n]$. We say an element ξ of $H^1(K, E[n])$ has *trivial obstruction* if $\mathrm{Ob}_n(\xi) = 0$, equivalently the corresponding diagram $[C \to S]$ has $S \cong \mathbb{P}^{n-1}$.

Alternatively we can view an element ξ of $H^1(K, E[n])$ as a pair $(C, [D])$ where $[D]$ is a G_K-invariant divisor class on C. The class $[D]$ is represented by a rational divisor if and only if the element ξ has trivial obstruction.

Our algorithm applies not only to elements of the Selmer group, but more generally to any element in $H^1(K, E[n])$ with trivial obstruction.

The natural map $H^1(K, E[n]) \to H^1(K, E[n^2])$ brings the pair $(C, [D])$ to the pair $(C, [nD])$. Moreover, composing the above with Ob_{n^2} gives the zero map: there is a commutative diagram

$$\begin{array}{ccc} H^1(K, E[n]) & \xrightarrow{\mathrm{Ob}_n} & \mathrm{Br}(K)[n] \\ \downarrow & & \downarrow{\scriptstyle \cdot n} \\ H^1(K, E[n^2]) & \xrightarrow{\mathrm{Ob}_{n^2}} & \mathrm{Br}(K)[n^2] \end{array}$$

In other words, the divisor class $[nD]$ is always represented by a rational divisor of degree n^2, or equivalently, the above map takes any diagram $[C \to S]$ to a diagram $[C \to \mathbb{P}^{n^2-1}]$ with trivial obstruction. It is relatively easy to find equations for the image of this map. We do this in Section 3.

Our basic question then is, starting with an element of $H^1(K, E[n])$ with trivial obstruction, how do we *reverse* the map

$$[C \to \mathbb{P}^{n-1}] \longmapsto [C \to \mathbb{P}^{n^2-1}] \ ?$$

The diagram $[C \to S]$ naturally extends to give a map

$$\lambda_C : C \longrightarrow S \times S^\vee \longrightarrow \mathbb{P}(A)$$

where A is the *obstruction algebra,* the central simple K-algebra associated to the Brauer group element $\mathrm{Ob}_n(C \to S) = [S]$ (see [10, p. 160]). In this paper we describe an algorithm for writing down both structure constants for A and equations for C as a curve of degree n^2 in $\mathbb{P}(A) \cong \mathbb{P}^{n^2-1}$. In fact we specify the equations in Section 3 and the structure constants in Section 4.

In the case of trivial obstruction, we know that there exists an isomorphism of K-algebras $A \cong \mathrm{Mat}_n(K)$, which is called a *trivialisation* of A. Using this isomorphism, we may obtain equations for C in $\mathbb{P}^{n-1}$ as a curve of degree n by projecting onto a column.

The algorithm is split into parts, each of which (except the first) correspond to a piece of the 'master diagram' found in Theorem 8.1 below, which we reproduce here.

$$\begin{array}{ccccc} C & \xrightarrow{f'_C \times f'^{\vee}_C} & \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee & \xrightarrow{\text{Segre}} & \mathbb{P}(\mathrm{Mat}_n) \\ \downarrow{\scriptstyle g_C} & & & & \uparrow{\scriptstyle \text{proj}} \\ \mathbb{P}(R) & \xrightarrow[\varphi_\rho]{\sim} & \mathbb{P}(A_\rho) & \xrightarrow[\tau_\rho]{\sim} & \mathbb{P}(\mathrm{Mat}_n) \end{array}$$

The first step is to realize $H^1(K, E[n])$ as a subgroup of a concrete group. Let R be the affine algebra of the group scheme $E[n]$. Addition in $E[n]$ translates into the comultiplication homomorphism $\Delta : R \to R \otimes_K R$. We use this to define a group homomorphism

$$\partial : R^\times \longrightarrow (R \otimes_K R)^\times, \quad \alpha \longmapsto \frac{\alpha \otimes \alpha}{\Delta(\alpha)}.$$

Then there is a natural embedding of $H^1(K, E[n])$ into $(R \otimes_K R)^\times / \partial R^\times$. See Section 3 below and [3, Section 3]. We can then compute the Selmer group as a subgroup of $(R \otimes_K R)^\times / \partial R^\times$, see [4] for details. Therefore, in the following we can assume that our element of $H^1(K, E[n])$ is represented by some $\rho \in (R \otimes_K R)^\times$.

In the second step, starting with $\rho \in (R \otimes_K R)^\times$ coming from an element of $H^1(K, E[n])$, we construct an embedding $g_C : C \to \mathbb{P}(R)$, where $\mathbb{P}(R)$ is the projective space associated to the K-vector space R. We need to choose a K-basis of R in order to write down explicit equations for the image of g_C. This step is explained in Section 3.

In the third step, we define a new multiplication on R, which depends on ρ, that turns it into a central simple K-algebra A_ρ. This is the obstruction algebra for the element of $H^1(K, E[n])$ represented by ρ. In other words, we create an explicit isomorphism of K-vector spaces $\varphi_\rho : R \to A_\rho$. This will be explained in Section 4.

The fourth step makes use of the fact that $S \cong \mathbb{P}^{n-1}$, or equivalently that $A_\rho \cong \mathrm{Mat}_n(K)$, when ρ represents an element of $H^1(K, E[n])$ which has trivial obstruction. In Section 5, we give an explicit trivialisation of the algebra A_1, the central simple algebra coming from the trivial element of $H^1(K, E[n])$, which serves as a normalisation. For the general case a trivialisation map $\tau_\rho : A_\rho \to \mathrm{Mat}_n(K)$ will come from our 'Black Box', to be described in more detail in the third paper in this series [4].

In the fifth step, we project the image of $\tau_\rho \circ \varphi_\rho \circ g_C$ into the hyperplane of trace zero matrices and show that our total map factors through the Segre embedding:

$$C \longrightarrow \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee \stackrel{\text{Segre}}{\longrightarrow} \mathbb{P}(\mathrm{Mat}_n).$$

This step makes up Section 6 for the case $\rho = 1$, i.e. $[C \to \mathbb{P}^{n-1}] \cong [E \to \mathbb{P}^{n-1}]$. The general case is described in Sections 7 and 8.

The final step of the algorithm is to make use of the Segre factorisation. It is here that an explicit trivialisation of the obstruction algebra is required. We pull back under the Segre embedding and project to the

first factor, which gives us equations for $C \to \mathbb{P}^{n-1}$. This is explained in Section 8.

3. Finding Equations for C in $\mathbb{P}^{n^2-1}$

We continue to take K a number field, but in fact our algorithm works over any field whose characteristic is prime to n (although below, we assume for simplicity that the characteristic is neither 2 nor 3). We denote by $[n]$ the multiplication-by-n map on E. We fix a Weierstrass equation

$$E: \quad y^2 = x^3 + ax + b$$

and define for $T_1, T_2 \in E[n](\bar{K})$ a rational function $r_{(T_1,T_2)}$ in $\bar{K}(E)^\times$,

$$r_{(T_1,T_2)}(P) = \begin{cases} 1 & \text{if } T_1 = \mathcal{O} \text{ or } T_2 = \mathcal{O} \\ x(P) - x(T_1) & \text{if } T_1 + T_2 = \mathcal{O} \text{ and } T_1 \neq \mathcal{O} \\ \frac{y(P)+y(T_1+T_2)}{x(P)-x(T_1+T_2)} - \lambda(T_1,T_2) & \text{otherwise,} \end{cases}$$

where $\lambda(T_1, T_2)$ denotes the slope of the line joining T_1 and T_2, respectively of the tangent line at $T_1 = T_2$ if the points are equal.

For $T \in E[n](\bar{K})$, there exists a rational function $G_T \in \bar{K}(E)$ with divisor

$$\operatorname{div}(G_T) = \sum_{nS=T} (S) - \sum_{nS=\mathcal{O}} (S) = [n]^*(T) - [n]^*(\mathcal{O}).$$

(See [11, Section III.8].)

