Ann. Scient. Éc. Norm. Sup.,
4e série, t. 34, 2001, p. 891 à 912.

THE SOLUBILITY OF DIAGONAL CUBIC SURFACES

BY SIR PETER SWINNERTON-DYER

ABSTRACT. – Let F be an algebraic number field not containing the primitive cube roots of unity, and let

$$a_1X_1^3 + a_2X_2^3 = a_3X_3^3 + a_4X_4^3$$

be a diagonal cubic surface defined over F and everywhere locally soluble. Subject to the assumption that the Tate–Šafarevič group of every relevent elliptic curve is finite, the paper shows that under a very weak additional condition the surface contains points defined over F. Some condition (the Brauer–Manin obstruction) is known to be necessary, but the condition imposed in the paper (which is local) is slightly stronger. More remarkable is the condition on F, which seems to be an artefact of the proof and not intrinsic to the problem.

RÉSUMÉ. – Soit F un corps de nombres qui ne contient pas les racines primitives cubiques de l'unité. Considérons une surface cubique diagonale

$$a_1X_1^3 + a_2X_2^3 = a_3X_3^3 + a_4X_4^3$$

définie sur F et possédant des points rationnels sur tous les complétés de F. En admettant la finitude des groupes de Tate–Šafarevič de certaines courbes elliptiques, et en faisant une hypothèse assez faible sur les coefficients, on montre que la surface possède un point rationnel sur F. La condition sur les coefficients est un peu plus forte que la condition de Brauer–Manin. L'hypothèse sur le corps F lui-même est plus étonnante ; elle est due à la méthode utilisée et ne doit pas être inhérente au problème.

1. Introduction

Within the algebraic closure $\bar{\mathbf{Q}}$, let ω be a fixed primitive cube root of unity and k_0 an algebraic number field not containing ω. We shall be concerned with the solubility over k_0 of diagonal cubic surfaces

$$V\colon\ a_1X_1^3 + a_2X_2^3 = a_3X_3^3 + a_4X_4^3 \tag{1}$$

where $a_1a_2a_3a_4 \neq 0$. Without loss of generality we can assume that the a_i are integers of k_0. The condition that k_0 does not contain ω may appear perverse and unnatural, but it seems essential for the approach used here. It does cover the important case $k_0 = \mathbf{Q}$, but I do not see how to treat this case without treating at the same time a somewhat more general one. My approach is to construct a certain quadratic extension k/k_0, where k also does not contain ω, and to prove the solubility of (1) over k; as is well known, solubility over k_0 follows immediately. The motive for this is that we can impose additional conditions on k without putting corresponding constraints

on k_0. The construction of k/k_0 is given in Theorem 3 in §5, and k_0 will not appear again (after the end of the Introduction) until then.

Of the previous papers about Eq. (1), the most relevent are [5] and [8]; summaries of the results of [5], with a few more comments, can be found in [4] and [9], and [8] contains conditional proofs of the solubility of (1) in some special cases. It was shown by Cassels and Guy [3] that the Hasse principle does not hold for diagonal cubic surfaces. However, there is overwhelming numerical evidence in [5] that for Eq. (1) defined over $\mathbf{Q}$ the only obstruction to the Hasse principle is the Brauer–Manin obstruction.

A number of recent papers of which I have been author or co-author have studied rational points on certain types of surface by treating the surface as a pencil of curves of genus 1. These include [1,6] and [12]. The results have depended on two major conjectures: Schinzel's Hypothesis and the finiteness of the Tate–Šafarevič group for all relevent elliptic curves. The second of these is essential in this paper also; the elliptic curves for which we need it are those of the form $X^3 + Y^3 = AZ^3$ defined over certain quadratic extensions of k_0, where the identity under the group law is the point $O = (1, -1, 0)$. But we have avoided the use of Schinzel's Hypothesis by means of a device which in this context is due to Heath-Brown [8]. Instead of treating (1) as a pencil of curves of genus 1 by writing for example $X_3/X_4 = \lambda/\mu$, we look for solutions of the pair of equations

$$a_1X_1^3 + a_2X_2^3 = BX_0^3, \qquad a_3X_3^3 + a_4X_4^3 = BX_0^3 \tag{2}$$

for some suitably chosen B. The advantage of this method is that by using Dirichlet's theorem on primes in arithmetic progression we can arrange the prime factorization of B to suit our convenience; by contrast, any argument which invokes Schinzel's Hypothesis requires one to cope with what I have elsewhere called the Schinzel primes. (It is true that Dirichlet's theorem can be regarded as a special case of Schinzel's Hypothesis, but its use does not involve anything analogous to the Schinzel primes.) The disadvantage of the present methods is that we have to coordinate the descents on two elliptic curves; and to make the method work it appears necessary to impose on the surface V given by (1) additional conditions which do not always hold even when the Eq. (1) is soluble. For this and other reasons, it will be clear that the approach in this paper is not the right one; but as yet the right one is not known. In this paper the situation is made somewhat worse because, in the interests of simplicity, I have chosen not to make full use of the primes of k_0 which divide 3; but even if I had used them I could not have obtained the whole truth. Even if stronger results could be obtained by means of second descents, using the methodology of Cassels [2], such an approach appears incapable of proving the conjecture that for surfaces (1) the Brauer–Manin obstruction is the only obstruction to the Hasse principle. Indeed, in the present context there are two ways in which the Brauer–Manin obstruction on V can vanish. Let $\mathcal{A}$ be the relevent Azumaya algebra, as described for example in [5]. Either there is a place v such that $\mathrm{inv}_v\mathcal{A}(P_v)$ is not constant as P_v runs through $V(k_v)$, or each $\mathrm{inv}_v\mathcal{A}(P_v)$ is constant but the sum of these values over all v vanishes. One might hope to improve the approach in this paper so as to prove solubility of (1) in the first case, subject always to the condition that ω is not in k_0; but the second case appears to require quite different methods. In consequence, though this paper can be regarded as modelled on the earlier parts of [6], there is in the main theorems no mention of the Brauer–Manin obstruction nor indeed of any non-local obstruction.

In the course of this paper, we repeatedly use the following version of Dirichlet's theorem on primes in an arithmetic progression.

DIRICHLET'S THEOREM. – *Let L be an algebraic number field and $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ distinct primes of L. For $i = 1, \dots, r$ let n_i be a positive integer and α_i an element of $\mathfrak{o}_{\mathfrak{p}_i}^*$; and let $\mathfrak{a}$ be a nonzero*

ideal of L whose prime factorization does not involve any of the $\mathfrak{p}_i$. Then there is an element β of L such that $\beta \equiv \alpha_i \bmod \mathfrak{p}_i^{n_i}$ for each i and $(\beta) = \mathfrak{a}\mathfrak{p}$ for some prime ideal $\mathfrak{p}$.

To prove this requires only minor modifications of the standard analytic proof of Dirichlet's theorem for an algebraic number field in its customary form. Alternatively, it follows easily from Class Field Theory; see for example [7], §8, Satz 13.

With minor exceptions, in this paper $K = k(\omega)$ where k is an algebraic number field not containing ω, and σ is the nontrivial automorphism of K/k. If $\mathfrak{P}$ is a prime in K, then Π will always be a uniformizing variable for $\mathfrak{P}$. The ring of integers of K will be denoted by $\mathfrak{O}$ and that of k by $\mathfrak{o}$. Suppose that ξ is an element of some vector space over $\mathbf{F}_3$ associated with $\bigoplus_{\mathfrak{P}\in\mathcal{S}} K_{\mathfrak{P}}^*$ where $\mathcal{S}$ is a finite set of places of K. We shall write $\mathfrak{P}_0^{\nu} \| \xi$ for ν in $\mathbf{Z}/(3)$ if every representative $x = \sum x_{\mathfrak{P}}$ of ξ satisfies $\mathfrak{P}_0^n \| x_{\mathfrak{P}_0}$ where ν is the image of n in $\mathbf{Z}/(3)$. In particular we shall say that ξ is a unit at $\mathfrak{P}_0$ if $\nu = 0$ and a non-unit at $\mathfrak{P}_0$ otherwise. There are similar definitions for k.

Let $\mathcal{S}_0$ be a finite set of places of K which contains the archimedean places, the primes dividing 3, and a set of generators for the ideal class group of K; and let $\mathcal{S}_1$ be a finite set of places of K which contains $\mathcal{S}_0$ and all the primes which divide $a_1a_2a_3a_4$. We assume that $\mathcal{S}_0$ and $\mathcal{S}_1$ are chosen to be stable under σ. The sets $\mathcal{S}$ and $\mathcal{S}_+$ will always be finite sets of places of K, stable under σ and satisfying $\mathcal{S}_+ \supset \mathcal{S} \supset \mathcal{S}_0$. The letter Σ with any affix will denote the set of places of k lying under a place of the set $\mathcal{S}$ with the corresponding affix. Note that Σ_0 already includes all places which ramify in K/k. We retain all this notation throughout the paper.

In formulating a solubility theorem for (1), we may clearly assume that none of the a_i/a_j is in k^{*3}; for otherwise solubility is trivial. Moreover it has long been known (Selmer [11]) that if for example a_1a_2/a_3a_4 is in k^{*3} then (1) obeys the Hasse principle. Hence it costs us nothing to assume that none of the expressions like a_1a_2/a_3a_4 is in k^{*3}. These restrictions, which are equivalent to the corresponding ones over k_0, are worthwhile because they eliminate a number of special cases in the arguments which follow.

Condition 1. – Each of the fields like $K(\sqrt[3]{a_1/a_2})$ and $K(\sqrt[3]{a_1a_2/a_3a_4})$ is an extension of degree 3 over $K = k(\omega)$.

Subject to all this, the strongest result which I have been able to obtain by means of first descents alone is that stated in Theorem 3; and Theorem 1 summarizes the consequences of Theorem 3 if we make no use of the primes which divide 3. The proof of Theorem 1, together with a more elementary but less succinct version of the criterion in (iii), can be found in §6.

THEOREM 1. – *Let k_0 be an algebraic number field not containing the primitive cube roots of unity. Assume that the Tate–Šafarevič group of every elliptic curve* (4) *over any quadratic extension of k_0 is finite. If Eq.* (1) *is everywhere locally soluble, then each of the following three criteria is sufficient for its solubility in k_0.*

(i) *There exist primes $\mathfrak{p}_1, \mathfrak{p}_3$ of k_0 not dividing 3 such that a_1 is a non-unit at $\mathfrak{p}_1$ and a_3 is a non-unit at $\mathfrak{p}_3$, but for $j = 1$ or 3 the three a_i with $i \neq j$ are units at $\mathfrak{p}_j$.*

(ii) *There is a prime $\mathfrak{p}$ of k_0 not dividing 3 such that a_1 is a non-unit at $\mathfrak{p}$ but the other a_i are units there; and a_2, a_3, a_4 are not all in the same coset of $(k_0)_{\mathfrak{p}}^{*3}$.*

(iii) *There is a prime $\mathfrak{p}$ of k_0 not dividing 3 such that exactly two of the a_i are units at $\mathfrak{p}$, and* (1) *is not birationally equivalent to a plane over $(k_0)_{\mathfrak{p}}$.*

The obstructions in this theorem and the Brauer–Manin obstruction appear to be related as follows. The arguments in §5 of [5], generalized to the present context, show that under each of the criteria above there is a prime $\mathfrak{p}$ of bad reduction for V such that V is not birationally equivalent to a plane over $(k_0)_{\mathfrak{p}}$. (Indeed, criterion (i) demands two such primes.) Provided $\mathfrak{p} \nmid 3$ this implies that there is no Brauer–Manin obstruction for our surface – for if $\mathcal{A}$ is the relevent

Azumaya algebra, $\mathrm{inv}_{\mathfrak{p}}\mathcal{A}(P_{\mathfrak{p}})$ is not constant as $P_{\mathfrak{p}}$ runs through the $\mathfrak{p}$-adic points of V. One would hope that this holds even if $\mathfrak{p}|3$.

There has also been some recent interest in the solubility of diagonal cubic threefolds. The idea of proving a solubility theorem for a variety by considering suitably chosen sections is an old one; for it in this context see [5], §9. Subject always to the finiteness of the relevent Tate–Šafarevič groups, our methods are adequate to prove that the Hasse principle holds in this case.

THEOREM 2. – *Assume that k_0 does not contain the primitive cube roots of unity and that the Tate–Šafarevič group of every elliptic curve* (4) *over any quadratic extension of k_0 is finite. If $b_1, \dots, b_5$ are nonzero elements of k_0 such that*

$$b_1X_1^3 + b_2X_2^3 + b_3X_3^3 + b_4X_4^3 + b_5X_5^3 = 0 \tag{3}$$

is everywhere locally soluble, then it is soluble in k_0.

The proof of this theorem can also be found in §6.

I am indebted to Jean-Louis Colliot-Thélène and the referee for a number of valuable comments on earlier drafts, and to Tom Fisher and Alexei Skorobogatov for permission to reproduce Lemmas 5 and 6.

2. First descent on $X^3 + Y^3 = AZ^3$

Let A be an element of k^* which without loss of generality we can assume to be in $\mathfrak{o}$; for simplicity we shall also assume that A is not a cube. We write ρ for the isogeny whose kernel consists of the 3-division points with $Z = 0$. The curve E given by (4) admits complex multiplication, so that $\mathrm{End}_K(E) = \mathbf{Z}[\omega]$; we may suppose that ω acts on E by $(X, Y, Z) \mapsto (X, Y, \omega Z)$. Thus the action of ρ is given by

$$(X, Y, Z) \mapsto \big(\omega X^3 - \omega^2 Y^3, \omega Y^3 - \omega^2 X^3, \big(\omega - \omega^2\big)XYZ\big).$$

If P is (X, Y, Z) then $-P$ is (Y, X, Z); thus also $\sigma(\rho(P)) = -\rho(\sigma(P))$.

