A NEW METHOD FOR CERTAIN DIOPHANTINE EQUATIONS

1. *Introduction.*
The original purpose of the research described in this article was to obtain results about Diophantine problems on rational surfaces — that is, surfaces defined over a field k which are birationally equivalent to $\mathbf{P}^2$ over the algebraic closure $\bar{k}$. (Throughout this article, K and k will always denote algebraic number fields, with respective rings of integers $\mathfrak{O}$ and $\mathfrak{o}$. Except in the phrase 'rational surface' as defined above, 'rational' will always mean defined over k.) But as often happens, the research turns out to be also applicable to other problems: in this case, to certain K3 surfaces. This is significant, because Diophantine problems on K3 surfaces have hitherto been almost wholly intractable. Much of the research, which is still ongoing, is joint with one or both of Jean-Louis Colliot-Thélène and Alexei Skorobogatov; and I am grateful to both of them for their constructive comments.

This article is almost self-contained; but for some definitions and comments the reader is advised to refer back to the previous article: 'Diophantine Equations: Progress and Problems.' Most of the results depend on one or both of two major conjectures. The first, which I shall refer to as Hypothesis Ш, is as follows:

> *If E is an elliptic curve defined over an algebraic number field K, then the Tate-Shafarevich group $Ш(E/K)$ is finite.*

The second, which is Schinzel's Hypothesis, is described in §2. But if one is content to study rational 0-cycles of degree 1 instead of rational points, then Schinzel's Hypothesis can almost always be replaced by Lemma 4. This illustrates a general truth: that one expects to have a more satisfactory theory for 0-cycles of degree 1 than for points, because the former are a coset of the group of 0-cycles of degree 0 whereas the set of rational points has in general no apparent structure. Unfortunately, most families $\mathcal{F}$ of varieties do not have the property that if V in $\mathcal{F}$ is defined over the algebraic number field k, and if V contains a 0-cycle of degree 1 defined over k, then $V(k)$ is not empty. One important family which does have this property consists of the Del Pezzo surfaces of degree 4. For a proof of this, and some applications of the associated ideas, see §8.

From the number-theoretic point of view, there are two kinds of rational surface defined over an algebraic number field k:

- Pencils of conics, given by an equation of the form

$$a_0(U,V)X_0^2 + a_1(U,V)X_1^2 + a_2(U,V)X_2^2 = 0 \qquad (1)$$

  where the $a_i(U,V)$ are homogeneous polynomials of the same degree with coefficients in k. Pencils of conics can be further classified according to the number of bad fibres, but in this article we shall not need to do so. If one assumes Schinzel's Hypothesis the obstructions to weak approximation and to the Hasse principle on pencils of conics are given by Theorem 1 in §4. The corresponding results for 0-cycles, which do not depend on any unproved hypotheses, can be found in and after Theorem 2.

- Del Pezzo surfaces of degree d, where $0 < d < 9$. Over $\mathbf{C}$, such a surface is obtained by blowing up $(9-d)$ points of $\mathbf{P}^2$ in general position. It is known that Del Pezzo surfaces of degree $d > 4$ over k satisfy the Hasse principle and weak approximation; indeed those of degree 5 necessarily contain rational points and are therefore birationally equivalent to $\mathbf{P}^2$ over k. Del Pezzo surfaces of degree 2 or 1 have no aesthetic merits and have attracted relatively little attention; it seems sensible to ignore them until the problems coming from those of degrees 4 and 3 have been solved. The Del Pezzo surfaces of degree 3 are the nonsingular cubic surfaces, which have an enormous but largely irrelevent literature; and those of degree 4 are the nonsingular intersections of two quadrics in $\mathbf{P}^4$. For historical reasons, attention has been concentrated on the Del Pezzo surfaces of degree 3; but the problems presented by those of degree 4 are simpler. That fact is illustrated in §8.

In both these cases the main conjecture, due to Colliot-Thélène and Sansuc, is that the only obstruction to either the Hasse principle or weak approximation is the Brauer-Manin obstruction. Unfortunately, in our present state of knowledge it seems very difficult to deduce anything from the absence of a Brauer-Manin obstruction; indeed the only paper I know of in which the Brauer-Manin obstruction plays a natural part in the argument is the proof by Salberger and Skorobogatov [11] that it is the only obstruction to weak approximation on Del Pezzo surfaces of degree 4. Usually, what one does is to obtain a sufficient condition for the Hasse principle, or a subset of $V(\mathbf{A})$ contained in the closure of $V(k)$; and one then compares the obstruction thus obtained with the Brauer-Manin obstruction. These notes are concerned with

the first half of this programme, so the Brauer-Manin obstruction will not be defined and will only be peripherally mentioned. For a fuller account of it, see [7] and [6].

Our proofs of results for pencils of conics depend in an essential way on the fact that the Hasse principle holds for conics, and indeed for all curves of genus 0. A Del Pezzo surface of degree 4 or 3 defined over k does contain an infinity of curves of genus 0 defined over k, but it appears that we can only find any of them explicitly if we already know at least one rational point on the surface. This seems to block any approach to the Hasse principle by the methods already described; and for rather deeper reasons it also appears to block any such approach to weak approximation on Del Pezzo surfaces of degree 3. One can prove weak approximation on Del Pezzo surfaces of degree 4 by these methods (and indeed without using Schinzel's Hypothesis), though the argument involves some additional complications; for this, see Theorem 10 in §8.

One is therefore led to study the existence of rational points on pencils of curves of genus 1. But here we run into a new complication, because the Hasse principle notoriously does not hold for curves of genus 1. There is however a weaker version which it is often possible to exploit. Most, but not all, of the known applications of the following lemma are when $n = 2$.

Lemma 1 *Let E be an elliptic curve defined over an algebraic number field k, and suppose that the Tate-Shafarevich group of E is finite and that for some $n > 1$ the image of the Mordell-Weil group of E in the n-Selmer group of E has index strictly less than n^2 in the latter. Then every curve which represents an element of order exactly n in the n-Selmer group contains a point defined over k.*

Proof By hypothesis the Tate-Shafarevich group is a torsion group, so by a theorem of Cassels there is a non-singular alternating form on it — and in particular on its n-torsion subgroup. Hence this subgroup must have an even number of generators of order n. It is given that this subgroup cannot have as many as two generators of order n, so it must have none. But the elements of the n-Selmer group which lie in the image of the Mordell-Weil group certainly contain points defined over k. □

Now suppose that we are given a pencil of curves C of genus 1, each of which is a 2-covering of its Jacobian J. To be able to apply this lemma, we need to be able to implement a 2-descent on every J. Because of this, the natural pencils to examine are those for which all the 2-division points of

each J are defined over its field of definition $k(J)$. To prove solubility of such a pencil of curves, it is then enough to find some C in the pencil such that the 2-Selmer group of the corresponding J is generated by C and the 2-coverings corresponding to the 2-division points. The general theory of 2-descents, in a form convenient for this application, is given in §5 and applied in §6. A particularly interesting example follows from the fact that the K3 surface

$$a_0X_0^4 + a_1X_1^4 + a_2X_2^4 + a_3X_3^4 = 0$$

can be fibred by curves of genus 1 of this kind, provided that

$$a_0a_1a_2a_3 \text{ is a square.} \tag{2}$$

This case is worked out in detail in §9, where (subject to the two major hypotheses stated above) necessary and sufficient conditions for solubility are obtained in the general case in which no $\pm a_ia_j$ is a square and $a_0a_1a_2a_3$ is not a fourth power. These conditions turn out to be just the Brauer-Manin conditions. To the best of my knowledge, this is the first significant solubility theorem for any family of K3 surfaces. Similar arguments could undoubtedly be applied to the remaining special cases, but the method makes essential use of (2). Numerical evidence suggests that if we drop (2) then the Brauer-Manin conditions cease to be sufficient.

By means of an additional trick, we can actually apply Lemma 1 when we only know that J has one 2-division point defined over $k(J)$; this trick is given in §7.2, and its application to Del Pezzo surfaces of degree 4 is in §8. The ideas underlying Lemma 1 can also be applied to diagonal cubic surfaces

$$a_0X_0^3 + a_1X_1^3 = a_2X_2^3 + a_3X_3^3;$$

but now there are considerable additional complications, some but not all of which are due to the fact that we have to carry out descent simultaneously on two unrelated elliptic curves. A very brief summary of this work is given in §7.1.

2. *Schinzel's Hypothesis and Salberger's device.*
Schinzel's Hypothesis gives a conjectural answer to the following question: given finitely many polynomials $F_1(X), \dots, F_n(X)$ in $\mathbf{Z}[X]$ with positive leading coefficients, is there an arbitrarily large integer x at which they all take prime values? There are two obvious obstructions to this:

- One or more of the $F_i(X)$ may factorize in $\mathbf{Z}[X]$.
- There may be a prime p such that for any value of x mod p at least one of the $F_i(x)$ is divisible by p.

If the congruence $F_i(x) \equiv 0 \bmod p$ is non-trivial, it has at most $\deg(F_i)$ solutions; so the second obstruction can only happen for $p \leq \sum \deg(F_i)$ or if p divides every coefficient of some F_i. Schinzel's Hypothesis is that these are the only obstructions: in other words, if neither of them happens then we can choose an arbitrarily large x so that every $F_i(x)$ is a prime.

Serre deduced the corresponding result over any algebraic number field; here we shall in addition need to approximate to the arguments at finitely many bad places. In most applications there is a predetermined set $\mathfrak{B}$ of bad places, and we need to impose local conditions on x at some or all of them. But these conditions constrain the values of the $F_i(x)$ at those places, and therefore we cannot necessarily require these values to be units at the bad primes; nor in the applications will we need to. Because in this article we try to preserve homogeneity as far as possible, we have stated Lemma 2 in a form which applies to homogeneous polynomials G_i in two variables; but the reader who wishes to do so will have no difficulty in stating and proving the corresponding (stronger) result for polynomials in one variable. Just as with the original version of Schinzel's Hypothesis, provided that the coefficients of G_i for each i have no common factor we need only verify the existence of the $y_\mathfrak{p}, z_\mathfrak{p}$ in the statement of the lemma when the absolute norm of $\mathfrak{p}$ does not exceed $\sum \deg(G_i)$.

Lemma 2 *Let k be an algebraic number field and $\mathfrak{o}$ the ring of integers of k. Let $G_1(Y,Z), \dots, G_n(Y,Z)$ be homogeneous irreducible elements of $\mathfrak{o}[Y,Z]$ and $\mathfrak{B}$ a finite set of primes of k. Suppose that for each $\mathfrak{p}$ not in $\mathfrak{B}$ there exist $y_\mathfrak{p}, z_\mathfrak{p}$ in $\mathfrak{o}$ such that none of the $G_i(y_\mathfrak{p}, z_\mathfrak{p})$ is in $\mathfrak{p}$. For each $\mathfrak{p}$ in $\mathfrak{B}$, let $V_\mathfrak{p}$ be a non-empty open subset of $k_\mathfrak{p} \times k_\mathfrak{p}$; and for each infinite place v of k let V_v be a non-empty open subset of k_v^*. Assume Schinzel's Hypothesis; then there is a point $\eta \times \zeta$ in $k^* \times k^*$, with η, ζ integral outside $\mathfrak{B}$, such that*

- *$\eta \times \zeta$ lies in each $V_{\mathfrak{p}}$;*
- *η/ζ lies in each V_v;*
- *each ideal $(G_i(\eta, \zeta))$ is the product of a prime ideal not in $\mathfrak{B}$ and possibly powers of primes in $\mathfrak{B}$.*

Proof Choose α, β in $\mathfrak{o}$ so that α/β lies in V_v for each infinite place v and no $G_i(\alpha, \beta)$ vanishes. We can repeatedly adjoin a further prime $\mathfrak{p}$ to $\mathfrak{B}$ provided we define the corresponding $V_{\mathfrak{p}}$ to be the set of all $y \times z$ in $\mathfrak{o}_{\mathfrak{p}} \times \mathfrak{o}_{\mathfrak{p}}$ such that each $G_i(y, z)$ is a unit at $\mathfrak{p}$. We can therefore assume that $\mathfrak{B}$ contains all primes $\mathfrak{p}$ such that

- the absolute norm of $\mathfrak{p}$ is not greater than $[k : \mathbf{Q}] \sum \deg(G_i)$; or
- $\mathfrak{p}$ divides any $G_i(\alpha, \beta)$.

Let $\mathcal{B}$ be the set of primes in $\mathbf{Q}$ which lie below some prime of $\mathfrak{B}$, and further adjoin to $\mathfrak{B}$ all the primes of k not already in $\mathfrak{B}$ which lie above some prime of $\mathcal{B}$. By the Chinese Remainder Theorem we can choose η_0, ζ_0 in k, integral outside $\mathfrak{B}$ and such that each $G_i(\eta_0, \zeta_0)$ is nonzero and $\eta_0 \times \zeta_0$ lies in $V_{\mathfrak{p}}$ for each $\mathfrak{p}$ in $\mathfrak{B}$. For reasons which will become clear after (3), we also need to ensure that $\beta\eta_0 \neq \alpha\zeta_0$; this can be done by varying η_0 or ζ_0 by a suitable element of $\mathfrak{o}$ divisible by large powers of each $\mathfrak{p}$ in $\mathfrak{B}$. As an ideal, write

$$(G_i(\eta_0, \zeta_0)) = \mathfrak{a}_i \mathfrak{b}_i$$

where the prime factors of each $\mathfrak{a}_i$ are outside $\mathfrak{B}$ and those of each $\mathfrak{b}_i$ are in $\mathfrak{B}$; thus $\mathfrak{a}_i$ is integral. Let N_i be the absolute norm of $\mathfrak{b}_i$. Now choose $\gamma \neq 0$ in $\mathfrak{o}$ to be a unit at all the primes outside $\mathfrak{B}$ which divide any $G_i(\eta_0, \zeta_0)$ and to be divisible by such large powers of each $\mathfrak{p}$ in $\mathfrak{B}$ that

$$\eta \times \zeta = (\alpha\gamma\xi + \eta_0) \times (\beta\gamma\xi + \zeta_0)$$

is in $V_{\mathfrak{p}}$ for all $\xi \in \mathfrak{o}$ and all $\mathfrak{p} \in \mathfrak{B}$, and that if we write

$$g_i(X) = G_i(\alpha\gamma X + \eta_0, \beta\gamma X + \zeta_0), \tag{3}$$

then every coefficient of $g_i(X)$ is divisible by at least as great a power of $\mathfrak{p}$ as is $\mathfrak{b}_i$. We have arranged that the two arguments of G_i in (3), considered as linear forms in X, are not proportional; thus if $g_i(X)$ factorizes in $k[X]$

then $G_i(\alpha\gamma U + \eta_0 V, \beta\gamma U + \zeta_0 V)$ would factorize in $k[U, V]$, contrary to the irreducibility of $G_i(Y, Z)$. We shall also require for each i that $g_i(X)$ is prime to all its conjugates as elements of $\bar{k}[X]$; since the zeros of $g_i(X)$ have the form $\gamma^{-1}\xi_{ij}$ for some ξ_{ij} independent of γ, this merely requires the ratios of γ to its conjugates to avoid finitely many values. Write

$$R_i(X) = \mathrm{Norm}_{k(X)/\mathbf{Q}(X)}(g_i(X))/N_i;$$

then $R_i(X)$ has all its coefficients integral, for at each prime it is the norm of a polynomial with locally integral coefficients. An irreducible factor of $R_i(X)$ in $\mathbf{Q}[X]$ cannot be prime to $g_i(X)$, because then it would also be prime to all the conjugates of $g_i(X)$ and therefore to their product — which is absurd. If $R_i(X)$ had two coprime factors in $\mathbf{Q}[X]$, their highest common factors with $g_i(X)$ would be nontrivial coprime factors of $g_i(X)$ in $k[X]$, whence $g_i(X)$ would not be irreducible in $k[X]$. Finally, $R_i(X)$ cannot have a repeated factor because the conjugates of $g_i(X)$ are pairwise coprime. So $R_i(X) = A_i H_i(X)$ in $\mathbf{Z}[X]$, with $H_i(X)$ irreducible. Clearly we can require the leading coefficient of each $H_i(X)$ to be positive. But the only primes which divide the constant term in $R_i(X)$ are the primes outside $\mathcal{B}$ which divide $G_i(\eta_0, \zeta_0)$, and none of them divide the leading coefficient of $R_i(X)$; hence $A_i = \pm 1$. Now apply Schinzel's Hypothesis to the $H_i(X)$, which we can do because no $H_i(0)$ is divisible by any prime in $\mathcal{B}$. But if $H_i(x)$ is equal to a prime not in $\mathcal{B}$ then the ideal $(g_i(x))$ must be equal to the product of $\mathfrak{b}_i$ and a prime ideal not in $\mathfrak{B}$. □

If we are content to obtain results about 0-cycles of degree 1 instead of results about points, we can replace Schinzel's Hypothesis by an argument which depends on the partial fraction formula (5); its use in this context was pioneered by Salberger. Of the various versions of the consequent algorithm, Lemma 4 seems the simplest, both in its proof and in the way in which it is used; in particular, it does not involve an auxiliary set of primes and its proof does not depend on a deep result of Waldschmidt. We need a preliminary lemma about approximation.

Lemma 3 *Let L be an algebraic number field, $\mathfrak{B}$ a finite set of places of L and $\mathfrak{S}$ a finite set of primes of L not necessarily disjoint from $\mathfrak{B}$. Let $b > 1$ be in $\mathbf{Z}$ and such that no prime of L which divides b is in $\mathfrak{B}$. Let $M > 0$ be a rational integer and for each v in $\mathfrak{B}$ let ξ_v be in L_v. Then there exists ξ in L^* as close as we like to each ξ_v and such that $\xi = \alpha\gamma^M$, where (α) is*

the product of a first degree prime $\mathfrak{p}$ *not in* $\mathfrak{B} \cup \mathfrak{S}$ *and primes in* $\mathfrak{B}$*, and* $\gamma = \gamma_1/\gamma_2$ *for coprime integers* γ_1, γ_2 *such that the prime factorization of* γ_1 *does not include any prime in* $\mathfrak{B} \cup \mathfrak{S} \cup \{\mathfrak{p}\}$ *and the only primes which divide* γ_2 *also divide* b*.*

Proof. By Dirichlet's theorem on primes in arithmetic progression, we can choose $\mathfrak{p}$ and α as in the statement of the lemma so that α is as close as we like to ξ_v for each finite v in $\mathfrak{B}$ and $\xi_v/\alpha > 0$ for each real v in $\mathfrak{B}$. For each infinite v in $\mathfrak{B}$ we choose γ_v in L_v so that $\gamma_v^M = \xi_v/\alpha$. Using weak approximation, choose γ' in L, a unit at every finite prime in $\mathfrak{B} \cup \mathfrak{S} \cup \{\mathfrak{p}\}$, so that γ' is arbitrarily close to 1 at every finite prime in $\mathfrak{B}$ and arbitrarily close to γ_v at every infinite place v in $\mathfrak{B}$. By writing $\gamma' b^N$ for large enough N in terms of a base for $\mathfrak{o}_L/\mathbf{Z}$ and then changing the coefficients by elements of $\mathbf{Q}$ which are small at each finite prime in $\mathcal{B} \cup \mathcal{S}$ and bounded at every infinite place in $\mathcal{B}$, we can obtain an integer γ_1 which is prime to $\mathcal{S} \cup \{\mathfrak{p}\}$ and to b and close to $\gamma' b^N$ at every place in $\mathcal{B}$. Now take $\gamma_2 = b^N$; then $\xi = \alpha\gamma^M$ satisfies all our requirements. □

For the statement and proof of the following lemma, we shall call a place of k *bad* if it lies in $\mathcal{B}$ or divides b; and we shall call a place in $\mathbf{Q}$ or in a field containing k *bad* if it lies below or above a bad place of k. For our purposes, the most important difference between places in $\mathcal{B}$ and primes dividing b is that the latter have no approximation conditions associated with them.

Lemma 4 *Let* k *be an algebraic number field and* $P_1(X), \ldots, P_n(X)$ *monic irreducible non-constant polynomials in* $k[X]$*; and let* $N \geq \sum \deg(P_i)$ *be a given integer. Let* $\mathfrak{B}$ *be a finite set of places of* k *which contains the infinite places, the primes which divide* 2*, the primes at which some coefficient of some* P_i *is not integral and any other primes* $\mathfrak{p}$ *at which* $\prod P_i(X)$ *does not remain separable when reduced* mod $\mathfrak{p}$*. Let* b *be as in Lemma* 3*. For each* v *in* $\mathfrak{B}$ *let* U_v *be a non-empty open set of separable monic polynomials of degree* N *in* $k_v[X]$*. Let* $M > 0$ *be a fixed rational integer. Then we can find an irreducible monic polynomial* $G(X)$ *in* $k[X]$ *of degree* N *which lies in each* U_v *and for which* λ*, the image of* X *in* $K = k[X]/G(X)$*, satisfies*

$$(P_i(\lambda)) = \mathfrak{P}_i \mathfrak{A}_i \mathfrak{C}_i^M \tag{4}$$

for each i*, where the* $\mathfrak{P}_i$ *are distinct first degree primes in* K *not lying above any prime in* $\mathfrak{B}$*, the* $\mathfrak{A}_i$ *are products of bad primes in* K *and the* $\mathfrak{C}_i$ *are integral ideals in* K*. Moreover we can arrange that* $\lambda = \alpha/\beta$ *where* α *is integral and* β *is an integer all of whose prime factors are bad.*

Proof We shall need to apply Lemma 3 repeatedly with the same value of M as in Lemma 4. We can assume, after adding a constant to X if necessary, that none of the $P_i(X)$ is a multiple of X. Write $R(X) = \prod P_i(X)$ and $R_i(X) = R(X)/P_i(X)$. Any polynomial $G(X)$ in $k[X]$ can be written in just one way in the form

$$G(X) = R(X)Q(X) + \sum R_i(X)\psi_i(X) \tag{5}$$

with $\deg \psi_i < \deg P_i$; for if λ_i is a zero of $P_i(X)$ this is just the classical partial fractions formula

$$\frac{G(X)}{\prod P_i(X)} = Q(X) + \sum \frac{\psi_i(X)}{P_i(X)}$$

with $\psi_i(\lambda_i) = G(\lambda_i)/R_i(\lambda_i)$. This property determines for each i a unique $\psi_i(X)$ in $k[X]$ of degree less than $\deg P_i$. The same result holds over any k_v. If the coefficients of G are integral at v, for some v not in $\mathfrak{B}$, then so are those of Q and each ψ_i because R and the R_i are monic and $R_i(\lambda_i)$ is a unit outside $\mathfrak{B}$. For each v in $\mathfrak{B}$ let $G_v(X)$ be a polynomial of degree N lying in U_v, and write

$$G_v(X) = R(X)Q_v(X) + \sum R_i(X)\psi_{iv}(X)$$

with $\deg \psi_{iv} < \deg P_i$. We adjoin to $\mathfrak{B}$ a further finite place w at which b is a unit, and associate with it a monic irreducible polynomial $G_w(X)$ in $k_w[X]$ of degree N; the only purpose of G_w is to ensure that the $G(X)$ which we shall construct is irreducible over k. We build $G(X)$, close to $G_v(X)$ for every $v \in \mathfrak{B}$ including w, in the following manner.