Proposition 3.1. *We can scale the $\{G_T\}$ such that*

(i) *The map $T \mapsto G_T$ is G_K-equivariant,*
(ii) *For each $T_1, T_2 \in E[n](\bar{K})$ and $P \in E(\bar{K}) \backslash E[n^2](\bar{K})$ we have*

$$r_{(T_1,T_2)}(nP) = \frac{G_{T_1}(P) G_{T_2}(P)}{G_{T_1+T_2}(P)}.$$

(iii) *$G_{\mathcal{O}} = 1$, and for $T \neq \mathcal{O}$ the residue of G_T at $\mathcal{O}$ with respect to the local parameter x/y is $\frac{1}{n}$.*

Proof. Define the scalings of the G_T so that condition (iii) holds. That means that with respect to the local parameter $t = x/y$, when $T \neq \mathcal{O}$, we can write $G_T(t) = \frac{1}{n} t^{-1} + \ldots$, where '$\ldots$' signifies 'higher order terms.' This choice of scaling makes the map $T \mapsto G_T$ visibly G_K-equivariant.

When $T_1 = \mathcal{O}$ or $T_2 = \mathcal{O}$, condition (ii) holds trivially. In any case, a calculation of divisors gives

$$\operatorname{div}(r_{(T_1,T_2)}) = (T_1) + (T_2) - (\mathcal{O}) - (T_1 + T_2)$$

for all choices of T_1 and T_2. So the divisor of $r_{(T_1,T_2)} \circ [n]$ is

$$\operatorname{div}(r_{(T_1,T_2)} \circ [n]) = \sum_{nS=T_1} (S) + \sum_{nS=T_2} (S) - \sum_{nS=\mathcal{O}} (S) - \sum_{nS=T_1+T_2} (S).$$

This is exactly the divisor of $P \mapsto G_{T_1}(P)G_{T_2}(P)/G_{T_1+T_2}(P)$. Therefore condition (ii) holds up to a scalar. In the following, we consider the case $T_1 + T_2 \neq \mathcal{O}$. We write $x(t) = t^{-2} + \dots$ and $y(t) = t^{-3} + \dots$. Then locally at $\mathcal{O}$,

$$\begin{aligned} r_{(T_1,T_2)}(t) &= \frac{y(t) + y(T_1 + T_2)}{x(t) - x(T_1 + T_2)} - \lambda(T_1, T_2) \\ &= \frac{t^{-3} + \dots}{t^{-2} + \dots} - \lambda(T_1, T_2) \\ &= t^{-1} + \dots \end{aligned}$$

Next, from [11, Prop. IV.2.3], we have $[n](t) = nt + \dots$, hence

$$r_{(T_1,T_2)} \circ [n](t) = (nt)^{-1} + \dots = \frac{1}{n} t^{-1} + \dots$$

Comparing this with

$$\frac{G_{T_1}(t)G_{T_2}(t)}{G_{T_1+T_2}(t)} = \frac{(\frac{1}{n}t^{-1} + \dots)(\frac{1}{n}t^{-1} + \dots)}{\frac{1}{n}t^{-1} + \dots} = \frac{1}{n} t^{-1} + \dots$$

shows that the scalar is 1. The case $T_1 + T_2 = \mathcal{O}$ is similar. □

In preparation for defining the embedding of C in $\mathbb{P}^{n^2-1}$, we recall some facts from [3]. Let R be the affine algebra of $E[n]$, i.e.,

$$R = \operatorname{Map}_K(E[n](\bar{K}), \bar{K}).$$

It is isomorphic to a product of (finite) field extensions of K, one for each G_K-orbit in $E[n](\bar{K})$. We also work with the algebra

$$\bar{R} = R \otimes_K \bar{K} = \operatorname{Map}(E[n](\bar{K}), \bar{K}).$$

The Weil pairing $e_n : E[n] \times E[n] \to \mu_n$ determines an injection

$$w : E[n](\bar{K}) \hookrightarrow \bar{R}^\times = \operatorname{Map}(E[n](\bar{K}), \bar{K}^\times)$$

via $w(S)(T) = e_n(S, T)$.

As in Section 2, we define $\partial : \bar{R}^\times \to (\bar{R} \otimes_{\bar{K}} \bar{R})^\times$ via

$$(1) \qquad \partial\alpha = \frac{\alpha \otimes \alpha}{\Delta(\alpha)}, \qquad \text{i.e.,} \qquad (\partial\alpha)(T_1, T_2) = \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1 + T_2)};$$

then there is an exact sequence (cf. [3, Section 3])

$$0 \longrightarrow E[n](\bar{K}) \xrightarrow{w} \bar{R}^\times \xrightarrow{\partial} (\bar{R} \otimes_{\bar{K}} \bar{R})^\times. \tag{2}$$

For V a vector space over K, we write $\mathbb{P}(V) = \mathrm{Proj}(K[V])$, where $K[V] = \oplus_{d \geq 0} \mathrm{Sym}^d(V^*)$ is the ring of polynomial functions on V.

We define $\mathcal{R} = \mathrm{Res}_{R/K}(\mathbb{A}^1)$, or equivalently, $\mathcal{R} = \mathrm{Spec}(K[R])$. For any K-scheme X, we have

$$\mathcal{R}(X) = \mathbb{A}^1(\mathrm{Spec}(R) \times_{\mathrm{Spec}(K)} X).$$

In particular, $\mathcal{R}(L) = R \otimes_K L$ for any field extension L/K.

We also define $\mathcal{R}^\times = \mathrm{Res}_{R/K}(\mathbb{G}_\mathrm{m})$ and $\mathcal{S}^\times = \mathrm{Res}_{R \otimes_K R/K}(\mathbb{G}_\mathrm{m})$. These schemes inherit a multiplication from $\mathbb{G}_\mathrm{m}$. The groups of K-rational points are $\mathcal{R}^\times(K) = R^\times$ and $\mathcal{S}^\times(K) = (R \otimes_K R)^\times$. We may identify $\mathcal{R}^\times$ with an open subscheme of $\mathcal{R}$.

With this notation, the exact sequence of G_K-modules (2), becomes an exact sequence of K-group schemes:

$$0 \longrightarrow E[n] \xrightarrow{w} \mathcal{R}^\times \xrightarrow{\partial} \mathcal{S}^\times. \tag{3}$$

Part (i) of Proposition 3.1 allows us to package the functions G_T to form a scheme map $g_E : E \to \mathbb{P}(R)$ sending $P \in E(\bar{K})$ to the class of the map $T \mapsto G_T(P)$. Away from the subscheme $E[n^2]$, the map g_E can be lifted to a map g_E^0 to $\mathcal{R}^\times$. Then we have a commutative diagram:

$$\begin{array}{ccc} E \setminus E[n^2] & \xrightarrow{g_E^0} & \mathcal{R}^\times \\ \downarrow & & \downarrow \\ E & \xrightarrow{g_E} & \mathbb{P}(R) \end{array}$$

Next, we use the G_K-equivariance of $(T_1, T_2) \mapsto r_{(T_1,T_2)}$ to package the functions $r_{(T_1,T_2)}$ to form a scheme map $r : E \setminus E[n] \to \mathcal{S}^\times$ sending $P \in E(\bar{K}) \setminus E[n](\bar{K})$ to the map $r(P) : (T_1, T_2) \mapsto r_{(T_1,T_2)}(P)$.

Proposition 3.2. *The following diagram commutes.*

$$\begin{array}{ccc} E \setminus E[n^2] & \xrightarrow{[n]} & E \setminus E[n] \\ {\scriptstyle g_E^0}\downarrow & & \downarrow{\scriptstyle r} \\ \mathcal{R}^\times & \xrightarrow{\partial} & \mathcal{S}^\times \end{array}$$

Proof. We take a geometric point $P \in E(\bar{K}) \setminus E[n^2](\bar{K})$ and observe that

$$\partial(g_E^0(P))(T_1, T_2) = \frac{G_{T_1}(P)G_{T_2}(P)}{G_{T_1+T_2}(P)}.$$

By Proposition 3.1(ii), this equals $r_{(T_1,T_2)}(nP)$. □

For $T \in E[n](\bar{K})$ we denote by z_T the coordinate function on $\mathcal{R} \times_{\mathrm{Spec}(K)} \mathrm{Spec}(K(T))$ given by evaluating at T, so $z_T(\alpha) = \alpha(T)$.