The most naïve form of the ρ-descent, also called the first descent in the older literature, operates over K; it replaces the elliptic curve

$$E\colon\ X^3 + Y^3 = AZ^3 \tag{4}$$

by the equations $Z = Z_1Z_2Z_3$ and

$$\omega X + \omega^2 Y = m_1 Z_1^3, \qquad \omega^2 X + \omega Y = m_2 Z_2^3, \qquad X + Y = AZ_3^3/m_1m_2 \tag{5}$$

for some m_1, m_2. If we write

$$X = \xi/m_1m_2, \qquad Y = \eta/m_1m_2, \qquad m = m_1/m_2,$$
$$Z_1 = \zeta_1/m_1, \qquad Z_2 = \zeta_2/m_2, \qquad Z_3 = -\zeta_3,$$

the Eqs. (5) become

$$\omega\xi + \omega^2\eta = m^{-1}\zeta_1^3, \qquad \omega^2\xi + \omega\eta = m\zeta_2^3, \qquad \xi + \eta = -A\zeta_3^3,$$

a system which is equivalent to

$$m^{-1}\zeta_1^3 + m\zeta_2^3 = A\zeta_3^3. \tag{6}$$

Here we should regard m as an element of K^*/K^{*3}. Thus in particular over K the Jacobians of the two curves (2) are

$$X^3+Y^3=Ba_1a_2Z^3, \qquad X^3+Y^3=Ba_3a_4Z^3. \tag{7}$$

The curves (6) are called ρ-coverings of (4); those which are everywhere locally soluble are by definition the elements of the ρ-Selmer group, which is canonically isomorphic through m to a subgroup of K^*/K^{*3}. The ρ-Selmer group contains A because the curve (6) with $m=A$ is soluble in K.

Throughout this section, $\mathcal{S}$ will be a finite set of places of K containing $\mathcal{S}_0$ and all the primes which divide A. The curves (6) defined over K and soluble in K_v for every v outside $\mathcal{S}$ correspond to the m which are units outside $\mathcal{S}$; so they are indexed by the elements of $X_{\mathcal{S}}=\mathfrak{O}_{\mathcal{S}}^*/\mathfrak{O}_{\mathcal{S}}^{*3}$, where $\mathfrak{O}_{\mathcal{S}}^*$ consists of the elements of K which are units outside $\mathcal{S}$. We can regard $X_{\mathcal{S}}$ as a finite-dimensional $\mathbf{F}_3$-vector space. Those curves which are also soluble in K_v for every v in $\mathcal{S}$ determine a subspace of $X_{\mathcal{S}}$. Hence the conditions for the solubility of (6) in the K_v with v in $\mathcal{S}$ can be described by a finite set of homomorphisms $X_{\mathcal{S}}\to\mathbf{F}_3$, which can be regarded as generators of an $\mathbf{F}_3$-vector space V. The left kernel of the induced map $\psi: X_{\mathcal{S}}\times V\to\mathbf{F}_3$ is precisely the ρ-Selmer group of E. Calculation shows that $X_{\mathcal{S}}$ and V have the same dimension. It is therefore tempting to hope that there is a natural isomorphism between $X_{\mathcal{S}}$ and V, and that it makes ψ either symmetric or antisymmetric. This is not true; but there is indeed an interesting symmetry property, though a less straightforward one, and the main purpose of this section is to display it. A similar symmetry statement, though in a simpler context, has already appeared in [6]; there, as here, it plays a crucial role.

For every finite set $\mathcal{S}$ of places of K, of order n and containing $\mathcal{S}_0$, write

$$X_{\mathcal{S}}=\mathfrak{O}_{\mathcal{S}}^*/\mathfrak{O}_{\mathcal{S}}^{*3}, \qquad Y_v=K_v^*/K_v^{*3}, \qquad Y_{\mathcal{S}}=\bigoplus_{v\in\mathcal{S}}Y_v. \tag{8}$$

Since K contains the cube roots of unity, the $\mathbf{F}_3$-vector space $X_{\mathcal{S}}$ has dimension n by Dirichlet's unit theorem. $Y_{\mathcal{S}}$ has dimension $2n$ by the product formula, since K_v^*/K_v^{*3} contains $9/|3|_v$ elements and $\mathcal{S}$ contains every v with $|3|_v\neq 1$. Moreover Y_v is trivial if v is archimedean. Here as in Proposition 1.1.1 of [6] the map $X_{\mathcal{S}}\to Y_{\mathcal{S}}$ is injective, because $\mathcal{S}$ contains a set of generators for the ideal class group of K. There is a non-degenerate alternating bilinear form e_v on Y_v given by the Hilbert symbol, and thus a non-degenerate alternating bilinear form $e_{\mathcal{S}}=\sum_{\mathcal{S}}e_v$ on $Y_{\mathcal{S}}$. (We write the Hilbert symbol additively, to accord with the argument in §5. Consequently the symbol depends on the choice of ω; compare the discussion around Lemma 7 of [5].) By the Hilbert product formula and a comparison of dimensions, $X_{\mathcal{S}}$ is maximal isotropic in $Y_{\mathcal{S}}$. For any place v of K, let T_v be the image of $\mathfrak{O}_v^*/\mathfrak{O}_v^{*3}$ in Y_v, where $\mathfrak{O}_v$ is the ring of integers of K_v. Unless v divides 3, T_v is a maximal isotropic subspace of Y_v. The following lemma has been designed for application to the special situation described in Lemma 2; it is stated in greater generality purely in order to simplify the proof. We introduce the following notation, which we shall use repeatedly. Let U be a vector space over a field F with $\operatorname{char}F\neq 2$, and let $\sigma: U\to U$ be an automorphism of order 2; then U is the direct sum of the subspace U^+ of elements fixed by σ and the subspace U^- of elements whose sign is reversed by σ.

LEMMA 1. – *Let $\mathfrak{Y}_i, \sigma\mathfrak{Y}_i$ $(i=1,\dots,n)$ be pairs of finite dimensional vector spaces over a field F with $\operatorname{char}F\neq 2$, where σ is an isomorphism $\mathfrak{Y}_i\to\sigma\mathfrak{Y}_i$ for each i and is such that σ^2 is the identity. Suppose that each $\mathfrak{Y}_i$ is equipped with a non-degenerate alternating bilinear form*

(x, y), and let each $\sigma\mathfrak{Y}_i$ be equipped with the bilinear form defined by

$$(\sigma x, \sigma y) = -(x, y). \tag{9}$$

Write $\mathfrak{Y} = \bigoplus_i (\mathfrak{Y}_i \oplus \sigma\mathfrak{Y}_i)$, equipped with the sum of these forms. Let $\mathfrak{X}$ be maximal isotropic in $\mathfrak{Y}$ and mapped to itself by σ. Then there exist maximal isotropic subspaces $\mathfrak{Z}_i \subset (\mathfrak{Y}_i \oplus \sigma\mathfrak{Y}_i)$ such that σ maps each $\mathfrak{Z}_i$ to itself and $\mathfrak{Y} = \mathfrak{X} \oplus \mathfrak{Z}$ where $\mathfrak{Z} = \bigoplus_i \mathfrak{Z}_i$. Moreover, given any $\mathfrak{W} = \bigoplus_i (\mathfrak{W}_i \oplus \sigma\mathfrak{W}_i)$ with each $\mathfrak{W}_i$ maximal isotropic in $\mathfrak{Y}_i$, the $\mathfrak{Z}_i$ can be chosen so that

$$\dim(\mathfrak{W} \cap \mathfrak{Z})^+ - \dim(\mathfrak{W} \cap \mathfrak{Z})^- = \tfrac{1}{2}(\dim \mathfrak{X}^- - \dim \mathfrak{X}^+). \tag{10}$$

Proof. – We show first that we can reduce to the special case where every $\mathfrak{Y}_i$ has dimension 2. If some $\dim \mathfrak{Y}_i > 2$ let y_i be a nonzero element of $\mathfrak{W}_i$; because the bilinear form is nondegenerate on $\mathfrak{Y}_i$ we can find v_i in $\mathfrak{Y}_i$ such that $(y_i, v_i) \neq 0$. Here v_i cannot be in $\mathfrak{W}_i$. Now $\mathfrak{Y}_i = \{y_i, v_i\} \oplus \{y_i, v_i\}^\perp$ and one easily checks that this induces an orthogonal decomposition

$$\mathfrak{W}_i = \big(\mathfrak{W}_i \cap \{y_i, v_i\}\big) \oplus \big(\mathfrak{W}_i \cap \{y_i, v_i\}^\perp\big).$$

Thus we have split off from $\mathfrak{Y}_i$ a subspace of dimension 2 which contains a subspace of $\mathfrak{W}_i$ of dimension 1. This only reduces our freedom to choose the $\mathfrak{Z}_i$; so we can assume that every $\mathfrak{Y}_i$ has dimension 2.

We now proceed by induction on n, the case $n = 0$ being trivial. Since $\mathfrak{X}$ is isotropic it cannot contain $\mathfrak{Y}_n$; so there is an element y_n in $\mathfrak{Y}_n$ but not in $\mathfrak{X}$, whence $y_n + \sigma y_n$ and $y_n - \sigma y_n$ cannot both lie in $\mathfrak{X}$. Let y_n, v_n be a base for $\mathfrak{Y}_n$. Since σ maps $\mathfrak{X}$ to itself, we have three possibilities:

(i) The intersection of $\mathfrak{X}$ and the space spanned by $y_n + \sigma y_n$ and $y_n - \sigma y_n$ is trivial; in this case we take $\mathfrak{Z}_n$ to be the latter space.

(ii) If $y_n - \sigma y_n$ is in $\mathfrak{X}$ then $(y_n - \sigma y_n, v_n + \sigma v_n) = 2(y_n, v_n) \neq 0$; thus the only elements of $(\mathfrak{Y}_n \oplus \sigma\mathfrak{Y}_n)^+$ orthogonal to $y_n - \sigma y_n$ are the multiples of $y_n + \sigma y_n$, whence $\mathfrak{X} \cap (\mathfrak{Y}_n \oplus \sigma\mathfrak{Y}_n)^+ = \{0\}$. In this case we take $\mathfrak{Z}_n$ to be $(\mathfrak{Y}_n \oplus \sigma\mathfrak{Y}_n)^+$.

(iii) If $y_n + \sigma y_n$ is in $\mathfrak{X}$ a similar argument holds; in this case we take $\mathfrak{Z}_n$ to be $(\mathfrak{Y}_n \oplus \sigma\mathfrak{Y}_n)^-$.

Now write

$$\mathfrak{Y}^* = (\mathfrak{Y}_1 \oplus \sigma\mathfrak{Y}_1) \oplus \cdots \oplus (\mathfrak{Y}_{n-1} \oplus \sigma\mathfrak{Y}_{n-1}), \qquad \mathfrak{X}^* = \mathfrak{Y}^* \cap (\mathfrak{X} \oplus \mathfrak{Z}_n). \tag{11}$$

If x^* is in $\mathfrak{X}^*$ then $x^* = x + z_n$ for some z_n in $\mathfrak{Z}_n$ and x in $\mathfrak{X}$; so the projection of x to $\mathfrak{Y}_n \oplus \sigma\mathfrak{Y}_n$ is $-z_n$. Since x^* is orthogonal to $\mathfrak{Z}_n$, so is x; and the isotropy of $\mathfrak{X}^*$ follows from that of $\mathfrak{X}$ and $\mathfrak{Z}_n$. Since $\dim \mathfrak{X}^* \geqslant 2n - 2$ by the second equation (11), $\mathfrak{X}^*$ is maximal isotropic in $\mathfrak{Y}^*$. Applying the induction hypothesis to $\mathfrak{X}^*$ and $\mathfrak{Y}_1, \ldots, \mathfrak{Y}_{n-1}$ we can construct $\mathfrak{Z}_i$ maximal isotropic in $\mathfrak{Y}_i \oplus \sigma\mathfrak{Y}_i$ for $i = 1, \ldots, n-1$ and with $\mathfrak{Y}^* = \mathfrak{X}^* \oplus (\mathfrak{Z}_1 \oplus \cdots \oplus \mathfrak{Z}_{n-1})$. But now, using (11) again,

$$(\mathfrak{X} \oplus \mathfrak{Z}_n) \cap (\mathfrak{Z}_1 \oplus \cdots \oplus \mathfrak{Z}_{n-1}) \subset \mathfrak{X}^* \cap (\mathfrak{Z}_1 \oplus \cdots \oplus \mathfrak{Z}_{n-1}) = \{0\}$$

and $\mathfrak{Y} = \mathfrak{X} \oplus \mathfrak{Z}$ follows by dimension count. To prove the final assertion we have to split cases according to the three possibilities above. If (i) holds then the general element of $\mathfrak{Z}_n$ has the form $ay_n + a'\sigma y_n$ with a, a' in F. If y_n is in $\mathfrak{W}_n$ then every such element is in $\mathfrak{W}_n \oplus \sigma\mathfrak{W}_n$, so that $(\mathfrak{W}_n \oplus \sigma\mathfrak{W}_n) \cap \mathfrak{Z}_n = \mathfrak{Z}_n$; if y_n is not in $\mathfrak{W}_n$ then the only element of this form which is in $\mathfrak{W}_n \oplus \sigma\mathfrak{W}_n$ is 0, so that $(\mathfrak{W}_n \oplus \sigma\mathfrak{W}_n) \cap \mathfrak{Z}_n = \{0\}$. If (ii) or (iii) holds then

$$(\mathfrak{W}_n \oplus \sigma\mathfrak{W}_n) \cap \mathfrak{Z}_n = (\mathfrak{W}_n \oplus \sigma\mathfrak{W}_n)^+ \quad \text{or} \quad (\mathfrak{W}_n \oplus \sigma\mathfrak{W}_n)^-$$

respectively. Thus in all cases we have

$$\dim\big((\mathfrak{W}_n \oplus \sigma\mathfrak{W}_n) \cap \mathfrak{Z}_n\big)^+ - \dim\big((\mathfrak{W}_n \oplus \sigma\mathfrak{W}_n) \cap \mathfrak{Z}_n\big)^- = \tfrac{1}{2}(\dim \mathfrak{Z}_n^+ - \dim \mathfrak{Z}_n^-).$$

By induction this gives

$$\dim(\mathfrak{W} \cap \mathfrak{Z})^+ - \dim(\mathfrak{W} \cap \mathfrak{Z})^- = \tfrac{1}{2}(\dim \mathfrak{Z}^+ - \dim \mathfrak{Z}^-).$$