For the first step let $k_i = k[X]/P_i(X)$ and for each $v \in \mathfrak{B}$ let ϕ_{iv} be the class of ψ_{iv} in $k_v[X]/P_i(X) = k_i \otimes_k k_v$. Take $\mathfrak{S}$ to consist of those primes in k at which the constant terms of the $P_i(X)$ are not all units. We apply Lemma 3 to each set of ϕ_{iv} in turn, replacing L by k_i and $\mathfrak{B}$ and $\mathfrak{S}$ by the sets of places of k_i which lie above $\mathfrak{B}$ and $\mathfrak{S}$ respectively; let ϕ_i be the element of k_i thus obtained, and let $\mathfrak{P}_i$ be the associated prime in k_i. Let $\psi_i'(X)$ be the unique polynomial in $k[X]$ with $\deg \psi_i' < \deg P_i$ whose class in k_i is ϕ_i. Clearly $\psi_i'(X)$ is arbitrarily close to each $\psi_{iv}(X)$, and its coefficients are integers outside $\mathfrak{B}$ because $\mathfrak{B}$ contains all the primes which ramify in k_i/k. Now choose positive c, T in $\mathbf{Z}$ so that c is a unit at all bad primes, divisible by all the primes outside $\mathfrak{B} \cup \{\mathfrak{P}_i\}$ which divide the numerator of any ϕ_i,

and close to b^T at the real place and at all the primes below primes in $\mathfrak{B}$. Let $\psi_i(X) = (c/b^T)^M \psi_i'(X)$.

We now choose $Q(X)$ to be close to $Q_v(X)$ for each v in $\mathfrak{B}$, and to be such that each coefficient other than the leading coefficient (which is 1) is integral except perhaps at bad primes and is divisible by c. We can do this by an argument like, but very much simpler than, that in the proof of Lemma 3. This construction ensures that $G(X)$ is monic and arbitrarily close to each $G_v(X)$ including $G_w(X)$. The assumptions made about $G_w(X)$ ensure that $G(X)$ is irreducible in k_w and therefore in k. Moreover, the coefficients of $Q(X)$ are integers except perhaps at bad primes; and since $G(X)$ is monic the denominator of any $P_i(\lambda)$ only contains bad primes. A consequence of the choice of $\mathfrak{S}$ is that every λ_i, and therefore every $Q(\lambda_i)$, is prime to c.

We have still to prove (4). Let $\mathfrak{p}_i$ be the prime in k below $\mathfrak{P}_i$. By computing the resultant of $P_i(X)$ and $G(X)$ in two different ways, we obtain

$$\mathrm{Norm}_{K/k} P_i(\lambda) = \pm \mathrm{Norm}_{k_i/k} G(\lambda_i) = \pm \mathrm{Norm}_{k_i/k}(\phi_i R_i(\lambda_i)) \tag{6}$$

where λ_i is a zero of $P_i(X)$. By hypothesis $R_i(\lambda_i)$ is a unit at every place of $k(\lambda_i)$ which does not lie above a place in $\mathfrak{B}$; and we have arranged that the denominator of $\mathrm{Norm}_{k_i/k}\phi_i$ is only divisible by bad primes, and its numerator is the product of the first degree prime $\mathfrak{p}_i$, powers of primes in $\mathfrak{B}$ and Mth powers of norms of primes which come from the $\mathfrak{C}_i$ of Lemma 3. Also λ, and therefore $P_i(\lambda)$, is integral outside bad primes in K. None of the latter lie above $\mathfrak{p}_i$. Hence $P_i(\lambda)$ is an integer at each prime of K lying above $\mathfrak{p}_i$. It follows that the ideal $(P_i(\lambda))$ is divisible by just one prime of K above $\mathfrak{p}_i$, and that to the first power. It only remains to show that, apart from this prime and bad primes, what we have is an Mth power.

Let L be a splitting field for all the $P_i(X)$ and let $\mathfrak{P}$ be a prime in $L(\lambda)$ which divides the numerator of $P_i(\lambda)$. By (6) and the remarks on either side of it, $\mathfrak{P}$ must divide $\mathrm{Norm}_{k_i/k}(\phi_i)$ and therefore must divide c. Hence

$$\tilde{G}(X) = \tilde{R}(X)\tilde{Q}(X) \tag{7}$$

where the tilde denotes reduction mod $\mathfrak{P}$ of the coefficients. But the construction of $Q(X)$ has ensured that the resultant of $Q(X)$ and $R(X)$, which is $\pm \prod_i \mathrm{Norm}_{k_i/k}(Q(\lambda_i))$, is prime to c; hence $\tilde{R}(X)$ and $\tilde{Q}(X)$ are coprime. Moreover $\tilde{R}(X)$ is a product of distinct linear factors over the residue field of L at $\mathfrak{P}$. It follows that (7) can be lifted to a factorization of $G(X)$ in the completion of $L(\lambda)$ at $\mathfrak{P}$; and the roots of $G(X)$ in this field consist of one

near each root of each $P_i(X)$ together with roots which come (after a further field extension) from the lift of $\tilde{Q}(X)$. The latter are not close to any root of any $P_i(X)$.

I now claim that the power of $\mathfrak{P}$ which divides $P_i(\lambda)$ is $\mathfrak{P}^m$ where m is a multiple of M. For if λ is not close to a root of $P_i(X)$ then $m = 0$. On the other hand, (5) can be written

$$G(X) = R_i(X)\psi_i(X) + f_i(X)P_i(X)$$

where

$$f_i(X) = R_i(X)Q(X) + \sum_{j \neq i} \psi_j(X)R_j(X)/P_i(X).$$

By construction, if λ is close to a root of $P_i(X)$ then $f_i(\lambda)$ is a unit at $\mathfrak{P}$, as is $R_i(\lambda)$. If λ_i is that root of $P_i(X)$ which is close to λ, then the standard successive approximation process shows that $\lambda - \lambda_i$ has the same valuation as $\psi_i(\lambda_i) = \phi_i$; and by construction $\mathfrak{P}^m \| \phi_i$ where $M|m$. It follows that $\mathfrak{P}^m \| P_i(\lambda)$ with $M|m$, as claimed, in both cases.

Now let $\mathfrak{p}$ be a prime in k which divides c, and let $\mathfrak{q}$ be any prime of $k(\lambda)$ above $\mathfrak{p}$. The factors of $P_i(\lambda)$ coming from primes of $L(\lambda)$ above $\mathfrak{q}$ have the form

$$\prod_{\mathfrak{P}|\mathfrak{q}} \mathfrak{P}^{m(\mathfrak{P})} \text{ where each } m(\mathfrak{P}) \text{ is divisible by } M. \tag{8}$$

This is equal to the corestriction of $\mathfrak{q}^n$, where $\mathfrak{q}^n$ is the exact power of $\mathfrak{q}$ which divides $P_i(\lambda)$. But the extension $L(\lambda)/k(\lambda)$ is unramified at $\mathfrak{q}$, because it is only ramified at places above places in $\mathfrak{B}$. Hence each $m(\mathfrak{P})$ in (8) is equal to n, and so n is divisible by M. This holds for all primes in $k(\lambda)$ which divide c. □

3. *The Legendre-Jacobi function.*
If α, β are elements of k^* and v is a place of k, the *Hilbert symbol* $(\alpha, \beta)_v$ is defined by

$$(\alpha, \beta)_v = \begin{cases} 1 & \text{if } \alpha X^2 + \beta Y^2 = Z^2 \text{ is soluble in } k_v, \\ -1 & \text{otherwise.} \end{cases}$$

The Hilbert symbol is symmetric in α, β. Its principal properties are

- $(\alpha_1\alpha_2, \beta)_v = (\alpha_1, \beta)_v(\alpha_2, \beta)_v$ and $(\alpha, \beta_1\beta_2)_v = (\alpha, \beta_1)_v(\alpha, \beta_2)_v$;
- for fixed α, β, $(\alpha, \beta)_v = 1$ for almost all v, and $\prod(\alpha, \beta)_v = 1$ where the product is taken over all places v of k.

The first of these can be deduced from symmetry and

$$(Z_1^2 - \beta Y_1^2)(Z_2^2 - \beta Y_2^2) = (Z_1Z_2 + \beta Y_1Y_2)^2 - \beta(Y_1Z_2 + Y_2Z_1)^2.$$

The second is one of the main results of class field theory.

Many of the proofs in these notes use the Legendre-Jacobi function L, which is a mild modification of a function (also called L) which was defined in rather crude form in [13] and more correctly in [14]. Let $F(U, V), G(U, V)$ be homogeneous coprime square-free polynomials in $k[U, V]$. Let $\mathcal{B}$ be a finite set of places of k containing the infinite places, the primes dividing 2, those at which any coefficient of F or G is not integral, and any other primes $\mathfrak{p}$ at which FG does not remain separable when reduced mod $\mathfrak{p}$. Note that we do not assume that $\mathcal{B}$ contains a base for the ideal class group of k.

Let $\mathcal{N}^2 = \mathcal{N}^2(k)$ be the set of $\alpha \times \beta$ with α, β integral and coprime outside $\mathcal{B}$, and let $\mathcal{N}^1 = \mathcal{N}^1(k)$ be $k \cup \{\infty\}$. For $\alpha \times \beta$ in $\mathbf{A}^2(k)$ with α, β not both zero, we shall consistently write $\lambda = \alpha/\beta$ with λ in $\mathcal{N}^1(k)$. Provided $F(\alpha, \beta)$ and $G(\alpha, \beta)$ are nonzero, we define the function

$$L(\mathcal{B}; F, G; \alpha, \beta) : \ \alpha \times \beta \mapsto \prod_{\mathfrak{p}} (F(\alpha, \beta), G(\alpha, \beta))_{\mathfrak{p}} \tag{9}$$

on $\mathcal{N}^2$, where the outer bracket on the right is the multiplicative Hilbert symbol and the product is taken over all primes $\mathfrak{p}$ of k outside $\mathcal{B}$ which divide $G(\alpha, \beta)$. By the definition of $\mathcal{B}$, $F(\alpha, \beta)$ is a unit at any such prime. Clearly we can restrict the product in (9) to those $\mathfrak{p}$ which divide $G(\alpha, \beta)$ to an odd power; thus we can also write it as $\prod \chi_{\mathfrak{p}}(F(\alpha, \beta))$ where $\chi_{\mathfrak{p}}$ is

the quadratic character mod $\mathfrak{p}$ and the product is taken over all $\mathfrak{p}$ outside $\mathcal{B}$ which divide $G(\alpha,\beta)$ to an odd power. This relationship with the quadratic residue symbol underlies the proof of Lemma 5. The function L does depend on $\mathcal{B}$, but the effect on the right hand side of (9) of increasing $\mathcal{B}$ is obvious. Some of the more interesting properties of L only hold when $\deg F$ is even, but this usually holds in applications; this parity condition did not appear in [14], but it is already needed if we are to make use of the results of [7].

In the course of the proofs, however, we need to consider functions (9) with $\deg F$ odd; and for this reason it is expedient to introduce

$$M(\mathcal{B};F,G;\alpha,\beta) = L(\mathcal{B};F,G;\alpha,\beta)(L(\mathcal{B};U,V;\alpha,\beta))^{(\deg F)(\deg G)}.$$

Here of course $L(\mathcal{B};U,V;\alpha,\beta) = \prod(\alpha,\beta)_{\mathfrak{p}}$ taken over all $\mathfrak{p}$ outside $\mathcal{B}$ which divide β and therefore do not divide α.

Lemma 5 *The value of M is continuous in the topology induced on $\mathcal{N}^2$ by $\mathcal{B}$. For each v in $\mathcal{B}$ there is a function $m(v;F,G;\alpha,\beta)$ with values in $\{\pm 1\}$ which is continuous on $\mathcal{N}^2$ in the v-adic topology, such that*

$$M(\mathcal{B};F,G;\alpha,\beta) = \prod_{v\in\mathcal{B}} m(v;F,G;\alpha,\beta). \tag{10}$$

.

Proof If $\deg F$ is even, so that $M = L$, the neatest proof of the lemma is by means of the evaluation formula in [7], Lemma 7.2.4. When $\deg G$ is even but $\deg F$ may not be, the result follows from (12), and (11) then gives the general case. (The proof in [7] is for $k = \mathbf{Q}$, but there is not much difficulty in modifying it to cover all k.) However, the proof which we shall give, using the ideas of [14], provides a more convenient method of evaluation.

For this proof we have to impose on $\mathcal{B}$ the additional condition that it contains all primes whose absolute norm does not exceed $\deg(FG)$. As the proof in [7] shows, this condition is not needed for the truth of Lemma 5 itself; but we use it in the proof of (16) below, and the latter is crucial to the subsequent argument. In any case, to classify all small enough primes as bad is quite usual. We repeatedly use the fact that $L(\mathcal{B};F,G)$ and $M(\mathcal{B};F,G)$ are multiplicative in both F and G; the effect of this is that we can reduce to the case when both F and G are irreducible in $\mathfrak{o}_{\mathcal{B}}[U,V]$, where $\mathfrak{o}_{\mathcal{B}}$ is the ring of elements of k integral outside $\mathcal{B}$. Introducing M and dropping the

parity condition on $\deg F$ are not real generalizations since if we increase $\mathcal{B}$ so that the leading coefficient of F is a unit outside $\mathcal{B}$ then

$$M(\mathcal{B}; F, G) = L(\mathcal{B}; F, GV^{\deg G}) \tag{11}$$

by (13), and we can apply (12) to the right hand side.

It follows from the product formula for the Hilbert symbol that

$$L(\mathcal{B}; f, g; \alpha, \beta)L(\mathcal{B}; g, f; \alpha, \beta) = \prod_{v \in \mathcal{B}} (f(\alpha, \beta), g(\alpha, \beta))_v, \tag{12}$$

provided that $f(\alpha, \beta)$, $g(\alpha, \beta)$ are nonzero. The right hand side of (12) is the product of continuous terms each of which only depends on a single v in $\mathcal{B}$. This formula enables us to interchange F and G when we want to, and in particular to require that $\deg F \geq \deg G$ in the reduction process which follows. We also have

$$L(\mathcal{B}; f, g; \alpha, \beta) = L(\mathcal{B}; f - gh, g; \alpha, \beta) \tag{13}$$

for any homogeneous h in $k[U, V]$ with $\deg h = \deg f - \deg g$ provided the coefficients of h are integral outside $\mathcal{B}$, because corresponding terms in the two products are equal. Both (12) and (13) also hold for M.

We deal first with two special cases:

- G is a constant. Now $M(\mathcal{B}; F, G) = 1$ because all the prime factors of G must be in $\mathcal{B}$, so that $M(\mathcal{B}; F, G) = L(\mathcal{B}; F, G)$ and the product in the definition of $L(\mathcal{B}; F, G)$ is empty.
- $G = V$. Choose H so that $F - GH = \gamma U^{\deg F}$ for some nonzero γ. Now $M(\mathcal{B}; F, G) = 1$ follows from the previous case and (13), since all the prime factors of γ must be in $\mathcal{B}$.

We now argue by induction on $\deg(FG)$. Since we can assume that F and G are irreducible, we need only consider the case when

$$\deg F \geq \deg G > 0, \quad G = \gamma U^{\deg G} + \ldots, \quad F = \delta U^{\deg F} + \ldots$$

for some nonzero γ, δ. Let $\mathcal{B}_1$ be obtained by adjoining to $\mathcal{B}$ those primes of k not in $\mathcal{B}$ at which γ is not a unit. By (13) we have

$$M(\mathcal{B}_1; F, G) = M(\mathcal{B}_1; F - \gamma^{-1}\delta G U^{\deg F - \deg G}, G). \tag{14}$$

By taking a factor V out of the middle argument on the right, and using (12), the second special case above and the induction hypothesis, we see that $M(\mathcal{B}_1; F, G)$ is continuous in the topology induced by $\mathcal{B}_1$ and is a product taken over all v in $\mathcal{B}_1$ of continuous terms each one of which depends on only one of the v. Hence the same is true of $M(\mathcal{B}; F, G)$, because this differs from $M(\mathcal{B}_1; F, G)$ by finitely many continuous factors, each of which depends only on one prime in $\mathcal{B}_1 \setminus \mathcal{B}$.

But $\mathcal{B}_1 \setminus \mathcal{B}$ only contains primes whose absolute norm is greater than $\deg(FG)$. Thus by an integral unimodular transformation from U, V to U, V_1 we can arrange that $G = \gamma_1 U^{\deg G} + \dots$ and $F = \delta_1 U^{\deg F} + \dots$ where γ_1 is a unit at each prime in $\mathcal{B}_1 \setminus \mathcal{B}$. Let $\mathcal{B}_2$ be obtained from $\mathcal{B}$ by adjoining all the primes at which γ_1 is not a unit; then $M(\mathcal{B}; F, G)$ has the same properties with respect to $\mathcal{B}_2$ that we have already shown that it has with respect to $\mathcal{B}_1$. Since $\mathcal{B}_1 \cap \mathcal{B}_2 = \mathcal{B}$, this implies that $M(\mathcal{B}; F, G)$ already has these properties with respect to $\mathcal{B}$. □

Of course there will be finitely many values of α/β for which the right hand side of (12) appears to be indeterminate; but by means of a preliminary linear transformation on U, V one can in fact ensure that the formula (10) is meaningful except when $F(\alpha, \beta)$ or $G(\alpha, \beta)$ vanishes.

When $\deg F$ is even, the value of $L(\mathcal{B}; F, G; \alpha, \beta)$ is already determined by $\lambda = \alpha/\beta$ regardless of the values of α and β separately; here λ lies in $k \cup \{\infty\}$ with the roots of $F(\lambda, 1)$ and $G(\lambda, 1)$ deleted. We shall therefore also write this function as $L(\mathcal{B}; F, G; \lambda)$. But note that it is not necessarily a continuous function of λ; see the discussions in [13] and §9 of [7], or Lemma 8 below. Moreover if $\mathcal{B}$ does not contain a base for the ideal class group of k then not all elements of $k \cup \{\infty\}$ can be written in the form α/β with α, β integers coprime outside $\mathcal{B}$; so we have not yet defined $L(\mathcal{B}; F, G; \lambda)$ for all λ. To go further in the case when $\deg F$ is even, we modify the definition (9) so that it extends to all $\alpha \times \beta$ in $k \times k$ such that $F(\alpha, \beta)$ and $G(\alpha, \beta)$ are nonzero. For any such α, β and any $\mathfrak{p}$ not in $\mathcal{B}$, choose $\alpha_\mathfrak{p}, \beta_\mathfrak{p}$ integral at $\mathfrak{p}$, not both divisible by $\mathfrak{p}$ and such that $\alpha/\beta = \alpha_\mathfrak{p}/\beta_\mathfrak{p}$. Write

$$L(\mathcal{B}; F, G; \alpha, \beta) = \prod (F(\alpha_\mathfrak{p}, \beta_\mathfrak{p}), G(\alpha_\mathfrak{p}, \beta_\mathfrak{p}))_\mathfrak{p} \tag{15}$$

where the product is taken over all $\mathfrak{p}$ not in $\mathcal{B}$ such that $\mathfrak{p} | G(\alpha_\mathfrak{p}, \beta_\mathfrak{p})$. This is a finite product whose value does not depend on the choice of the $\alpha_\mathfrak{p}$ and $\beta_\mathfrak{p}$; indeed it only depends on $\lambda = \alpha/\beta$ and when α, β are integers coprime outside $\mathcal{B}$ it is the same as the function given by (9). Thus we can again

write it as $L(\mathcal{B}; F, G; \lambda)$. This generalization is not really needed until we come to (20); but at that stage we cannot take account of the ideal class group of K because we need $\mathcal{B}$ to be independent of K. Its disadvantage is that L is no longer necessarily a continuous function of $\alpha \times \beta$; we investigate this situation in more detail after the proof of Lemma 7.

In discussing the continuity properties of L as a function of λ, we shall need the following lemma.

Lemma 6 *Let $\lambda_0 = \alpha_0/\beta_0$ with α_0, β_0 non-zero and integral outside $\mathcal{B}$; and let $\mathfrak{a}$ be an integral ideal in k not divisible by any prime in $\mathcal{B}$. Then we can find α, β in k, integral outside $\mathcal{B}$, with $(\alpha, \beta) = \mathfrak{a}(\alpha_0, \beta_0)$ and such that $\alpha \times \beta$ is arbitrarily close to $\alpha_0 \times \beta_0$ at each finite prime in $\mathcal{B}$, α/β is arbitrarily close to α_0/β_0 at each infinite place of k and α/α_0 and β/β_0 are positive at each real infinite place of k.*

Proof Let $\mathcal{S}$ be the set of primes which divide α_0 or β_0. We can write $\mathfrak{a} = (\gamma_1, \gamma_2)$ where γ_1 and γ_2 are units at every prime in $\mathcal{B}$ and both $\gamma_1/\mathfrak{a}$ and $\gamma_2/\mathfrak{a}$ are units at every prime in $\mathcal{S}$. Let δ in $\mathfrak{o}$, a unit outside $\mathcal{B}$, be such that $\alpha_0\delta$ and $\beta_0\delta$ are in $\mathfrak{o}$. Choose positive coprime integers a, b in $\mathbf{Z}$ which are close to 1 at every finite prime in $\mathcal{B}$ and units at all the primes which divide γ_1 or γ_2; and let M, N be large positive integers. By writing $\alpha_0\delta a^M/\gamma_1$ in terms of a base for $\mathfrak{o}/\mathbf{Z}$ and changing the coefficients by elements of $\mathbf{Q}$ which are small at each finite prime in $\mathcal{B} \cup \mathcal{S}$ and $O(a)$ at the infinite place of $\mathbf{Q}$, we can obtain an integer α_1 in $\mathfrak{o}$ which is prime to a and $\gamma_2/\mathfrak{a}$ and such that $\alpha_0\delta a^M/\alpha_1\gamma_1$ is close to 1 at each place in $\mathcal{B}$ and α_0, α_1 are divisible by the same power of $\mathfrak{p}$ for each $\mathfrak{p}$ in $\mathcal{S}$. Similarly we can obtain β_1 in $\mathfrak{o}$ which is prime to b and $\gamma_1/\mathfrak{a}$ and such that $\beta_0\delta b^N/\beta_1\gamma_2$ is close to 1 at each place of $\mathcal{B}$ and β_0, β_1 are divisible by the same power of $\mathfrak{p}$ for each $\mathfrak{p}$ in $\mathcal{S}$. We can further ensure that β_1 is prime to α_1 outside $\mathcal{B} \cup \mathcal{S}$. Now $\alpha = \alpha_1 b^N \gamma_1/\delta$ and $\beta = \beta_1 a^M \gamma_2/\delta$ satisfy all the requirements in the lemma. The only difficult thing to verify is that $(\alpha, \beta) = \mathfrak{a}(\alpha_0, \beta_0)$. So far as primes in $\mathcal{B}$ are concerned, the two sides agree; and

$$(\alpha, \beta) = (\alpha_1\gamma_1, \beta_1\gamma_2) = \mathfrak{a}(\alpha_1(\gamma_1/\mathfrak{a}), \beta_1(\gamma_2/\mathfrak{a})) = \mathfrak{a}(\alpha_1, \beta_1)$$

up to such primes. □

The proof of Lemma 5 constructs an evaluation formula all of whose terms come from the right hand side of (12) for various pairs f, g. For $\alpha \times \beta$ in $\mathcal{N}^2$,

the formula can therefore be described by an equation of the form

$$m(v; F, G; \alpha, \beta) = \prod_j (\phi_j(\alpha, \beta), \psi_j(\alpha, \beta))_v. \tag{16}$$

Here the ϕ_j, ψ_j are homogeneous elements of $k[U, V]$ which depend only on F and G and not on v or $\mathcal{B}$. The decomposition (16) is not unique, and our next task is to display an invariant aspect of it.