Proposition 3.3. *Given a Weierstrass equation for E, we can explicitly compute a set of $n^2(n^2-3)/2$ linearly independent quadrics over K which define the image of*

$$g_E : E \longrightarrow \mathbb{P}(R) \cong \mathbb{P}^{n^2-1}.$$

If $E[n](\bar{K}) = E[n](K)$, then the z_T are coordinate functions on $\mathcal{R}$, and the defining quadrics can be split into two groups as follows. For all $T_1, T_2 \in E[n](\bar{K}) \setminus \{\mathcal{O}\}$, we have

$$\big(x(T_1) - x(T_2)\big) z_{\mathcal{O}}^2 + z_{T_1} z_{-T_1} - z_{T_2} z_{-T_2},$$

and for all $T_{11}, T_{12}, T_{21}, T_{22} \in E[n](\bar{K}) \setminus \{\mathcal{O}\}$ such that

$$T_{11} + T_{12} = T_{21} + T_{22} = T \neq \mathcal{O},$$

we have

$$\big(\lambda(T_{21}, T_{22}) - \lambda(T_{11}, T_{12})\big) z_{\mathcal{O}} z_T - z_{T_{11}} z_{T_{12}} + z_{T_{21}} z_{T_{22}}.$$

Proof. We first note that the G_T are linearly independent. This follows from the fact they are eigenfunctions for distinct characters with respect to the action of $E[n]$ by translation. (We are using the definition of the Weil pairing in [11, Section III.8].) Since there are n^2 functions G_T, they form a basis for the Riemann-Roch space of the divisor $[n]^*(\mathcal{O})$. Hence g_E embeds E into $\mathbb{P}(R) \cong \mathbb{P}^{n^2-1}$ as an elliptic normal curve of degree n^2.

Now let $P \in E(\bar{K}) \setminus E[n^2](\bar{K})$, and let $z = g_E^0(P) \in \mathcal{R}^\times(\bar{K})$ be projective coordinates for $g_E(P)$. By Proposition 3.2, we then have $r(nP) = \partial z$, or equivalently, $r(nP)\Delta(z) = z \otimes z$. We wish to eliminate P from this equation. Since $z_{\mathcal{O}}(g_E^0(P)) = 1$, we can make the equation homogeneous by multiplying the left hand side with $z(\mathcal{O})$. This gives

$$r(nP)\, z(\mathcal{O})\Delta(z) = z \otimes z.$$

Writing everything out in terms of a K-basis of R, we obtain n^4 quadrics, some of whose coefficients involve rational functions of nP. We can eliminate these rational functions by linear algebra over K, to obtain a set of quadrics in $K[R]$ — this is what we do in practice. In order to

determine the dimension of the space spanned by them and the geometry of the object defined by them, we can work over $\bar{K}$. In fact, it is sufficient to work over $L = K(E[n])$.

Over L, the coordinate functions z_T are defined. In terms of these, our system of equations is

$$r_{(T_1,T_2)}(nP)\, z_{\mathcal{O}} z_{T_1+T_2} = z_{T_1} z_{T_2},$$

parametrised by $(T_1, T_2) \in E[n](\bar{K}) \times E[n](\bar{K})$.

If $T_1 = \mathcal{O}$ or $T_2 = \mathcal{O}$, this reduces to a tautology.

If $T_1 = T \neq \mathcal{O}$ and $T_2 = -T$, then we get

$$\big(x(nP) - x(T)\big) z_{\mathcal{O}}^2 = z_T z_{-T}.$$

We can eliminate $x(nP)$ by taking differences. Taking into account the symmetry $T \leftrightarrow -T$, this gives us d_1 independent quadrics, where

$$d_1 = \#\Big(\frac{E[n](\bar{K}) \setminus \{\mathcal{O}\}}{\{\pm 1\}}\Big) - 1 = \begin{cases} (n^2-3)/2 & \text{if } n \text{ is odd} \\ n^2/2 & \text{if } n \text{ is even.} \end{cases}$$

If $T_1 + T_2 = T \neq \mathcal{O}$ and $T_1, T_2 \neq \mathcal{O}$, we obtain

$$\Big(\frac{y(nP) + y(T)}{x(nP) - x(T)} - \lambda(T_1, T_2)\Big) z_{\mathcal{O}} z_T = z_{T_1} z_{T_2}.$$

Fixing T, we can again eliminate the dependence on P by taking differences. Taking into account the symmetry $(T_1, T_2) \leftrightarrow (T_2, T_1)$, this provides us with d_2 independent quadrics, where

$$\begin{aligned} d_2 &= \#\Big(\frac{\{(T_1,T_2) : T_1, T_2, T_1+T_2 \neq \mathcal{O}\}}{(T_1,T_2) \sim (T_2,T_1)}\Big) - \#\big(E[n](\bar{K}) \setminus \{\mathcal{O}\}\big) \\ &= \begin{cases} (n^2-1)(n^2-3)/2 & \text{if } n \text{ is odd} \\ n^2(n^2-4)/2 & \text{if } n \text{ is even.} \end{cases} \end{aligned}$$

Together, we obtain $d_1 + d_2 = n^2(n^2-3)/2$ independent quadrics in either case.

We have found an $n^2(n^2-3)/2$-dimensional space of quadrics vanishing on the image of g_E. In general (see for example the Corollary to Theorem 8 in [8]) the homogeneous ideal of an elliptic normal curve of degree $m \geq 4$ is generated by a vector space of quadrics of dimension $m(m-3)/2$. Therefore, our quadrics define the image of E in $\mathbb{P}(R)$ under g_E. □

By Section 3 of [3], we can identify $H^1(K, E[n])$ with a subgroup of $(R \otimes_K R)^\times / \partial R^\times$. Specifically, we define an injective map

$$H^1(K, E[n]) \longrightarrow (R \otimes_K R)^\times / \partial R^\times$$

by sending $\xi \in H^1(K, E[n])$ to $\rho\, \partial R^\times$ where $\rho = \partial\gamma$ for some $\gamma \in \bar{R}^\times$ such that $w(\xi_\sigma) = \sigma(\gamma)/\gamma$ for all $\sigma \in G_K$.

Definition 3.4. We let H denote the subgroup of $(R \otimes_K R)^\times$ that maps to the image of $H^1(K, E[n])$ in $(R \otimes_K R)^\times / \partial R^\times$.

Starting with a representative $\rho \in H$, we fix a choice of γ as above. Then γ determines a cocycle class $\xi \in H^1(K, E[n])$. We let $\pi : C \to E$ be the twist of the trivial n-covering $[n] : E \to E$ by ξ. In other words, there is a genus 1 curve C defined over K and an isomorphism $\phi : C \to E$ defined over $\bar{K}$ with $\sigma(\phi) \circ \phi^{-1} = \tau_{\xi_\sigma}$ (translation by $\xi_\sigma \in E[n](\bar{K})$) for all $\sigma \in G_K$. The covering map is then $\pi = [n] \circ \phi$. It is easy to check that π is defined over K.

Proposition 3.5. *Given ρ and C as above, there are rational functions $G_{T,C} \in \bar{K}(C)$, indexed by $T \in E[n](\bar{K})$, such that*

(i) *The divisor of $G_{T,C}$ is*

$$\operatorname{div}(G_{T,C}) = \sum_{\pi(S)=T} (S) - \sum_{\pi(S)=\mathcal{O}} (S) = \pi^*(T) - \pi^*(\mathcal{O}).$$

(ii) *The map $T \mapsto G_{T,C}$ is G_K-equivariant.*

(iii) *The functions $G_{T,C}$ are scaled so that*

$$r_{(T_1,T_2)}(\pi(P)) = \rho(T_1, T_2) \frac{G_{T_1,C}(P) G_{T_2,C}(P)}{G_{T_1+T_2,C}(P)}.$$

(iv) *We can package these $G_{T,C}$ to form morphisms of schemes*

$$g_C : C \to \mathbb{P}(R) \qquad \text{and} \qquad g_C^0 : C \setminus \pi^* E[n] \to \mathcal{R}^\times.$$

(v) *The following diagram, with vertical maps defined over $\bar{K}$, commutes:*

$$\begin{array}{ccc} C & \xrightarrow{g_C} & \mathbb{P}(R) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\cdot\gamma} \\ E & \xrightarrow{g_E} & \mathbb{P}(R) \end{array}$$