But we have

$$\dim \mathfrak{X}^+ + \dim \mathfrak{Z}^+ = \dim \mathfrak{Y}^+ = \dim \mathfrak{Y}^- = \dim \mathfrak{X}^- + \dim \mathfrak{Z}^-$$

and (10) follows. We note for future reference that also

$$\dim \mathfrak{W}^+ = \dim \oplus \mathfrak{W}_i = \dim \mathfrak{W}^-. \tag{12}$$

The decomposition of the $\mathfrak{Y}_i$ which allows us to assume that each $\dim \mathfrak{Y}_i = 2$ constrains the choice of the $\mathfrak{Z}_i$, so we have only proved (10) for a highly particular choice of the $\mathfrak{Z}_i$; but I believe that (10) does hold for every choice of $\mathfrak{Z}_i$ satisfying the penultimate sentence in the lemma. □

Let W_v be the image of $E(K_v)$ in Y_v under the Kummer map

$$\partial\colon\ P = (X, Y) \mapsto \frac{\omega X + \omega^2 Y}{\omega^2 X + \omega Y}$$

in the notation of (4). Write $W_{\mathcal{S}}$ for the subset $\bigoplus_{\mathcal{S}} W_v$ of $Y_{\mathcal{S}}$. A ρ-covering of E is soluble in K_v if and only if the corresponding element m of K^*/K^{*3} is in W_v. Moreover Tate has shown that W_v is a maximal isotropic subspace of Y_v for the alternating form e_v. (In our case this can be proved along the lines of Lemma 3 of [1]. Tate's result is applicable to any isogeny, but I am not aware of any published proof in this generality; for the special case of multiplication by an element of $\mathbf{Z}$, see [10], p. 56.) These last two properties provide the easiest way to calculate the W_v explicitly. In particular, $W_v = T_v$ unless v is a prime of bad reduction for E. Because the ρ-division points of E are defined over K, they give rise to elements of the ρ-Selmer group; the corresponding elements of ∂E are $1, A$ and A^2. If $\mathfrak{P}$ is a prime of bad reduction for E which does not divide 3, $W_{\mathfrak{P}}$ is generated by A. If $\mathfrak{P}|3$ there seems to be no simple description of $W_{\mathfrak{P}}$; indeed even when $K = \mathbf{Q}(\omega)$ a considerable splitting of cases appears to be needed. A ρ-covering of E is soluble in K_v for all v not in $\mathcal{S}$ if and only if the corresponding element of K^*/K^{*3} is in $X_{\mathcal{S}}$. Hence the ρ-Selmer group of E can be identified with $X_{\mathcal{S}} \cap W_{\mathcal{S}}$; this group is both the left and the right kernel of the bilinear map $X_{\mathcal{S}} \times W_{\mathcal{S}} \to \mathbf{F}_3$ induced by $e_{\mathcal{S}}$.

If $\mathfrak{P}$ is a prime of K we write $\mathcal{P} = \{\mathfrak{P}\}$ or $\mathcal{P} = \{\mathfrak{P}, \sigma\mathfrak{P}\}$ according as $\mathfrak{P}$ is or is not fixed by σ; we write $T_{\mathcal{P}} = T_{\mathfrak{P}}$ in the former case and $T_{\mathcal{P}} = T_{\mathfrak{P}} \oplus T_{\sigma\mathfrak{P}}$ in the latter, and similarly for $W_{\mathcal{P}}, Y_{\mathcal{P}}$ and $Z_{\mathcal{P}}$.

If we ignore the primes dividing 3, the primes in k which split in K/k are those whose absolute norm is congruent to $1 \bmod 3$. These are the primes which lie in a certain group G_0, which is a subgroup of index 2 in the relevent ray class group. Usually G_0 will contain primes in every ideal class, but if K/k is totally unramified there is a subgroup Γ_0 of index 2 in the ideal class group of k such that a prime ideal in k splits in K/k if and only if its class lies in Γ_0. This is the case which primarily concerns us, since any place ramified in K/k must both lie in $\mathcal{S}_0$ and be fixed by σ; and this will usually be ruled out either by the hypotheses of Lemma 2 or by Condition 4 below. Because of this, G_0 will only appear explicitly in the proof of Lemma 2.

LEMMA 2. – *Suppose that no place of $\mathcal{S}_0$ is fixed by σ. Then there are maximal isotropic subspaces $Z_\mathcal{P} \subset Y_\mathcal{P}$ such that $Y_\mathcal{S} = X_\mathcal{S} \oplus (\bigoplus_{\mathcal{P}\in\mathcal{S}} Z_\mathcal{P})$, and σ maps each $Z_\mathcal{P}$ to itself. We can choose $Z_{\mathcal{S}_0}$ in a way that only depends on the classes of $A \bmod K_\mathfrak{P}^{*3}$ for the $\mathfrak{P}$ in $\mathcal{S}_0$; and once $Z_{\mathcal{S}_0}$ has been chosen we can take $Z_\mathcal{S} = Z_{\mathcal{S}_0} \oplus (\bigoplus_{\mathcal{P}\subset\mathcal{S}\setminus\mathcal{S}_0} T_\mathcal{P})$ for each $\mathcal{S} \supset \mathcal{S}_0$. Let N_1, N_2 be such that $\mathcal{S}$ contains $N_1 + N_2$ primes fixed by σ, and that E has good reduction at N_1 of them and bad reduction at the other N_2; then*

$$\dim W_\mathcal{S}^+ - \dim W_\mathcal{S}^- = N_2 - N_1, \tag{13}$$

$$\dim(W_\mathcal{S} \cap Z_\mathcal{S})^+ - \dim(W_\mathcal{S} \cap Z_\mathcal{S})^- = 1 - N_1. \tag{14}$$

Proof. – Consider first the second sentence for the particular case $\mathcal{S} = \mathcal{S}_0$. This is a straightforward transcription of Lemma 1. Let $\mathcal{S}_0^\sharp$ be such that $\mathcal{S}_0$ is the disjoint union of sets $\mathcal{S}_0^\sharp$ and $\sigma\mathcal{S}_0^\sharp$. We apply Lemma 1 to the case when, in our previous notation, the $\mathfrak{Y}_i$ are the $Y_\mathfrak{P}$ with $\mathfrak{P}$ in $\mathcal{S}_0^\sharp$, the $\mathfrak{W}_i$ are the $W_\mathfrak{P}$ for these $\mathfrak{P}$, $\mathfrak{X}$ is $X_{\mathcal{S}_0}$ and the non-degenerate alternating bilinear forms on the $\mathfrak{Y}_i$ are given by the local Hilbert symbol. We ignore the archimedean places, for which $\mathfrak{Y}_v$ is trivial. We need to check (9), but this follows from the definition of the Hilbert symbol; the reason for the sign reversal is that canonically the Hilbert symbol takes its values in $\mu_3 = \{1, \omega, \omega^2\}$, on which σ acts nontrivially. This proves the second sentence in this case.

For general $\mathcal{S}$ we consider the second and third sentences together. We must examine the effect of adjoining to $\mathcal{S}$ finitely many further primes $\mathfrak{P}$, where if $\sigma\mathfrak{P} \neq \mathfrak{P}$ we assume that we adjoin $\mathfrak{P}$ and $\sigma\mathfrak{P}$ together. We do this step by step, so that we have to consider the situation where $\mathcal{S} \supset \mathcal{S}_0$ is a finite set of places mapped to itself by σ and we replace $\mathcal{S}$ by $\mathcal{S}_+ = \mathcal{S} \cup \mathcal{P}$ where $\mathfrak{P}$ is a prime of K not in $\mathcal{S}$. We need to show that in going from $\mathcal{S}$ to $\mathcal{S}_+$ we can leave $Z_\mathcal{S}$ unchanged and choose $Z_\mathcal{P} = T_\mathcal{P}$. Because $\mathcal{S} \supset \mathcal{S}_0$, there is a natural embedding $X_\mathcal{S} \subset X_{\mathcal{S}_+}$ which identifies $X_\mathcal{S}$ with the elements of $X_{\mathcal{S}_+}$ which are trivial at primes of $\mathcal{P}$. Thus

$$X_{\mathcal{S}_+} \cap (Z_\mathcal{S} \oplus T_\mathcal{P}) = X_\mathcal{S} \cap Z_\mathcal{S} = \{0\},$$

and the second and third sentences of the lemma follow immediately. We shall henceforth assume that the $Z_\mathcal{P}$ are chosen in this way.

We turn now to (13). Let $\mathcal{S}^\flat \supset \mathcal{S}_0$ be the subset of $\mathcal{S}$ consisting of those places in $\mathcal{S}$ not fixed by σ; then (13) holds when $\mathcal{S} = \mathcal{S}^\flat$, by (12). Now let $\mathfrak{P}$ be a prime of K fixed by σ, and $\mathfrak{p}$ the prime of k below it; thus all the elements of $\mathfrak{o}_\mathfrak{p}^*$ are $\mathfrak{p}$-adic cubes. If E has good reduction at $\mathfrak{P}$ then σ acts on $T_\mathcal{P} = W_\mathcal{P} = Z_\mathcal{P}$ like -1; thus

$$\dim W_\mathcal{P}^+ = \dim(W_\mathcal{P} \cap Z_\mathcal{P})^+ = 0, \quad \dim W_\mathcal{P}^- = \dim(W_\mathcal{P} \cap Z_\mathcal{P})^- = 1.$$

On the other hand, if E has bad reduction at $\mathfrak{P}$ then $W_\mathcal{P} \cap Z_\mathcal{P} = \{0\}$ and σ acts on $W_\mathcal{P}$ like $+1$, because $W_\mathcal{P}$ is generated by A which is in k. Hence in both cases adjoining $\mathfrak{P}$ does not alter the validity of (13); and we can go from $\mathcal{S}^\flat$ to $\mathcal{S}$ by repeated steps of this kind. A corresponding argument holds for (14), so to complete the proof of the lemma it is enough to prove (14) for the special case $\mathcal{S} = \mathcal{S}^\flat$.

In this case I claim that $X_\mathcal{S}^+$ is $\mathfrak{o}_\Sigma^*/\mathfrak{o}_\Sigma^{*3}$. For let ξ in $\mathfrak{O}_\mathcal{S}^*$ be a representative of an element in $X_\mathcal{S}^+$; then $\xi/\sigma\xi = \eta^3$ for some η in $\mathfrak{O}_\mathcal{S}^*$ and so $(\mathrm{Norm}_{K/k}\eta)^3 = \mathrm{Norm}_{K/k}(\xi/\sigma\xi) = 1$. Since ω is not in k this implies $\mathrm{Norm}_{K/k}\eta = 1$, whence $\eta = \zeta/\sigma\zeta$ for some ζ in K by Hilbert's Theorem 90; so $\alpha = \xi/\zeta^3$ is fixed by σ and therefore lies in k. It is not obvious that ζ can be chosen to be in $\mathfrak{O}_\mathcal{S}^*$; but if ζ is divisible by a prime $\mathfrak{P}$ not in $\mathcal{S}$ it is divisible to the same power by $\sigma\mathfrak{P}$ also, and if $\mathfrak{P} = \sigma\mathfrak{P}$ then $\mathfrak{P}$ is the conorm of a prime $\mathfrak{p}$ in k because K/k is totally unramified. Thus as

ideals we can write $(\zeta) = \mathfrak{a}\mathfrak{B}$ where $\mathfrak{a}$ is an ideal in k none of whose prime factors lies in $\mathcal{S}$ and $\mathfrak{B}$ is an ideal in K whose factorization involves no primes outside $\mathcal{S}$. The ideal $\alpha\mathfrak{a}^3 = \xi\mathfrak{B}^{-3}$ lies in k and has all its prime factors in $\mathcal{S}$; since $\mathcal{S} = \mathcal{S}^\flat$ it must have the form $\mathfrak{B}_0.\sigma\mathfrak{B}_0$ where $\mathfrak{B}_0$ is an ideal of K all of whose prime factors lie in $\mathcal{S}$. This shows that the class of $\mathfrak{a}^3$ is in Γ_0, whence so is the class of $\mathfrak{a}$; hence we can write $\mathfrak{a} = \alpha_1\mathfrak{B}_1.\sigma\mathfrak{B}_1$ where α_1 is in k and all the prime factors of $\mathfrak{B}_1$ lie in $\mathcal{S}$. Here ζ/α_1 is in $X_\mathcal{S}$; so $\xi(\alpha_1/\zeta)^3$ is fixed by σ and represents the same class in $X_\mathcal{S}$ as ξ does. This proves that $X_\mathcal{S}^+$ is indeed $\mathfrak{o}_\Sigma^*/\mathfrak{o}_\Sigma^{*3}$, which is X_Σ for k.

Denote the order of $\mathcal{S} = \mathcal{S}^\flat$ by n; thus by hypothesis the order of $\Sigma = \Sigma^\flat$ is $\frac{1}{2}n$. Because k does not contain the primitive cube roots of unity, Dirichlet's unit theorem now gives

$$\dim X_\mathcal{S}^+ = \dim X_\Sigma = \tfrac{1}{2}n - 1 = \tfrac{1}{2}\dim X_\mathcal{S} - 1$$

and therefore $\dim X_\mathcal{S}^- = \frac{1}{2}\dim X_\mathcal{S} + 1$. Now (14) for the special case $\mathcal{S} = \mathcal{S}^\flat$ follows from (10). □

Now let $t_\mathcal{S} : Y_\mathcal{S} \to X_\mathcal{S}$ be the projection along $Z_\mathcal{S}$ and write

$$X'_\mathcal{S} = X_\mathcal{S} \cap (W_\mathcal{S} + Z_\mathcal{S}), \qquad W'_\mathcal{S} = W_\mathcal{S}/(W_\mathcal{S} \cap Z_\mathcal{S}) = \bigoplus\nolimits_{\mathcal{P}\subset\mathcal{S}} W'_\mathcal{P}$$

where $W'_\mathcal{P} = W_\mathcal{P}/(W_\mathcal{P} \cap Z_\mathcal{P})$. Note that if $\mathfrak{P}$ is not in $\mathcal{S}_0$ the choice of $Z_\mathcal{P}$ enables us to define the power of $\mathfrak{P}$ which divides an element of $W'_\mathfrak{P}$, under the convention in §1. The map $t_\mathcal{S}$ induces an isomorphism

$$\tau_\mathcal{S} : W'_\mathcal{S} \to X'_\mathcal{S}. \tag{15}$$

If w' in $W'_\mathcal{S}$ is represented by $\bigoplus w_\mathcal{P}$ in $W_\mathcal{S}$, it follows from Lemma 2 that $\tau_\mathcal{S} w'/w_\mathcal{P}$, considered as an element of $Y_\mathcal{P}$, is a unit at $\mathcal{P}$ for any $\mathfrak{P}$ outside $\mathcal{S}_0$. (This remark will be used repeatedly in §5.)