Let $\theta = \gamma_1 U + \gamma_2 V$ be a linear form with γ_1, γ_2 coprime integers in k. By using $(\phi, \psi)_v = (\phi, \theta\psi)_v(\phi, \theta)_v$ and $(-\theta, \theta)_v = 1$, we can ensure that all the ϕ_j, ψ_j in (16) have even degree except that $\psi_0 = \theta$. Denote by Θ the group of elements of k^* which are not divisible to an odd power by any prime of k outside $\mathcal{B}$, and by $\Theta_0 \subset \Theta$ the subgroup consisting of those ξ which are quadratic residues mod $\mathfrak{p}$ for all $\mathfrak{p}$ outside $\mathcal{B}$; thus we are free to multiply ϕ_0 by any element of Θ_0. (Actually $\Theta_0 \subset k^{*2}$, but we shall not use this fact.)

Lemma 7 *Suppose that* $\deg F$ *is even. With the convention for the* ϕ_j, ψ_j *just adopted, we can take* ϕ_0 *to be in* Θ.

Proof Let γ in k^* be a unit outside $\mathcal{B}$, and apply (16) to the identity

$$L(\mathcal{B}; F, G; \gamma\alpha, \gamma\beta) = L(\mathcal{B}; F, G; \alpha, \beta),$$

where $\alpha \times \beta$ is in $\mathcal{N}^2$. On cancelling common factors, we obtain

$$\prod_{v \in \mathcal{B}} (\phi_0(\alpha, \beta), \gamma)_v = 1. \tag{17}$$

If we can choose $\alpha \times \beta$ in $\mathcal{N}^2$ so that $\phi_0(\alpha, \beta)$ is not in Θ, this gives a contradiction. For let δ prime to $\phi_0(\alpha, \beta)$ be such that $\prod(\phi_0(\alpha, \beta), \delta)_\mathfrak{p} = -1$ where the product is taken over all primes $\mathfrak{p}$ outside $\mathcal{B}$ at which $\phi_0(\alpha, \beta)$ is not a unit. Let $\mathcal{B}_1$ be obtained by adjoining to $\mathcal{B}$ all the primes at which δ is not a unit; then $\prod(\phi_0(\alpha, \beta), \delta)_v = -1$ by the Hilbert product formula, where the product is taken over all places v in $\mathcal{B}_1$. Recalling that ϕ_0 does not depend on $\mathcal{B}$ and writing $\mathcal{B}_1, \delta$ for $\mathcal{B}, \gamma$ in (17), we obtain a contradiction. It follows that $\phi_0(\alpha, \beta)$ lies in Θ for all α, β; this can only happen if $\phi_0(U, V)$ is itself in Θ modulo squares of elements of $k[U, V]$. □

Let $\mathcal{S}$ be the set of primes $\mathfrak{p}$ outside $\mathcal{B}$ for which $\mathfrak{p}|F(\alpha_\mathfrak{p}, \beta_\mathfrak{p})$ or $\mathfrak{p}|G(\alpha_\mathfrak{p}, \beta_\mathfrak{p})$ in the notation of (15). We can write $\lambda = \alpha/\beta$ where (α, β) is not divisible by any prime in $\mathcal{S}$. Let $\mathfrak{a}$ be an integral ideal in the class of (α, β) not divisible

by any prime in $\mathcal{S}$, and let γ be such that $(\gamma) = \mathfrak{a}/(\alpha, \beta)$; then $\lambda = \alpha\gamma/\beta\gamma$ and $(\alpha\gamma, \beta\gamma) = \mathfrak{a}$. If $\mathcal{B}_1$ is obtained from $\mathcal{B}$ by adjoining all the primes which divide $\mathfrak{a}$, then

$$L(\mathcal{B}; F, G; \lambda) = L(\mathcal{B}; F, G; \alpha\gamma, \beta\gamma) = L(\mathcal{B}_1; F, G; \alpha\gamma, \beta\gamma),$$

where the second equality holds because the two products involved are term by term the same. By (16) the right hand side is equal to

$$\prod_{v \in \mathcal{B}_1} \prod_j (\phi_j(\alpha\gamma, \beta\gamma), \psi_j(\alpha\gamma, \beta\gamma))_v$$
$$= \left\{ \prod_{v \in \mathcal{B}_1} \prod_j (\phi_j(\alpha, \beta), \psi_j(\alpha, \beta))_v \right\} \prod_{v \in \mathcal{B}_1} (\phi_0, \gamma)_v$$

because of the parity properties above. If we further require that no prime which divides $\mathfrak{a}$ divides any of the $\phi_j(\alpha, \beta)$ or $\psi_j(\alpha, \beta)$, then each of the terms in curly brackets with v in $\mathcal{B}_1 \setminus \mathcal{B}$ is trivial; so the outer product there reduces to a product over v in $\mathcal{B}$. By the Hilbert product formula the product outside the curly brackets can be replaced by a product over all v not in $\mathcal{B}_1$. In view of Lemma 7 we can reduce this to a product over those v outside $\mathcal{B}_1$ which divide (α, β). If $\chi_{\mathfrak{p}}$ is again the quadratic residue symbol mod $\mathfrak{p}$, we can write the result which we have just obtained in the form

$$L(\mathcal{B}; F, G; \lambda) = \left\{ \prod_{v \in \mathcal{B}} \prod_j (\phi_j(\alpha, \beta), \psi_j(\alpha, \beta))_v \right\} \prod \chi_{\mathfrak{p}}(\phi_0) \qquad (18)$$

where the final product is taken over those $\mathfrak{p}$ outside $\mathcal{B}$ which divide (α, β) to an odd power.

Lemma 8 *Suppose that* $\deg F$ *is even and the conventions of Lemma* 7 *hold. Then* ϕ_0 *is uniquely determined by* F *and* G *as an element of* Θ/Θ_0*; and* ϕ_0 *is in* Θ_0 *if and only if* $L(\mathcal{B}; F, G; \lambda)$ *is continuous in* λ *in the topology induced by* $\mathcal{B}$*.*

Proof Suppose first that ϕ_0 is in Θ_0. Thus the final product in (18) is trivial. Now let $\lambda = \alpha/\beta$ and let λ' be close to λ in the topology induced by $\mathcal{B}$. Let γ in $\mathfrak{o}$ be such that $\lambda'\beta\gamma$ is integral. Applying (18) to the representations

$$\lambda = \alpha\gamma/\beta\gamma \quad \text{and} \quad \lambda' = \lambda'\beta\gamma/\beta\gamma$$

we deduce that $L(\mathcal{B}; F, G; \lambda) = L(\mathcal{B}; F, G; \lambda')$.

Conversely suppose that ϕ_0 is in Θ but not in Θ_0. Choose a prime $\mathfrak{p}$ outside $\mathcal{B}$ at which ϕ_0 is not a quadratic residue. As before, let $\lambda_0 = \alpha_0/\beta_0$, and let $\lambda = \alpha/\beta$ where α, β have the properties stated in Lemma 6 with $\mathfrak{a} = \mathfrak{p}$. Arguing as in the previous paragraph, but taking account of the final product in (18), we obtain

$$L(\mathcal{B}; F, G; \lambda) = L(\mathcal{B}; F, G; \lambda_0)\chi_{\mathfrak{p}}(\phi_0) = -L(\mathcal{B}; F, G; \lambda_0).$$

So $L(\mathcal{B}; F, G; \lambda)$ is not continuous at $\lambda = \lambda_0$ — which means that it is continuous nowhere.

Now suppose that $L(\mathcal{B}; F, G; \alpha, \beta)$ has two representations, say by the ϕ_i', ψ_i' and the ϕ_j'', ψ_j''. Taking their quotient, we obtain

$$1 = \prod_{v\in\mathcal{B}} \left\{ (\phi_0'/\phi_0'', \theta(\alpha,\beta))_v \prod_{i>0} (\phi_i'(\alpha,\beta), \psi_i'(\alpha,\beta))_v \prod_{j>0} (\phi_j''(\alpha,\beta), \psi_j''(\alpha,\beta))_v \right\}.$$

This is a representation of a function of λ which is continuous; and it is of a kind to which we can apply the results of the previous two paragraphs. Hence ϕ_0'/ϕ_0'' is in Θ_0.

It remains only to show that ϕ_0 is independent of the choice of θ. Using a notation like that of the previous paragraph, there is a representation of 1 in which the terms with subscript 0 produce a quotient

$$\prod_{v\in\mathcal{B}} \{(\phi_0'/\phi_0'', \theta')_v (\phi_0'', \theta'\theta'')_v\};$$

and since $\deg(\theta'\theta'')$ is even it follows as there that ϕ_0'/ϕ_0'' is in Θ_0. □

If $\deg F$ or $\deg G$ is 0 or 1, it is easy to obtain an evaluation formula; so the first case of interest is when $\deg F = \deg G = 2$. Suppose that

$$F = a_1U^2 + b_1UV + c_1V^2, \quad G = a_2U^2 + b_2UV + c_2V^2 \tag{19}$$

and that $\mathcal{B}$ contains the infinite places and the primes which divide 2 or

$$R = (a_1c_2 - a_2c_1)^2 - b_1b_2(a_1c_2 + a_2c_1) + a_1c_1b_2^2 + a_2c_2b_1^2,$$

the resultant of F and G. Suppose also that $\eta \times \zeta$ and $\rho \times \sigma$ are in $\mathcal{N}^2$. Then

$$L(\mathcal{B};F, G; \eta, \zeta)L(\mathcal{B}; F, G; \rho, \sigma) = \prod_{v\in\mathcal{B}} \{(f/(\sigma\eta - \rho\zeta), R)_v (fG(\rho,\sigma), -fG(\eta,\zeta))_v\}$$

where

$$f = F(\eta,\zeta)G(\rho,\sigma) - F(\rho,\sigma)G(\eta,\zeta).$$

In accordance with Lemma 7, the value of R is in Θ. If we set ρ, σ to convenient values, this gives the value of $L(\mathcal{B}; F, G; \eta, \zeta)$.

In practice, what we usually need to study is the subspace of $\mathcal{N}^2$ given by n conditions $L(\mathcal{B}; F_\nu, G_\nu; \alpha, \beta) = 1$, or the subspace of $\mathcal{N}^1$ given by the $L(\mathcal{B}; F_\nu, G_\nu; \lambda) = 1$, where the $\deg F_\nu$ are all even. Let Λ be the abelian group of order 2^n whose elements are the n-tuples each component of which is ± 1; then there is a natural identification, which we shall write τ, of each element of Λ with a partial product of the $L(\mathcal{B}; F_\nu, G_\nu)$. Thus each element of Λ can be interpreted as a condition, which we shall write as $\mathcal{L} = 1$. If ϕ_0 is as in Lemma 7, there is a homomorphism

$$\phi_0 \circ \tau : \Lambda \to \Theta/\Theta_0;$$

let Λ_0 denote its kernel. In view of Lemma 8, the conditions which are continuous in λ are just those which come from Λ_0. The following lemma corresponds to Harari's Formal Lemma (Theorem 3.2.1 of [7]); it shows that for most purposes we need only consider the conditions coming from the elements of Λ_0. For obvious reasons, we call these the *continuous* conditions.

Lemma 9 *Suppose that every* $\deg F_\nu$ *is even and all the conditions corresponding to* Λ_0 *hold at some given* λ_0. *Then there exists* λ *arbitrarily close to* λ_0 *such that all the conditions* $L(\mathcal{B}; F_\nu, G_\nu) = 1$ *hold at* λ.

Proof Let $\lambda_0 = \alpha_0/\beta_0$. For a suitably chosen $\mathfrak{a} = (\gamma)$ we show that we can take $\lambda = \alpha/\beta$, where $\alpha \times \beta$ is as in Lemma 6. For any c in Λ, write $\phi_{0c} = \phi_0 \circ \tau(c)$ for the corresponding element of Θ/Θ_0. If θ is as defined just before Lemma 7, the corresponding partial product $\mathcal{L}$ of the $L(\mathcal{B}; F_\nu, G_\nu; \lambda)$ is equal to

$$f_c(\lambda) \prod_{v \in \mathcal{B}} (\phi_{0c}, \theta(\alpha_0, \beta_0))_v \prod_{v \in \mathcal{B}} (\phi_{0c}, \gamma)_v$$

where f_c comes from the ϕ_j, ψ_j with $j > 0$ and is therefore continuous. The map $c \mapsto f_c(\lambda)$ is a homomorphism $\Lambda \to \{\pm 1\}$ for any fixed λ; moreover if two distinct c give rise to the same ϕ_{0c} their quotient comes from an element of Λ_0; so the quotient of the corresponding f_c takes the value 1 at λ_0. In other words, if λ is close enough to λ_0 then $f_c(\lambda)$ only depends on the class of c in Λ/Λ_0. The map $c \mapsto \phi_{0c}$ is an embedding $\Lambda/\Lambda_0 \to \Theta/\Theta_0$, by Lemma

8. The homomorphism Image$(\Lambda/\Lambda_0) \to \{\pm 1\}$ induced by $c \mapsto f_c(\lambda)$ can be extended to a homomorphism $\Theta/\Theta_0 \to \{\pm 1\}$ because Θ/Θ_0 is killed by 2; and any such homomorphism can be written in the form

$$\theta \to \prod_{v \in \mathcal{B}} (\theta, \gamma)_v$$

for a suitably chosen γ, because the Hilbert symbol induces a nonsingular form on Θ/Θ_0. But given any such γ we can construct $\lambda = \alpha/\beta$ having the properties listed in Lemma 6 with $\mathfrak{a} = (\gamma)$. □

We shall need analogues of these last results for positive 0-cycles, and this will require more notation. We continue to assume that $\deg F$ is even. Let K be the direct product of finitely many fields k_i each of finite degree over k, and let $\mathfrak{B}$ be the set of places of K lying over some place v in $\mathcal{B}$, and $\mathfrak{B}_i$ the corresponding set of places of k_i. (The place $\prod v_i$, where v_i is a place of k_i, lies over v if each v_i does so.) For λ in $\mathbf{P}^1(K)$ write $\lambda = \prod \lambda_i$ with λ_i in $\mathbf{P}^1(k_i)$; for each place w in k_i write $\lambda_i = \alpha_{iw}/\beta_{iw}$ where α_{iw}, β_{iw} are in k_i and integral at w and at least one of them is a unit at w. For any λ in K such that each $F(\lambda_i, 1)$ and $G(\lambda_i, 1)$ is nonzero, we define the function

$$L^*(\mathcal{B}; K; F, G; \lambda) : \lambda \mapsto \prod_{\mathfrak{P}_i} (F(\alpha_{iw}, \beta_{iw}), G(\alpha_{iw}, \beta_{iw}))_{\mathfrak{P}_i} \tag{20}$$

where w is the place associated with the prime $\mathfrak{P}_i$ in k_i and the product is taken over all i and all primes $\mathfrak{P}_i$ of k_i not lying in $\mathfrak{B}_i$ and such that $G(\alpha_{iw}, \beta_{iw})$ is divisible by $\mathfrak{P}_i$. As with (9), we can restrict the product to those $\mathfrak{P}_i$ which divide $G(\alpha_{iw}, \beta_{iw})$ to an odd power. Note that the functions ϕ_j, ψ_j in the evaluation formula (16) are the same for $k_i \supset k$ as they are for k. Now let $\mathfrak{a}$ be a positive 0-cycle on $\mathbf{P}^1$ defined over k and let $\mathfrak{a} = \cup \mathfrak{a}_i$ be its decomposition into irreducible components. Let λ_i be a point of $\mathfrak{a}_i$ and write $k_i = k(\lambda_i)$. If $K = \prod k_i$ and $\lambda = \prod \lambda_i$, write

$$L^*(\mathcal{B}; F, G; \mathfrak{a}) = L^*(\mathcal{B}; K; F, G; \lambda) = \prod\nolimits_i L(\mathfrak{B}_i; F, G; \lambda_i). \tag{21}$$

This is legitimate, because the right hand side does not depend on the choice of the λ_i. If $K = k$ this L^* is the same as the previous function L. Moreover $L^*(\mathfrak{a} \cup \mathfrak{b}) = L^*(\mathfrak{a}) L^*(\mathfrak{b})$. We can define a topology on the set of positive 0-cycles $\mathfrak{a}$ of given degree N by means of the isomorphism between that set and the points on the N-fold symmetric power of $\mathbf{P}^1$. With this topology, it is straightforward to extend to L^* the results already obtained for L.

The product in (20) is finite; so there is a finite set $\mathcal{S}$ of primes of k, disjoint from $\mathcal{B}$ and such that every $\mathfrak{P}_i$ which appears in this product lies above a prime in $\mathcal{S}$. For each i we can write $\lambda_i = \alpha_i/\beta_i$ with α_i, β_i integers in k_i. As in the argument which follows the proof of Lemma 7, let $(\alpha_i, \beta_i) = \mathfrak{a}_i$ and choose an integral ideal $\mathfrak{b}_i$ in k_i which is prime to $\mathfrak{a}_i$, in the same ideal class as $\mathfrak{a}_i$ and such that no prime of k_i which divides $\mathfrak{b}_i$ also divides $G(\alpha_i, \beta_i)$ or any $\phi_j(\alpha_i, \beta_i)$ or $\psi_j(\alpha_i, \beta_i)$ or lies above any prime in $\mathcal{S}$. Let γ_i be such that $(\gamma_i) = \mathfrak{b}_i/\mathfrak{a}_i$ and let $\mathcal{B}_1$ be obtained from $\mathcal{B}$ by adjoining all the primes of k which lie below any prime of k_i which divides $\mathfrak{b}_i$. For most purposes it costs us nothing to replace $\mathcal{B}$ by $\mathcal{B}_1$, and we then have

$$\lambda = \prod \lambda_i = \prod (\alpha_i\gamma_i/\beta_i\gamma_i) \text{ where } \alpha_i\gamma_i \times \beta_i\gamma_i \text{ is in } \mathcal{N}^2(k_i).$$

The following lemma is a trivial consequence of earlier results.

Lemma 10 *Suppose that* $\deg F$ *is even, and let* $\mathcal{L} = 1$ *be a continuous condition derived from the* L *and* $\mathcal{L}^* = 1$ *the corresponding condition derived from the* L^**. For each* v *in* $\mathcal{B}$ *there is a function* $\ell^*(v; F, G; \mathfrak{a})$ *with values in* $\{\pm 1\}$ *which is a continuous function of* $\mathfrak{a}$ *in the* v*-adic topology and is such that*

$$\mathcal{L}^*(\mathcal{B}; F, G; \mathfrak{a}) = \prod_{v \in \mathcal{B}} \ell^*(v; F, G; \mathfrak{a}). \tag{22}$$

4. *Pencils of conics.*
Let W be the surface fibred by the pencil of conics

$$a_0(U,V)Y_0^2 + a_1(U,V)Y_1^2 + a_2(U,V)Y_2^2 = 0. \tag{23}$$

We normally expect this pencil to be presented in a form in which a_0, a_1, a_2 are homogeneous of the same degree. But this is not the most convenient form for the arguments which follow. Instead we shall call the pencil *reduced* if a_0, a_1, a_2 are homogeneous elements of $k[U,V]$ coprime in pairs and such that

$$\deg a_0 \equiv \deg a_1 \equiv \deg a_2 \bmod 2.$$

After a linear transformation on U, V if necessary, we can also assume that $a_0a_1a_2$ is not divisible by V. Clearly any pencil of conics can be put into reduced form; for if a_i has a squared factor f^2 we write $f^{-1}Y_i$ for Y_i, and if for example a_0 and a_1 have a common factor g we write gY_2 for Y_2 and divide (23) by g. Suppose that (23) is reduced and everywhere locally soluble. Let $\lambda = \alpha/\beta$ be a point of $\mathbf{P}^1(k)$; whether (23) is soluble at $\alpha \times \beta$ depends only on λ and not on the choice of α, β. Similar statements hold for local solubility at a place v and for solubility in the adeles. Denote by $c(U,V)$ an irreducible factor of $a_0a_1a_2$ in $k[U,V]$; we can assume that $c(U,V)$ has integer coefficients whose highest common factor is not divisible by any prime outside $\mathcal{B}$. Let $\mathcal{B}$ be a finite set of places of k containing the infinite places, the primes dividing 2, those whose absolute norm does not exceed $\deg(a_0a_1a_2)$, those at which any coefficient of any a_i or any c is not integral, and any other primes $\mathfrak{p}$ at which $a_0a_1a_2$ does not remain separable when reduced mod $\mathfrak{p}$. One effect of this definition is that we need only check local solubility at the places of $\mathcal{B}$, because it is trivial at any other prime. Local solubility of (23) at the place v is equivalent to $(-a_0a_1, -a_0a_2)_v = 1$, which can be written in the more symmetric form

$$(a_0, -a_1)_v(a_1, -a_2)_v(a_2, -a_0)_v = (-1,-1)_v. \tag{24}$$

For convenience, we also assume that $\mathcal{B}$ contains a base for the ideal class group of k.

The singular fibres of the pencil are given by the values of λ at which $a_0a_1a_2$ vanishes. If there is a singular fibre defined over k, then (23) is certainly soluble on it; but little if any of the argument which follows makes sense there. We must therefore work not on $\mathbf{P}^1$ but on the subset $\mathbf{L}^1$ obtained

by deleting the zeros of $a_0a_1a_2$, and not on W but on W_0, the inverse image of $\mathbf{L}^1$ in W. Let $\lambda \in k \cup \{\infty\}$ be a point of $\mathbf{L}^1(k)$, and write $\lambda = \alpha/\beta$ where α, β are integers of k coprime outside $\mathcal{B}$; it will not matter which pair α, β we choose. Similar conventions will hold for other $\mathbf{L}^1(\cdot)$.