Proof. We take $\gamma \in \bar{R}^\times$ as above and define

$$G_{T,C}(P) = \gamma(T)^{-1} G_T(\phi(P)) \tag{4}$$

for $P \in C(\bar{K})$. Since $\pi = [n] \circ \phi$, statement (i) is immediate from the corresponding statement for the G_T. Next we check Galois equivariance. Since $\sigma(\phi) \circ \phi^{-1} = \tau_{\xi_\sigma}$ we have

$$\sigma\big(G_T(\phi P)\big) = G_{\sigma T}\big(\phi(\sigma P) + \xi_\sigma\big) = e_n(\xi_\sigma, \sigma T) G_{\sigma T}\big(\phi(\sigma P)\big)$$

where the second equality is the definition of the Weil pairing in [11, Section III.8]. On the other hand, since $\sigma(\gamma)/\gamma = w(\xi_\sigma)$, we have

$$\sigma(\gamma(T)) = w(\xi_\sigma)(\sigma T)\gamma(\sigma T) = e_n(\xi_\sigma, \sigma T)\gamma(\sigma T).$$

We deduce that

$$\sigma(G_{T,C})(\sigma P) = \sigma(G_{T,C}(P)) = \gamma(\sigma T)^{-1} G_{\sigma T}(\phi(\sigma P)) = G_{\sigma T, C}(\sigma P).$$

This proves (ii). For (iii) we compute

$$\begin{aligned} r_{(T_1,T_2)}(\pi(P)) &= r_{(T_1,T_2)}(n \cdot \phi(P)) \\ &= \frac{G_{T_1}(\phi(P)) G_{T_2}(\phi(P))}{G_{T_1+T_2}(\phi(P))} = \rho(T_1, T_2) \frac{G_{T_1,C}(P) G_{T_2,C}(P)}{G_{T_1+T_2,C}(P)}. \end{aligned}$$

Here the second equality comes from Proposition 3.1. The third equality follows from (4) and $\partial\gamma = \rho$.

Statement (iv) is a formal consequence of (ii), and (v) then follows from (4). □

The proofs of the following propositions are very similar to those of Propositions 3.2 and 3.3, and so will be omitted.

Proposition 3.6. *The following diagram commutes.*

$$\begin{array}{ccccc} C \setminus \pi^* E[n] & & \xrightarrow{\quad\pi\quad} & & E \setminus E[n] \\ \Big\downarrow{\scriptstyle g_C^0} & & & & \Big\downarrow{\scriptstyle r} \\ \mathcal{R}^\times & \xrightarrow{\partial} & \mathcal{S}^\times & \xrightarrow{\cdot\rho} & \mathcal{S}^\times \end{array}$$

Proposition 3.7. *Given a Weierstrass equation for E and an element $\rho \in H$, with corresponding n-covering $\pi : C \to E$, we can explicitly compute a set of $n^2(n^2-3)/2$ linearly independent quadrics over K which define the image of*

$$g_C : C \longrightarrow \mathbb{P}(R) \cong \mathbb{P}^{n^2-1}.$$

If $E[n](\bar{K}) = E[n](K)$, then the z_T are coordinate functions on $\mathcal{R}$, and the defining quadrics can be split into two groups as follows. For all $T_1, T_2 \in E[n](\bar{K}) \setminus \{\mathcal{O}\}$, we have

$$\big(x(T_1) - x(T_2)\big) z_{\mathcal{O}}^2 + \rho(T_1, -T_1) z_{T_1} z_{-T_1} - \rho(T_2, -T_2) z_{T_2} z_{-T_2},$$

and for all $T_{11}, T_{12}, T_{21}, T_{22} \in E[n](\bar{K}) \setminus \{\mathcal{O}\}$ *such that*

$$T_{11} + T_{12} = T_{21} + T_{22} = T \neq \mathcal{O},$$

we have

$$\big(\lambda(T_{21}, T_{22}) - \lambda(T_{11}, T_{12})\big) z_{\mathcal{O}} z_T - \rho(T_{11}, T_{12}) z_{T_{11}} z_{T_{12}} + \rho(T_{21}, T_{22}) z_{T_{21}} z_{T_{22}}.$$

4. A Multiplication Table for the Obstruction Algebra

As noted in [11, Section III.8], for each $T \in E[n](\bar{K})$ there is a rational function $F_T \in \bar{K}(E)$ with

$$\operatorname{div}(F_T) = n(T) - n(\mathcal{O}).$$

In the last section we defined rational functions G_T. We now scale the F_T so that $F_T \circ [n] = G_T^n$. It is equivalent to demand that the leading coefficient of each F_T, when expanded as a Laurent series in the local parameter x/y at $\mathcal{O}$, should be 1. (See 'Step 1' in Section 5.3 of [3].) It turns out that the F_T are rather easy to compute; this will be explained in [4].

Following 'Step 2' (loc. cit.), we now define $\varepsilon \in (\bar{R} \otimes_{\bar{K}} \bar{R})^\times$ by

$$\varepsilon(T_1, T_2) = \frac{F_{T_1+T_2}(P)}{F_{T_1}(P) F_{T_2}(P - T_1)}.$$

for any $P \in E(\bar{K}) \setminus \{\mathcal{O}, T_1, T_1 + T_2\}$. By the discussion in Section 3 of [3], this does not depend on P and satisfies $\varepsilon(T_1, T_2)\varepsilon(T_2, T_1)^{-1} = e_n(T_1, T_2)$. Since the map defining ε is Galois-equivariant, we obtain an element $\varepsilon \in (R \otimes_K R)^\times$. The subgroup $H \subset (R \otimes_K R)^\times$ was defined in Definition 3.4.

Proposition 4.1. *There is a map*

$$H \longrightarrow \{\textit{central simple } K\textit{-algebras of dimension } n^2\}$$

sending ρ *to an algebra* A_ρ *such that*

$$\mathrm{Ob}_n(\xi) = [A_\rho] \in \mathrm{Br}(K)[n],$$

where $\xi \in H^1(K, E[n])$ *is the element represented by* $\rho \in H$*. In particular, if* $\rho' = \rho\, \partial z$ *for some* $z \in R^\times$*, then* $[A_\rho] = [A_{\rho'}]$*; in fact, the algebras* A_ρ *and* $A_{\rho'}$ *are isomorphic.*

Proof. In 'Step 3' (loc. cit.) we defined $A_\rho = (R, +, *_{\varepsilon\rho})$, where $*_{\varepsilon\rho}$ is a new multiplication on R. To define it we view $R \otimes_K R$ as an R-algebra via the comultiplication $\Delta : R \to R \otimes_K R$. Recall that this is defined by

$$\Delta(\alpha)(T_1, T_2) = \alpha(T_1 + T_2).$$

The corresponding trace map

$$\mathrm{Tr} : R \otimes_K R \longrightarrow R$$

is given by $(\mathrm{Tr}\, z)(T) = \sum_{T_1+T_2=T} z(T_1, T_2)$. Then we define

$$x *_{\varepsilon\rho} y = \mathrm{Tr}(\varepsilon\rho \cdot x \otimes y)$$

for all $x, y \in R$. The stated properties of A_ρ were established in Section 4 of [3]. If $\rho' = \rho\,\partial z$, then the isomorphism $A_{\rho'} \to A_\rho$ is given by $\alpha \mapsto z\alpha$ where the multiplication takes place in R. □

Definition 4.2. Let $\varphi_\rho : R \to A_\rho$ be the isomorphism of underlying K-vector spaces, inherent in the proof of Proposition 4.1.

The construction in the proof provides us with explicit structure constants of A_ρ in terms of a K-basis of R. In [4], we will discuss how to compute the structure constants in practice.

5. Trivialisation of the obstruction algebra

Recall that when $\rho \in R$ has trivial obstruction there is a trivialisation isomorphism $\tau_\rho : A_\rho \to \mathrm{Mat}_n(K)$, where A_ρ is the central simple algebra in Proposition 4.1. Our algorithm will need to make this trivialisation explicit. In general this will be carried out by the 'Black Box' to be discussed further in [4]; however, when $\rho = 1$ we can write down a standard trivialisation $\tau_1 : A_1 \to \mathrm{Mat}_n(K)$. In fact τ_1 will depend on a choice of morphism $f_E : E \to \mathbb{P}^{n-1}$ determined by the complete linear system $|n(\mathcal{O})|$. We make this choice now.