The bilinear function $e_\mathcal{S}$ induces a bilinear function

$$e'_\mathcal{S} : X'_\mathcal{S} \times W'_\mathcal{S} \to \mathbf{F}_3$$

because $W_\mathcal{S}$ and $Z_\mathcal{S}$ are both isotropic. We have seen that the ρ-Selmer group of E is $X_\mathcal{S} \cap W_\mathcal{S}$ and is therefore contained in $X'_\mathcal{S}$. Since it is both the left and the right kernel of $X_\mathcal{S} \times W_\mathcal{S} \to \mathbf{F}_3$, it is isomorphic to both the left and the right kernel of $e'_\mathcal{S}$.

LEMMA 3. – *Suppose that $\mathcal{S}$ contains $\mathcal{S}_0$ and all the primes of bad reduction for E, and no place of $\mathcal{S}_0$ is fixed by σ. Then the functions*

$$\Phi_\mathcal{S} : X'_\mathcal{S} \times X'_\mathcal{S} \to \mathbf{F}_3 \quad \textit{and} \quad \Psi_\mathcal{S} : W'_\mathcal{S} \times W'_\mathcal{S} \to \mathbf{F}_3$$

defined respectively by

$$x'_1 \times x'_2 \mapsto e'_\mathcal{S}\big(x'_1, \tau_\mathcal{S}^{-1}(x'_2)\big) \quad \textit{and} \quad w'_1 \times w'_2 \mapsto e'_\mathcal{S}(\tau_\mathcal{S} w'_1, w'_2)$$

are bilinear symmetric, with kernels isomorphic to the ρ-Selmer group of E.

Proof. – We need only prove that the functions are symmetric, and it is enough to do so for $\Phi_\mathcal{S}$. Given elements x'_1, x'_2 in $X'_\mathcal{S}$ choose w_1, w_2 in $W_\mathcal{S}$ so that $t_\mathcal{S} w_1 = x'_1$, $t_\mathcal{S} w_2 = x'_2$. Since $(1 - t_\mathcal{S})w_1$ and $(1 - t_\mathcal{S})w_2$ are in $Z_\mathcal{S}$

$$\begin{aligned}0 &= e_{\mathcal{S}}(w_1,w_2) = e_{\mathcal{S}}\big(t_{\mathcal{S}}w_1+(1-t_{\mathcal{S}})w_1,\, t_{\mathcal{S}}w_2+(1-t_{\mathcal{S}})w_2\big)\\ &= e_{\mathcal{S}}\big(t_{\mathcal{S}}w_1,\,(1-t_{\mathcal{S}})w_2\big)+e_{\mathcal{S}}\big((1-t_{\mathcal{S}})w_1,\,t_{\mathcal{S}}w_2\big)\\ &= e_{\mathcal{S}}(t_{\mathcal{S}}w_1,w_2)+e_{\mathcal{S}}(w_1,t_{\mathcal{S}}w_2) = e'_{\mathcal{S}}(x'_1,w'_2)-e'_{\mathcal{S}}(x'_2,w'_1)\end{aligned}$$

where w'_1, w'_2 are the images of w_1, w_2 in $W'_{\mathcal{S}}$. □

Strictly speaking, our notation for Φ and Ψ should also make explicit which elliptic curve is being considered. Until §5 this will always be obvious; the conventions which we use in §5 are explained there.

It is clear that σ maps X' and W' to themselves, and commutes with t and τ; in particular τ induces isomorphisms $W'^{+} \to X'^{+}$ and $W'^{-} \to X'^{-}$. Since the Hilbert symbol satisfies (9),

$$\Psi(\sigma w'_1, \sigma w'_2) = -\Psi(w'_1, w'_2)$$

for any w'_1, w'_2 in W'. Hence in particular Ψ vanishes on $W'^{+} \times W'^{+}$ and $W'^{-} \times W'^{-}$. If V is the kernel of Ψ then σ also maps V to itself, so we can write $V = V^{+} \oplus V^{-}$; and V^{+}, V^{-} are the left and right kernels respectively of the restriction of Ψ to $W'^{+} \times W'^{-}$. (It is here that we use the symmetry of Ψ.) In order to prove the solubility of (1) by the methods of this paper, we shall need to choose B so that for each of the two curves (7) the matrix of Ψ has corank 2: more explicitly, for the first curve (7) we shall need V to be generated by the images of Ba_1a_2 and a_1/a_2, and similarly for the second curve (7). Thus we shall need to ensure that $\dim V^{+} = 2$ and $\dim V^{-} = 0$ for each curve. If we require that no place of $\mathcal{S}_0$ is fixed by σ, so that Lemma 2 holds, then a prerequisite for this is

$$\dim {W'_{\mathcal{S}}}^{+} - \dim {W'_{\mathcal{S}}}^{-} = 2; \tag{16}$$

and in the notation of Lemma 2 this requires $N_2 = 3$. Since the processes in §5 do not alter N_2, we have to achieve this in §3. This accounts for the rather artificial manoeuvre in the corollary to Lemma 2.

3. Reduction to pairs of curves

We remind the reader that $\mathcal{S}_1$ denotes a finite set of places of K which contains $\mathcal{S}_0$ and all the primes dividing $a_1a_2a_3a_4$, and Σ_1 consists of the places in k below a place in $\mathcal{S}_1$. For the solubility of (1) in k it is certainly necessary that (1) should be everywhere locally soluble, a condition which it will be convenient to write in the following form.

Condition 2. – For every place v of k there exists C_v in k_v^*/k_v^{*3} such that each of the two equations

$$a_1X_1^3 + a_2X_2^3 = C_vX_0^3, \qquad a_3X_3^3 + a_4X_4^3 = C_vX_0^3 \tag{17}$$

is soluble in k_v.

Here it is only the v which divide 3 and those where some a_i is not a v-adic unit (up to a cube) which are of interest, and all of them lie in Σ_1; for any other v it is enough to choose C_v to be a unit. We have required C_v to be non-zero, for if (1) has solutions in k_v they must be Zariski dense; so there are solutions of (1) with $a_1X_1^3 + a_2X_2^3 \neq 0$. Here and hereafter, we identify an element of k_v^*/k_v^{*3} with any representative of it in k_v^*. Similar remarks apply to Condition 3 below.

The following condition, which is apparently stronger than Condition 2, is clearly also necessary for solubility.

Condition 3. – There exists C in k^*/k^{*3} such that each of the two equations

$$a_1X_1^3+a_2X_2^3=CX_0^3, \qquad a_3X_3^3+a_4X_4^3=CX_0^3 \tag{18}$$

is soluble in each k_v.

In both these conditions we need only consider non-archimedean v, because the conditions are trivial for archimedean ones. The next step should be to show that Condition 2 implies Condition 3; but the situation is complicated by the need to keep track of the number of primes outside Σ_1 which divide C and do not split in K/k. (See the final remark in §2.) We actually prove a rather stronger result. In general there is more than one set of $C_v \bmod k_v^{*3}$ for v in Σ_1 for which Eqs. (17) are soluble. But any C which satisfies Condition 3 must be such that C/C_v is in k_v^{*3} for all v in Σ_1 for one such set; so it is desirable to show that we can find such a C for any given set of C_v. The following lemma is a model for a more general result, which appears to have significant applications; so we state the proof in a form which does not require Condition 4, though the latter is needed for the corollary.

LEMMA 2. – *Suppose that the C_v satisfy Condition* 2; *then there exists C in $\mathfrak{o}$ satisfying Condition* 3 *and such that C/C_v is in k_v^{*3} for all v in Σ_1.*

Proof. – For each $\mathfrak{p}$ in Σ_1, let $n_\mathfrak{p}$ be such that $\mathfrak{p}^{n_\mathfrak{p}} \| C_\mathfrak{p}$, and write $\mathfrak{a}=\prod \mathfrak{p}^{n_\mathfrak{p}}$; then $C\mathfrak{a}^{-1}$ will need to be prime to every $\mathfrak{p}$ in Σ_1. If $\mathfrak{q}$ is a prime of k not in Σ_1 and such that $\mathfrak{q}^{m_\mathfrak{q}} \| C$ with $m_\mathfrak{q}$ prime to 3, the solubility of the two Eqs. (18) in $k_\mathfrak{q}$ is equivalent to requiring a_1/a_2 and a_3/a_4 to be in $k_\mathfrak{q}^{*3}$. Such $\mathfrak{q}$ fall into two families. If $\mathfrak{q}$ splits in K/k as the product of $\mathfrak{Q}$ and $\sigma\mathfrak{Q}$, then solubility of (18) in $k_\mathfrak{q}$ is equivalent to solubility in $K_\mathfrak{Q}$; and this in turn is equivalent to $\mathfrak{Q}$ splitting completely in $K(\sqrt[3]{a_1/a_2}, \sqrt[3]{a_3/a_4})/K$. As a condition on $\mathfrak{q}$ this is intractable, because it is a statement that $\mathfrak{q}$ splits completely in a certain nonabelian extension; and this is outside the scope of standard class field theory. So it is fortunate that we shall not need to use primes of this kind. If however $\mathfrak{q}$ remains prime in K, then the absolute norm of $\mathfrak{q}$ as a prime in k is congruent to $2 \bmod 3$; thus every element of $\mathfrak{o}_\mathfrak{q}^*$ is in $k_\mathfrak{q}^{*3}$ and in particular this is true of a_1/a_2 and a_3/a_4.

The $\mathfrak{q}$ outside Σ_1 which remain prime in K are just those which do not lie in the G_0 introduced just before Lemma 2. Let $\mathfrak{b}_0$ be an ideal in k which is prime to every $\mathfrak{p}$ in Σ_1 and is such that $\mathfrak{a}\mathfrak{b}_0=(\gamma_0)$ is principal; then $(C)=\mathfrak{a}\mathfrak{b}$ where $\mathfrak{b}=\beta\mathfrak{b}_0$ with β in k^*. We can take $C=\beta\gamma_0$, so that the condition that $C/C_\mathfrak{p}$ is in $k_\mathfrak{p}^{*3}$ translates into a requirement that β lies in $\mathfrak{o}_\mathfrak{p}^*$ and in an assigned class $\bmod k_\mathfrak{p}^{*3}$ for each $\mathfrak{p}$ in Σ_1. We can certainly find an element β_1 in k^* which satisfies the congruence conditions on β. Suppose first that $\beta_1\mathfrak{b}_0$ is not in G_0; then we can choose β_1' close to β_1 in the topology induced by Σ_1 and such that $\beta_1'\mathfrak{b}_0$ is a prime ideal $\mathfrak{q}_0$. In this case we take $C=\beta_1'\gamma_0$. If instead $\beta_1\mathfrak{b}_0$ is in G_0, choose any prime ideal $\mathfrak{q}_1$ not in $\Sigma_1 \cup G_0$; thus $\beta_1\mathfrak{b}_0\mathfrak{q}_1^{-1}$ will not be in G_0. We can now choose β_1'' close to β_1 and such that $\beta_1''\mathfrak{b}_0\mathfrak{q}_1^{-1}$ is a prime ideal $\mathfrak{q}_2$, and we take $C=\beta_1''\gamma_0$. In either case the C thus constructed will satisfy the conditions of the lemma except perhaps the integrality; and we can satisfy that by multiplying C by a suitable element of k^{*3}. □

In a number of places, of which this is the first, we shall need the following assumption on k; the corresponding assumption for $\mathcal{S}_0$ has already appeared in Lemma 2. We shall show in §5 that this assumption is not a constraint on k_0.

Condition 4. – No place in $\mathcal{S}_1$ is fixed by σ.

To fix ideas, we have included in this assumption the requirement that all the archimedean places of k are complex; this simplifies matters but is not essential. Condition 4 implies the analogous condition in Lemma 2.

COROLLARY. – *Suppose also that Condition* 4 *holds*; *then we can choose* C *in Lemma* 4 *so that it is integral and* $(C) = \mathfrak{a}\mathfrak{q}_2^2\mathfrak{q}_3\mathfrak{q}_4$ *where all the prime factors of* $\mathfrak{a}$ *lie in* Σ_1 *and the* $\mathfrak{q}_i$ *are primes of* k *outside* Σ_1 *which do not split in* K/k. *Moreover* (16) *holds for this value of* C.

Proof. – In the notation introduced just before Lemma 2, each prime in Σ_1 is in Γ_0. We use the same notation as in the proof of the lemma, and note that $\mathfrak{a}$ will be in Γ_0 by Condition 4. Much as in the proof of the lemma, we can find distinct prime ideals $\mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4$ not in Γ_0 and an element C in k^* such that $(C) = \mathfrak{a}\mathfrak{q}_2^2\mathfrak{q}_3\mathfrak{q}_4$ and $C/C_{\mathfrak{p}}$ is in $k_{\mathfrak{p}}^{*3}$ for each $\mathfrak{p}$ in Σ_1. If we then multiply C by a suitably chosen element of k^{*3}, we satisfy all the conditions of the corollary. The final sentence of the corollary follows from (13), (14) and $N_2 = 3$. □

The set $\mathcal{S}$ of bad primes for the curves (18) is obtained by adjoining to $\mathcal{S}_1$ the additional primes at which C is not a unit. In §5 we shall iteratively modify C and therefore $\mathcal{S}$. Each step will consist of multiplying C by some $c = \gamma.\sigma\gamma$ where (γ) is a first degree prime in K but not in the $\mathcal{S}$ so far obtained, or the product of two such primes. Such a step replaces $\mathcal{S}$ by $\mathcal{S}_+$ where $\mathcal{S}_+$ is obtained from $\mathcal{S}$ by adjoining the primes of K at which c is not a unit; the latter set will be the union of one or two sets $\mathcal{P}$. It follows from (13) and (14) that if (16) holds for $\mathcal{S}$ and C it holds for $\mathcal{S}_+$ and cC.