There is a non-empty set $\mathcal{N} \subset \mathbf{L}^1(k)$, open in the topology induced by $\mathcal{B}$, such that the conic (23) is soluble at every place of $\mathcal{B}$ if and only if λ lies in $\mathcal{N}$. Let $\mathfrak{p}$ be a prime of k not in $\mathcal{B}$ and consider the solubility of (23) in $k_\mathfrak{p}$ at the point λ. If none of the $a_i(\alpha, \beta)$ is divisible by $\mathfrak{p}$, then local solubility of (23) is trivial. Otherwise there is just one c such that $c(\alpha, \beta)$ is divisible by $\mathfrak{p}$; to fix ideas, suppose that this c divides a_2. The condition for local solubility at $\mathfrak{p}$ is then

$$(-a_0(\alpha, \beta)a_1(\alpha, \beta), c(\alpha, \beta))_\mathfrak{p} = 1 \tag{25}$$

where the outer bracket is the multiplicative Hilbert symbol. Hence necessary conditions for the local solubility of (23) at λ for all $\mathfrak{p}$ outside $\mathcal{B}$ are the conditions like

$$L(\mathcal{B}; -a_0a_1, c; \lambda) = \prod (-a_0(\alpha, \beta)a_1(\alpha, \beta), c(\alpha, \beta))_\mathfrak{p} = 1 \tag{26}$$

where the product is taken over all $\mathfrak{p}$ outside $\mathcal{B}$ which divide $c(\alpha, \beta)$, and the function L is well defined since $-a_0a_1$ has even degree. There is one of these conditions for each c.

What makes the set of conditions (26) interesting is that they give not merely a necessary but also a sufficient condition for solubility — at least if one assumes Schinzel's Hypothesis. The following theorem provides the exact obstruction both to the Hasse principle and to weak approximation. In view of Lemma 9, it is enough to require the continuous conditions derived from the conditions (26) to hold; and the resulting $\mathcal{A}$ is both open and closed.

Theorem 1 *Assume Schinzel's Hypothesis. Let $\mathcal{A} \subset \mathcal{N}$ be the subset of $\mathbf{L}^1(k)$ at which all the continuous conditions derived from* (26) *hold and* (23) *is locally soluble at each place in $\mathcal{B}$. Then the λ in $\mathbf{L}^1(k)$ at which* (23) *is soluble form a dense subset of $\mathcal{A}$ in the topology induced by $\mathcal{B}$.*

Proof Let $\alpha_0 \times \beta_0$ correspond to a point λ_0 in $\mathcal{A}$, and let $\mathcal{N}_0 \subset \mathcal{A}$ be an open neighbourhood of λ_0. We have to show that we can find λ_2 in $\mathcal{N}_0$ such that (23) is soluble at λ_2; for this it is enough to show that (23) is everywhere locally soluble there. Let c_i run through the factors c. By Lemma 9 we can

find α_1, β_1 in k^*, integral and coprime outside $\mathcal{B}$ and such that $\lambda_1 = \alpha_1/\beta_1$ is in $\mathcal{N}_0$ and all the conditions (26) hold at $\alpha_1 \times \beta_1$. By Lemma 2 we can now find $\alpha_2 \times \beta_2$ close to $\alpha_1 \times \beta_1$ and such that each ideal $(c_i(\alpha_2, \beta_2))$ is the product of a prime ideal $\mathfrak{p}_i$ not in $\mathcal{B}$ and prime ideals in $\mathcal{B}$. We claim that (23) is everywhere locally soluble at $\alpha_2 \times \beta_2$. Since $\mathcal{N}_0 \subset \mathcal{A}$, local solubility at each place of $\mathcal{B}$ is automatic. If $\mathfrak{p}$ is a prime outside $\mathcal{B}$ which does not divide any of the $a_j(\alpha_2, \beta_2)$ then (23) at $\alpha_2 \times \beta_2$ is certainly soluble at $\mathfrak{p}$; so it only remains to consider the $\mathfrak{p}_i$. To fix ideas, suppose that $c_i(U, V)$ is a factor of $a_2(U, V)$. Taking $\alpha = \alpha_2, \beta = \beta_2$ and $c = c_i$, the product in (26) reduces to the single term with $\mathfrak{p} = \mathfrak{p}_i$. In other words, (25) holds in this case, and this proves local solubility at $\mathfrak{p}_i$. □

The corresponding theorem for positive 0-cycles, or equivalently for 0-cycles of degree 1, does not require Schinzel's Hypothesis; instead we use Lemma 4 and the notation introduced at (20). We apply Lemma 4 to the surface W_0 fibred by the pencil (23), again assuming that $\mathcal{B}$ satisfies the conditions listed after (23) and that $\mathbf{L}^1$ has the same meaning as there.

Theorem 2 *With the notation above, let $N \geq \deg(a_0 a_1 a_2)$ be a fixed integer. Let $\mathfrak{a}$ be a positive 0-cycle of degree N on $\mathbf{L}^1$ defined over k, and for each place v of k suppose that W_0 contains a positive 0-cycle $\mathfrak{b}_v$ of degree N defined over k_v; for v in $\mathcal{B}$ suppose further that $\mathfrak{b}_v$ is so chosen that its projection on $\mathbf{L}^1$ is $\mathfrak{a}$. If all the continuous conditions derived from the conditions*

$$L^*(\mathcal{B}; -a_0 a_1, c; \mathfrak{a}) = 1 \tag{27}$$

hold, then there is a positive 0-cycle of degree N on W_0 defined over k whose projection is arbitrarily close to $\mathfrak{a}$ in the topology induced by $\mathcal{B}$.

Proof We must first show that for the purpose of proving this theorem we are allowed to increase $\mathcal{B}$. Suppose that $\mathcal{B}_0$ satisfies the conditions which were imposed on $\mathcal{B}$ after (23), and let $\mathfrak{p}$ be a prime of k not in $\mathcal{B}_0$. Suppose also that the hypotheses of the theorem hold for $\mathcal{B} = \mathcal{B}_0$ and $\mathfrak{a} = \mathfrak{a}_0$. Having chosen $\mathfrak{b}_\mathfrak{p}$ we can find a positive 0-cycle $\mathfrak{a}'$ on $\mathbf{L}^1$ of degree N and defined over k which is close at every v in $\mathcal{B}_0$ to $\mathfrak{a}$ and close at $\mathfrak{p}$ to the projection of $\mathfrak{b}_\mathfrak{p}$. Now

$$L^*(\mathcal{B}_0 \cup \{\mathfrak{p}\}; -a_0 a_1, c; \mathfrak{a}') = L^*(\mathcal{B}_0; -a_0 a_1, c; \mathfrak{a}');$$

for writing both sides as products by means of (20), if there is a factor on the right hand side which is not present on the left, that factor must come from

$\mathfrak{p}$ and is therefore equal to 1. But a continuous condition for $\mathcal{B}_0$ holds at $\mathfrak{a}'$ if and only if it holds at $\mathfrak{a}$, which it does by hypothesis. Hence the continuous conditions for $\mathcal{B}_0 \cup \{\mathfrak{p}\}$ hold at $\mathfrak{a}'$. Now suppose that the theorem holds for $\mathcal{B}_0 \cup \{\mathfrak{p}\}$; then there is a positive 0-cycle $\mathfrak{b}$ of degree N on W_0 defined over k whose projection on $\mathbf{L}^1$ is close to $\mathfrak{a}'$ in the topology induced by $\mathcal{B}_0 \cup \{\mathfrak{p}\}$. The same projection is close to $\mathfrak{a}$ in the topology induced by $\mathcal{B}_0$. So the theorem also holds for $\mathcal{B}_0$.

Note that if $\mathfrak{a}$ is actually the projection of a positive 0-cycle of degree N in W_0, then the continuous conditions certainly hold in view of (21); thus imposing the hypothesis that they all hold costs us nothing. To simplify the notation, we assume henceforth that K is an algebraic number field; this will be true for the application in this article because K will be constructed by means of Lemma 4. In view of the previous paragraph, we can assume that $\mathcal{B}$ is so large that it satisfies the conditions imposed on $\mathfrak{B}$ in the statement of Lemma 4 and contains the additional place w which was adjoined to $\mathfrak{B}$ in the first paragraph of the proof of Lemma 4; and if b is as in Lemma 4 we also adjoin to $\mathcal{B}$ all the primes in k which divide b. By the analogue of Lemma 9, we can now choose $\mathfrak{a}''$ close to $\mathfrak{a}$ so that all the conditions like $L^*(\mathcal{B}; -a_0a_1, c; \mathfrak{a}'') = 1$ hold. As was remarked in the previous paragraph, we can now increase $\mathcal{B}$ so that if $\lambda_0 = \alpha_0/\beta_0$ is a point of $\mathbf{L}^1(K)$ in $\mathfrak{a}''$ then α_0, β_0 are coprime and integral except perhaps at primes of K above a prime in $\mathcal{B}$. Now apply Lemma 4 with $M = 2$, where we take the $c(X, 1)$, normalized to be monic, to be the $P_i(X)$ and each U_v to be a small neighbourhood of the monic polynomial whose roots determine $\mathfrak{a}''$. Let $G(X)$ be given by Lemma 4; let $\mathfrak{a}'$ be the associated 0-cycle on $\mathbf{L}^1(k)$ and λ a point of $\mathbf{L}^1(K)$ in $\mathfrak{a}'$. For each v in $\mathcal{B}$, the cycle $\mathfrak{a}'$ is close to $\mathfrak{a}''$ in the v-adic topology; so (23) at λ is soluble in K_w for each w above v, by continuity. But $\lambda = \alpha/\beta$ with α, β coprime except at primes of K above a prime of $\mathcal{B}$. So

$$\prod_{\mathfrak{P}} (-a_0(\alpha, \beta)a_1(\alpha, \beta), c(\alpha, \beta))_{\mathfrak{P}} = L^*(\mathcal{B}; -a_0a_1, c; \alpha, \beta) = 1,$$

where the product is taken over all primes $\mathfrak{P}$ not above a prime in $\mathcal{B}$ and such that $c(\alpha, \beta)$ is divisible to an odd power by $\mathfrak{P}$. Here the first equality holds by definition and the second one follows from the evaluation formula (16) by continuity. But if $c(X, 1) = P_i(X)$ then the product on the left reduces to the single term for which $\mathfrak{P}$ is the prime of K above $\mathfrak{p}_i$ whose existence was proved by means of (6). Hence (23) at λ is locally soluble at this prime; and because these are the only primes not lying above a prime of $\mathcal{B}$ which divide

any $c(\alpha,\beta)$ or any $a_i(\alpha,\beta)$ to an odd power, they are the only primes not lying above a prime of $\mathcal{B}$ at which local solubility might present any difficulty. Thus λ can be lifted to a point of the fibre above λ, which is a conic, and the theorem now follows because weak approximation holds on conics. $\square$

Since (23) contains positive 0-cycles of degree 2 defined over k, it is trivial to deduce from Theorem 2 the corresponding result for 0-cycles of degree 1; conversely, if we know the analogue of Theorem 2 for 0-cycles of degree 1 we can deduce that (23) contains positive 0-cycles of some odd degree defined over k. It is tempting to hope that if a pencil of conics contains 0-cycles of degree 1 then it contains points; indeed, the corresponding result is true for Del Pezzo surfaces of degree 4, as is proved in Theorem 11. But this hope is false. A simple example is given by the pencil

$$Y_0^2 + Y_1^2 - 7(U^2 - UV - V^2)(U^2 + UV - V^2)(U^2 - 2V^2)Y_2^2 = 0. \qquad (28)$$

This is insoluble in $\mathbf{Q}$. For we can take $\mathcal{B} = \{\infty, 2, 3, 5, 7\}$, and the three possible $c(U,V)$ are $U^2 - UV - V^2$, $U^2 + UV - V^2$ and $U^2 - 2V^2$. By (12) we have

$$L(\mathcal{B}; -1, c) = (-1, c)_\infty (-1, c)_2 (-1, c)_7,$$

the factors at 3 and 5 being trivial. Local solubility of (28) holds at each place; at $\alpha \times \beta$ local solubility at 2 and at 7 requires respectively that $4|\alpha$ and $\alpha^2 - 2\beta^2$ is divisible by an odd power of 7. Hence

$$(-1, \alpha^2 \pm \alpha\beta - \beta^2)_2 = -1, \quad (-1, \alpha^2 - 2\beta^2)_2 = -1$$

and

$$(-1, \alpha^2 \pm \alpha\beta - \beta^2)_7 = 1, \quad (-1, \alpha^2 - 2\beta^2)_7 = -1.$$

To satisfy the conditions (26) we therefore need

$$(-1, \alpha^2 \pm \alpha\beta - \beta^2)_\infty = -1, \quad (-1, \alpha^2 - 2\beta^2)_\infty = 1;$$

but this is equivalent to $\alpha^2 \pm \alpha\beta - \beta^2 < 0 < \alpha^2 - 2\beta^2$, which is impossible. Now let $K = \mathbf{Q}(\rho)$ where $\rho = 2\cos(2\pi/7)$, so that $\rho^3 + \rho^2 - 2\rho - 1 = 0$. If $U = \rho^2 + 2\rho - 3$ and $V = \rho^2 + \rho - 2$ then

$$Y_0 = (\rho - 2)^2(\rho^2 - \rho + 1),\ Y_1 = (\rho - 2)^2(\rho^2 - 1),\ Y_2 = 1$$

gives a solution in K.

It was asserted in the Introduction that on pencils of conics the appropriate Brauer-Manin condition is a necessary and sufficient condition for the Hasse principle and for weak approximation (in each case subject to Schinzel's Hypothesis) and for the existence of positive 0-cycles of degree N for all large enough N. This is the same as saying that the appropriate Brauer-Manin condition is equivalent to the necessary and sufficient conditions stated in Theorems 1 and 2. That is the content of the following lemma.

Lemma 11 *Let W_0 be everywhere locally soluble. Then the continuous conditions derived from* (23) *are collectively equivalent to the Brauer-Manin conditions for the existence of points of W_0 defined over k. The continuous conditions similarly derived from the $L^*(\mathfrak{a})$ are collectively equivalent to the Brauer-Manin conditions for the existence of positive* 0*-cycles of degree N on W_0 defined over k.*

Proof The first assertion is proved for $k = \mathbf{Q}$ in [7], §8; as with Lemma 5, the proof there can easily be extended to our more general case. The second sentence follows trivially from the first in the light of (21). □

5. *Descent on certain curves of genus* 1.
Throughout this section, we shall be concerned with an elliptic curve E which is defined over an algebraic number field k and has all its 2-division points rational. Such a curve can be written in the form

$$E:\ Y^2 = (X - c_1)(X - c_2)(X - c_3), \tag{29}$$

where without loss of generality we can assume that the c_i are integers. We mainly discuss 2-descent on E, but there is a brief mention of 4-descent at the end of the section. The first usable exposition of 4-descent is due to Cassels [2]. He showed, without any assumption about the 2-division points, that a 4-descent requires no bigger a field extension than a 2-descent. We shall state his algorithm, without proof, for the particular case (29).

The classical theory of 2-descent is expounded in the next few paragraphs. But there is also a well concealed symmetry property, stated in Theorem 3, and the proof of this requires extra apparatus. This extra apparatus, suitably modified, enables us to prove some results about the effect of twisting on the 2-Selmer group of E.

The odd primes of bad reduction for E are those which divide

$$R = (c_1 - c_2)(c_2 - c_3)(c_3 - c_1).$$

We shall need several distinct sets of bad places of k, the first two being independent of E:

- $\mathcal{S}_0$ consists of the infinite places and the primes which lie above 2.
- $\mathcal{S}_0^+$ consists of $\mathcal{S}_0$ and a set of generators of the ideal class group of k; for simplicity we require the latter to be odd primes of good reduction for E.
- $\mathcal{S}_1$ is the union of $\mathcal{S}_0$ and the odd primes of bad reduction for E.
- $\mathcal{S}_1^+$ is the union of $\mathcal{S}_1$ and $\mathcal{S}_0^+$.

We shall usually denote by $\mathcal{B}$ a finite set of places such that $\mathcal{B} \supset \mathcal{S}_1^+$. In the Corollaries to Lemmas 15 and 16 we shall need to write $\mathcal{B}$ as a disjoint union $\mathcal{B}' \cup \mathcal{B}''$ where $\mathcal{B}' \supset \mathcal{S}_0^+$.

To any triple $m = (m_1, m_2, m_3)$ of elements of k^* with $m_1 m_2 m_3 = 1$ we associate the 2-covering given by

$$m_i Y_i^2 = X - c_i \text{ for } i = 1, 2, 3 \quad \text{and} \quad Y = Y_1 Y_2 Y_3. \tag{30}$$

We shall frequently treat the m_i as elements of k^*/k^{*2}; this involves some abuse of notation. This system is equivalent to the three equations

$$m_i Y_i^2 - m_j Y_j^2 = (c_j - c_i) Y_0^2, \tag{31}$$

of which only two are independent; we denote by $\Gamma = \Gamma(m)$ the curve of genus 1 given by the three equations (31) and by $C_{ij} = C_{ij}(m)$ the conic given by the single equation (31). These equations define an isomorphism between the $\mathbf{F}_2$-vector space of all 2-coverings of E and $(k^*/k^{*2})^2$, the addition of two 2-coverings corresponding to componentwise multiplication of the triples m. The 2-covering corresponding to the 2-division point $(c_1, 0)$, for example, is given by the triple

$$((c_1 - c_2)(c_1 - c_3), c_1 - c_2, c_1 - c_3). \tag{32}$$

If $\mathcal{B}$ is a finite set of places of k containing $\mathcal{S}_1^+$, then the 2-coverings soluble in k_v for every v outside $\mathcal{B}$ can be identified with the elements of $(\mathfrak{o}_\mathcal{B}^*/\mathfrak{o}_\mathcal{B}^{*2})^2$, where $\mathfrak{o}_\mathcal{B}^*$ consists of the elements of k^* which are units outside $\mathcal{B}$. Moreover, if for example $\mathfrak{p}$ divides $c_2 - c_3$ but not $c_1 - c_2$ or $c_1 - c_3$, it is easy to check that $\mathfrak{p} \| m_1$ implies the local insolubility of Γ at $\mathfrak{p}$.

For every finite set $\mathcal{B} \supset \mathcal{S}_0^+$ of places of k, of order n, write

$$X_\mathcal{B} = \mathfrak{o}_\mathcal{B}^*/\mathfrak{o}_\mathcal{B}^{*2}, \quad Y_v = k_v^*/k_v^{*2}, \quad Y_\mathcal{B} = \bigoplus\nolimits_{v\in\mathcal{B}} Y_v.$$

More generally, if $\mathcal{S}$ is any finite set of places we shall write $Y_\mathcal{S} = \oplus_{v\in\mathcal{S}} Y_v$, and similarly for $V_\mathcal{S}, T_\mathcal{S}, W_\mathcal{S}$ and $K_\mathcal{S}$; but note that the spaces $\mathfrak{o}_\mathcal{S}^*, X_\mathcal{S}$ and $U_\mathcal{S}$ do not follow this convention. Here $X_\mathcal{B}$ has dimension n by Dirichlet's unit theorem, and $Y_\mathcal{B}$ has dimension $2n$ because Y_v contains $4/|2|_v$ elements. It is known from class field theory that $X_\mathcal{B} \to Y_\mathcal{B}$ is injective. Now write

$$V_v = Y_v \times Y_v, \quad V_\mathcal{B} = \bigoplus\nolimits_{v\in\mathcal{B}} V_v = Y_\mathcal{B} \times Y_\mathcal{B}$$

and let $U_\mathcal{B}$ be the image of $X_\mathcal{B} \times X_\mathcal{B}$ in $V_\mathcal{B}$. Thus $\dim U_\mathcal{B} = \frac{1}{2} \dim V_\mathcal{B} = 2n$. Define the non-degenerate alternating bilinear form $e_\mathcal{S}$ on $V_\mathcal{S}$ by

$$e_\mathcal{S} = \prod\nolimits_{v\in\mathcal{S}} e_v \quad \text{where} \quad e_v((a,b),(c,d)) = (a,d)_v (b,c)_v, \tag{33}$$

the factors on the right being Hilbert symbols. By the Hilbert product formula $U_\mathcal{B}$ is isotropic with respect to $e_\mathcal{B}$, and comparison of dimensions shows that it is maximal isotropic in $V_\mathcal{B}$.

Let T_v be the image of $(\mathfrak{o}_v^*/\mathfrak{o}_v^{*2})^2$ in V_v, where $\mathfrak{o}_v$ is the ring of integers of k_v, and let W_v be the image of $E(k_v)$ in V_v under the Kummer map

$$\partial : \ P = (X, Y) \mapsto (X - c_1, X - c_2)$$

in the notation of (29). Tate has shown (see [9], p.56) that W_v is a maximal isotropic subspace of V_v for the alternating form e_v, and $W_v = T_v$ if v is not in $\mathcal{S}_1$. A 2-covering of E is soluble in k_v if and only if the corresponding point of V_v is in W_v.

The importance of isotropy in this context depends on the following result.

Lemma 12 *Let $\mathcal{S}$ be a finite set of places and let G be a maximal isotropic subspace of $V_\mathcal{S}$ with respect to $e_\mathcal{S}$. If G contains $\sigma_1 \times \tau_1$ and $\sigma_2 \times \tau_2$ then*

$$(\sigma_1 \times \tau_1) + (\sigma_2 \times \tau_2) = \sigma_1\sigma_2 \times \tau_1\tau_2.$$

Proof Because $e_\mathcal{S}$ is non-degenerate it is enough to show that

$$e_\mathcal{S}(\sigma_1 \times \tau_1, \sigma \times \tau)e_\mathcal{S}(\sigma_2 \times \tau_2, \sigma \times \tau) = e_\mathcal{S}(\sigma_1\sigma_2 \times \tau_1\tau_2, \sigma \times \tau)$$

for every element $\sigma \times \tau$ of $V_\mathcal{S}$. This follows immediately from the multiplicitivity of the Hilbert symbol. □

Now suppose that $\mathcal{B} \supset \mathcal{S}_1^+$. A 2-covering of E is soluble in k_v for v not in $\mathcal{B}$ if and only if the corresponding point of $(k^*/k^{*2})^2$ is in $U_\mathcal{B}$. Hence the 2-Selmer group of E can be identified with $U_\mathcal{B} \cap W_\mathcal{B}$. Because $U_\mathcal{B}$ and $W_\mathcal{B}$ are both maximal isotropic, this group is both the left and the right kernel of the bilinear map $U_\mathcal{B} \times W_\mathcal{B} \to \{\pm 1\}$ induced by $e_\mathcal{B}$.

In §6 we shall need to know in a particular case how the local solubility of Γ is related to the local solubility of its images C_{ij}.

Lemma 13 *Let $\mathfrak{p}$ be a prime in k not dividing 2, and suppose that $\mathfrak{p}$ divides $(c_2 - c_3)$ but not $(c_1 - c_2)$ or $(c_1 - c_3)$. Then local solubility of all the C_{ij} at $\mathfrak{p}$ implies local solubility of Γ at $\mathfrak{p}$, except in the case when $v_\mathfrak{p}(m_2)$, $v_\mathfrak{p}(m_3)$, $v_\mathfrak{p}(c_2 - c_3)$ are all even and $(c_3 - c_1)$ is in $k_\mathfrak{p}^{*2}$. In this case local solubility of Γ further requires that m_1 is in $k_\mathfrak{p}^{*2}$.*

Proof We separate three cases. In each of them the first step is to give necessary and sufficient conditions for the image of the element $a \times b$ of $k_\mathfrak{p} \times k_\mathfrak{p}$ to lie in $W_\mathfrak{p}$. The verification becomes easier if one uses the fact that $W_\mathfrak{p}$ has dimension 2. We have already noted that $v_\mathfrak{p}(a)$ must always be even.