Let $f_E^\vee : E \to (\mathbb{P}^{n-1})^\vee$ be the dual map of f_E, i.e., the map that takes $P \in E(\bar{K})$ to the osculating hyperplane at $f_E(P)$. The elements of $\mathbb{P}^{n-1}$ will be written as column vectors, and the elements of $(\mathbb{P}^{n-1})^\vee$ as row vectors. For each $T \in E[n](\bar{K})$ there is a matrix $M_T \in \mathrm{GL}_n(\bar{K})$ such that translation by T on E extends to the automorphism of $\mathbb{P}^{n-1}$ defined by M_T.

Proposition 5.1. *We may fix the scalings of the M_T's so that*

$$F_T(P) = \frac{f_E^\vee(\mathcal{O}) \cdot M_T^{-1} \cdot f_E(P)}{f_E^\vee(\mathcal{O}) \cdot f_E(P)} \tag{5}$$

where the F_T's are the rational functions on E defined in Section 4. In particular, $M_\mathcal{O} = I$.

Proof. The right hand side is well-defined (the undetermined scalings of $f_E^\vee(\mathcal{O})$ and of $f_E(P)$ cancel out) and has divisor $n(T) - n(\mathcal{O})$. □

Let $\delta_T \in \bar{R}$ be the characteristic function of T, i.e., the map that takes T to 1 but sends all other elements of $E[n](\bar{K})$ to 0. It is clear that the set of δ_T for $T \in E[n](\bar{K})$ are a basis for $\bar{R}$ as a $\bar{K}$-vector space.

Definition 5.2. Recall the isomorphism $\varphi_1 : R \to A_1$ of underlying K-vector spaces. Let $\tau_1 : A_1 \to \mathrm{Mat}_n(K)$ be the linear map of K-vector spaces given by

$$\tau_1\big(\varphi_1(\alpha)\big) = \sum_{T \in E[n](\bar{K})} \alpha(T) M_T.$$

(Since $T \mapsto M_T$ is G_K-equivariant, the map τ_1, though *a priori* defined as a map of $\bar{K}$-vector spaces, is G_K-equivariant.) Note that τ_1 sends $\varphi_1(\delta_T) \in A_1 \otimes_K \bar{K}$ to $M_T \in \mathrm{Mat}_n(\bar{K})$.

Proposition 5.3. *The map $\tau_1 : A_1 \to \mathrm{Mat}_n(K)$ is an isomorphism of K-algebras.*

Proof. (See also [3, Prop. 5.8.(ii)].) By [3, Lemma 4.8] the set of M_T for $T \in E[n](\bar{K})$ form a basis for $\mathrm{Mat}_n(\bar{K})$. So it is clear that τ_1 is an isomorphism of K-vector spaces. We must show that it is also a ring homomorphism.

We recall that $A_1 = (R, +, *_\varepsilon)$. The new multiplication $*_\varepsilon$ extends to a multiplication on $\bar{R}$ given by

$$\delta_{T_1} *_\varepsilon \delta_{T_2} = \mathrm{Tr}(\varepsilon \cdot \delta_{T_1} \otimes \delta_{T_2}) = \varepsilon(T_1, T_2)\delta_{T_1+T_2}.$$

Applying τ_1 to both sides, it is apparent that what we have to show is that

$$M_{T_1} M_{T_2} = \varepsilon(T_1, T_2) M_{T_1+T_2}$$

for all $T_1, T_2 \in E[n](\bar{K})$. In any case it is clear that $M_{T_1} M_{T_2} = c\, M_{T_1+T_2}$ for some constant $c \in \bar{K}^\times$.

Substituting $T = T_1 + T_2$ in (5), we get

$$F_{T_1+T_2}(P) = c\, \frac{f_E^\vee(\mathcal{O}) \cdot M_{T_2}^{-1} M_{T_1}^{-1} \cdot f_E(P)}{f_E^\vee(\mathcal{O}) \cdot f_E(P)}. \tag{6}$$

We arbitrarily lift f_E and $f_E^\vee$ to rational maps $E \dashrightarrow \mathbb{A}^n$. The definition of M_T gives

$$M_{T_1}^{-1} \cdot f_E(P) = h(P) f_E(P - T_1) \tag{7}$$

for some rational function $h \in \bar{K}(E)$. Premultiplying by $f_E^\vee(\mathcal{O})$ we get

$$h(P) = \frac{f_E^\vee(\mathcal{O}) \cdot M_{T_1}^{-1} \cdot f_E(P)}{f_E^\vee(\mathcal{O}) \cdot f_E(P - T_1)}. \tag{8}$$

Substituting (7) into (6) gives

$$F_{T_1+T_2}(P) = c\,\frac{f_E^\vee(\mathcal{O})\cdot M_{T_2}^{-1}\cdot f_E(P-T)}{f_E^\vee(\mathcal{O})\cdot f_E(P)}\,h(P).$$

Then by (5) and (8) we obtain

$$F_{T_1+T_2}(P) = c\,F_{T_2}(P-T_1)F_{T_1}(P).$$

Comparing with the definition of ε in Section 4, it follows that $c = \varepsilon(T_1, T_2)$ as required. □

6. The Segre Factorisation for E

Recall our convention that for V a vector space over K, we write $\mathbb{P}(V) = \mathrm{Proj}(K[V])$ where $K[V] = \oplus_{d\geq 0}\mathrm{Sym}^d(V^*)$ is the ring of polynomial functions on V. We abbreviate $\mathbb{P}(\mathrm{Mat}_n(K))$ as $\mathbb{P}(\mathrm{Mat}_n)$. The K-points of $\mathbb{P}(\mathrm{Mat}_n)$ may be identified with the set $\mathrm{Mat}_n(K)/K^\times$.

In the last section we fixed a morphism $f_E : E \to \mathbb{P}^{n-1}$ determined by the complete linear system $|n(\mathcal{O})|$, and wrote $f_E^\vee : E \to (\mathbb{P}^{n-1})^\vee$ for the dual map. We now consider the composite map

$$\lambda_E : E \xrightarrow{f_E\times f_E^\vee} \mathbb{P}^{n-1}\times(\mathbb{P}^{n-1})^\vee \xrightarrow{\text{Segre}} \mathbb{P}(\mathrm{Mat}_n).$$

We recall that we represent elements of $\mathbb{P}^{n-1}$ as column vectors, and elements of $(\mathbb{P}^{n-1})^\vee$ as row vectors. The Segre map is then given by matrix multiplication. In particular, its image is the locus of rank 1 matrices. Since each point of E lies on its own osculating hyperplane, for $P \in E(\bar{K})$ we have $f_E^\vee(P)\cdot f_E(P) = 0$. Then

$$\mathrm{Tr}(\lambda_E(P)) = \mathrm{Tr}(f_E(P)\cdot f_E^\vee(P)) = \mathrm{Tr}(f_E^\vee(P)\cdot f_E(P)) = 0.$$

That is, the image of λ_E is contained in the locus of trace zero matrices, which is a hyperplane in $\mathbb{P}(\mathrm{Mat}_n)$. There is a direct sum decomposition $\mathrm{Mat}_n(K) = \langle I_n\rangle \oplus \{\mathrm{Tr} = 0\}$. Note that the trace zero subspace contains all the matrices M_T for $T \neq \mathcal{O}$. We write proj for the rational map $\mathbb{P}(\mathrm{Mat}_n) \dashrightarrow \mathbb{P}(\mathrm{Mat}_n)$ induced by the second projection.

We defined maps $g_E : E \to \mathbb{P}(R)$, $\varphi_1 : R \to A_1$ and $\tau_1 : A_1 \to \mathrm{Mat}_n(K)$ in Sections 3, 4 and 5, respectively.