4. Tom Fisher's lemma

A key step in this paper, as in previous papers in the series, is to show that if some Selmer group has all but one of its generators represented by soluble curves, then the remaining generator also has this property. The proofs of this in earlier papers depended on assuming the finiteness of the Tate–Šafarevič group Ш; but under that hypothesis the result followed immediately from the existence and properties of the Cassels bilinear form on Ш. The present case, however, is more complicated because the curve (4) admits complex multiplication. The result which one would like to have would assert that (subject to the finiteness of the Tate–Šafarevič group) if the curve E given by (4) is defined over an algebraic number field K which contains ω, and if its ρ-Selmer group has order 9, then every element of that group has a representative which is soluble in K. I do not know whether this is true or false; what is clear is that it does not follow straightforwardly from the properties of the Cassels bilinear form over K. One could instead use the Cassels form over an algebraic number field k which does not contain ω; but this would involve reworking the results of §2 over such a field and then proceeding as in [1], and that is not at all attractive. Instead I use an unpublished lemma of Tom Fisher. The original idea is due to him and the current presentation to Alexei Skorobogatov; and I am indebted to both of them for permission to reproduce the material in this section.

For the following lemma we temporarily drop our standard conventions on k and K.

LEMMA 5. – *Let* E *be an elliptic curve defined over an algebraic number field* k, *and let* K *be a Galois extension of* k *of degree* n. *If* $(m, n) = 1$ *then*

$$Ш(E/k)[m] = Ш(E/K)[m]^{\mathrm{Gal}(K/k)}.$$

If $Ш(E/k)$ *is finite then the order of* $Ш(E/K)[m]^{\mathrm{Gal}(K/k)}$ *is a square.*

Proof. – Consider the restriction-inflation sequence for E and the commutative diagram obtained from the multiplication by m. Multiplication by m is an isomorphism on $H^i(K/k, E(K))$ for any $i \geqslant 1$. An easy diagram chase now gives

$$H^1(k, E)[m] = H^1(K, E)[m]^{\mathrm{Gal}(K/k)}.$$

Since K/k is Galois the degrees of the local extensions K_w/k_v divide n, where w is a place of K lying over some place v of k; so these degrees are prime to m. The previous argument is valid for any field extension of degree prime to m, so we can use it for K_w/k_v. Thus if the restriction of an element of $H^1(k,E)[m]$ in $H^1(K,E)[m]$ belongs to $Ш(E/K)$, this element must actually be in $Ш(E/k)$; so the natural restriction map

$$Ш(E/k)[m] \to Ш(E/K)[m]^{\mathrm{Gal}(K/k)}$$

is an isomorphism. The last sentence of the lemma follows from the non-degeneracy of the Cassels alternating bilinear form on $Ш(E/k)$, which implies that for any $m>0$ the order of the m-torsion subgroup of the Tate–Šafarevič group is a square. □

We now revert to the standard conventions of this paper, that k does not contain ω, that $K=k(\omega)$ and that σ is the nontrivial element of $\mathrm{Gal}(K/k)$. Let E_1 be an elliptic curve defined over k which has complex multiplication over K by $\mathbf{Z}[\omega]$. Any elliptic curve over k has an automorphism of order 2 given by $P \mapsto -P$. Twisting the curve by a cocycle from $H^1(k,\mathbf{Z}/2) = k^*/k^{*2}$ gives a quadratic twist of the elliptic curve: if the curve is given by $y^2=f(x)$ then the twist corresponding to d in k^* is given by $dy^2=f(x)$. Now let E_2, also defined over k, be the quadratic twist of E_1 by -3. Over K the curves E_1 and E_2 are naturally isomorphic. Let $\psi : E_1 \to E_2$ be this isomorphism; then $\sigma\psi = -\psi$. Let $\phi_1 : E_1 \to E_2$ be the composition $\psi\rho$ and $\phi_2 : E_2 \to E_1$ the composition $-\rho\psi^{-1}$, so that $\phi_2\phi_1 = 3$. Thus $\sigma\phi_1 = \phi_1$ and $\sigma\phi_2 = \phi_2$, so that ϕ_1 and ϕ_2 are defined over k. In the case that interests us, E_1 is given by $x^3+y^3=Az^3$ and E_2 by $X(X^2-Y^2)=4AZ^3$, and ϕ_1 is $(x,y,z) \mapsto (x^3+y^3, x^3-y^3, xyz)$. Since E_1 contains nontrivial 3-division points defined over K, if its ρ-Selmer group has order 9 then the order of $Ш(E_1/K)[\rho]$ must be either 1 or 3. The following lemma shows that the second case is impossible. We retain the notation above, including the condition that E_1 is defined over k.

LEMMA 6. – *If $Ш(E_1/k)$ is finite so is $Ш(E_2/k)$, and neither $Ш(E_1/K)[\rho]$ nor $Ш(E_2/K)[\rho]$ can have order 3.*

Proof. – Since E_1 and E_2 are isomorphic over K and isogenous over k we have

$$Ш(E_1/K)[\rho] = Ш(E_2/K)[\rho];$$

and if one of $Ш(E_1/k)$ and $Ш(E_2/k)$ is finite so is the other. Hence we can interchange E_1 and E_2 if we wish. Suppose that $Ш(E_1/K)[\rho]$ has order 3. Then either σ acts trivially on it or σ interchanges its two non-trivial elements. As a $\mathrm{Gal}(K/k)$-module, $Ш(E_1/K)[\rho]$ can be identified with $\mathbf{Z}/3$ in the former case and with μ_3 in the latter one. The $\mathrm{Gal}(K/k)$-module structure of $Ш(E_2/K)[\rho]$ is obtained by twisting by the non-trivial quadratic character $\mathrm{Gal}(K/k) \to \pm 1$. The twist of $\mathbf{Z}/3$ is μ_3 and vice versa. After possibly interchanging E_1 and E_2 we can therefore assume that

$$Ш(E_1/K)[\rho] = \mathbf{Z}/3 \quad \text{and} \quad Ш(E_2/K)[\rho] = \mu_3.$$

There is an exact sequence of $\mathrm{Gal}(K/k)$-modules

$$0 \to Ш(E_1/K)[\rho] \to Ш(E_1/K)[3] \to Ш(E_2/K)[\rho] \tag{19}$$

where the second arrow is the natural injection and the last arrow is ϕ_1. Now (19) implies that $Ш(E_1/K)[3]^{\mathrm{Gal}(K/k)} = \mathbf{Z}/3$. So this contradicts Lemma 5 with $m=3$ and $E=E_1$, according to which the order of this group must be a square. □

We shall apply this result to the two curves (7), which are the Jacobians of the two curves (2).

5. The paired first descents

Throughout this section we shall assume Condition 4. In view of the results in the previous section, to prove that (1) is soluble it is sufficient to find C in k^* such that each of the two Eqs. (18) is everywhere locally soluble and the ρ-Selmer groups over K of their Jacobians both have order 9. In the notation of §2 and working over K, these Jacobians have $A = a_1a_2C$ and $A = a_3a_4C$ respectively, and the curves (18) have $m = a_1/a_2$ and $m = a_3/a_4$ respectively.

We initially choose C in k^* as in the corollary to Lemma 2, using the hypothesis that (1) is everywhere locally soluble; thus both Eqs. (18) are everywhere locally soluble. We write $m_0 = a_1/a_2$ when we are considering the first Eq. (18) and $m_0 = a_3/a_4$ when we are considering the second one; thus (6) is required to be everywhere locally soluble for $m = m_0$, where A is as above. Since m_0 is by hypothesis not in k^{*3}, the element of the ρ-Selmer group which it generates is nontrivial. Our strategy is to multiply C repeatedly by suitably chosen elements of k^* so as eventually to reduce the ρ-Selmer group over K of the Jacobian of the first Eq. (18) to the subgroup of $X'_{\mathcal{S}}$ generated by Ca_1a_2 and a_1/a_2 where C is the new C, together with the corresponding property for the second Eq. (18). (The construction in Lemma 2 and its corollary ensures that C is a non-unit at three primes outside Σ_1; so for example Ca_1a_2 and a_1/a_2 are independent mod k^{*3}.) We proceed step by step. Each step will involve multiplying C by a suitably chosen c in k^* which is a unit at every prime in the current Σ; we shall arrange that any prime $\mathfrak{p}$ which divides c will split in K/k, and that such primes only divide c to the first power. Thus (16) will continue to hold in view of the argument at the end of §3. In order to preserve the C_v of §3 unchanged, each c must be in $k_{\mathfrak{p}}^{*3}$ for every $\mathfrak{p}$ in Σ_1; this is equivalent to requiring c to be in $K_{\mathfrak{P}}^{*3}$ for every $\mathfrak{P}$ in $\mathcal{S}_1$. In particular, it follows from Lemma 2 that this operation will not change $Z_{\mathcal{S}_0}$, so $Z_{\mathcal{S}}$ is only changed by adding the direct summands corresponding to the primes dividing c. For m_0 to remain in the ρ-Selmer group under this operation, we also need m_0 to be in $k_{\mathfrak{p}}^{*3}$ for every $\mathfrak{p}$ which divides c. Having done this, we replace $\mathcal{S}$ by the set $\mathcal{S}_+$ obtained by adjoining to $\mathcal{S}$ the primes in K which divide c. Of course $\Phi_{\mathcal{S}}$ and $\Psi_{\mathcal{S}}$ will refer to whichever of the curves

$$X^3 + Y^3 = a_1a_2CZ^3, \qquad X^3 + Y^3 = a_3a_4CZ^3$$

we are considering, and $\Phi_{\mathcal{S}_+}$ and $\Psi_{\mathcal{S}_+}$ will refer to the corresponding one of

$$X^3 + Y^3 = a_1a_2CcZ^3, \qquad X^3 + Y^3 = a_3a_4CcZ^3.$$

We retain this convention for the entire section.

It is basic to the process which follows that the action of σ on the structure described in §2 should be the natural one; this follows from Lemma 2. The process is carried out in two stages, each of which is broken down into a number of steps.

(i) Stage 1 ensures that for each of the two Jacobians with A as above the only elements of the kernel of Φ which are units outside $\mathcal{S}_1$ are $1, m_0$ and m_0^2. To achieve this, we require Condition 5 below.

(ii) Stage 2 ensures that for each of the two Jacobians the ρ-Selmer group over K is generated by A and m_0.

Once these stages have been completed, it will follow from Lemma 6 that both Eqs. (18) are soluble in K and therefore in k; and the solubility of (1) will follow. Condition 5 is not unduly restrictive; it will appear in Theorem 3 and in disguised form in Theorem 1. Moreover, for the solubility of (1) it is known that it is not enough to have local solubility everywhere, so some further condition must appear in the argument. (Compare [5,6] and [12].) On the other hand, Condition 4 is an unacceptable restriction; at the end of this section we shall get rid of it.

To implement Stage 1 we need the following lemma.

LEMMA 7. – *Let ξ be an element of $\mathfrak{O}^*_{\mathcal{S}_1}$, and let $\lambda_1, \lambda_2, \lambda_3$ be in $\mathbf{Z}$ and not all divisible by* 3. *Suppose that none of the expressions*

$$\eta = (a_1/a_2)^{\lambda_1}(a_3/a_4)^{\lambda_2}\xi^{\lambda_3} \tag{20}$$

lies in K^{*3}. Then there are an infinity of first degree primes $\mathfrak{P}$ in K such that a_1/a_2 and a_3/a_4 are in $K^{*3}_{\mathfrak{P}}$ but ξ is not.

Proof. – The field extension $K(\sqrt[3]{a_1/a_2}, \sqrt[3]{a_3/a_4}, \sqrt[3]{\xi})/K$ is abelian of degree 27; so the lemma follows from Dirichlet's theorem on primes in arithmetic progression or from the Tchebotarev density theorem. □

We note here the obvious fact that if $\mathfrak{P}$ is a prime of K and $\mathfrak{p}$ is the prime below it in k, then $k \cap K^{*3}_{\mathfrak{P}} = k^{*3}_{\mathfrak{p}}$; this will be used repeatedly below. Now suppose that ξ is in the kernel of $\Phi_{\mathcal{S}}$ and satisfies the conditions of Lemma 7, and choose $\mathfrak{P}$ not in $\mathcal{S}$ as in that lemma. Let $\mathfrak{P}_1$ be another first degree prime ideal of K, in the ideal class of $\mathfrak{P}^{-1}$ and such that $\mathfrak{P}\mathfrak{P}_1 = (\Theta)$ where Θ is in K^{*3}_v for every v in $\mathcal{S}$; such a $\mathfrak{P}_1$ exists by Dirichlet's theorem. If we multiply C by $c = \Theta.\sigma\Theta$ then we do not alter the class of $C_v \bmod k^{*3}_v$ for any v below a place in $\mathcal{S}$. Also ξ is not in the kernel of $\Phi_{\mathcal{S}_+}$ because ξ is not in $K^{*3}_{\mathfrak{P}}$ and therefore $\xi x^3 + \xi^{-1}y^3 = Ccz^3$ is insoluble in $K_{\mathfrak{P}}$; but m_0 is in the kernel of $\Phi_{\mathcal{S}_+}$ because m_0 is in $K^{*3}_{\mathfrak{P}}$ and also by cubic reciprocity in $K^{*3}_{\mathfrak{P}_1}$. (Since this kind of argument occurs several times, of which this is the first, the referee has suggested that I should supply the details. We have $\sum(m_0, \Theta)_v = 0$ where the sum is over all places v of K; and $(m_0, \Theta)_v = 0$ for any v outside $\mathcal{S} \cup \{\mathfrak{P}, \mathfrak{P}_1\}$ because then m_0 and Θ are both v-adic units. Also $(m_0, \Theta)_v = 0$ for v in $\mathcal{S}$ because then Θ is in K^{*3}_v; and $(m_0, \Theta)_{\mathfrak{P}} = 0$ because m_0 is in $K^{*3}_{\mathfrak{P}}$ by Lemma 7. Hence $(m_0, \Theta)_{\mathfrak{P}_1} = 0$, so that m_0 is in $K^{*3}_{\mathfrak{P}_1}$.) There may be elements in the kernel of $\Phi_{\mathcal{S}_+}$ which were not in the kernel of $\Phi_{\mathcal{S}}$; but these will not be in $\mathfrak{O}^*_{\mathcal{S}_1}$.