(i) If $(c_3 - c_1)$ is in $k_\mathfrak{p}^{*2}$ then a is in $k_\mathfrak{p}^{*2}$.

(ii) If $(c_3 - c_1)$ is not in $k_\mathfrak{p}^{*2}$ and $v_\mathfrak{p}(c_2 - c_3)$ is odd, then either a is in $k_\mathfrak{p}^{*2}$ and $v_\mathfrak{p}(b)$ is even or a is in $(c_3 - c_1)k_\mathfrak{p}^{*2}$ and $v_\mathfrak{p}(b)$ is odd.

(iii) If $(c_3 - c_1)$ is not in $k_\mathfrak{p}^{*2}$ and $v_\mathfrak{p}(c_2 - c_3)$ is even, then $v_\mathfrak{p}(a)$ and $v_\mathfrak{p}(b)$ are both even.

Suppose first that $v_\mathfrak{p}(m_2)$ and $v_\mathfrak{p}(m_3)$ are both odd. Now local solubility of C_{13} implies that $(c_3 - c_1)m_1$ is a square; and Γ is locally soluble by (i) or (ii) above. Next suppose that $v_\mathfrak{p}(m_2)$ and $v_\mathfrak{p}(m_3)$ are both even but $v_\mathfrak{p}(c_2 - c_3)$ is odd; then local solubility of C_{23} implies that $m_2 m_3$ is a square and hence so is m_1. Now Γ is locally soluble by (i) or (ii) above. Finally suppose that $v_\mathfrak{p}(m_2)$, $v_\mathfrak{p}(m_3)$ and $v_\mathfrak{p}(c_2 - c_3)$ are all even. Now the local solubility of the C_{ij} provides no useful information. If $(c_3 - c_1)$ is not a square then Γ is locally soluble by (iii); but if $(c_3 - c_1)$ is a square then (i) shows that Γ is locally soluble if and only if a is a square. □

Except perhaps for Lemma 13, this is traditional folklore, first systematically described by Tate. The next step, which is due to Skorobogatov, is the construction inside each V_v of a maximal isotropic subspace K_v such that $V_\mathcal{B} = U_\mathcal{B} \oplus K_\mathcal{B}$. There is considerable freedom in choosing the K_v, and the way in which we do it in any particular case depends on the additional properties which are needed for the intended application. The construction starts with two general vector space lemmas, the second of which has a setting which generalizes the structure obtained above. The only reason for stating these lemmas, and also Lemma 16 below, in this more general form is notational convenience.

Lemma 14 *Let V be a finite dimensional vector space over a field k, equipped with a non-degenerate alternating bilinear form ψ; and let W be a maximal isotropic subspace of V. Then V can be expressed as a direct sum $\oplus V_i$ of mutually orthogonal subspaces, each of dimension 2, such that the restriction of ψ to any V_i is non-degenerate and each $V_i \cap W$ has dimension 1.*

Proof The existence of ψ shows that $\dim V$ is even; so let $\dim V = 2n$ with $n > 1$, the case $n = 1$ being trivial. It is enough to show that if w_1 is a non-trivial element of W then w_1 lies in a subspace V_1 satisfying the conditions of the lemma, and that if V' is the orthogonal complement of V_1 in V then $\dim(V' \cap W) = n - 1$; for we can then complete the proof by

induction on n. For this, choose x_1 in V not orthogonal to w_1. Let V_1 be the vector space generated by w_1 and x_1 and let V' be its orthogonal complement in V. Since V_1 is not isotropic, the restriction of ψ to V_1 is non-degenerate and $\dim(V_1 \cap W) = 1$. Now $V' \cap W$ is the subspace of W orthogonal to x_1; so $\dim(V' \cap W) \geq n-1$. On the other hand, w_1 is not in $V' \cap W$; so $\dim(V' \cap W) \leq n-1$. □

Lemma 15 *Let the V_i be n vector spaces over a field k, each equipped with a non-degenerate alternating bilinear form. Let $V = \bigoplus V_i$ be equipped with the direct sum of these forms; let U be maximal isotropic in V and for each i let W_i be maximal isotropic in V_i. Then there exist maximal isotropic subspaces $K_i \subset V_i$ such that $V = U \oplus (\bigoplus K_i)$. We can also ensure whichever we choose of $V_i = K_i \oplus W_i$ for each i or $W = (U \cap W) \oplus (K \cap W)$ where $W = \oplus W_i$ and $K = \oplus K_i$.*

Proof If any V_i has dimension greater than 2, we can by Lemma 14 decompose it as a direct sum of mutually orthogonal subspaces of dimension 2, on each of which the restriction of the bilinear form is non-degenerate and each of which meets W_i in a subspace of dimension 1. This only reduces our freedom to choose the K_i; so we can assume that every V_i has dimension 2. We proceed by induction on n, the case $n = 0$ being trivial. Suppose first that W_n is contained in U; then since U is isotropic it cannot contain V_n, and we can choose α_n in V_n but not in U. If instead W_n is not contained in U then it meets U only in the origin. Now V_n contains one element in $W_n \cap U$, at most one element in U but not in W_n, one element in W_n but not in U, and at least one element in neither W_n nor U. How we now choose α_n depends on what we are trying to achieve. For the first alternative in the lemma we take α_n to be in neither W_n nor U; for the second we take α_n to be in W_n but not in U. In either case, let K_n be the vector space generated by α_n. Write

$$V^- = V_1 \oplus \ldots \oplus V_{n-1}, \quad U^- = V^- \cap (U \oplus K_n). \tag{34}$$

If u^- is in U^- then $u^- = u + c\alpha_n$ for some c in k and u in U; so the last component of u as an element of V is $-c\alpha_n$ and U^- is isotropic. Since $\dim U^- \geq n-1$ by the second equation (34), U^- is maximal isotropic in V^-. Applying the induction hypothesis to the pair $U^- \subset V^-$, we can find K_i maximal isotropic in V_i for each $i < n$ such that $V^- = U^- \oplus (K_1 \oplus \ldots \oplus K_{n-1})$. But now, using (34) again,

$$(U \oplus K_n) \cap (K_1 \oplus \ldots \oplus K_{n-1}) \subset U^- \cap (K_1 \oplus \ldots \oplus K_{n-1}) = \{0\}.$$

By dimension count, this means that the sum of the two spaces on the left is the whole space V, which is the first assertion in the lemma. The second one is obvious from the construction. □

There is more freedom in the choice of the K_i than we have so far exploited. What we shall actually use in §6 is the result below, which represents a compromise between the two conclusions in Lemma 15. Let $\mathcal{B} \supset \mathcal{S}_1^+$ be the disjoint sum of the sets $\mathcal{B}' \supset \mathcal{S}_0^+$ and $\mathcal{B}''$.

Corollary *In the notation introduced in the first part of this section there exist maximal isotropic subspaces $K_v \subset V_v$ such that $V_\mathcal{B} = U_\mathcal{B} \oplus K_\mathcal{B}$,*

$$W_{\mathcal{B}'} = (U_{\mathcal{B}'} \cap W_{\mathcal{B}'}) \oplus (K_{\mathcal{B}'} \cap W_{\mathcal{B}'}),$$

and $K_v = T_v$ for all v in $\mathcal{B}''$.

Proof For $\mathcal{B} = \mathcal{B}'$ this follows from the lemma. In the general case, let the K_v for v in $\mathcal{B}'$ be those constructed for $\mathcal{B} = \mathcal{B}'$ and let $K_v = T_v$ for v in $\mathcal{B}''$. Now we need only prove that $V_\mathcal{B} = U_\mathcal{B} \oplus K_\mathcal{B}$, and by dimension count it is enough to prove that $K_\mathcal{B} \cap U_\mathcal{B}$ is trivial. By Lemma 12 any element of $K_\mathcal{B}$ has the form $\sigma \times \tau$. If $\sigma \times \tau$ is an element of $K_\mathcal{B} \cap U_\mathcal{B}$ then σ, τ must be units at v for any v in $\mathcal{B}''$; so $\sigma \times \tau$ belongs to the image of $U_{\mathcal{B}'}$ in $V_\mathcal{B} = V_{\mathcal{B}'} \oplus V_{\mathcal{B}''}$. Hence the projection onto $V_{\mathcal{B}'}$ of $\sigma \times \tau$ lies in $K_{\mathcal{B}'} \cap U_{\mathcal{B}'}$, which is trivial; so $\sigma = \tau = 1$. □

Let $t_\mathcal{B} : V_\mathcal{B} \to U_\mathcal{B}$ be the projection along $K_\mathcal{B}$ and write

$$U'_\mathcal{B} = U_\mathcal{B} \cap (W_\mathcal{B} + K_\mathcal{B}), \quad W'_\mathcal{B} = W_\mathcal{B}/(W_\mathcal{B} \cap K_\mathcal{B}) = \bigoplus\nolimits_{v \in \mathcal{B}} W'_v$$

where $W'_v = W_v/(W_v \cap K_v)$. The map $t_\mathcal{B}$ induces an isomorphism

$$\tau_\mathcal{B} : W'_\mathcal{B} \to U'_\mathcal{B};$$

and the bilinear function $e_\mathcal{B}$ induces a bilinear function

$$e'_\mathcal{B} : U'_\mathcal{B} \times W'_\mathcal{B} \to \{\pm 1\}.$$

We have already identified the 2-Selmer group with $U_\mathcal{B} \cap W_\mathcal{B}$, so it is contained in $U'_\mathcal{B}$ and is therefore the left kernel of $e'_\mathcal{B}$. Dimension counting shows that it is also isomorphic to the right kernel of $e'_\mathcal{B}$. If we choose the first alternative in Lemma 15 then $U'_\mathcal{B} = U_\mathcal{B}$ and $W'_\mathcal{B} = W_\mathcal{B}$; so we have constructed a natural (though not unique) isomorphism between $U_\mathcal{B}$ and $W_\mathcal{B}$.

The following symmetry property is of central importance. Later in this section we shall see that the K_i can be chosen so that the bilinear functions in Theorem 3 are actually alternating — that is, they take the value 1 when $u'_1 = u'_2$ or $w'_1 = w'_2$ respectively. But that result lies deeper.

Theorem 3 *The bilinear functions $U'_{\mathcal{B}} \times U'_{\mathcal{B}} \to \{\pm 1\}$ and $W'_{\mathcal{B}} \times W'_{\mathcal{B}} \to \{\pm 1\}$ defined respectively by*

$$u'_1 \times u'_2 \mapsto e'_{\mathcal{B}}(u'_1, \tau_{\mathcal{B}}^{-1}(u'_2)) \quad \textit{and} \quad w'_1 \times w'_2 \mapsto e'_{\mathcal{B}}(\tau_{\mathcal{B}} w'_1, w'_2) \tag{35}$$

are symmetric and their kernels are isomorphic to the 2-Selmer group of E.

Proof We need only prove the symmetry, and it is enough to do so for the first map. Given u'_1, u'_2 in $U'_{\mathcal{B}}$ let w_1, w_2 in $W_{\mathcal{B}}$ be such that $t_{\mathcal{B}} w_j = u'_j$. Since both the $(1 - t_{\mathcal{B}})w_j$ are in $K_{\mathcal{B}}$,

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

where the w'_j are the images in $W'_{\mathcal{B}}$ of the w_j. □

These results raise two obvious questions:

- How small can we make U' and W'?
- Can we ensure that the functions (35) are not merely symmetric but alternating?

Since $U'_{\mathcal{B}} \supset U_{\mathcal{B}} \cap W_{\mathcal{B}}$, for the first question the best that we can hope to achieve is $U'_{\mathcal{B}} = U_{\mathcal{B}} \cap W_{\mathcal{B}}$; and this follows from

$$W_{\mathcal{B}} = (U_{\mathcal{B}} \cap W_{\mathcal{B}}) \oplus (K_{\mathcal{B}} \cap W_{\mathcal{B}}) \tag{36}$$

which is the second alternative in Lemma 15. For suppose that (36) holds; then

$$W_{\mathcal{B}} + K_{\mathcal{B}} = (U_{\mathcal{B}} \cap W_{\mathcal{B}}) + K_{\mathcal{B}}$$

and it follows immediately that $U'_{\mathcal{B}} = U_{\mathcal{B}} \cap (W_{\mathcal{B}} + K_{\mathcal{B}}) = U_{\mathcal{B}} \cap W_{\mathcal{B}}$. Since this is the 2-Selmer group, and it can be identified with the left and right kernels of each of the functions (35), these functions are trivial and therefore alternating. We can summarize what we have so far achieved as follows.

Theorem 4 *We can choose the K_v so that* (36) *holds and $U'_{\mathcal{B}} = U_{\mathcal{B}} \cap W_{\mathcal{B}}$ is the 2-Selmer group of E.*

We also need to consider other recipes for choosing the K_v, for which (36) does not hold but we still wish to prove that the functions (35) are alternating. One important reason for this is that it enables us to study the effect of twisting on the 2-Selmer group. The *quadratic twist* of (29) by an element b of k^* is defined to be the elliptic curve

$$Y^2 = (X - bc_1)(X - bc_2)(X - bc_3)$$

where we can require the bc_i as well as the c_i to be integers. It simplifies the exposition to restrict ourselves to the case when $b = \kappa c$ where κ is a unit outside $\mathcal{S}_1^+$ and c is a unit at every prime in $\mathcal{S}_1^+$; this is not the most general case, though it is so when k has class number 1. Now if we replace every c_i by κc_i and E_κ by E, we are reduced to studying twisting by an integer c which is a unit at every prime in $\mathcal{S}_1^+$. We now formulate a strengthened version of Lemma 15; what we shall actually use is the Corollary to Lemma 16, which is a strengthened version of the Corollary to Lemma 15.

Lemma 16 *Suppose that the conditions of Lemma* 15 *hold, and that there are functions ϕ_i on V_i with values in $\{\pm 1\}$ which satisfy*

$$\phi_i(\xi + \eta) = \phi_i(\xi)\phi_i(\eta)\psi_i(\xi, \eta) \tag{37}$$

for any ξ, η in V_i. Let ϕ on V be the product of the ϕ_i. Assume that ϕ is trivial on U and ϕ_i is trivial on W_i. Then in addition to $V = U \oplus K$ and (36) *we can ensure that ϕ_i is trivial on K_i and ϕ is trivial on K.*

Proof As in the proof of Lemma 15, we can assume that every V_i has dimension 2; for if we prove that ϕ_i is trivial on K_i in this special case, the corresponding result for the general case will follow from (37). As before we proceed by induction on n, the case $n = 0$ being trivial; and we split cases according as W_n is contained in U or not. In the former case, since U is isotropic it cannot contain V_n; so there are two elements of V_n which do not lie in U. Denote them by α'_n and α''_n, and let β_n be the nontrivial element of W_n; thus $\alpha''_n = \alpha'_n + \beta_n$. Now $\phi_n(\beta_n) = 1$; so it follows from (37) that

$$\phi_n(\alpha'_n)\phi_n(\alpha''_n) = \psi_n(\alpha'_n, \beta_n) = -1$$

and we can choose α_n so that $\phi_n(\alpha_n) = 1$. In the latter case V_n meets $W_n \cap U$ only in the trivial element; so it contains at most one element in U but not in W_n, exactly one element in W_n but not in U, and at least one element in neither W_n nor U; we take α_n to be in W_n but not in U. In this case, $\phi_n(\alpha_n) = 1$ by hypothesis. Now that we have constructed α_n the remainder of the proof is identical with the last part of the proof of Lemma 15. In contrast with the situation in Lemma 15, any freedom in the choice of the K_i is restricted to the way in which the V_i of dimension greater than 2 are decomposed. □

When we apply Lemma 16 (with v for i) we replace ψ_i by e_v and take

$$\phi_v(\lambda \times \mu) = (\lambda, (c_2 - c_1)(c_2 - c_3))_v(\mu, (c_1 - c_2)(c_1 - c_3))_v(\lambda, \mu)_v. \qquad (38)$$

This formula can be put into a more convenient form, for

$$((c_1 - c_2)(c_1 - c_3), (c_1 - c_2)(c_3 - c_2))_v = \left(\frac{c_1 - c_3}{c_1 - c_2}, \frac{c_3 - c_2}{c_1 - c_2}\right)_v = 1$$

because the sum of the two arguments is 1. Hence

$$\phi_v(\lambda \times \mu) = (\lambda(c_1 - c_2)(c_1 - c_3), \mu(c_2 - c_1)(c_2 - c_3))_v.$$

The reason for this choice of ϕ_v will become evident below; but we need to check that these ϕ_v satisfy the conditions of Lemma 16. Here (37) is obvious, as is the triviality of ϕ on U. To verify that ϕ_v is trivial on W_v we argue as follows. It follows from (31) that

$$(c_2 - c_3)m_1Y_1^2 + (c_3 - c_1)m_2Y_2^2 + (c_1 - c_2)m_3Y_3^2 = 0 \qquad (39)$$

and therefore

$$(c_2 - c_1)(c_2 - c_3)m_2(m_1Y_1)^2 + (c_1 - c_2)(c_1 - c_3)m_1(m_2Y_2)^2 \\ = m_1m_2m_3((c_1 - c_2)Y_3)^2.$$

If the 2-covering (31) is soluble, then since $m_1m_2m_3$ is in k_v^{*2} this implies

$$((c_1 - c_2)(c_1 - c_3)m_1, (c_2 - c_1)(c_2 - c_3)m_2)_v = 1, \qquad (40)$$

which is just the result that we need.

We now combine the ideas of Lemma 16 and the Corollary to Lemma 15. The proof of the following result, apart from $U'_{\mathcal{B}'} = U_{\mathcal{B}'} \cap W_{\mathcal{B}'}$ which as we have already seen follows from (41), is essentially the same as that of the proof of the Corollary to Lemma 15. Let $\mathcal{B} \supset \mathcal{S}_1^+$ be the disjoint sum of the sets $\mathcal{B}' \supset \mathcal{S}_0^+$ and $\mathcal{B}''$, let $\psi_v = e_v$, and let ϕ_v be as above.

Corollary *In the notation above, there exist maximal isotropic subspaces $K_v \subset V_v$ such that $V_{\mathcal{B}} = U_{\mathcal{B}} \oplus K_{\mathcal{B}}$. Moreover we can ensure that the restriction of ϕ to $K_{\mathcal{B}'}$ is trivial,*

$$W_{\mathcal{B}'} = (U_{\mathcal{B}'} \cap W_{\mathcal{B}'}) \oplus (K_{\mathcal{B}'} \cap W_{\mathcal{B}'}), \tag{41}$$

$U'_{\mathcal{B}'} = U_{\mathcal{B}'} \cap W_{\mathcal{B}'}$, and $K_v = T_v$ for all v in $\mathcal{B}''$.

We use this machinery to study d_c, the dimension of the 2-Selmer group of E_c, under the constraint already introduced, that c is a unit at every prime in $\mathcal{S}_1^+$. Let $(c) = \mathfrak{p}_1 \dots \mathfrak{p}_M$ where none of the $\mathfrak{p}_i$ are in $\mathcal{S}_1^+$. As was said above, this restricts us to twisting by integers not divisible by any bad prime; any other twisting must be achieved by using E_κ instead of E. In the notation of the last Corollary, we take $\mathcal{B}' = \mathcal{S}_1^+$ and write $\mathcal{B}'' = \{\mathfrak{p}_1, \dots, \mathfrak{p}_M\}$. Since each $W_{\mathfrak{p}_\nu}$ is generated by the 2-division points of E_c and therefore has trivial intersection with $K_{\mathfrak{p}_\nu} = T_{\mathfrak{p}_\nu}$,

$$\dim U'_{\mathcal{B}} = \dim W'_{\mathcal{B}} = \dim W'_{\mathcal{B}'} + \dim W'_{\mathcal{B}''} = \dim U'_{\mathcal{B}'} + 2M. \tag{42}$$

Comparing dimensions now shows that the projection map

$$U'_{\mathcal{B}} \to V_{\mathcal{B}} \to V_{\mathcal{B}''} \to \oplus_{\nu=1}^{M} (k_{\mathfrak{p}_\nu}^* / \mathfrak{o}_{\mathfrak{p}_\nu}^* k_{\mathfrak{p}_\nu}^{*2})^2 \sim W_{\mathcal{B}''},$$

whose kernel is $U'_{\mathcal{B}'}$, is onto; here the map $V_{\mathcal{B}''} \to W_{\mathcal{B}''}$ is projection along $K_{\mathcal{B}''} = T_{\mathcal{B}''}$. In particular, there are elements $\alpha_\nu \times \beta_\nu$ and $\gamma_\nu \times \delta_\nu$ of

$$U'_{\mathcal{B}' \cup \{\mathfrak{p}_\nu\}} = U_{\mathcal{B}' \cup \{\mathfrak{p}_\nu\}} \cap ((W_{\mathcal{B}'} + K_{\mathcal{B}'}) \oplus V_{\mathfrak{p}_\nu}) \tag{43}$$

such that $\mathfrak{p}_\nu \| \alpha_\nu$, $\mathfrak{p}_\nu \| \delta_\nu$ and β_ν, γ_ν are units at $\mathfrak{p}_\nu$; and $U'_{\mathcal{B}'}$ and the $\alpha_\nu \times \beta_\nu$ and $\gamma_\nu \times \delta_\nu$ are linearly independent and span $U'_{\mathcal{B}}$. Here $\alpha_\nu \times \beta_\nu$ and $\gamma_\nu \times \delta_\nu$ are only determined up to elements of $U'_{\mathcal{B}'}$; and their images in $V_{\mathcal{B}'}$ lie in $W_{\mathcal{B}'} + K_{\mathcal{B}'}$ by (43), and therefore in $U'_{\mathcal{B}'} \oplus K_{\mathcal{B}'}$. We denote these images by $\widehat{\alpha_\nu} \times \widehat{\beta_\nu}$ and $\widehat{\gamma_\nu} \times \widehat{\delta_\nu}$; thus for example $\widehat{\alpha_\nu} \times \widehat{\beta_\nu}$ lies in $Y_{\mathcal{B}'} \times X_{\mathcal{B}'}$. By subtracting suitable elements of $U'_{\mathcal{B}'}$ from $\alpha_\nu \times \beta_\nu$ and $\gamma_\nu \times \delta_\nu$, we normalize them so that their images actually lie in $K_{\mathcal{B}'}$.

More generally, let $\sigma \times \tau$ be any element of $U'_{\mathcal{B}}$ and let $\hat{\sigma} \times \hat{\tau}$ be its projection onto $V_{\mathcal{B}'}$; then $\hat{\sigma} \times \hat{\tau}$ lies in $U'_{\mathcal{B}'} \oplus K_{\mathcal{B}'}$. It will be shown below that all the values which interest us can be expressed in terms of such projections and the places in $\mathcal{B}'$; so we can largely confine ourselves to these.