Theorem 6.1. *The following diagram commutes.*

$$\begin{array}{ccccc} E & & \xrightarrow{\quad\lambda_E\quad} & & \mathbb{P}(\mathrm{Mat}_n) \\ \downarrow{\scriptstyle g_E} & & & & \uparrow{\scriptstyle \mathrm{proj}} \\ \mathbb{P}(R) & \xrightarrow[\varphi_1]{\sim} & \mathbb{P}(A_1) & \xrightarrow[\tau_1]{\sim} & \mathbb{P}(\mathrm{Mat}_n) \end{array}$$

The maps g_E and τ_1 were defined using the G_T's and the M_T's, respectively. Note that the matrices M_T depend on our choice of the embedding $f_E : E \to \mathbb{P}^{n-1}$.

The proof of Theorem 6.1 is based on the following result.

Theorem 6.2. *For $P \in E(\bar{K}) \setminus E[n](\bar{K})$ we have*

$$\lambda_E(P) = \sum_{T \neq \mathcal{O}} G_T(P) M_T.$$

Let us show how Theorem 6.1 follows from this. Since the commutativity of the diagram is a geometric question, we are free to work over $\bar{K}$. From the definitions we have $\tau_1 \circ \varphi_1 \circ g_E(P) = \sum_T G_T(P) M_T$. Then composing with the projection map to the trace zero subspace we get $P \mapsto \sum_{T \neq \mathcal{O}} G_T(P) M_T$, which equals $\lambda_E(P)$ by Theorem 6.2.

The proof of Theorem 6.2 is split into a series of lemmas. The following notation will be used throughout. Let $Q_1, \ldots, Q_n$ be n points in $E(\bar{K})$ and let $P = \sum_{i=1}^n Q_i$. We define morphisms $h_E : E^n \to \mathbb{P}^{n-1}$ and $h_E^\vee : E^n \to (\mathbb{P}^{n-1})^\vee$ as follows. For the first map we put

$$h_E(Q_1, \ldots, Q_n) = f_E(P).$$

The second map takes $(Q_1, \ldots, Q_n)$ to the hyperplane meeting E (or rather the image of f_E) in the divisor $(P - nQ_1) + \ldots + (P - nQ_n)$. Notice that since this divisor has sum $\mathcal{O}$, it is indeed linearly equivalent to the hyperplane section.

The first lemma can be seen as a multi-variable generalisation of formula (5) in Proposition 5.1.

Lemma 6.3. *If $Q_1, \ldots, Q_n \in E(\bar{K}) \setminus E[n](\bar{K})$ then*

$$G_T(Q_1) \ldots G_T(Q_n) = \frac{h_E^\vee(Q_1, \ldots, Q_n) \cdot M_T^{-1} \cdot h_E(Q_1, \ldots, Q_n)}{h_E^\vee(Q_1, \ldots, Q_n) \cdot h_E(Q_1, \ldots, Q_n)}$$

for all $T \in E[n](\bar{K})$.

Proof. We view each side as a rational function on E^n. The strategy of the proof is first to compare divisors, and then to check scalings by specialising to the case $Q_1 = Q_2 = \ldots = Q_n$.

Let $\mathrm{pr}_i : E^n \to E$ be projection to the ith factor. The left hand side has divisor

$$\sum_{i=1}^n \sum_{nx=T} \mathrm{pr}_i^*(x) - \sum_{i=1}^n \sum_{nx=\mathcal{O}} \mathrm{pr}_i^*(x).$$

From the definitions of h_E and $h_E^\vee$ the right hand side has a zero whenever $nQ_i = T$ for some i, and a pole whenever $nQ_i = \mathcal{O}$ for some i. Therefore the right hand side has divisor

$$\sum_{i=1}^{n} \sum_{nx=T} a_x \operatorname{pr}_i^*(x) - \sum_{i=1}^{n} \sum_{nx=\mathcal{O}} b_x \operatorname{pr}_i^*(x)$$

where the a_x and b_x are positive integers.

If we replace Q_1 by $Q_1 + S$ for $S \in E[n](\bar{K})$, then the right hand side is multiplied by a non-zero scalar (the commutator of M_S and M_T). It follows that the integers a_x and b_x do not depend on x. So the right hand side has divisor

$$a \sum_{i=1}^{n} \sum_{nx=T} \operatorname{pr}_i^*(x) - b \sum_{i=1}^{n} \sum_{nx=\mathcal{O}} \operatorname{pr}_i^*(x)$$

where a and b are positive integers.

Since this divisor is principal, its pull-back by any morphism $E \to E^n$ has degree 0. This enables us to show that $a = b$. Since E^n is a projective variety, it follows that the right hand side is

$$c\, G_T(Q_1)^a \cdots G_T(Q_n)^a$$

for some constant $c \in \bar{K}^\times$.

We now specialise by taking $Q_1 = Q_2 = \ldots = Q_n$ ($= Q$ say). Then $P = nQ$ and

$$c\, G_T(Q)^{na} = \frac{f_E^\vee(\mathcal{O}) \cdot M_T^{-1} \cdot f_E(P)}{f_E^\vee(\mathcal{O}) \cdot f_E(P)}.$$

The definition of F_T in Section 4 gives $F_T(P) = F_T(nQ) = G_T(Q)^n$. Finally we compare with (5) to get $c = 1$ and $a = 1$. □

Lemma 6.4. *If $Q_1, \ldots, Q_n \in E(\bar{K}) \setminus E[n](\bar{K})$ then*

$$\frac{1}{n} \sum_{T \in E[n](\bar{K})} G_T(Q_1) \ldots G_T(Q_n) M_T = \frac{h_E(Q_1, \ldots, Q_n) \cdot h_E^\vee(Q_1, \ldots, Q_n)}{h_E^\vee(Q_1, \ldots, Q_n) \cdot h_E(Q_1, \ldots, Q_n)}$$

Proof. Since the M_T form a basis for $\mathrm{Mat}_n(\bar{K})$, we can write the right hand side as $n^{-1} \sum_T a_T(Q_1, \ldots, Q_n) M_T$ for some rational functions a_T on E^n. To compute the a_T's we premultiply by M_T^{-1} and take the trace. Since

$$\operatorname{Tr}(M_T) = \begin{cases} n & \text{if } T = \mathcal{O}, \\ 0 & \text{otherwise,} \end{cases}$$

on the left hand side we get $G_T(Q_1)\dots G_T(Q_n)$. On the right hand side, using $\mathrm{Tr}(AB)=\mathrm{Tr}(BA)$ gives

$$\begin{aligned} a_T(Q_1,\dots,Q_n) &= \mathrm{Tr}\Big(M_T^{-1}\cdot\frac{h_E(Q_1,\dots,Q_n)\cdot h_E^\vee(Q_1,\dots,Q_n)}{h_E^\vee(Q_1,\dots,Q_n)\cdot h_E(Q_1,\dots,Q_n)}\Big)\\ &= \mathrm{Tr}\Big(\frac{h_E^\vee(Q_1,\dots,Q_n)\cdot M_T^{-1}\cdot h_E(Q_1,\dots,Q_n)}{h_E^\vee(Q_1,\dots,Q_n)\cdot h_E(Q_1,\dots,Q_n)}\Big)\\ &= G_T(Q_1)\dots G_T(Q_n), \end{aligned}$$

where we have used Lemma 6.3 in the last equality. □

Lemma 6.5. *There is a commutative diagram of morphisms*

$$\begin{array}{ccccc} E^n & \xrightarrow{h_E\times h_E^\vee} & \mathbb{P}^{n-1}\times(\mathbb{P}^{n-1})^\vee & \xrightarrow{\text{Segre}} & \mathbb{P}(\mathrm{Mat}_n)\\ \downarrow{\scriptstyle \prod g_E} & & & & \| \\ \mathbb{P}(R) & \xrightarrow[\varphi_1]{\sim} & \mathbb{P}(A_1) & \xrightarrow[\tau_1]{\sim} & \mathbb{P}(\mathrm{Mat}_n) \end{array}$$

where $(\prod g_E)(Q_1,\dots,Q_n)=\prod_{i=1}^n g_E(Q_i)$.

Proof. From the definitions we have

$$\tau_1\circ\varphi_1\circ(\prod g_E)(Q_1,\dots,Q_n)=\sum_T G_T(Q_1)\dots G_T(Q_n)M_T.$$

So the commutativity is already clear from Lemma 6.4.

It only remains to check that $\prod g_E$ is a morphism. To do this we write it as a composite

$$E^n \xrightarrow{g_E^n} \mathbb{P}(R)^n \overset{\Pi}{\dashrightarrow} \mathbb{P}(R)$$

where the second map is induced by multiplication in R. We check that the image of the first map is contained in the domain of definition of the second.