By repeating this process a finite number of times, we can remove from the kernel of Φ all elements of $\mathfrak{O}^*_{\mathcal{S}_1}$ except perhaps those which fail to satisfy the conditions of the lemma. We know by Condition 1 that if $\lambda_3 = 0$ then η is not in K^{*3}; so these exceptional elements are all ones for which we can take $\lambda_3 = 1$ – in other words, they are a_1/a_2, a_3/a_4, a_1a_3/a_2a_4 and a_1a_4/a_2a_3 and their inverses. It appears that no analogous argument will work for such elements, and if they are to be outside the kernel it can only be because of the insolubility of (6) in K_v for some v in $\mathcal{S}_1$. This must therefore be imposed as a constraint on the C_v in Condition 2. For the first curve E we know that $m_0 = a_1/a_2$ is in the kernel of Φ and does not need to be removed; so it is enough to ensure that we do not have a problem with $\xi = a_3/a_4$, for if this is not in the kernel nor will a_1a_3/a_2a_4 or a_1a_4/a_2a_3 be.

Condition 5. – The equation $a_3^2X_1^3 + a_4^2X_2^3 = a_1a_2a_3a_4C_vX_0^3$ is insoluble in k_v for some v in Σ_1. The same property holds, though not necessarily with the same v, for the equation $a_1^2X_3^3 + a_2^2X_4^3 = a_1a_2a_3a_4C_vX_0^3$.

In what follows, we shall always assume that the C_v have been chosen to satisfy Condition 5 as well as Condition 2. This completes Stage 1.

The object of each step in Stage 2 is to reduce the corank of the bilinear form Ψ for one of the two Jacobians E while not increasing it for the other, until both coranks are reduced to 2. As has already been pointed out, it is enough to work with the restriction of Ψ to $W'^+ \times W'^-$; and since each step of Stage 2 will adjoin a pair of conjugate primes to $\mathcal{S}$, it will increase the dimensions of W'^+ and W'^- by 1. As at the end of §2, we denote by $V^+_{\mathcal{S}}$ and $V^-_{\mathcal{S}}$ the left and right kernels of the restriction of $\Psi_{\mathcal{S}}$ to $W'^+_{\mathcal{S}} \times W'^-_{\mathcal{S}}$. To prove that Stage 2 can be completed it is enough to

show that so long as $\dim V^- > 0$ for one of the two Jacobians we can choose γ so as to decrease $\dim V^+$ and $\dim V^-$ for that one without increasing them for the other.

Denote temporarily by n_1 and n_2 the ranks of the restrictions of $\Psi_{\mathcal{S}}$ to $W'^+ \times W'^-$ for the two Jacobians; then the largest pairs of subspaces on which these restrictions are nonsingular have dimensions n_1 and n_2 respectively. To fix ideas, we shall suppose that it is the Jacobian of the first Eq. (18) which has $\dim V^- > 0$ and for which we are trying to diminish $\dim V^+$ and $\dim V^-$. Our notation is that a step takes us from $\mathcal{S}$ to $\mathcal{S}_+$; we therefore need to choose our step in such a way that we can exhibit pairs of subspaces of W'^+ and W'^-, of dimension $n_1 + 2$ for the first equation and $n_2 + 1$ for the second one, on which the restrictions of the $\Psi_{\mathcal{S}_+}$ are nonsingular. The subspaces we use are given by (26) and (30) respectively; it is not hard to see that any serious candidates must be of these kinds.

Each step in Stage 2 will consist of multiplying C by $c = \gamma.\sigma\gamma$ where (γ) is a first degree principal prime ideal in K. We shall require γ to be in $K_{\mathfrak{P}}^{*3}$ for each $\mathfrak{P}$ in $\mathcal{S}_1$, which incidentally ensures that m_0 is in K_γ^{*3} by cubic reciprocity. Further conditions on γ will be imposed later, but they are not relevent to the evaluations which follow and which extend up to (25). Up to that point, our task is to develop formulae for the values of $\Psi_{\mathcal{S}_+}$.

If $\mathfrak{P}$ is in $\mathcal{S}_1$ then replacing C by cC does not alter $W_{\mathfrak{P}}$, since it only changes $E/K_{\mathfrak{P}}$ by a linear transformation on the variable Z in (4); and it does not alter the space $Z_{\mathfrak{P}}$, by Lemma 2. Hence the replacement does not alter $W'_{\mathcal{P}}$. If $\mathfrak{P}$ is in $\mathcal{S} \setminus \mathcal{S}_1$ the effect of the replacement is that $W_{\mathfrak{P}}$ is generated by the class of Ac instead of that of A but $Z_{\mathcal{P}}$ remains the same. For each such $\mathfrak{P}$, there is an isomorphism from the old to the new $W_{\mathfrak{P}}$, given by mapping the class of A^n to that of $(Ac)^n$ for each n; and this induces an isomorphism from the old to the new $W'_{\mathfrak{P}}$. Using these, we can define a natural injection $\phi : W'_{\mathcal{S}} \to W'_{\mathcal{S}_+}$ by requiring the image to have trivial components at all the primes dividing c. Since c is in $Z_{\mathfrak{P}}$ for every $\mathfrak{P}$ in $\mathcal{S}$, the actions of $\tau_{\mathcal{S}}$ and $\tau_{\mathcal{S}_+} \circ \phi$ on $W'_{\mathcal{S}}$ are identical.

If w'_1 and w'_2 are in $W'_{\mathcal{S}}$ we need to compare the values of $\Psi_{\mathcal{S}_+}(\phi w'_1, \phi w'_2)$ and $\Psi_{\mathcal{S}}(w'_1, w'_2)$. The components coming from a prime $\mathfrak{P}$ in $\mathcal{S}_1$ are identical. If $\mathfrak{P}|c$ the component of $\phi w'_2$ at $\mathfrak{P}$ is trivial and hence so is the contribution to $\Psi_{\mathcal{S}_+}(\phi w'_1, \phi w'_2)$ from $\mathfrak{P}$. If $\mathfrak{P}$ is in $\mathcal{S} \setminus \mathcal{S}_1$ then we define $m_{\mathfrak{P}}$, $n_{\mathfrak{P}}$ as elements of $\mathbf{Z}/(3)$ by $\mathfrak{P}^{m_{\mathfrak{P}}} \| w'_1$ and $\mathfrak{P}^{n_{\mathfrak{P}}} \| w'_2$. The difference between the contributions at $\mathfrak{P}$ to $\Psi_{\mathcal{S}_+}(\phi w'_1, \phi w'_2)$ and $\Psi_{\mathcal{S}}(w'_1, w'_2)$ is

$$(\tau_{\mathcal{S}_+}\phi w'_1, \phi w'_2)_{\mathfrak{P}} - (\tau_{\mathcal{S}} w'_1, w'_2)_{\mathfrak{P}} = \left(\tau_{\mathcal{S}} w'_1, c^{n_{\mathfrak{P}}} w'_2\right)_{\mathfrak{P}} - (\tau_{\mathcal{S}} w'_1, w'_2)_{\mathfrak{P}} = \left(\tau_{\mathcal{S}} w'_1, c^{n_{\mathfrak{P}}}\right)_{\mathfrak{P}}$$

and since $\mathfrak{P}^{m_{\mathfrak{P}}} \| \tau_{\mathcal{S}} w'_1$ this is $m_{\mathfrak{P}} n_{\mathfrak{P}} (\Pi, c)_{\mathfrak{P}}$ where Π is as usual a uniformizing variable for $\mathfrak{P}$. Here we have used the remark immediately after (15). Thus

$$\Psi_{\mathcal{S}_+}(\phi w'_1, \phi w'_2) = \Psi_{\mathcal{S}}(w'_1, w'_2) + \sum m_{\mathfrak{P}} n_{\mathfrak{P}} (\Pi, c)_{\mathfrak{P}} \tag{21}$$

where the sum is taken over all $\mathfrak{P}$ in $\mathcal{S} \setminus \mathcal{S}_1$. In particular if c is in $K_{\mathfrak{P}}^{*3}$ for every $\mathfrak{P}$ in $\mathcal{S}$, then $\Psi_{\mathcal{S}_+}(\phi w'_1, \phi w'_2) = \Psi_{\mathcal{S}}(w'_1, w'_2)$.

It only remains to evaluate

$$\Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, \phi w'^-), \quad \Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, w'_\gamma - \sigma w'_\gamma) \quad \text{and} \quad \Psi_{\mathcal{S}_+}(\phi w'^+, w'_\gamma - \sigma w'_\gamma)$$

for any w'^+ in ${W'_{\mathcal{S}}}^+$ and w'^- in ${W'_{\mathcal{S}}}^-$; here w'_γ denotes the element of $W'_{\mathcal{S}_+}$ which is represented by Ac in W'_γ and is trivial elsewhere. I claim that $\tau_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma) = c$. For $w'_\gamma + \sigma w'_\gamma$ is represented by Ac in W'_γ and $W'_{\sigma\gamma}$, and by 1 in $W'_{\mathfrak{P}}$ for each $\mathfrak{P}$ in $\mathcal{S}$. It is therefore enough to note that A is a unit at (γ) and $(\sigma\gamma)$ and therefore induces elements of Z_γ and $Z_{\sigma\gamma}$, that c is a

unit at $\mathfrak{P}$ for each $\mathfrak{P}$ in $\mathcal{S} \setminus \mathcal{S}_0$ and therefore induces elements of $Z_{\mathfrak{P}}$ for such $\mathfrak{P}$, and that c is in $\mathfrak{O}_{\mathfrak{P}}^{*3}$ for each $\mathfrak{P}$ in $\mathcal{S}_0$ and therefore induces elements of $Z_{\mathfrak{P}}$ for such $\mathfrak{P}$. If for each $\mathfrak{P}$ in $\mathcal{S}$ we define $n_{\mathfrak{P}}$ by $\mathfrak{P}^{n_{\mathfrak{P}}} \| {w'}^-$ then

$$\Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, \phi {w'}^-) = \sum\nolimits_{\mathfrak{P} \in (\mathcal{S} \setminus \mathcal{S}_1)} n_{\mathfrak{P}} (c, \Pi)_{\mathfrak{P}}. \tag{22}$$

Here we have dropped the terms for which $\mathfrak{P}$ is in $\mathcal{S}_1$ since each of them vanishes. By a similar argument

$$\Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, w'_\gamma - \sigma w'_\gamma) = (c, Ac)_\gamma - (c, Ac)_{\sigma\gamma} = 2(\gamma, A)_\gamma. \tag{23}$$

By the Hilbert product formula this is equal to $\sum_{\mathfrak{P} \in \mathcal{S}} (\gamma, A)_{\mathfrak{P}}$, and here we again can drop the terms with $\mathfrak{P}$ in $\mathcal{S}_1$ because each of them vanishes. Writing $\sigma\mathfrak{P}$ for $\mathfrak{P}$ and applying σ, this is also equal to $-\sum_{\mathfrak{P} \in \mathcal{S}} (\sigma\gamma, A)_{\mathfrak{P}}$. Hence

$$\Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, w'_\gamma - \sigma w'_\gamma) = -\sum\nolimits_{\mathfrak{P} \in (\mathcal{S} \setminus \mathcal{S}_1)} v_{\mathfrak{P}}(A) (\gamma/\sigma\gamma, \Pi)_{\mathfrak{P}}. \tag{24}$$

Note that $v_{\mathfrak{P}}(A) = 1$ for all but one of the primes in $\mathcal{S} \setminus \mathcal{S}_1$; the exception is the prime $\mathfrak{Q}_2$ lying above the $\mathfrak{q}_2$ introduced in the corollary to Lemma 2, for which $v_{\mathfrak{Q}_2}(A) = 2$.

Again $\Psi_{\mathcal{S}_+}(\phi {w'}^+, w'_\gamma - \sigma w'_\gamma) = (\tau_{\mathcal{S}} {w'}^+, Ac)_\gamma - (\tau_{\mathcal{S}} {w'}^+, Ac)_{\sigma\gamma}$; here we can drop the factor $A\sigma\gamma$ in the first Hilbert symbol and the factor $A\gamma$ in the second, giving $2(\tau_{\mathcal{S}} {w'}^+, \gamma)_\gamma$. This last expression is equal to $\sum_{\mathfrak{P} \in \mathcal{S}} (\tau_{\mathcal{S}} {w'}^+, \gamma)_{\mathfrak{P}}$ by the reciprocity law. We can again drop the terms with $\mathfrak{P}$ in $\mathcal{S}_1$; if we define $m_{\mathfrak{P}}$ for $\mathfrak{P}$ in $\mathcal{S} \setminus \mathcal{S}_1$ by $\mathfrak{P}^{m_{\mathfrak{P}}} \| {w'}^+$ and use the remark which follows (15) then we obtain

$$\Psi_{\mathcal{S}_+}(\phi {w'}^+, w'_\gamma - \sigma w'_\gamma) = \sum\nolimits_{\mathfrak{P} \in (\mathcal{S} \setminus \mathcal{S}_1)} m_{\mathfrak{P}} (\Pi, \gamma)_{\mathfrak{P}}.$$

Here again we can write $\sigma\mathfrak{P}$ for $\mathfrak{P}$ and apply σ; remembering that $m_{\mathfrak{P}} = m_{\sigma\mathfrak{P}}$ because ${w'}^+$ is fixed by σ, we finally obtain

$$\Psi_{\mathcal{S}_+}(\phi {w'}^+, w'_\gamma - \sigma w'_\gamma) = -\sum\nolimits_{\mathfrak{P} \in (\mathcal{S} \setminus \mathcal{S}_1)} m_{\mathfrak{P}} (\Pi, \gamma/\sigma\gamma)_{\mathfrak{P}}. \tag{25}$$

Note that in each of the three formulae (22), (24) and (25) the terms on the right coming from $\mathfrak{P}$ and $\sigma\mathfrak{P}$ are equal. In the evaluations of matrix elements later in this section, this will give rise to a factor 2 for terms for which $\mathfrak{P}$ and $\sigma\mathfrak{P}$ are distinct.