The recipe for calculating $\tau_{\mathcal{B}}^{-1}u$ for any u in $U'_{\mathcal{B}}$ is to project u to an element u_v of V_v for each v in $\mathcal{B}$ and then add whatever element of K_v is needed for the sum to lie in W_v; this sum is then projected into W'_v. Thus for example, if $\lambda\times\mu$ is in $U'_{\mathcal{B}'}$ then it is in $W_{\mathcal{B}'}$ and the component of $\tau_{\mathcal{B}}^{-1}(\lambda\times\mu)$ in W'_v for v in $\mathcal{B}'$ is just the coset of $W_v\cap K_v$ containing $\lambda\times\mu$; the component of $\tau_{\mathcal{B}}^{-1}(\lambda\times\mu)$ in W'_v for v in $\mathcal{B}''$ is trivial. Again the component of $\tau_{\mathcal{B}}^{-1}(\alpha_\nu\times\beta_\nu)$ in W'_v for v in $\mathcal{B}'$ is trivial because of the normalization above; since $W'_{\mathfrak{p}_\nu}=W_{\mathfrak{p}_\nu}$ is generated by the 2-division points, the component of $\tau_{\mathcal{B}}^{-1}(\alpha_\nu\times\beta_\nu)$ in $W'_{\mathfrak{p}_\nu}$ is $c(c_2-c_1)\times(c_2-c_1)(c_2-c_3)$ and its component in $W'_{\mathfrak{p}_\rho}$ for $\rho\neq\nu$ is again trivial. Similar statements hold for $\gamma_\nu\times\delta_\nu$. Denote by U_ν the subspace of $V_{\mathcal{B}}$ generated by $\alpha_\nu\times\beta_\nu$ and $\gamma_\nu\times\delta_\nu$, and write $U_0=U'_{\mathcal{B}'}$; thus

$$U'_{\mathcal{B}}=U_0\oplus U_1\oplus\ldots\oplus U_M. \tag{44}$$

Our next task is to obtain formulae for θ in terms of the decomposition (44), where $\theta=\theta_{\mathcal{B}}$ is the first of the bilinear functions in (35).

By the recipe above, if $\lambda\times\mu$ is in $U_0=U'_{\mathcal{B}'}$ then it follows from (33) that $\theta(\lambda\times\mu,\lambda\times\mu)=1$. Let χ_ν denote the quadratic character mod $\mathfrak{p}_\nu$; if $\lambda\times\mu$ is an element of U_0 we have

$$\theta(\lambda\times\mu,\alpha_\nu\times\beta_\nu)=\chi_\nu(\mu),\quad \theta(\lambda\times\mu,\gamma_\nu\times\delta_\nu)=\chi_\nu(\lambda).$$

If ρ, ν are distinct and nonzero, the restriction of θ to $U_\rho\times U_\nu$ is given by

$$\begin{aligned}\theta(\alpha_\rho\times\beta_\rho,\alpha_\nu\times\beta_\nu)&=\chi_\nu(\beta_\rho),\quad \theta(\gamma_\rho\times\delta_\rho,\gamma_\nu\times\delta_\nu)=\chi_\nu(\gamma_\rho),\\ \theta(\alpha_\rho\times\beta_\rho,\gamma_\nu\times\delta_\nu)&=\chi_\nu(\alpha_\rho),\quad \theta(\gamma_\rho\times\delta_\rho,\alpha_\nu\times\beta_\nu)=\chi_\nu(\delta_\rho).\end{aligned}$$

Similarly the restriction of θ to $U_\nu\times U_\nu$, where $\nu\neq 0$, is given by

$$\begin{aligned}&\theta(\alpha_\nu\times\beta_\nu,\alpha_\nu\times\beta_\nu)=\chi_\nu(\beta_\nu(c_2-c_1)(c_2-c_3)),\\ &\theta(\gamma_\nu\times\delta_\nu,\gamma_\nu\times\delta_\nu)=\chi_\nu(\gamma_\nu(c_1-c_2)(c_1-c_3)),\\ &\theta(\alpha_\nu\times\beta_\nu,\gamma_\nu\times\delta_\nu)=(c(c_2-c_1),\delta_\nu)_{\mathfrak{p}_\nu}=\chi_\nu(c\delta_\nu(c_1-c_2)),\\ &\theta(\gamma_\nu\times\delta_\nu,\alpha_\nu\times\beta_\nu)=(c(c_1-c_2),\alpha_\nu)_{\mathfrak{p}_\nu}=\chi_\nu(c\alpha_\nu(c_2-c_1)).\end{aligned}$$

Here symmetry gives us some non-trivial identities — for example that $\chi_\nu(-\alpha_\nu\delta_\nu)=1$. We can also write all the right hand sides above in terms of hatted letters and places in $\mathcal{B}'$; for example

$$\begin{aligned}\theta(\alpha_\nu\times\beta_\nu,\alpha_\nu\times\beta_\nu)&=(\alpha_\nu,\beta_\nu(c_2-c_1)(c_2-c_3))_{\mathfrak{p}_\nu}\\ &=\prod_{v\in\mathcal{B}'}(\alpha_\nu,\beta_\nu(c_2-c_1)(c_2-c_3))_v=\prod_{v\in\mathcal{B}'}(\widehat{\alpha_\nu},\widehat{\beta}_\nu(c_2-c_1)(c_2-c_3))_v.\end{aligned}$$

Let $\sigma \times \tau$ be any element of $U_1 \oplus \ldots \oplus U_M$; then $\hat{\sigma} \times \hat{\tau}$ lies in $K_{\mathcal{B}'}$ and an argument similar to that above shows that

$$\theta(\sigma \times \tau, \sigma \times \tau) = \{\prod \chi_\nu(\tau(c_2 - c_1)(c_2 - c_3))\}$$
$$\{\prod \chi_\nu(\sigma(c_1 - c_2)(c_1 - c_3))\}\{\prod \chi_\nu(\sigma\tau(c_3 - c_1)(c_3 - c_2))\}$$

where the three products are taken over the following sets of $\mathfrak{p}_\nu$ in $\mathcal{B}''$:

first product	$\mathfrak{p}_\nu$ divides σ but not τ to an odd power;
second product	$\mathfrak{p}_\nu$ divides τ but not σ to an odd power;
third product	$\mathfrak{p}_\nu$ divides both σ and τ to an odd power.

Replacing $\chi_\nu(\cdot)$ in the first product by $(\sigma, \cdot)_{\mathfrak{p}_\nu}$ and in the second by $(\tau, \cdot)_{\mathfrak{p}_\nu}$, using the fact that in the third product

$$\chi_\nu(\sigma\tau(c_3 - c_1)(c_3 - c_2))$$
$$= (\sigma, (c_2 - c_1)(c_2 - c_3))_{\mathfrak{p}_\nu}(\tau, (c_1 - c_2)(c_1 - c_3))_{\mathfrak{p}_\nu}(\sigma, -\sigma\tau)_{\mathfrak{p}_\nu}$$

where the last factor is equal to $(\sigma, \tau)_{\mathfrak{p}_\nu}$, and inserting some extra trivial factors, we obtain

$$\theta(\sigma \times \tau, \sigma \times \tau) = \prod_{\mathfrak{p} \in \mathcal{B}''} \{(\sigma, (c_2 - c_1)(c_2 - c_3))_{\mathfrak{p}}(\tau, (c_1 - c_2)(c_1 - c_3))_{\mathfrak{p}}(\sigma, \tau)_{\mathfrak{p}}\}.$$

By the Hilbert product formula this last expression is equal to

$$\prod_{v \in \mathcal{B}'} \{(\hat{\sigma}, (c_2 - c_1)(c_2 - c_3))_v(\hat{\tau}, (c_1 - c_2)(c_1 - c_3))_v(\hat{\sigma}, \hat{\tau})_v\}, \qquad (45)$$

which is just $\prod_{v \in \mathcal{B}'} \phi_v(\hat{\sigma}, \hat{\tau})$ in the notation of (38). By the Corollary to Lemma 16, this is equal to 1.

Theorem 5 *If d_c is the dimension of the 2-Selmer group of E_c and c is a unit at every place in $\mathcal{B}' = \mathcal{S}_1^+$, then d_c is congruent mod 2 to the dimension of $U_{\mathcal{B}'} \cap W_{\mathcal{B}'}$.*

Proof We choose $K_{\mathcal{B}'}$ in accordance with the Corollary to Lemma 16. What we have just shown is that $\theta(\sigma \times \tau, \sigma \times \tau)$ is trivial on $U_1 \oplus \ldots \oplus U_M$, and we already know that it is trivial on U_0. Since θ is a symmetric bilinear form with values in $\{\pm 1\}$, this implies that $\theta(\sigma \times \tau, \sigma \times \tau)$ is trivial on $U'_{\mathcal{B}}$. Hence

θ is alternating on $U'_{\mathcal{B}}$, so its rank is even and therefore its corank (which is d_c) is congruent mod 2 to $\dim U'_{\mathcal{B}}$ and therefore to $\dim U'_{\mathcal{B}'} = \dim(U_{\mathcal{B}'} \cap W_{\mathcal{B}'})$ by (42). This last expression is independent of the choice of $K_{\mathcal{B}'}$. □

We remind the reader that $W_{\mathcal{B}'}$ does depend on c, or more precisely on the image of c in $Y_{\mathcal{B}'}$. If one wishes to compute the d_b mod 2 for any particular curve (29), where $b = \kappa c$ as before, the best way appears to be as follows. One considers all the elements of $V_{\mathcal{B}'}$ for which the associated equation (39) is locally soluble at each place in $\mathcal{B}'$, and for each of them one determines the possible images of κc in $Y_{\mathcal{B}'}$ from one of the three relations like

$$m_2 Y_2^2 - m_3 Y_3^2 = \kappa c(c_3 - c_2).$$

Because weak approximation holds for the conic (39), these calculations can be carried out separately for each place in $\mathcal{B}'$. One then reverses the table thus generated, so that for each element of $Y_{\mathcal{B}'}$ one obtains a list of the possible triples m. Each such list is an $\mathbf{F}_2$-vector space, of dimension $d_{\kappa c}$.

The algorithm of Cassels carries out a 4-descent; more precisely he shows how to determine which elements of the 2-Selmer group survive the second descent. For this purpose he defines a skew-symmetric bilinear form $\langle \cdot, \cdot \rangle$ on the 2-Selmer group, whose kernel consists of those elements which survive the second descent. Here we confine ourselves to curves of the form (29). As before let $\mathcal{B} \supset \mathcal{S}_1^+$ and let $m^\sharp$ and $m^\flat$ be two triples which correspond to elements of the 2-Selmer group of (29). We can assume that the components of $m^\sharp$ and $m^\flat$ are integers all of whose prime factors lie in $\mathcal{B}$.

Each conic $C_{ij}^\sharp$ is an image of the 2-covering associated with $m^\sharp$; so it is soluble everywhere locally and therefore globally. Let $P_{ij}^\sharp$ be a rational point on $C_{ij}^\sharp$ and let $f_{ij}^\sharp = f_{ij}^\sharp(Y_0, Y_i, Y_j)$ be a homogeneous linear form such that $f_{ij}^\sharp = 0$ is the tangent to $C_{ij}^\sharp$ at $P_{ij}^\sharp$. For any v in $\mathcal{B}$ let $Q_v^\sharp$ be a v-adic point on the affine 2-covering induced by $m^\sharp$; we can clearly ensure that each $f_{ij}^\sharp(Q_v^\sharp)$ is a nonzero element of k_v. Then Cassels's skew-symmetric bilinear form is defined by

$$\langle m^\sharp, m^\flat \rangle = \prod_{v \in \mathcal{B}} \prod (f_{ij}^\sharp(Q_v^\sharp), m_k^\flat)_v \tag{46}$$

where the inner product is taken over the three cyclic permutations i, j, k of $1, 2, 3$.

6. *Pencils of curves of genus* 1.
In this section we shall be concerned with pencils of 2-coverings of elliptic curves, where the underlying pencil of elliptic curves has the form

$$E:\ Y^2 = (X - c_1(U,V))(X - c_2(U,V))(X - c_3(U,V)). \tag{47}$$

Here the $c_i(U,V)$ are homogeneous polynomials in $\mathfrak{o}[U,V]$ all having the same even degree. By means of a linear transformation on U, V we can ensure that the leading coefficients of the $c_i(U,V)$ are nonzero. Write

$$R(U,V) = p_{12}(U,V)p_{23}(U,V)p_{31}(U,V)$$

where $p_{ij} = c_i - c_j$.

The 2-coverings of (47) are given by

$$m_i(U,V)Y_i^2 = X - c_i(U,V) \text{ for } i = 1,2,3 \tag{48}$$

where the $m_i(U,V)$ are square-free homogeneous polynomials in $\mathfrak{o}[U,V]$ of even degree such that $m_1m_2m_3$ is a square. We should really regard the m_i as homogeneous polynomials modulo squares, but this complicates the notation. The equations (48) are equivalent to the three equations

$$m_iY_i^2 - m_jY_j^2 = (c_j - c_i)Y_0^2 \tag{49}$$

of which only two are independent. The sum of two such 2-coverings is obtained by multiplying the corresponding triples (m_1, m_2, m_3) componentwise and then removing squared factors. Denote by $V = V(m)$ the surface fibred by the curves (48) or (49), by $\Gamma = \Gamma(m; U, V)$ the curve given by the three equations (48) or the three equations (49) for particular values of m, U, V, and by $C_{ij} = C_{ij}(m; U, V)$ the conic given by a single equation (49). There are natural maps $\Gamma \to C_{ij}$. The equations (49) also imply

$$m_1(c_2 - c_3)Y_1^2 + m_2(c_3 - c_1)Y_2^2 + m_3(c_1 - c_2)Y_3^2 = 0, \tag{50}$$

and for Γ to be soluble so too must be this conic. This additional condition does not appear in the statement of Theorem 6, and in fact it follows from the conditions stated there; but it can be useful in some circumstances, as we shall see in §9.

Our objective is to provide sufficient conditions for the solubility of a particular pencil of curves Γ. We shall use a superscript 0 to denote this

particular curve and other objects connected with it. We need to distinguish between $\mathcal{S}$, the set of bad places for the pencil of curves Γ^0, and the larger set $\mathcal{B}$ of bad places for the particular curve $\Gamma^0(\alpha, \beta)$ on which we want to prove that there are rational points. The latter is the same $\mathcal{B} \supset \mathcal{S}_1^+$ as in §5. Thus $\mathcal{S}$ is a finite set containing the infinite places, the primes above 2, those which divide the resolvent of any two coprime factors of $R(U, V)$ in $\mathfrak{o}[U, V]$ or have norm not greater than $\deg(R(U, V))$, and those which are bad in the sense of §4 for any of the pencils of conics C_{ij}^0. In terms of the definitions below, $\mathcal{B}$ must contain $\mathcal{S}$ and all the $\mathfrak{p}_{k\tau}$. The additional prime $\mathfrak{p}$ which we introduce at each step of the algorithm should be thought of as being thereby adjoined to $\mathcal{S}$.

We denote the irreducible factors of $p_{ij}(U, V)$ in $k[U, V]$ by $f_{k\tau}(U, V)$, and we assume that the coefficients of any $f_{k\tau}$ are integers and that there is no prime outside $\mathcal{S}$ which divides all of them. When we apply the results of §5 it will be with $U = \alpha, V = \beta$ where $\alpha \times \beta$ is so chosen that each ideal $(f_{k\tau}(\alpha, \beta))$ is the product of primes in $\mathcal{S}$ and one prime outside $\mathcal{S}$; to do this we appeal to Lemma 2. The arguments of §5 show that we can confine ourselves to those triples m whose components take values in $\mathfrak{o}_{\mathcal{B}}^*$ when $U = \alpha, V = \beta$. This means that we can restrict the components of m to be products of some of the $f_{k\tau}(U, V)$ by elements of $\mathfrak{o}_{\mathcal{S}}^*$. In view of the description of 2-descents in §5, we can further restrict ourselves to the triples m such that $m_1 m_2 m_3$ divides R^2 and m_i is prime to p_{jk} in $k[U, V]$, where here and throughout this section i, j, k is any permutation of $1, 2, 3$.

We shall also assume that the $p_{ij}(U, V)$ are coprime in $k[U, V]$. The case when this condition fails is also of interest, but the methods used and the conclusions are quite different; for a more detailed account see [4]. This assumption is weaker than that in [6], which was that $R(U, V)$ is square-free in $k[U, V]$, and it enables us to bring the example in §9 within the scope of the general theory. But because we need to use Lemma 13, we do have to assume that if an irreducible factor $f_{k\tau}(U, V)$ divides p_{ij} to an even power, it also divides m_i^0 and m_j^0.

The parity conditions on the degrees of the c_i and m_i are needed to ensure that the curves (47) and Γ with $U = \alpha, V = \beta$ only depend on $\lambda = \alpha/\beta$ and not on α, β separately; otherwise we would not be dealing with pencils. But even if two of the m_i have odd degree, which can happen if R has factors of odd degree, the curve Γ given by (48) or (49) is a 2-covering of E; and such 2-coverings do play a part in our arguments. For given E, let G be the group of all triples (m_1, m_2, m_3) satisfying the conditions above, including that the

degrees of the m_i are even, and define $G^* \supset G$ by dropping the condition that the m_i have even degree. Provided we take the m_i modulo squares, both G and G^* are finite; and either G or G^* can be regarded as defining those pencils of 2-coverings of the pencil E which are of number-theoretic interest.

Now suppose that we are given a triple $m^0 = (m_1^0, m_2^0, m_3^0)$ in G. Denote by $\Gamma^0 = \Gamma(m^0, U, V)$ the curve of genus 1 given by the three equations (49) with $m = m^0$, and similarly for the C_{ij}^0. For the pencil of curves Γ^0 to contain rational points it must be everywhere locally soluble, and we shall always assume this. For simplicity we also assume that the elliptic curve (47) has no primitive 4-division points defined over $k(U, V)$, and to avoid trivialities we also assume that the 2-covering Γ^0 does not correspond to a 2-division point.

An essential tool in proving solubility will be the special case $n = 2$ of Lemma 1, which we restate for ease of reference.

Lemma 17 *Suppose that the Tate-Shafarevich group of E/k is finite and the 2-Selmer group of E has order 8. Then every curve representing an element of the 2-Selmer group contains rational points.*

As this shows, everything in this section will depend on Hypothesis Ш; and almost everything will also depend on Schinzel's Hypothesis. We retain the notation for 2-descents introduced in §5, and in the notation of the Corollary to Lemma 15 we take $\mathcal{B}' = \mathcal{S}_0^+$.

The only values of U/V for which Γ^0 can be soluble are ones for which Γ^0 is everywhere locally soluble; so for any such value of U/V the 2-Selmer group of E must contain the subgroup of order 8 generated by Γ^0 and the 2-coverings coming from the 2-division points. We shall call this the *inescapable* part of the 2-Selmer group.

In contrast to what happened in §4, we cannot simply apply Lemma 2 to choose α, β so that all the $f_{k\tau}(\alpha, \beta)$ are prime up to possible factors in $\mathcal{S}$, because this might give rise to a 2-Selmer group too big for us to be able to apply Lemma 17. (Note that by (iii) below, the order of this 2-Selmer group will be independent of the choice of α, β, provided that $\alpha \times \beta$ is confined to a small enough open set in the topology induced by $\mathcal{S}$.) What we do instead is most conveniently described as an algorithm, which consists of repeatedly introducing a further well-chosen prime $\mathfrak{p}$ into $\mathcal{S}$, with a corresponding extra condition on the set $\mathcal{A}$ of possible values of $U \times V$, in such a way that if we then apply Lemma 2 the dimension of the 2-Selmer group is one less than it would have been before. If we can go on doing this as long as the 2-Selmer

group remains too big, we shall eventually reach a situation to which we can apply Lemma 17. What we thereby obtain is Theorem 6 below.

The process of introducing a new prime $\mathfrak{p}$ is as follows. We choose an $f_{k\tau}$ and integers $\alpha_\mathfrak{p}, \beta_\mathfrak{p}$ not both divisible by $\mathfrak{p}$ and such that $\mathfrak{p}|f_{k\tau}(\alpha_\mathfrak{p}, \beta_\mathfrak{p})$. Without loss of generality we can assume that $\alpha_\mathfrak{p}, \beta_\mathfrak{p}$ are coprime and that $\mathfrak{p}\|f_{k\tau}(\alpha_\mathfrak{p}, \beta_\mathfrak{p})$. Choose integers $\gamma_\mathfrak{p}, \delta_\mathfrak{p}$ such that $\alpha_\mathfrak{p}\delta_\mathfrak{p} - \beta_\mathfrak{p}\gamma_\mathfrak{p} = 1$, make the change of variables

$$U = \alpha_\mathfrak{p}U_1 + \gamma_\mathfrak{p}V_1, \quad V = \beta_\mathfrak{p}U_1 + \delta_\mathfrak{p}V_1$$

and impose on $\mathcal{A}$ the additional condition $\mathfrak{p}^2|V_1$. Thus at any point of $\mathcal{A}$ the value of $f_{k\tau}$ is exactly divisible by $\mathfrak{p}$, and hence the values of all the other functions $f_{..}$ are prime to $\mathfrak{p}$.

As we noted just after (32), in the notation of §5 all the triples in $W_\mathfrak{p}$ have $v_\mathfrak{p}(m_k)$ even. Since $K_\mathfrak{p} = T_\mathfrak{p}$, the set of triples all whose components are units at $\mathfrak{p}$, it follows that $W_\mathfrak{p} \cap K_\mathfrak{p}$ has dimension 1 and so has $W'_\mathfrak{p}$. A similar argument holds for the primes $\mathfrak{p}_{k\tau}$ provided by Lemma 2.

Which $\mathfrak{p}$ satisfy the condition that there exist $\alpha_\mathfrak{p}, \beta_\mathfrak{p}$ as above? For any irreducible factor $f_{k\tau}(U, V)$ of $p_{ij}(U, V)$, let $K_{k\tau} = k[X]/f_{k\tau}(X, 1)$ be the field obtained by adjoining to k a root of $f_{k\tau}$, and let $\xi_{k\tau}$ be the class of X in $K_{k\tau}$; thus $f_{k\tau}(\xi_{k\tau}, 1) = 0$. For the time being we suppose m fixed, and the field $L_{k\tau}$ which we shall define will depend on m. The singular fibres of the pencil of elliptic curves (47), as also those of the pencil of 2-coverings (49), correspond to the roots of the $f_{k\tau}$. The reason for being interested in the singular fibres is as follows. Let $\mathfrak{p}$ be a prime of k not in $\mathcal{S}$, and let $\alpha_\mathfrak{p}, \beta_\mathfrak{p}$ in $\mathfrak{o}$ be such that $\mathfrak{p}\|f_{k\tau}(\alpha_\mathfrak{p}, \beta_\mathfrak{p})$; such $\alpha_\mathfrak{p}, \beta_\mathfrak{p}$ exist if and only if there is a prime $\mathfrak{P}$ in $K_{k\tau}$ whose relative norm over k is $\mathfrak{p}$. This last condition may appear tiresome. But what one really does is to choose a first-degree prime $\mathfrak{P}$ in $K_{k\tau}$ and define $\mathfrak{p}$ to be the prime below it in k. Now norm$\mathfrak{P} = \mathfrak{p}$ is automatic.