If $Q\in E(\bar K)\setminus E[n](\bar K)$, then $g_E(Q)$ is the class of $T\mapsto G_T(Q)$, whereas if $Q\in E[n](\bar K)$, then $g_E(Q)$ is the class of $T\mapsto \mathrm{res}_Q(G_T)$, where the residue is taken with respect to a local parameter at Q. (The choice of local parameter does not matter.)

Now suppose $Q_1,\dots,Q_n\in E(\bar K)$ and $\prod_{i=1}^n g_E(Q_i)$ is undefined as an element of $\mathbb{P}(R)$. Then for each $T\neq\mathcal{O}$ there exists $1\le i\le n$ such that $G_T(Q_i)=0$, and hence $nQ_i=T$. But there are n^2-1 such choices of T and only n choices of i. So this is impossible. It follows that $\prod g_E$ is a morphism as claimed. □

To complete the proof of Theorem 6.2, and hence of Theorem 6.1, we put $Q_1 = Q$ and $Q_2 = \ldots = Q_n = \mathcal{O}$ in Lemma 6.5. Notice that $h_E(Q, \mathcal{O}, \ldots, \mathcal{O}) = f_E(Q)$ and $h_E^\vee(Q, \mathcal{O}, \ldots, \mathcal{O}) = f_E^\vee(Q)$. Also, with the G_T's scaled as in Proposition 3.1(iii), $g_E(\mathcal{O})$ is the class of $\sum_{T \neq \mathcal{O}} \delta_T$. So for $Q \in E(\bar{K}) \setminus E[n](\bar{K})$ we obtain

$$\begin{aligned}
\lambda_E(Q) &= \text{Segre} \circ (f_E \times f_E^\vee)(Q) \\
&= \text{Segre} \circ (h_E \times h_E^\vee)(Q, \mathcal{O}, \ldots, \mathcal{O}) \\
&= \tau_1 \circ \varphi_1(g_E(\mathcal{O})^{n-1} g_E(Q)) \\
&= \sum_{T \neq \mathcal{O}} G_T(Q) M_T
\end{aligned}$$

7. The Segre Factorisation for C

Let A be a central simple algebra over K of dimension n^2. Let S and $S^\vee$ be the Brauer-Severi varieties given by the minimal right and left ideals of A, respectively (see [10, p. 160]). There is a natural map $\text{Segre} : S \times S^\vee \to \mathbb{P}(A)$ given by intersecting ideals. We say an element $a \in A$ has rank r if the map $x \mapsto ax$ is an endomorphism of A (as a K-vector space) of rank rn.

Lemma 7.1. *The* Segre *map $S \times S^\vee \to \mathbb{P}(A)$ is an embedding, with image the locus of rank 1 elements in $\mathbb{P}(A)$.*

Proof. If $A \cong \text{Mat}_n(K)$ then $S \cong \mathbb{P}^{n-1}$ and the Segre map reduces to that studied in Section 6. The description of the image is no more than the observation that a (non-zero) matrix has rank 1 if and only if it can be written as a column vector times a row vector. In general we use that there is an isomorphism of $\bar{K}$-algebras $A \otimes_K \bar{K} \cong \text{Mat}_n(\bar{K})$.

The Segre map is an embedding since, on the rank 1 locus in $\mathbb{P}(A)$, an inverse is given by sending the class of $a \in A$ to the pair of ideals (aA, Aa). □

From now on, we call the Segre map the (generalised) Segre embedding. We write 1_A for the multiplicative identity of A, and $\text{Trd} : A \to K$ for the reduced trace. There is a decomposition of K-vector spaces $A = \langle 1_A \rangle \oplus \{\text{Trd} = 0\}$. As in Section 6 we write proj for projection onto the second factor.

The subgroup $H \subset (R \otimes_K R)^\times$ was defined in Definition 3.4.

Theorem 7.2. *Let $\rho \in H$, and let $\pi : C \to E$ be the corresponding n-covering. Let S and $S^\vee$ be the Brauer-Severi varieties given by the*

minimal right and left ideals in $\mathbb{P}(A_\rho)$. Then there is a morphism $f_C : C \to S$ with dual $f_C^\vee : C \to S^\vee$ such that

(i) *the following diagram commutes:*

$$\begin{array}{ccccc} C & \xrightarrow{f_C \times f_C^\vee} & S \times S^\vee & \xrightarrow{\text{Segre}} & \mathbb{P}(A_\rho) \\ \downarrow{\scriptstyle g_C} & & & & \uparrow{\scriptstyle \text{proj}} \\ \mathbb{P}(R) & & \xrightarrow[\varphi_\rho]{\sim} & & \mathbb{P}(A_\rho) \end{array}$$

(ii) *the Brauer-Severi diagram $[C \to S]$ and the class of ρ in H correspond to the same element of $H^1(K, E[n])$.*

The theorem is proved by combining Theorem 6.1 with the next lemma. First we recall how the element $\rho \in H$ and n-covering $\pi : C \to E$ are related. In Section 3 we fixed an element $\gamma \in \bar{R}^\times$ with $\rho = \partial\gamma$ and defined a cocycle $\xi \in H^1(K, E[n])$ via $w(\xi_\sigma) = \sigma(\gamma)/\gamma$ for all $\sigma \in G_K$. Then we let $\pi : C \to E$ be the ξ-twist of the trivial n-covering. Thus there is an isomorphism $\phi : C \to E$ defined over $\bar{K}$ with $\pi = [n] \circ \phi$ and $\sigma(\phi) \circ \phi^{-1} = \tau_{\xi_\sigma}$ for all $\sigma \in G_K$.

Lemma 7.3. *There is an isomorphism of $\bar{K}$-algebras $\beta : A_\rho \otimes_K \bar{K} \to A_1 \otimes_K \bar{K}$ making the following diagram commute.*

$$\begin{array}{ccccccccc} C & \xrightarrow{g_C} & \mathbb{P}(R) & \xrightarrow[\varphi_\rho]{\sim} & \mathbb{P}(A_\rho) & \overset{\text{proj}}{\dashrightarrow} & \mathbb{P}(A_\rho) & & \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \cdot\gamma} & & \downarrow{\scriptstyle \beta} & \searrow^{\tau_1 \circ \beta} & & \searrow^{\tau_1 \circ \beta} & \\ E & \xrightarrow{g_E} & \mathbb{P}(R) & \xrightarrow[\varphi_1]{\sim} & \mathbb{P}(A_1) & \xrightarrow{\tau_1} & \mathbb{P}(\mathrm{Mat}_n) & \overset{\text{proj}}{\dashrightarrow} & \mathbb{P}(\mathrm{Mat}_n) \end{array} \tag{9}$$

Proof. The first square commutes by Proposition 3.5(v). We define $\beta : A_\rho \otimes_K \bar{K} \to A_1 \otimes_K \bar{K}$ to make the second square commute. It is an isomorphism of $\bar{K}$-algebras by [3, Lemma 4.6]. We recall from Proposition 5.3 that τ_1 is an isomorphism of K-algebras. Finally, since proj is defined purely in terms of the algebra structure, it commutes with the algebra isomorphism $\tau_1 \circ \beta$. □

Theorem 6.1 identifies the composite of the second row of (9) as λ_E, where we recall

$$\lambda_E : E \xrightarrow{f_E \times f_E^\vee} \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee \xrightarrow{\text{Segre}} \mathbb{P}(\mathrm{Mat}_n).$$

Since λ_E factors via the Segre embedding, its image belongs to the rank 1 locus of $\mathbb{P}(\mathrm{Mat}_n)$. Let $\lambda_C = \text{proj} \circ \varphi_\rho \circ g_C$ be the composite

of the first row of (9). Recalling that $\tau_1 \circ \beta$ is an isomorphism of $\bar{K}$-algebras, it follows that λ_C has image belonging to the rank 1 locus of $\mathbb{P}(A_\rho)$. By Lemma 7.1 it therefore factors via the Segre embedding.