For the first curve E, for which we are trying to diminish $\dim V^+$ and $\dim V^-$, let ${v'}^+$ be an element of $V_{\mathcal{S}}^+$ such that $\tau_{\mathcal{S}} {v'}^+$ is independent of m_0 and A as an element of $X'_{\mathcal{S}}$, and let ${v'}^-$ be a nonzero element of $V_{\mathcal{S}}^-$. After dividing ${v'}^+$ by a power of $\tau_{\mathcal{S}}^{-1} A$ if necessary, we can assume that there is a prime $\mathfrak{P}_1$ in $\mathcal{S} \setminus \mathcal{S}_1$ at which ${v'}^+$ is a unit. Because of Stage 1, each of ${v'}^+$ and ${v'}^-$ has valuation prime to 3 at some prime in $\mathcal{S} \setminus \mathcal{S}_1$. Let $\mathfrak{P}_+$ and $\mathfrak{P}_-$ be such primes, where if possible we choose $\mathfrak{P}_+$ and $\mathfrak{P}_-$ to be equal; if this is not possible we rechoose $\mathfrak{P}_1$ to be $\mathfrak{P}_-$. Let $w_1^+, \dots, w_r^+$ be a set of representatives in $W_{\mathcal{S}}^+$ of a base for ${W'_{\mathcal{S}}}^+ / V_{\mathcal{S}}^+$; by multiplying each w_i^+ first by a power of $\tau_{\mathcal{S}}^{-1} A$ and then by a power of a representative of ${v'}^+$, we can ensure that the w_i^+ are units at $\mathfrak{P}_1$ and $\mathfrak{P}_+$. Let $w_1^-, \dots, w_r^-$ be a set of representatives in $W_{\mathcal{S}}^-$ of a base for ${W'_{\mathcal{S}}}^- / V_{\mathcal{S}}^-$; by multiplying each w_i^- by a power of a representative of ${v'}^-$, we can similarly ensure that the w_i^- are units at $\mathfrak{P}_-$. Let U^+ be the subspace of ${W'_{\mathcal{S}}}^+$ spanned by the images of the

w_i^+ and similarly for U^-; and consider the restriction of $\Psi_{\mathcal{S}_+}$ to the subspace of $W'^+_{\mathcal{S}_+} \times W'^-_{\mathcal{S}_+}$ given by

$$\big(\phi U^+ \oplus \{\phi v'^+\} \oplus \{w'_\gamma + \sigma w'_\gamma\}\big) \times \big(\phi U^- \oplus \{\phi v'^-\} \oplus \{w'_\gamma - \sigma w'_\gamma\}\big), \tag{26}$$

where $\{w'\}$ for any w' denotes the subspace of $W'_{\mathcal{S}_+}$ generated by w' and ϕ is the natural injection $W'_{\mathcal{S}} \to W'_{\mathcal{S}_+}$. For the calculations involving the first curve, we shall require γ to be such that $(\gamma, \Pi)_{\mathfrak{P}} = 0$ for all $\mathfrak{P}$ in $\mathcal{S}$ except possibly for $\mathfrak{P}_1, \sigma\mathfrak{P}_1, \mathfrak{P}_+$ and $\sigma\mathfrak{P}_+$ and that $(\Pi_-, \gamma/\sigma\gamma)_{\mathfrak{P}_-} = 0$ where Π_- is a uniformizing variable for $\mathfrak{P}_-$; we shall need to impose a further condition on γ when we consider the second curve. (Similarly Π_+ and Π_1 will be uniformizing variables for $\mathfrak{P}_+$ and $\mathfrak{P}_1$ respectively. We do not claim that $\mathfrak{P}_1 \neq \sigma\mathfrak{P}_1$ nor that $\mathfrak{P}_+ \neq \sigma\mathfrak{P}_+$, though there will be some abuse of language if either of these fails.) With the obvious bases, the matrix of the restriction of $\Psi_{\mathcal{S}_+}$ to (26) has the form

$$\begin{pmatrix} \Psi_{\mathcal{S}}(U^+, U^-) & 0 & 0 \\ \Psi(\phi v'^+, U^-) & \Psi(\phi v'^+, \phi v'^-) & \Psi(\phi v'^+, w'_\gamma - \sigma w'_\gamma) \\ \Psi(w'_\gamma + \sigma w'_\gamma, U^-) & \Psi(w'_\gamma + \sigma w'_\gamma, \phi v'^-) & \Psi(w'_\gamma + \sigma w'_\gamma, w'_\gamma - \sigma w'_\gamma) \end{pmatrix} \tag{27}$$

where to save space we have written Ψ for $\Psi_{\mathcal{S}_+}$ in the second and third rows. Here we need only justify the first row. In each term we take w'_1 to be the image in U^+ of some w_i^+. For the first term we take w'_2 to be the image in U^- of some w_j^- and use (21); thus we need to show that the sum on the right there vanishes. Suppose first that $\mathfrak{P}$ in $\mathcal{S} \setminus \mathcal{S}_1$ is not $\mathfrak{P}_1, \sigma\mathfrak{P}_1, \mathfrak{P}_+$ or $\sigma\mathfrak{P}_+$; then by construction γ is in $K^{*3}_{\mathfrak{P}}$ and $K^{*3}_{\sigma\mathfrak{P}}$, so $\sigma\gamma$ is also in $K^{*3}_{\mathfrak{P}}$ and so is $c = \gamma.\sigma\gamma$, whence $(\Pi, c)_{\mathfrak{P}} = 0$. But w'_1 is fixed by σ and is a unit at $\mathfrak{P}_1$ and $\mathfrak{P}_+$, and hence also at $\sigma\mathfrak{P}_1$ and $\sigma\mathfrak{P}_+$; so $m_{\mathfrak{P}} = 0$ if $\mathfrak{P}$ is one of $\mathfrak{P}_1, \sigma\mathfrak{P}_1, \mathfrak{P}_+$ or $\sigma\mathfrak{P}_+$. Hence each term in the sum on the right of (21) vanishes. For the second term we take $w'_2 = v'^-$; now the sum on the right of (21) vanishes for the same reason as before, and $\Psi_{\mathcal{S}}(w'_1, w'_2) = \Psi_{\mathcal{S}}(w'_1, v'^-)$ vanishes because v'^- is in $V^-_{\mathcal{S}}$. For the third term we use (25), and the same arguments show that again each term in the sum on the right vanishes. We know that $\Psi_{\mathcal{S}}(U^+, U^-)$ is nonsingular, so to prove that the matrix (27) is nonsingular it is enough to prove the nonsingularity of the 2×2 matrix in the bottom right hand corner.

We now split cases. If $\mathfrak{P}_+ = \mathfrak{P}_-$ the 2×2 matrix reduces to

$$\begin{pmatrix} \nu(\Pi_+, c)_{\mathfrak{P}_+} & 0 \\ \Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, \phi v'^-) & \varepsilon_1 v_{\mathfrak{P}_1}(A)(\gamma/\sigma\gamma, \Pi_1)_{\mathfrak{P}_1} \end{pmatrix} \tag{28}$$

for some ν prime to 3; here $\varepsilon_1 = 1$ if $\mathfrak{P}_1 \neq \sigma\mathfrak{P}_1$ and $\varepsilon_1 = -1$ if $\mathfrak{P}_1 = \sigma\mathfrak{P}_1$. The evaluation of the element in the top left-hand corner follows from (21) in much the same way as did that of the middle element in the top row of (27); we use the fact that $m_{\mathfrak{P}} = 0$ for $\mathfrak{P}_1$ and $\sigma\mathfrak{P}_1$, but now the valuations of v'^+ and v'^- at $\mathfrak{P}_+$ are both prime to 3 and ν is equal to their product if $\mathfrak{P}_+$ is fixed by σ and to twice their product otherwise. Similarly the zero in the top right-hand corner comes from (25) in much the same way as the zero in the top right-hand corner of (27); as in the previous sentence $m_{\mathfrak{P}} = 0$ for $\mathfrak{P}_1$ and $\sigma\mathfrak{P}_1$, but also $(\Pi_+, \gamma/\sigma\gamma)_{\mathfrak{P}_+} = 0$ by the construction of γ and the fact that $\mathfrak{P}_+ = \mathfrak{P}_-$. For the element in the bottom right-hand corner we use (24); the terms coming from $\mathfrak{P}_+$ and $\sigma\mathfrak{P}_+$ vanish for the same reason as in the last sentence, and the value of ε_1 comes from the fact that if $\mathfrak{P}_1 = \sigma\mathfrak{P}_1$ we have one corresponding term on the right of (24) but otherwise we have two. The matrix (28) is nonsingular if $(\Pi_+, c)_{\mathfrak{P}_+}$ and $(\gamma/\sigma\gamma, \Pi_1)_{\mathfrak{P}_1}$ are both nonzero.

If v'^- is a unit at $\mathfrak{P}_+$ then $\mathfrak{P}_- = \mathfrak{P}_1$ and the 2×2 matrix reduces to

$$\begin{pmatrix} 0 & \nu_1(\Pi_+, \gamma/\sigma\gamma)_{\mathfrak{P}_+} \\ \nu_2(c, \Pi_1)_{\mathfrak{P}_1} & \varepsilon_+ v_{\mathfrak{P}_+}(A)(\gamma/\sigma\gamma, \Pi_+)_{\mathfrak{P}_+} \end{pmatrix} \tag{29}$$

for some ν_1, ν_2 prime to 3; here $\varepsilon_+ = 1$ if $\mathfrak{P}_+ \neq \sigma\mathfrak{P}_+$ and $\varepsilon_+ = -1$ if $\mathfrak{P}_+ = \sigma\mathfrak{P}_+$. Here the zero in the top left-hand corner comes from (21) by a calculation like that for the corresponding element in (28); the only difference is that now v'^- is a unit at $\mathfrak{P}_+$ and $\sigma\mathfrak{P}_+$, so the corresponding terms in (21) vanish. The element in the top right-hand corner comes from (25), because in contrast with (28) the terms on the right of (25) coming from $\mathfrak{P}_+$ and $\sigma\mathfrak{P}_+$ need not vanish, though they are equal; here ν_1 is the valuation of v'^+ at $\mathfrak{P}_+$ or twice it according as $\sigma\mathfrak{P}_+ \neq \mathfrak{P}_+$ or $\sigma\mathfrak{P}_+ = \mathfrak{P}_+$. For the element in the bottom left-hand corner we use (22), where as usual in the sum on the right $(c, \Pi)_{\mathfrak{P}}$ vanishes unless $\mathfrak{P}$ is $\mathfrak{P}_+, \sigma\mathfrak{P}_+, \mathfrak{P}_1$ or $\sigma\mathfrak{P}_1$, and $n_{\mathfrak{P}} = 0$ for $\mathfrak{P}_+$ and $\sigma\mathfrak{P}_+$; here ν_2 is the valuation of v'^- at $\mathfrak{P}_1$ or twice it according as $\sigma\mathfrak{P}_1 = \mathfrak{P}_1$ or $\sigma\mathfrak{P}_1 \neq \mathfrak{P}_1$. For the element in the bottom right-hand corner (whose value is not important here but will be needed in (31)) we use (24) much as for (28); but this time it is the terms coming from $\mathfrak{P}_1$ which vanish because now $\mathfrak{P}_1 = \mathfrak{P}_-$. The matrix (29) will be nonsingular if $(\Pi_+, \gamma/\sigma\gamma)_{\mathfrak{P}_+}$ and $(c, \Pi_1)_{\mathfrak{P}_1}$ are both nonzero. Note that in each case we have also ensured that the value of $\Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, w'_\gamma - \sigma w'_\gamma)$ is nonzero.

We now turn to the other curve E. Although the functions $\Psi_{\mathcal{S}_+}$ for the two curves are different, the values of the left hand sides of (23) for the two curves are the same, because their difference is

$$2(\gamma, a_1a_2/a_3a_4)_\gamma = \sum\nolimits_{\mathfrak{P} \in \mathcal{S}_1} (\gamma, a_1a_2/a_3a_4)_{\mathfrak{P}} = 0.$$

In particular $\Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, w'_\gamma - \sigma w'_\gamma)$ is nonzero for the second curve, by the last remark in the previous paragraph. We define the w_i^+, w_i^- and U^+, U^- for the second curve in the same way as we did for the first. We still denote by $\mathfrak{P}_1, \mathfrak{P}_+, \mathfrak{P}_-, \mathfrak{P}_0$ the same primes as for the first curve; what matters now is that $\mathfrak{P}_0, \sigma\mathfrak{P}_0, \mathfrak{P}_-$ and $\sigma\mathfrak{P}_-$ are the only primes in $\mathcal{S} \setminus \mathcal{S}_1$ at which c is not required to be locally a cube. By dividing the w_i^+ by appropriate powers of $\tau_{\mathcal{S}}^{-1}A$ we can further ensure that each of the w_i^+ is a unit at $\mathfrak{P}_0$, where $\mathfrak{P}_0$ is as before that one of $\mathfrak{P}_+$ and $\mathfrak{P}_1$ which is not equal to $\mathfrak{P}_-$. Thus when we use (21) to evaluate the $\Psi_{\mathcal{S}_+}(\phi w_i^+, \phi w_j^-)$ the only terms in the sum on the right which can be nonzero are those from $\mathfrak{P}_-$ and $\sigma\mathfrak{P}_-$. We can then require that at most one of the w_i^+ is a non-unit at $\mathfrak{P}_-$. Whether $\mathfrak{P}_-$ is equal to $\mathfrak{P}_+$ or to $\mathfrak{P}_1$, it will then follow from (25) and $(\Pi_-, \gamma/\sigma\gamma)_{\mathfrak{P}_-} = 0$ that $\Psi_{\mathcal{S}_+}(U^+, w'_\gamma - \sigma w'_\gamma) = 0$. Hence the matrix of the restriction of $\Psi_{\mathcal{S}_+}$ to

$$\big(U^+ \oplus \{w'_\gamma + \sigma w'_\gamma\}\big) \times \big(U^- \oplus \{w'_\gamma - \sigma w'_\gamma\}\big) \tag{30}$$

has the form

$$\begin{pmatrix} \Psi_{\mathcal{S}_+}(U^+, U^-) & 0 \\ \Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, U^-) & \Psi_{\mathcal{S}_+}(w'_\gamma + \sigma w'_\gamma, w'_\gamma - \sigma w'_\gamma) \end{pmatrix} \tag{31}$$

and this will be nonsingular if $\Psi_{\mathcal{S}_+}(U^+, U^-)$ is nonsingular. But $\Psi_{\mathcal{S}_+}(U^+, U^-)$ only differs from $\Psi_{\mathcal{S}}(U^+, U^-)$ in that the elements of one row have been changed by multiples of $(c, \Pi_-)_{\mathfrak{P}_-}$, the multiples being independent of γ. Hence

$$\det\big(\Psi_{\mathcal{S}_+}(U^+, U^-)\big) = \det\big(\Psi_{\mathcal{S}}(U^+, U^-)\big) + b(c, \Pi_-)_{\mathfrak{P}_-}$$

for some b in $\mathbf{F}_3$ independent of γ; and there is a nonzero value of $(c, \Pi_-)_{\mathfrak{P}_-}$ which makes this nonzero. This is the additional condition on γ which we noted above that we would need to impose.