The solubility of Γ^0 certainly requires that each pencil C^0_{ij} be soluble; so Theorem 1 provides necessary conditions for the solubility of Γ^0. But we have examples to show that they are not sufficient to ensure that there is a point $\alpha \times \beta$ at which Γ^0 is soluble. In previous papers we have therefore introduced a further condition, which we call Condition D; and we shall do this again in the last part of the proof of Theorem 6. The formulation of Condition D here, which can be found near the end of this section, is superficially rather different to that in previous papers; but the new version is easily seen to be essentially the same as the older one. It is in fact a stronger condition than we need; see the discussion at the end of this section.

As in §4, we need to work not in $\mathbf{P}^1$ but in the subset $\mathbf{L}^1$ obtained by deleting the points $\lambda = \alpha/\beta$ at which $R(\alpha, \beta)$ vanishes. The topology on $\mathbf{L}^1(k)$ will be that induced by $\mathcal{S}$. There is an open set $\mathcal{N} \subset \mathbf{L}^1(k)$ such that $\Gamma^0(\alpha, \beta)$ is soluble at every place of $\mathcal{S}$ if and only if λ lies in $\mathcal{N}$. We have already imposed the condition that $\mathcal{N}$ is not empty.

Theorem 6 *Assume Schinzel's Hypothesis and Hypothesis* Ш*, and suppose that the three $p_{ij}(U, V)$ are coprime in $k[U, V]$ and that any $f_{k\tau}$ which divides p_{ij} to an even power divides m_i^0 and m_j^0 to odd powers. Suppose that Condition D holds, and let $\mathcal{A} \subset \mathcal{N}$ be the open subset of $\mathbf{L}^1(k)$ at which each pencil of C_{ij}^0 is soluble. Then $\mathcal{A}$ lies in the closure of the set of λ in $\mathbf{L}^1(k)$ at which $\Gamma^0(\alpha, \beta)$ is soluble in k.*

Technically Theorem 6 is not a weak approximation theorem, in contrast with the situation for conics, because weak approximation does not hold on curves of genus 1; but it can be regarded as a theorem of 'weak approximation type'. Theorem 6 gives a sufficient condition for the Hasse principle to hold, though the condition is not always necessary. Indeed, we shall see at the end of this section that we can replace Condition D by a potentially weaker Condition E; but even the latter is not always necessary for solubility. The relation between Condition D and the Brauer-Manin obstructions is addressed in [6].

The arguments needed to validate each step of the algorithm are lengthy, and for clarity we list them as (i) to (v) below. We impose further conditions on the additional prime $\mathfrak{p}$, which ensure (i); we then deduce (ii), (iii) and (iv). Finally we show that unless the process is complete, we can choose $\mathfrak{p}$ so that (v) holds. After all this we choose $\alpha \times \beta$ according to the recipe in Lemma 2 for the $f_{k\tau}$, and with the additional property that $L(\mathcal{S}; U, V; \alpha, \beta) = 1$ if there is any $f_{k\tau}$ of odd degree. One can satisfy this additional requirement by a slight modification of the construction used to prove Lemma 2. Alternatively, one can render it unnecessary by replacing U, V by homogeneous quadratic forms in U_1, V_1; this does not alter the values of the functions L.

Denote by $\mathfrak{p}_{k\tau}$ the additional prime in k which divides $f_{k\tau}(\alpha, \beta)$ when $\alpha \times \beta$ is chosen according to the recipe in Lemma 2; then every $f_{k\tau}(\alpha, \beta)$ is a unit outside the set $\mathcal{B}$ obtained by adjoining $\mathfrak{p}$ and all the $\mathfrak{p}_{k\tau}$ to $\mathcal{S}$, and $f_{k\tau}(\alpha, \beta)$ is divisible to precisely the first power by $\mathfrak{p}_{k\tau}$ and by $\mathfrak{p}$. The set $\mathcal{B}$ thus defined will be the appropriate set $\mathcal{B}$ for applying the results of §5. What is crucial is that we have good local information about the $\mathfrak{p}_{k\tau}$ at each place in $\mathcal{S}$ before α and β are chosen; thus the descent process in §5 can be

carried out uniformly in α, β provided that $\alpha \times \beta$ lies in a small enough open set.

(i) We determine necessary and sufficient conditions for $\Gamma(\alpha, \beta)$ to be locally soluble at $\mathfrak{p}$. We use these immediately to ensure that $\Gamma^0(\alpha, \beta)$ is locally soluble at $\mathfrak{p}$; but in (v) we shall also need them to ensure for a particular m that the corresponding $\Gamma(\alpha, \beta)$ is not locally soluble at $\mathfrak{p}$.

By requiring that $\lambda = \alpha/\beta$ is in $\mathcal{A}$ we have ensured that $\Gamma^0(\alpha, \beta)$ is soluble in k_v for every v in $\mathcal{S}$. From (i) we deduce:

(ii) The curve $\Gamma^0(\alpha, \beta)$ is locally soluble at each $\mathfrak{p}_{k\tau}$.

Thus (i) and (ii) prove that the class of $\Gamma^0(\alpha, \beta)$ is in the 2-Selmer group of the curve $E(\alpha, \beta)$ given by (47) provided that α, β are chosen according to the recipe in Lemma 2. The $\mathfrak{p}_{k\tau}$ are not determined until we know α and β; but this is unimportant because of the next result:

(iii) The bilinear form $e^*_{\mathcal{B}} : \ W'_{\mathcal{B}} \times W'_{\mathcal{B}} \to \{\pm 1\}$ defined in Theorem 3 is effectively independent of the choice of $\alpha \times \beta$ and hence of the $\mathfrak{p}_{k\tau}$.

By this we mean that if we change α, β, thereby replacing the old W' by a new W' canonically isomorphic to it and replacing the old $\mathfrak{p}_{k\tau}$ in $\mathcal{B}$ by the new ones, then this isomorphism preserves $e^*_{\mathcal{B}}$. The next result which we need, which is only meaningful once we have proved (iii), is as follows:

(iv) We determine the effect on the function $e^*_{\mathcal{B}}$ of introducing a new prime $\mathfrak{p}$ in the way described above.

Finally, the condition which we need for our algorithm to achieve what we want is as follows:

(v) If m is in the kernel of the old $e^*_{\mathcal{B}}$ but not in the inescapable part of it, then we can introduce a new prime $\mathfrak{p}$ which removes m from the kernel and does not put anything new in.

It is in the proof of (v) that we need Condition D. Once we have (v), we can after a sufficient number of steps satisfy the conditions of Lemma 17, and this implies that $\Gamma^0(\alpha, \beta)$ has rational solutions.

Achieving (i). The condition that any particular Γ is soluble in $k_{\mathfrak{p}}$ throughout some neighbourhood of $\alpha_{\mathfrak{p}} \times \beta_{\mathfrak{p}}$ is that the reduction of $\Gamma(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$ mod $\mathfrak{p}$ should

contain a point defined over $\mathfrak{o}/\mathfrak{p}$ which is liftable to a point on Γ defined over $k_\mathfrak{p}$. Denote by $L_{k\tau}$ the least extension of $K_{k\tau}$ over which some absolutely irreducible component of the singular fibre at $\xi_{k\tau} \times 1$ is defined; conveniently, all these components are defined over the same least extension, which is normal over $K_{k\tau}$. The decomposition of $\Gamma(\alpha_\mathfrak{p}, \beta_\mathfrak{p}) \bmod \mathfrak{p}$ corresponds to the decomposition of the fibre $\Gamma(\xi_{k\tau}, 1)$; so we can solve Γ in $k_\mathfrak{p}$ in a suitable neighbourhood of $\alpha_\mathfrak{p} \times \beta_\mathfrak{p}$ if and only if $\mathfrak{P}$ splits completely in $L_{k\tau}$.

If $f_{k\tau} \| p_{ij}$, each singular fibre given by $f_{k\tau} = 0$ of the pencil of curves Γ splits as a pair of irreducible conics which meet in two points and are each defined over the field $L_{k\tau} = K_{k\tau}(\sqrt{g_{k\tau}(\xi_{k\tau}, 1)})$; here $g_{k\tau} = m_k$ if $f_{k\tau}$ divides neither of m_i and m_j or $g_{k\tau} = m_k p_{jk}$ if $f_{k\tau}$ divides both of them. The same holds if $f_{k\tau}^2 | p_{ij}$ and $f_{k\tau}$ divides neither m_i nor m_j, and again we have $g_{k\tau} = m_k$; note that this is the case in which the supplementary condition in Lemma 13 applies. If $f_{k\tau}^2 | p_{ij}$ and $f_{k\tau}$ divides both m_i and m_j, then each singular fibre given by $f_{k\tau} = 0$ splits as a set of four lines which form a skew quadrilateral, and each of these lines is defined over

$$L_{k\tau} = K_{k\tau}\left(\sqrt{m_k(\xi_{k\tau}, 1)}, \sqrt{p_{jk}(\xi_{k\tau}, 1)}\right). \tag{51}$$

Write $L_{k\tau}^0$ for the field corresponding to Γ^0 under this construction. To test for Condition D, we need to list those m for which $L_{k\tau}$ is contained in $L_{k\tau}^0$. It is easy to verify that they form a group, which contains m^0 and the triples coming from the 2-division points.

Proof of (ii). It follows from Lemma 13 and the hypotheses of Theorem 6 that $\Gamma^0(\alpha, \beta)$ is locally soluble at each $\mathfrak{p}_{k\tau}$ if and only if the same is true for each $C_{ij}^0(\alpha, \beta)$; and similarly for $\mathfrak{p}$. We know by (i) that $\Gamma^0(\alpha, \beta)$ is locally soluble at $\mathfrak{p}$. We have assumed that the solubility conditions (26) for the $C_{ij}^0(\alpha, \beta)$ hold. In the product (26) if there is a factor for $\mathfrak{p}$ its value is 1, so the value of the factor for $\mathfrak{p}_{k\tau}$ is also 1; hence each $C_{ij}^0(\alpha, \beta)$ is locally soluble at $\mathfrak{p}_{k\tau}$. Now Lemma 13 shows that $\Gamma^0(\alpha, \beta)$ is locally soluble at $\mathfrak{p}_{k\tau}$. It is the escape clause in Lemma 13 which forces on us the additional condition in the first sentence of Theorem 6.

Proof of (iii). We are allowed to choose $\alpha \times \beta$ only within a set which is small in the topology induced by $\mathcal{S}$. In particular, this means that the power of any prime in $\mathcal{S}$ which divides any $f_{k\tau}(\alpha, \beta)$ is independent of α and β. Since the only other prime which divides any particular $f_{k\tau}(\alpha, \beta)$ is $\mathfrak{p}_{k\tau}$, which does so to the first power, the ideal class of $\mathfrak{p}_{k\tau}$ is fixed. If the place v is given by

some $\mathfrak{p}_{k\tau}$ then a generator of W'_v can be lifted back to $\sigma \times \tau$ where each of σ and τ is either 1 or $f_{k\tau}(\alpha, \beta)$; and if v is in $\mathcal{S}$ the elements of a base for W'_v can be lifted back to elements $\sigma \times \tau$ independent of α, β with σ, τ in $\mathfrak{o}^*_{\mathcal{S}}$. We choose a base for $W'_{\mathcal{B}}$ composed of these two kinds of elements; then the value of $e^*_{\mathcal{B}}$ at any pair of elements of this base is a product of expressions of the form $(\sigma'(\alpha, \beta), \tau'(\alpha, \beta))_v$ where v is in $\mathcal{B}$ and each of σ' and τ' is the product of an element of $\mathfrak{o}^*_{\mathcal{S}}$ and possibly an $f_{k\tau}$. If v is in $\mathcal{S}$ the value of this expression is independent of α, β. If v is given by $\mathfrak{p}_{k\tau}$ then using symmetry and $(\xi, -\xi)_v = 1$ if necessary we can reduce to the case when σ' is not divisible by $f_{k\tau}$. If also τ' is not divisible by $f_{k\tau}$ then $(\sigma'(\alpha, \beta), \tau'(\alpha, \beta))_v = 1$; otherwise $(\sigma'(\alpha, \beta), \tau'(\alpha, \beta))_v = L(\mathcal{S}; \sigma', \tau'; \alpha, \beta)$ is continuous by Lemma 5 and the proviso shortly after the statement of Theorem 6.

Achieving (iv). Let α', β' be such that every ideal $(f_{i\sigma}(\alpha', \beta'))$ is the product of a prime ideal $\mathfrak{p}'_{i\sigma}$ and ideals in $\mathcal{S}$; and let α'', β'' be such that $(f_{k\tau}(\alpha'', \beta''))$ is the product of $\mathfrak{p}\mathfrak{p}''_{k\tau}$ and ideals in $\mathcal{S}$, while any other $(f_{i\sigma}(\alpha'', \beta''))$ is the product of $\mathfrak{p}''_{i\sigma}$ and ideals in $\mathcal{S}$. In the obvious notation, we take a base for $W'_{\mathcal{B}'}$ as in the proof of (iii); replacing $\alpha' \times \beta'$ by $\alpha'' \times \beta''$ in this base, we obtain a linearly independent set of elements of $W'_{\mathcal{B}''}$ and we do not change the values of e^*. By adjoining the non-trivial element of $W'_{\mathfrak{p}}$ we can extend this linearly independent set to a base for $W'_{\mathcal{B}''}$. In other words, there is a natural injection of $W'_{\mathcal{B}'}$ into $W'_{\mathcal{B}''}$ which preserves e^*.

Choice of $\mathfrak{p}$. Let $w_{\mathfrak{p}}$ be a lift to $W_{\mathfrak{p}}$ of the non-trivial element of $W'_{\mathfrak{p}}$, and let m be an element of $U_{\mathcal{B}} \cap W_{\mathcal{B}}$ which is not in the inescapable part of the 2-Selmer group. Thus $\tau_{\mathcal{B}}^{-1} m$ is in the kernel of $e^*_{\mathcal{B}}$. Suppose that we can choose $\mathfrak{p}$ so that the 2-covering corresponding to m is locally insoluble at $\mathfrak{p}$. On the one hand this is equivalent to $e^*(\tau_{\mathcal{B}}^{-1} m, w_{\mathfrak{p}}) = -1$, which in the notation of the previous paragraph implies that the kernel of $e^*_{\mathcal{B}''}$ is contained in the image of the kernel of $e^*_{\mathcal{B}'}$. On the other hand it requires $\mathfrak{P}$ to split completely in $L^0_{k\tau}$ but not in $L_{k\tau}$. The condition below, which in these notes we call Condition D, ensures that such a choice is possible. We shall see later that Condition D can be replaced by a weaker condition, but one which is less natural and sometimes less computationally convenient.

> Condition D: *If m is not in the inescapable subgroup of the 2-Selmer group, then there is a pair k, τ such that the field $L_{k\tau}$ is not contained in $L^0_{k\tau}$.*

We can incorporate the definitions of $L_{k\tau}$ and $L^0_{k\tau}$ into this condition, thereby

putting it into a form closer to that of earlier papers, as follows:

The kernel of the composite map

$$m \mapsto \oplus_{k,\tau} g_{k\tau}(m) \mapsto \oplus_{k,\tau} K^*_{k\tau}/\langle K^{*2}_{k\tau}, H_{k\tau}\rangle$$

is generated by the inescapable subgroup of the 2-Selmer group, where

$$g_{k\tau} = \begin{cases} m_k & \text{if } f_k \text{ divides neither of } m_i \text{ and } m_j, \\ m_k p_{jk} & \text{if } f_k \text{ divides both of } m_i \text{ and } m_j, \end{cases}$$

and

$$H_{k\tau} = \begin{cases} m_k(\xi_{k\tau}, 1) & \text{if } f_{k\tau} \text{ divides neither of } m_i \text{ and } m_j, \\ m_k(\xi_{k\tau}, 1)p_{jk}(\xi_{k\tau}, 1) & \text{if } f_{k\tau} \| p_{ij} \text{ and } f_{k\tau} \text{ divides } m_i \text{ and } m_j, \\ \{m_k(\xi_{k\tau}, 1), p_{jk}(\xi_{k\tau}, 1)\} & \text{if } f^2_{k\tau} \| p_{ij} \text{ and } f_{k\tau} \text{ divides } m_i \text{ and } m_j. \end{cases}$$

By a slight abuse of language, we shall say that the m for which $L_{k\tau}$ is contained in $L^0_{k\tau}$ are those which do not satisfy Condition D. If Condition D holds we can choose k, τ and a $\mathfrak{P}$ which splits in $L^0_{k\tau}$ but not in $L_{k\tau}$. The underlying $\mathfrak{p}$ has the properties we want. But the arguments in (iv) show that the process has removed m from the 2-Selmer group without creating any new elements of that group. So we have certainly decreased the dimension of the 2-Selmer group, which is what we needed to show to justify the algorithm. In fact it is easy to show that we have decreased it by exactly 1.

It will be seen that we have not used the full force of Condition D; indeed it is stated for all elements of G^*, but we have only used it for those elements which lie in the initial 2-Selmer group. These are the ones for which the corresponding 2-covering is locally soluble at each place in $\mathcal{B}$. The proof of (ii) above shows that local solubility in $\mathcal{S}$ implies local solubility at each $\mathfrak{p}_{k\tau}$; and the proof of (iii) shows that this 2-Selmer group, considered as a subgroup of G^*, does not vary as $\alpha \times \beta$ varies within a small enough open set. We actually use Condition D only for the m which lie in this 2-Selmer group; and to require merely that such m satisfy Condition D is weaker than the full Condition D. We call this weaker condition, an equivalent form of which has already appeared in [14] and [15], Condition E. Its disadvantage is that Condition D is independent of α and β, whereas this is only true

of Condition E when $\alpha \times \beta$ is restricted to a small enough open set. A particularly favourable case is when the 2-Selmer group has order 8, so that Condition E is trivial. I do not know whether Condition E, together with the conditions imposed in Theorem 6, is necessary as well as sufficient for global solubility, nor whether these conditions are together equivalent to the Brauer-Manin conditions.

Suppose however that even Condition E fails, and let $m^\sharp, m^\flat$ be any two elements of the kernel; to avoid trivialities we may assume that neither of them is $(1,1,1)$ or comes from a 2-division point. We have examples in which the Cassels form (46) for such triples can be evaluated as a function of α, β; and whenever we can evaluate it, it turns out to be continuous in the topology induced by $\mathcal{S}$. It would be very interesting to know if this is a general phenomenon.

7. *Some variants.*
In this section we outline two ways of extending the results of §6. What they have in common is that each of them involves the simultaneous consideration of descent on two pencils of elliptic curves, rather than just the one pencil which we were concerned with in §6. For each of these pencils we have a pencil of coverings ($\sqrt{-3}$-coverings in §7.1 and 2-coverings in §7.2), both pencils being parametrized by the same parameter. Our objective is to choose a value of the parameter in such a way that both the coverings are simultaneously soluble; as in §6 we have to do this by ensuring that both Selmer groups are small. There is however one major difference between the two subsections; in §7.1 the two elliptic curves which we have to deal with are unrelated, whereas in §7.2 they are isogenous to each other. We continue to need Hypothesis Ш.

The arguments in §7.1 enable us, without using Schinzel's Hypothesis, to prove the solubility of diagonal cubic surfaces

$$a_0X_0^3 + a_1X_1^3 = a_2X_2^3 + a_3X_3^3 \tag{52}$$

over certain algebraic number fields k, subject to a condition on the a_i which is stronger, but not much stronger, than the Brauer-Manin condition. The reason why we do not need Schinzel's Hypothesis in this case is that we need the results of Lemma 2 only for a single linear polynomial, so that Lemma 2 can be replaced by Dirichlet's theorem on primes in arithmetic progression.

In §7.2 we mimic the ideas of §6 in the case when the Jacobian has only one rational 2-division point; in particular this enables us to address in §8 the question of the existence of rational points on Del Pezzo surfaces of degree 4. The approach in §8 also does not require Schinzel's Hypothesis, though for a totally different reason. The price of each of these refinements is that the corresponding argument becomes more intricate; what we give here is only an outline sufficient to show the ideas involved, and we refer any sufficiently intrepid reader to the original papers for the details. These papers are [16] for the first case, and [1] or [3] for the second.

7.1 *Diagonal cubic surfaces.*
Without loss of generality we can assume that the a_i in (52) are integers. To show that (52) has a rational solution it is enough to show that there exists c in k^* such that each of the two curves

$$a_0X_0^3 + a_1X_1^3 = cX^3, \quad \text{and} \quad a_2X_2^3 + a_3X_3^3 = cX^3 \tag{53}$$

is soluble. The hypothesis that (52) is everywhere locally soluble implies that for each place v in k there exists c_v in k_v^* such that each of

$$a_0X_0^3 + a_1X_1^3 = c_vX^3, \quad \text{and} \quad a_2X_2^3 + a_3X_3^3 = c_vX^3$$

is soluble in k_v. The first step in the argument is to deduce the existence of c in k^* such that each of the two equations (53) is everywhere locally soluble. Such a c always exists; and indeed if $\mathcal{S}$ is any given finite set of places of k, we can choose c integral and such that c/c_v is in k_v^{*3} for each v in $\mathcal{S}$. Following the methods of §6, we denote by $\mathbf{L}^1$ the affine line with the origin deleted. Let $\mathcal{S}$ be a set of bad places for the surface (52), which means that $\mathcal{S}$ must contain all the primes of k dividing $3a_0a_1a_2a_3$; and let $\mathcal{B} \supset \mathcal{S}$ be a set of bad places for the pair of curves (53), so that $\mathcal{B}$ must also contain all the primes dividing c. Under the topology induced by $\mathcal{S}$, let $\mathcal{A}$ be the open subset of $\mathbf{L}^1(k)$ on which each of the two curves (53) is locally soluble at each place of $\mathcal{S}$, let c_0 be a given point of $\mathcal{A}$ and let $\mathcal{N}_0 \subset \mathcal{A}$ be an open neighbourhood of c_0. Because of the possible presence of Brauer-Manin obstructions, it is not necessarily true that there exists c in $\mathcal{N}_0$ such that the two equations (53) are both soluble. But one may still ask what additional assumptions are needed in order to prove solubility by the methods of §6 — always of course on the basis that Hypothesis Ш holds.