In other words, there are morphisms $f_C : C \to S$ and $f_C^\vee : C \to S^\vee$ making the diagram in the first part of Theorem 7.2 commute. It remains to show that $[C \to S]$ is a Brauer-Severi diagram, that $f_C^\vee$ is dual to f_C and that $[C \to S]$ and ρ correspond to the same element of $H^1(K, E[n])$.

The isomorphism of $\bar{K}$-algebras $\tau_1 \circ \beta : A_\rho \otimes_K \bar{K} \to \mathrm{Mat}_n(\bar{K})$ induces isomorphisms $\psi : S \to \mathbb{P}^{n-1}$ and $\psi^\vee : S^\vee \to (\mathbb{P}^{n-1})^\vee$ defined over $\bar{K}$ making the following diagram commute.

$$\begin{array}{ccccc} C & \xrightarrow{f_C \times f_C^\vee} & S \times S^\vee & \xrightarrow{\text{Segre}} & \mathbb{P}(A_\rho) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi \times \psi^\vee} & & \downarrow{\scriptstyle \tau_1 \circ \beta} \\ E & \xrightarrow{f_E \times f_E^\vee} & \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee & \xrightarrow{\text{Segre}} & \mathbb{P}(\mathrm{Mat}_n) \end{array}$$

This shows that via (ϕ, ψ), the morphism $f_C : C \to S$ is isomorphic over $\bar{K}$ to $f_E : E \to \mathbb{P}^{n-1}$. Hence $[C \to S]$ is a Brauer-Severi diagram. Since $\sigma(\phi) \circ \phi^{-1}$ is translation by ξ_σ this diagram is the ξ-twist of $[E \to \mathbb{P}^{n-1}]$, and therefore the Brauer-Severi diagram corresponding to ρ. At the same time, we see that $f_C^\vee$ is dual to f_C (since $f_E^\vee$ is dual to f_E). This completes the proof of Theorem 7.2.

8. Finding Equations for C in $\mathbb{P}^{n-1}$

We continue to represent elements of $H^1(K, E[n])$ by elements $\rho \in H$, where the subgroup $H \subset (R \otimes_K R)^\times$ was defined in Section 3. The obstruction algebra A_ρ was introduced in Section 4. If ρ represents an element of $H^1(K, E[n])$ with trivial obstruction, then we make use of an explicit trivialisation isomorphism of K-algebras $\tau_\rho : A_\rho \to \mathrm{Mat}_n(K)$.

Theorem 8.1. *Let $\rho \in H$, and let $\pi : C \to E$ be the corresponding n-covering. Suppose given an isomorphism of K-algebras $\tau_\rho : A_\rho \to \mathrm{Mat}_n(K)$. Then there is a morphism $f'_C : C \to \mathbb{P}^{n-1}$ with dual ${f'_C}^\vee$ such that*

(i) *the following diagram commutes:*

$$\begin{array}{ccccc} C & \xrightarrow{f'_C \times {f'_C}^\vee} & \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee & \xrightarrow{\text{Segre}} & \mathbb{P}(\mathrm{Mat}_n) \\ \downarrow{\scriptstyle g_C} & & & & \uparrow{\scriptstyle \text{proj}} \\ \mathbb{P}(R) & \xrightarrow[\varphi_\rho]{\sim} & \mathbb{P}(A_\rho) & \xrightarrow[\tau_\rho]{\sim} & \mathbb{P}(\mathrm{Mat}_n) \end{array}$$

(ii) *the Brauer-Severi diagram* $[C \to \mathbb{P}^{n-1}]$ *and the class of* ρ *in* H *correspond to the same element of* $H^1(K, E[n])$.

Proof. Let S and $S^\vee$ be the Brauer-Severi varieties given by the minimal right and left ideals in $\mathbb{P}(A_\rho)$. The isomorphism τ_ρ induces K-isomorphisms $\psi' : S \to \mathbb{P}^{n-1}$ and $\psi'^\vee : S^\vee \to (\mathbb{P}^{n-1})^\vee$. We modify the maps f_C and $f_C^\vee$ of Theorem 7.2 to give maps f'_C and ${f'_C}^\vee$ making the following diagram commute.

$$\begin{array}{ccccc} C & \xrightarrow{f'_C \times {f'_C}^\vee} & \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee & \xrightarrow{\text{Segre}} & \mathbb{P}(\mathrm{Mat}_n) \\ \| & & \uparrow{\scriptstyle \psi' \times \psi'^\vee} & & \uparrow{\scriptstyle \tau_\rho} \\ C & \xrightarrow{f_C \times f_C^\vee} & S \times S^\vee & \xrightarrow{\text{Segre}} & \mathbb{P}(A_\rho) \end{array}$$

Since proj is defined purely in terms of the algebra structure, it commutes with the algebra isomorphism τ_ρ. The theorem now follows by combining the above diagram with that in Theorem 7.2. □

In Section 3 we explained how to write down equations for C as a curve of degree n^2 in $\mathbb{P}(R) \cong \mathbb{P}^{n^2-1}$. Theorem 8.1 now tells us how to convert these to equations for C as a curve of degree n in $\mathbb{P}^{n-1}$. First we use τ_ρ to get equations for C in $\mathbb{P}(\mathrm{Mat}_n)$. Then we project onto the trace zero matrices. Next we write $x_{11}, x_{12}, \ldots, x_{nn}$ for our coordinate functions on $\mathbb{P}(\mathrm{Mat}_n)$ and substitute $x_{ij} = x_i y_j$, where the x_i and y_j are new indeterminates ($2n$ in total). This corresponds to pulling the image of C in $\mathbb{P}(\mathrm{Mat}_n)$ back under the Segre map. To project to the first factor $\mathbb{P}^{n-1}$, we eliminate the y_j. We are left with equations in the x_i, and these define the image of $f'_C : C \to \mathbb{P}^{n-1}$. We will describe in [4] how this computation can be reduced to linear algebra for any specific value of n.

For aesthetic as well as practical reasons, it is desirable to find a change of coordinates on $\mathbb{P}^{n-1}$ so that the equations for C have small coefficients. The necessary minimisation and reduction procedures will be described in a forthcoming paper [5] for the cases $n = 3$ and $n = 4$.

It is also desirable to have explicit equations for the covering map $\pi : C \to E$. In principle these could be obtained using the methods of Section 3. However in the cases $n = 2, 3, 4$ equations for π are already given by classical formulae, reproduced in [1].

References

[1] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum and A.R. Perlis, Jacobians of genus one curves, *J. Number Theory* 90 (2001), no. 2, 304–315.

[2] J.W.S. Cassels, *Lectures on elliptic curves*, LMS Student Texts 24, Cambridge University Press, Cambridge, 1991.

[3] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, *Explicit n-descent on elliptic curves, I Algebra*, submitted for publication. arXiv: math.NT/0606580

[4] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, *Explicit n-descent on elliptic curves, III Algorithms*, in preparation.

[5] J.E. Cremona, T.A. Fisher and M. Stoll, *Minimisation and reduction for 3- and 4-coverings of elliptic curves*, in preparation.

[6] M. Hindry and J.H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics 201, Springer-Verlag, New York, 2000.

[7] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* 24, 235–265 (1997). The Magma home page is at `http://magma.maths.usyd.edu.au/magma/`

[8] D. Mumford, Varieties defined by quadratic equations, *Questions on Algebraic Varieties* (C.I.M.E., III Ciclo, Varenna, 1969), pp. 29–100, Edizioni Cremonese, Rome, 1970.

[9] C. O'Neil, The period-index obstruction for elliptic curves, *J. Number Theory* 95 (2002), no. 2, 329–339.

[10] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag, New York, 1979.

[11] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1992.

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, UK

E-mail address: John.Cremona@nottingham.ac.uk

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

E-mail address: T.A.Fisher@dpmms.cam.ac.uk

Barnard College, Columbia University, Department of Mathematics, 2990 Broadway MC 4418, New York, NY 10027-6902,USA

E-mail address: oneil@math.columbia.edu

Université de Caen, Campus II - Boulevard Maréchal Juin, BP 5186–14032, Caen, France

E-mail address: Denis.Simon@math.unicaen.fr

School of Engineering and Science, International University Bremen (Jacobs University Bremen as of spring 2007), P.O. Box 750561, 28725 Bremen, Germany

E-mail address: M.Stoll@iu-bremen.de