This step will therefore achieve what we want if the conditions on γ imposed just after (26) hold and the matrices (27) and (31) are nonsingular. For this it is enough to ensure that

- γ lies in $K_{\mathfrak{P}}^{*3}$ for each $\mathfrak{P}$ in $\mathcal{S}_1$,
- $(\gamma, \Pi)_{\mathfrak{P}} = 0$ for all $\mathfrak{P}$ in $\mathcal{S}$ outside $\mathcal{P}_0 \cup \mathcal{P}_- = \mathcal{P}_1 \cup \mathcal{P}_+$,
- $(\Pi_0, \gamma/\sigma\gamma)_{\mathfrak{P}_0}$ is nonzero,
- $(\Pi_-, c)_{\mathfrak{P}_-}$ takes an assigned nonzero value, and
- $(\Pi_-, \gamma/\sigma\gamma)_{\mathfrak{P}_-} = 0$.

Now

$$(\Pi, \gamma/\sigma\gamma)_{\mathfrak{P}} = (\Pi, \gamma)_{\mathfrak{P}} + (\sigma\Pi, \gamma)_{\sigma\mathfrak{P}}, \qquad (\Pi, c)_{\mathfrak{P}} = (\Pi, \gamma)_{\mathfrak{P}} - (\sigma\Pi, \gamma)_{\sigma\mathfrak{P}}.$$

Bearing in mind that we cannot have $\sigma\mathfrak{P}_- = \mathfrak{P}_-$ because v'^- is a nonunit at $\mathfrak{P}_-$, these reduce to conditions on the $(\Pi, \gamma)_{\mathfrak{P}}$ for $\mathfrak{P}$ in $\mathcal{S}$, and by Dirichlet's theorem they can all be satisfied.

What we have so far proved is that if

(i) the Tate–Šafarevič group of any elliptic curve (4) over k is finite,
(ii) Conditions 1 and 4 hold,
(iii) Condition 2 holds and we can choose the C_v to satisfy Condition 5,

then (1) is soluble in k. As was explained in the Introduction, Condition 1 presents no problems because if it fails (1) is certainly soluble; we must now get rid of Condition 4.

THEOREM 3. – *Assume that the Tate–Šafarevič group of any elliptic curve* (4) *over any quadratic extension of k_0 is finite. If we can choose the C_v in Condition* 2 *so that for some places v_1, v_3* (*which may be the same*) *the first equation*

$$a_3^2 X_1^3 + a_4^2 X_2^3 = a_1 a_2 a_3 a_4 C_v X_0^3, \qquad a_1^2 X_3^3 + a_2^2 X_4^3 = a_1 a_2 a_3 a_4 C_v X_0^3 \tag{32}$$

is insoluble in $(k_0)_{v_1}$ and the second equation is insoluble in $(k_0)_{v_3}$, then (1) *is soluble in k_0.*

Proof. – We construct a quadratic extension $k = k_0(\sqrt{\alpha})$ with α in k_0, such that if k_0 satisfies the conditions of Theorem 3 then either k satisfies the conditions listed above for the solubility of (1) or we know independently that (1) is soluble over k. In the former case it will again follow that (1) is soluble over k, and it is well known that this implies solubility over k_0. As was remarked above, we can assume that Condition 1 holds over k. Let Σ_2 be a finite set of places of k_0 which includes the archimedean places, the primes which divide 3 and the other primes of bad reduction for (1). Choose α in k_0 so that -3α is in $(k_0)_v^{*2}$ for every place v in Σ_2, including the archimedean ones, but -3α is not in k_0^{*2}. This implies that -3 is a square at every place v_1 of $k = k_0(\sqrt{\alpha})$ above a place in Σ_2, and therefore that every such v_1 splits in K/k where $K = k(\omega)$. We retain the C_v which we chose for Condition 2 over k_0; so the insolubility of each of Eqs. (32) for k follows from the corresponding statement for k_0. We can find a set of generators of the ideal class group of K which are first degree primes; taking $\mathcal{S}_1$ to be the union of these and the places of K which lie above places in Σ_2, we satisfy Condition 4. We have therefore satisfied (i) to (iii) above. Thus (1) is soluble in k and therefore also in k_0. □

6. Proof of Theorems 1 and 2

The condition appearing in Theorem 3, which has already been stated as Condition 5, is not very demanding. For a finite place $\mathfrak{p}$ which does not divide 3, it is easy to give a detailed analysis

of this condition; if $\mathfrak{p}|3$ the number of cases to be considered would become tedious, so we restrict the following discussion to places which do not divide 3. We can multiply Eq. (1) by a power of a uniformizing variable at $\mathfrak{p}$ before taking cubes out of the a_i. Using also symmetry, we have only the following cases to consider:

(i) $\mathfrak{p}|a_1$ and a_2, a_3, a_4 are in $\mathfrak{o}_\mathfrak{p}^*$. We can certainly take $C_\mathfrak{p} = a_2$, in which case the second Eq. (32) is insoluble and the first one is insoluble unless a_3/a_4 is in $k_\mathfrak{p}^{*3}$. If a_3/a_4 is in $k_\mathfrak{p}^{*3}$ we could instead take $C_\mathfrak{p} = a_1$ but we gain nothing by doing so.

(ii) $\mathfrak{p}\|a_1$, $\mathfrak{p}\|a_2$ and a_3, a_4 are in $\mathfrak{o}_\mathfrak{p}^*$. For local solubility of the system (17) at least one of a_1/a_2 and a_3/a_4 must be in $k_\mathfrak{p}^{*3}$. If both of them are in $k_\mathfrak{p}^{*3}$ then we can give $C_\mathfrak{p}$ any value in $\mathfrak{p}\mathfrak{o}_\mathfrak{p}^*$ or $\mathfrak{o}_\mathfrak{p}^*$; but both Eqs. (32) are then necessarily soluble. If for example a_1/a_2 is in $k_\mathfrak{p}^{*3}$ but a_3/a_4 is not, we must take $C_\mathfrak{p}$ in $\mathfrak{o}_\mathfrak{p}^*$; then the second Eq. (32) is soluble but the first is not. Similarly if a_3/a_4 is in $k_\mathfrak{p}^{*3}$ but a_1/a_2 is not, then we must take $C_\mathfrak{p}$ in $\mathfrak{p}\mathfrak{o}_\mathfrak{p}^*$ and the first Eq. (32) is soluble but the second is not.

(iii) $\mathfrak{p}\|a_1$, $\mathfrak{p}\|a_3$ and a_2, a_4 are in $\mathfrak{o}_\mathfrak{p}^*$. For local solubility of the system (17), at least one of a_1/a_3 and a_2/a_4 must be in $k_\mathfrak{p}^{*3}$. If both of them are in $k_\mathfrak{p}^{*3}$ then both Eqs. (32) will be soluble whenever both Eqs. (17) are. But if say a_1/a_3 is in $k_\mathfrak{p}^{*3}$ but a_2/a_4 is not, then we must take $C_\mathfrak{p} = a_1$ and neither Eq. (32) is soluble.

(iv) $\mathfrak{p}^2\|a_1$, $\mathfrak{p}\|a_2$ and a_3, a_4 are in $\mathfrak{o}_\mathfrak{p}^*$. For local solubility of the system (17), a_3/a_4 must be in $k_\mathfrak{p}^{*3}$ and we must choose $C_\mathfrak{p}$ to be a_1 or a_2. Now the first Eq. (32) is soluble, and the second one is soluble if and only if $a_1a_2a_3$ is in $k_\mathfrak{p}^{*3}$.

(v) $\mathfrak{p}^2\|a_1$, $\mathfrak{p}\|a_3$ and a_2, a_4 are in $\mathfrak{o}_\mathfrak{p}^*$. For local solubility of the system (17), a_2/a_4 must be in $k_\mathfrak{p}^{*3}$ and we must choose $C_\mathfrak{p} = a_2$. Now both Eqs. (32) are soluble if $a_1a_2a_3$ is in $k_\mathfrak{p}^{*3}$, and neither of them is soluble otherwise.

The reader will notice that if $\mathfrak{p}$ is in Σ_1 and does not divide 3 then both Eqs. (32) are soluble in $k_\mathfrak{p}$ if and only if (1) is birationally equivalent to a plane over $k_\mathfrak{p}$; compare Proposition 2 of [5]. This is unlikely to be a coincidence, but I have not been able to make serious use of it.

Theorem 1(i) is a special case of Theorem 3. For if $v = \mathfrak{p}_1$ we can choose $C_v = a_2$ to make the second Eq. (32) insoluble, and a similar argument with $v = \mathfrak{p}_3$ works for the first Eq. (32). Theorem 1(ii) follows from (i) above after permuting the subscripts if necessary; and Theorem 1(iii) follows similarly from (iii) and (v) above after taking account of the penultimate sentence in the previous paragraph.

We now turn to the proof of Theorem 2. Choose k as before. We can clearly assume that none of the b_i/b_j are in k^{*3}. I claim that after renumbering we can assume that the fields $K(\sqrt[3]{b_1/b_5})$ and $K(\sqrt[3]{b_2/b_3})$ are distinct. For if not, $K(\sqrt[3]{b_4/b_5})$ would be the same as each of the three fields $K(\sqrt[3]{b_i/b_j})$ with $i, j = 1, 2, 3$ and $i \neq j$. After interchange of b_4 and b_5 if necessary, this would imply that

$$b_4/b_5 = b_1/b_2 = b_2/b_3 \text{ as elements of } k^{*3};$$

and now $K(\sqrt[3]{b_1/b_5}) = K(\sqrt[3]{b_2/b_3})$ would imply that either b_2/b_5 or b_3/b_5 is in k^{*3}.

Hence we can find a prime $\mathfrak{P}_0$ of K at which 3 and all the b_i are units and which splits in $K(\sqrt[3]{b_1/b_5})$ but not in $K(\sqrt[3]{b_2/b_3})$; thus b_1/b_5 is in $K_{\mathfrak{P}_0}^{*3}$ but b_2/b_3 is not. Now the corresponding statements are true for $k_{\mathfrak{p}_0}^{*3}$ where $\mathfrak{p}_0$ is the prime in k below $\mathfrak{P}_0$. For each prime $\mathfrak{p}$ in k which is a prime of bad reduction of (3), choose $c_\mathfrak{p}$ in $k_\mathfrak{p}$ so that (3) has a solution in $k_\mathfrak{p}$ with $X_5 = c_\mathfrak{p}X_1$. Let c in k be such that c is close to each $c_\mathfrak{p}$ and $\mathfrak{p}_0\|(b_1 + c^3b_5)$. If we write $X_5 = cX_1$ in (3) we obtain an equation

$$\big(b_1 + c^3b_5\big)X_1^3 + b_2X_2^3 + b_3X_3^3 + b_4X_4^3 = 0 \tag{33}$$

which is soluble in k by Theorem 1(ii). For if $\mathfrak{p}$ is a prime of k at which (3) has good reduction, the same is true of $b_2X_2^3 + b_3X_3^3 + b_4X_4^3 = 0$; hence this equation is soluble in $k_\mathfrak{p}$ and so is (33). Since (33) is soluble in k, so is (3); and hence it is also soluble in k_0.

REFERENCES

[1] BENDER A.O., SIR SWINNERTON-DYER P., Solubility of certain pencils of curves of genus 1, and of the intersection of two quadrics in $\mathbf{P}^4$, *Proc. London Math. Soc.* **83** (3) (2001) 299–329.

[2] CASSELS J.W.S., Arithmetic on curves of genus 1, I. On a conjecture of Selmer, *J. Reine Angew. Math.* **202** (1959) 52–99.

[3] CASSELS J.W.S., GUY M.J.T., On the Hasse principle for cubic surfaces, *Mathematika* **13** (1966) 111–120.

[4] COLLIOT-THÉLÈNE J.-L., Surfaces cubiques diagonales, in: *Séminaire de théorie des nombres, Paris 1984–85*, Progress in Math., Vol. **63**, Birkhäuser, 1986, pp. 51–66.

[5] COLLIOT-THÉLÈNE J.-L., KANEVSKY D., SANSUC J.-J., Arithmétique des surfaces cubiques diagonales, in: *Diophantine Approximation and Transcendence Theory*, Springer Lecture Notes, Vol. **1290**, 1987, pp. 1–108.

[6] COLLIOT-THÉLÈNE J.-L., SKOROBOGATOV A.N., SIR SWINNERTON-DYER P., Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, *Invent. Math.* **134** (1998) 579–650.

[7] HASSE H., Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I, *Jahresbericht der D.M.V.* **35** (1926) 1–55.

[8] HEATH-BROWN D.R., The solubility of diagonal cubic diophantine equations, *Proc. London Math. Soc. (3)* **79** (1999) 241–259.

[9] KANEVSKY D., Application of the conjecture on the Manin obstruction to various Diophantine problems, *Astérisque* **147–148** (1987) 307–314.

[10] MILNE J.S., *Arithmetic Duality Theorems*, Academic Press, 1986.

[11] SELMER E.S., Sufficient congruence conditions for the existence of rational points on certain cubic surfaces, *Math. Scand.* **1** (1953) 113–119.

[12] SIR SWINNERTON-DYER P., Some applications of Schinzel's Hypothesis to Diophantine Equations, in: Györy, Iwaniec, Urbanowicz (Eds.), *Number Theory in Progress*, 1999.

(Manuscript received May 17, 2000;
accepted, after revision, October 12, 2000.)

Sir Peter SWINNERTON-DYER
Trinity College,
Cambridge CB2 1TQ, UK
E-mail: hpfs100@newton.cam.ac.uk