The Jacobians of the two curves (53) are

$$Y_0^3 + Y_1^3 = a_0a_1cY^3 \quad \text{and} \quad Y_2^3 + Y_3^3 = a_2a_3cY^3 \tag{54}$$

respectively. The obvious descent to apply to each of them is the ρ-descent, where $\rho = \sqrt{-3}$. Applying this to the elliptic curve

$$X^3 + Y^3 = AZ^3 \tag{55}$$

replaces it by the equations

$$\rho X + \rho^2 Y = m_1Z_1^3, \quad \rho^2 X + \rho Y = m_2Z_2^3, \quad X + Y = AZ_3^3/m_1m_2$$

where $Z = Z_1Z_2Z_3$. Here m_1, m_2, Z_1, Z_2 are in $K = k(\rho)$ and m_1, m_2 are conjugate over k, as are Z_1, Z_2; but Z_3 is in k. It would appear natural to work in K rather than k, since if (52) is soluble in K it is soluble in k. But actually our methods could not then be applied, for complex multiplication by ρ induces an isomorphism on (55), so that the Mordell-Weil group of (55) over K has an even number of generators of infinite order and there is no

possibility of applying Lemma 1. In other words, a prerequisite for applying the methods of §6 is the following unexpected constraint:

$$\sqrt{-3} \text{ is not in } k. \tag{56}$$

This does however allow us to take $k = \mathbf{Q}$, for example. But even if (56) holds, there is considerable interplay between the descent theory over K and that over k; and it seems necessary to make use of this interplay in the argument.

The basic idea is to write c as a product of primes in $\mathcal{S}$ (which are forced on us by the choice of $\mathcal{N}_0$) and some other well-chosen primes; the latter make up the set $\mathcal{B} \setminus \mathcal{S}$. We need to choose the latter so that the ρ-Selmer group of each of the curves (54) has order 9; and following the precedent of §6 we expect to do this by adjoining additional primes one by one to $\mathcal{B}$, always preserving the local solubility of the curves (53) and keeping c within $\mathcal{N}_0$. The latter condition simply means that each new prime $\mathfrak{p}$ should be close to 1 in our topology and should be such that a_0/a_1 and a_2/a_3 are in $k_{\mathfrak{p}}^{*3}$. But here we encounter the final pair of complications. To adjoin one more prime divides or multiplies the order of each ρ-Selmer group by 3. If one of these orders has already been reduced to 9 we cannot reduce it further; so adjoining one more prime can no longer improve the situation. Instead we eventually reach the stage when we have to adjoin two more primes simultaneously, in such a way that the order of one of the ρ-Selmer groups remains unchanged, while the order of the other is divided by 9. To be able to reduce the orders of both ρ-Selmer groups to 9, we therefore need the initial choice of c to satisfy the following additional condition:

> The product of the orders of the ρ-Selmer groups of the two curves (54) is a power of 9.

As should be clear from the preceding discussion, the truth or falsehood of this statement depends only on $\mathcal{N}_0$ (provided it is small enough) and not on the value of c within $\mathcal{N}_0$. In other words, it depends only on the choice of c_0; and we need to show that we can choose c_0 so that (in addition to the previous requirements) this condition holds at c_0. Having done all this, we still need the equivalent of Condition D or Condition E.

However, at the end of all these complications we do obtain a solubility theorem for (52). It would be an act of supererogation to work hard to obtain the best theorem which the method could yield, because the sufficient

condition for solubility which we obtain would almost certainly always be stronger (though not much stronger) than the actual necessary condition. The latter is conjectured to be that there is no Brauer-Manin obstruction. The theorem which is obtained in [16] is as follows.

Theorem 7 *Let k be an algebraic number field not containing the primitive cube roots of unity. Assume that Hypothesis* Ш *holds. If* (52) *is everywhere locally soluble and the a_i are all cubefree, then each of the following criteria is sufficient for the solubility of* (52) *in k.*

(i) *There exist primes $\mathfrak{p}_1, \mathfrak{p}_3$ of k 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 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 $k_{\mathfrak{p}}^{*3}$.*

(iii) *There is a prime $\mathfrak{p}$ of k not dividing* 3 *such that exactly two of the a_i are units at $\mathfrak{p}$, and* (52) *is not birationally equivalent to a plane over $k_{\mathfrak{p}}$.*

7.2 *The case of one rational* 2*-division point.*
In this subsection we shall be concerned with pencils of 2-coverings whose pencil of Jacobians has the form

$$Y^2 = (X - c(U,V))(X^2 - d(U,V))$$

where c, d are homogeneous polynomials in $k[U,V]$ with $\deg d = 2 \deg c$. We start by recalling the standard machinery for 2-descent on

$$E' : \ Y^2 = (X - c)(X^2 - d)$$

for c, d in k and d not in k^2.

If O' is the point at infinity on E' and P' the 2-division point $(c, 0)$ then there is an isogeny $\phi' : \ E' \to E'' = E'/\{O', P'\}$ where E'' is

$$E'' : \ Y_1^2 = (X_1 + 2c)(X_1^2 + 4(d - c^2));$$

the places of bad reduction for E'' are the same as those for E'. Explicitly, ϕ' is given by

$$X_1 = \frac{d - X^2}{c - X} - 2c, \quad Y_1 = \frac{Y(X^2 - 2cX + d)}{(X - c)^2}.$$

There is also a dual isogeny $\phi'' :\ E'' \to E'$, and $\phi'' \circ \phi'$ and $\phi' \circ \phi''$ are the doubling maps on E' and E'' respectively. We are primarily interested in the case when neither d nor $c^2 - d$ is a square in k, so that E' and E'' each contain only one primitive 2-division point defined over k.

The elements of $\mathrm{H}^1(k, \{O', P'\}) \sim k^*/k^{*2}$ classify the ϕ'-coverings of E''; the covering corresponding to the class of m' is

$$V_1^2 = m'(X_1 + 2c), \quad V_2^2 = m'(X_1^2 + 4(d - c^2)) \tag{57}$$

with the obvious two-to-one map to E''. The ϕ'-covering corresponding to P'' is given by $m' = d$. Similarly the ϕ''-coverings of E' are classified by the elements of $\mathrm{H}^1(k, \{O'', P''\}) \sim k^*/k^{*2}$, the covering corresponding to the class of m'' being

$$W_1^2 = m''(X - c), \quad W_2^2 = m''(X^2 - d). \tag{58}$$

The ϕ''-covering corresponding to P' is given by $m'' = c^2 - d$. We denote by S_2' the 2-Selmer group of E', and by S_ϕ', S_ϕ'' the ϕ'-Selmer group of E'' and the ϕ''-Selmer group of E' respectively.

Write $K = k(d^{1/2})$; then the group of 2-coverings of E' is naturally isomorphic to K^*/K^{*2}, where the 2-covering corresponding to the class of $a + bd^{1/2}$ is given by

$$Z_1^2 = (a^2 - db^2)(X - c), \quad (Z_2 \pm d^{1/2} Z_3)^2 = (a \pm bd^{1/2})(X \pm d^{1/2}).$$

In homogeneous form, this can be written

$$\left.\begin{array}{c} Z_2^2 + dZ_3^2 = aZ_1^2/(a^2 - db^2) + (ac + bd)Z_0^2, \\ 2Z_2 Z_3 = bZ_1^2/(a^2 - db^2) + (a + bc)Z_0^2. \end{array}\right\} \tag{59}$$

Call this curve Γ'; then the map $\Gamma' \to E'$ has degree 4 and is given by

$$X = \frac{Z_1^2}{(a^2 - db^2)Z_0^2} + c, \quad Y = \frac{Z_1(Z_2^2 - dZ_3^2)}{(a^2 - db^2)Z_0^3}.$$

The map $\Gamma' \to E'$ can be factorized as $\Gamma' \to C''' \to E'$, where C''' is the ϕ''-covering of E' given by (58) with $m'' = a^2 - db^2$ and the map $\Gamma' \to C'''$ is

$$W_1 = Z_1/Z_0, \quad W_2 = (Z_2^2 - dZ_3^2)/Z_0^2.$$

Conversely, suppose that we have a curve of genus 1 defined over k and given by the equations

$$\left.\begin{array}{c}\alpha_0U_0^2+\alpha_1U_1^2+\alpha_2U_2^2+\alpha_3U_3^2+2\alpha_4U_2U_3=0,\\ \beta_0U_0^2+\beta_1U_1^2+\beta_2U_2^2+\beta_3U_3^2+2\beta_4U_2U_3=0,\end{array}\right\} \tag{60}$$

where the α_i, β_i are in $\mathfrak{o}$. We have just seen that any 2-covering of an elliptic curve with one rational 2-division point can be put in this form, and we shall now prove the converse. Write $d_{ij}=\alpha_i\beta_j-\alpha_j\beta_i$; then the curve (60) takes the more convenient form

$$\left.\begin{array}{c}d_{10}U_0^2+d_{12}U_2^2+2d_{14}U_2U_3+d_{13}U_3^2=0,\\ d_{01}U_1^2+d_{02}U_2^2+2d_{04}U_2U_3+d_{03}U_3^2=0.\end{array}\right\} \tag{61}$$

If we write $U_0=2Z_0(d_{14}^2-d_{12}d_{13})$ and $U_1=Z_1/4d_{34}(d_{14}^2-d_{12}d_{13})$, this last pair of equations can be identified with (59) provided that

$$\begin{gathered}a=-2(2d_{14}d_{34}+d_{13}d_{23})(d_{14}^2-d_{12}d_{13}),\\ b=d_{01}^{-1}d_{13}(d_{14}^2-d_{12}d_{13}),\\ c=4d_{04}d_{14}-2d_{02}d_{13}-2d_{03}d_{12},\\ d=4d_{01}^2(d_{23}^2+4d_{24}d_{34});\end{gathered}$$

it also follows from these that

$$\begin{gathered}c^2-d=16(d_{04}^2-d_{02}d_{03})(d_{14}^2-d_{12}d_{13}),\\ m''=a^2-db^2=16d_{34}^2(d_{14}^2-d_{12}d_{13})^3.\end{gathered}$$

We assume that $d(c^2-d)\neq 0$, so that (60) defines a nonsingular curve of genus 1.

Now let $\mathcal{S}$ be a finite set of places which contains the infinite places, the primes which divide 2, the odd primes of bad reduction for E' (or E'') and a set of generators for the ideal class group of k. For any v in $\mathcal{S}$ we write

$$V_v'=\mathrm{H}^1(k_v,\{O',P'\})\sim k_v^*/k_v^{*2}$$

and similarly for V_v''; and we denote by W_v' the image of $E''(k_v)/\phi'E'(k_v)$ in V_v' and similarly for W_v''. Thus m' lies in W_v' if and only if Γ' is soluble over k_v, and similarly for W_v''. There is a non-degenerate canonical pairing

$$V_v'\times V_v''\to\{\pm1\} \tag{62}$$

induced by the Hilbert symbol, under which the orthogonal complement of W'_v is W''_v. As in §5, we write

$$V'_{\mathcal{S}} = \oplus_{v\in\mathcal{S}} V'_v, \quad W'_{\mathcal{S}} = \oplus_{v\in\mathcal{S}} W'_v$$

and similarly for V'' and W''. The machinery in the first half of §5 needs to be modified to take account of the changed circumstances, but the proofs (which can be found in [1] or [3]) involve no new ideas. The appropriate replacement of the Corollary to Lemma 15 is as follows.

Lemma 18 *Let $\mathcal{S}_0^+, \mathcal{S}_1^+$ be as in §5 and let $\mathcal{S} \supset \mathcal{S}_1^+$. For each v in $\mathcal{S}$ there exist subspaces $K'_v \subset V'_v$ and $K''_v \subset V''_v$ such that*

(i) *K''_v is the orthogonal complement of K'_v under the pairing* (62)*;*

(ii) *$V'_{\mathcal{S}} = U'_{\mathcal{S}} \oplus K'_{\mathcal{S}}$ and $V''_{\mathcal{S}} = U''_{\mathcal{S}} \oplus K''_{\mathcal{S}}$ where $U'_{\mathcal{S}}, U''_{\mathcal{S}}$ are the images of $X_{\mathcal{S}} \times X_{\mathcal{S}} = (\mathfrak{o}_{\mathcal{S}}^*/\mathfrak{o}_{\mathcal{S}}^{*2})^2$ in $V'_{\mathcal{S}}$ and $V''_{\mathcal{S}}$ respectively;*

(iii) *if v is not in $\mathcal{S}_0^+$ we can take K'_v and K''_v to be the images of $(\mathfrak{o}_v^*/\mathfrak{o}_v^{*2})^2$.*

It follows from (62) that there is a non-degenerate canonical pairing

$$V'_{\mathcal{S}} \times V''_{\mathcal{S}} \to \{\pm 1\} \tag{63}$$

and from (i) that $K''_{\mathcal{S}} = \oplus_{v\in\mathcal{S}} K''_v$ is the orthogonal complement of $K'_{\mathcal{S}}$ under this pairing.

Lemma 19 *If $\mathcal{S} \supset \mathcal{S}_1^+$ then S'_ϕ is isomorphic to each of $U'_{\mathcal{S}} \cap W'_{\mathcal{S}}$, the left kernel of the map $U'_{\mathcal{S}} \times W''_{\mathcal{S}} \to \{\pm 1\}$ induced by* (63)*, and the left kernel of the map $W'_{\mathcal{S}} \times U''_{\mathcal{S}} \to \{\pm 1\}$ induced by* (63)*. A similar result holds for S''_ϕ.*

Let $t'_{\mathcal{S}} : V'_{\mathcal{S}} \to U'_{\mathcal{S}}$ be the projection along $K'_{\mathcal{S}}$ and similarly for $t''_{\mathcal{S}}$. We now diverge from the notation of §5, writing

$$\mathbf{U}'_{\mathcal{S}} = U'_{\mathcal{S}} \cap (W'_{\mathcal{S}} + K'_{\mathcal{S}}), \quad \mathbf{W}'_{\mathcal{S}} = W'_{\mathcal{S}}/(W'_{\mathcal{S}} \cap K'_{\mathcal{S}})$$

and similarly for $\mathbf{U}''_{\mathcal{S}}$ and $\mathbf{W}''_{\mathcal{S}}$; as in §5, the map $t'_{\mathcal{S}}$ induces an isomorphism $\tau'_{\mathcal{S}} : \mathbf{W}'_{\mathcal{S}} \to \mathbf{U}'_{\mathcal{S}}$, and there is an analogous isomorphism $\tau''_{\mathcal{S}} : \mathbf{W}''_{\mathcal{S}} \to \mathbf{U}''_{\mathcal{S}}$. The pairing (63) induces pairings

$$\mathbf{U}'_{\mathcal{S}} \times \mathbf{W}''_{\mathcal{S}} \to \{\pm 1\}, \quad \mathbf{W}'_{\mathcal{S}} \times \mathbf{U}''_{\mathcal{S}} \to \{\pm 1\} \tag{64}$$

and the action of $\tau'_{\mathcal{S}} \times (\tau''_{\mathcal{S}})^{-1}$ takes the first pairing into the second. The left kernel of either of these pairings is isomorphic to S'_ϕ and the right kernel to S''_ϕ. The action of $\tau'_{\mathcal{S}} \times 1$ takes the first pairing into the pairing

$$\mathbf{W}'_{\mathcal{S}} \times \mathbf{W}''_{\mathcal{S}} \to \{\pm 1\}.$$

Our objective is to prove the solubility in k of pencils of curves (60), where we assume that the α_i, β_i are homogeneous polynomials in U, V, that all the α_i have the same degree and that all the β_i have the same degree. Henceforth we denote by $\mathcal{S}$ the set of bad places for the pencil (60). As in §6, we need to work not in $\mathbf{P}^1(k)$ but in the open subset $\mathbf{L}^1(k)$ in which $d(c^2 - d) \neq 0$. In order to make the proof work, we shall have to impose additional conditions, some but not all of which are necessary for solubility; these will be introduced at the places in the proof where they are first needed. Our eventual result will be as follows:

Theorem 8 *Assume Schinzel's Hypothesis and Hypothesis* Ш. *Suppose that Conditions* 1 *to* 4 *below hold in an open subset* $\mathcal{A} \subset \mathcal{N}$ *of* $\mathbf{L}^1(k)$ *in which* $\Gamma'(\alpha, \beta)$ *is locally soluble at all places of* $\mathcal{S}$. *Then* $\mathcal{A}$ *lies in the closure of the set of* $\lambda = \alpha/\beta$ *in* $\mathbf{L}^1(k)$ *at which* $\Gamma'(\alpha, \beta)$ *is soluble in* k. *If instead of solubility we merely require* $\Gamma'(\alpha, \beta)$ *to contain a* 0*-cycle of odd degree, then we need no longer assume Schinzel's Hypothesis.*

The proof of the last sentence is derived from the proof of the rest of the theorem by applying Lemma 4 instead of Lemma 2, and we shall make no further mention of it. Now suppose that α, β are such that $\Gamma'(\alpha, \beta)$ is everywhere locally soluble. In order to use Lemma 2 to prove that $\Gamma'(\alpha, \beta)$ is soluble in k, we have to show that the 2-Selmer group of E' has order 4. Unfortunately the obvious way of computing the 2-Selmer group requires us to know the ideal class group of $k(\sqrt{d(\alpha, \beta)})$, and we know very little about how this depends on $\alpha \times \beta$. However Lemma 20 below provides a way round this difficulty. It is now necessary to split cases according as Γ' is in S'_ϕ or not; we confine ourselves in these notes to the latter case, which is the more general and also the more complicated. (A treatment of the other case can be found in [1] or [3].) To ensure that we are in this latter case, we need C'' above not to be E''; in other words, m'' must not be a square. In view of the formulae above, the condition for this is that $d_{14}^2 - d_{12}d_{13}$ is not a square in $k[U, V]$. This is included in Condition 1 below.

Lemma 20 *Suppose that* P' *is the only primitive* 2*-division point of* E' *defined over* k *and similarly for* P'' *on* E''. *If the orders of* S'_ϕ *and* S''_ϕ *are* 2 *and* 4 *respectively then the order of* S'_2 *is at most* 4.

Proof. Let Γ' be a 2-covering of E' and denote by C'' the quotient of Γ' by the action of the group $\{O', P'\}$; then C'' is a ϕ''-covering of E' and we have

a commutative diagram

$$\begin{array}{ccccc} E' & \xrightarrow{\phi'} & E'' & \xrightarrow{\phi''} & E' \\ \| & & \| & & \| \\ \Gamma' & \longrightarrow & C'' & \longrightarrow & E' \end{array}$$

where the first two vertical double lines mean that Γ' and C'' are principal homogeneous spaces for E' and E'' respectively. If Γ' is identified with the element f of $\mathrm{H}^1(k, E'[2])$ then C'' is identified with $\phi' \circ f$ as an element of $\mathrm{H}^1(k, E''[\phi''])$. If Γ' is in S'_2 then C'' is in S''_ϕ; so we can construct all the elements of S'_2 by lifting back the elements of S''_ϕ. But by hypothesis P'' is not in $\phi' E'(k)$, so the two elements of S'_ϕ must correspond to the points O'' and P'' as members of $E''(k)/\phi' E'(k)$; hence regarded as elements of S'_2 they are equivalent. In other words, E'' regarded as an element of S''_ϕ lifts back to only one element of S'_2; so the same is true of each element of S''_ϕ. □

To make use of Lemma 20 we have to study simultaneously the ϕ'-descent on E'' and the ϕ''-descent on E'. We imitate as far as possible the machinery of the proof of Theorem 6. Write

$$R = d_{01}(d_{23}^2 + 4d_{24}d_{34})(d_{04}^2 - d_{02}d_{03})(d_{14}^2 - d_{12}d_{13}),$$

so that the singular fibres of any of our pencils are given by $R = 0$. As in the proof of Theorem 6, we let f_τ for $\tau = 1, 2, \ldots$ run through the distinct irreducible factors of R; without loss of generality we can suppose that the coefficients of any f_τ are integers and that there is no prime outside $\mathcal{S}$ which divides all of them. When we choose α, β by Lemma 2 so that all the $f_\tau(\alpha, \beta)$ are prime up to factors in $\mathcal{S}$, we shall denote this additional prime factor of $f_\tau(\alpha, \beta)$ by $\mathfrak{p}_\tau$. We shall see in (iii) below that S'_ϕ and S''_ϕ are effectively independent of the choice of α, β. Each step of our algorithm will consist of introducing a new prime $\mathfrak{p}$ in such a way that we diminish one of S'_ϕ and S''_ϕ without increasing the other. Write $K_\tau = k[X]/f_\tau(X, 1)$ and let ξ_τ be the class of X in K_τ; then those $\mathfrak{p}$ which we can introduce in such a way that $\mathfrak{p}$ will divide the value of $f_\tau(\alpha, \beta)$ are just the ones such that $\mathfrak{p}$ has a factor $\mathfrak{P}$ in K_τ whose relative norm for K_τ/k is $\mathfrak{p}$. The arguments needed to validate each step are again lengthy, and as in the proof of Theorem 6 we list them as (i) to (v). Here (ii), (iii) and (iv) are essentially identical with those in the earlier proof, (i) is similar but considerably more complicated, and (v) is substantially different.

(i) *Local solubility at* $\mathfrak{p}$. As before, for the local solubility of $\Gamma'(\alpha, \beta)$ at $\mathfrak{p}$ we need to study the decomposition of $\Gamma'(\xi_\tau, 1)$. Condition 1 primarily restricts the multiplicity of the singular fibres; but in order to simplify the rest of the argument, it is rather stronger than is needed for this purpose, and than the corresponding condition in §6.

Condition 1. *R has no repeated factor in $k[U, V]$.*

Lemma 21 *If Condition* 1 *holds then the absolutely irreducible components of $\Gamma'(\xi_\tau, 1)$ have multiplicity one and there are at most two of them.*

Proof We shall write L_τ^0 for the least field of definition of any of these components. Condition 1 implies that f_τ cannot divide both of α_0 and β_0, nor both of α_1 and β_1. If $f_\tau \| d_{01}$ it follows that f_τ cannot divide one of α_0 and α_1 and also one of β_0 and β_1. Suppose that it divides neither α_0 nor α_1. Since f_τ does not divide $d_{04}^2 - d_{02}d_{03}$ the second equation (61) splits over $L_\tau^0 = K_\tau(\sqrt{d_{04}^2 - d_{02}d_{03}})$ where the right hand side is to be evaluated at $\xi_\tau \times 1$. Now if the values of $\alpha_2 U_2^2 + \alpha_3 U_3^2 + 2\alpha_4 U_2 U_3$ and $d_{02}U_2^2 + d_{03}U_3^2 + 2d_{04}U_2U_3$ at $\xi_\tau \times 1$, considered as quadratic forms in U_2, U_3, have a common factor then $f_\tau | (d_{23}^2 + 4d_{24}d_{34})$; but this contradicts Condition 1. Hence on either of the planes given by the second equation (61) at $\xi_\tau \times 1$ the first equation (60) determines an irreducible conic. In other words, if $f_\tau | d_{01}$ the singular fibre is the union of two irreducible conics each defined over L_τ^0.

If instead $f_\tau \| (d_{04}^2 - d_{02}d_{03})$ then f_τ cannot divide both d_{02} and d_{03}, so to fix ideas we can assume that $f_\tau \nmid d_{02}$. The second equation (61) splits over $L_\tau^0 = K_\tau(\sqrt{-d_{01}d_{02}})$ where the right hand side is again to be evaluated at $\xi_\tau \times 1$; and the first equation (61) is absolutely irreducible. Hence the singular fibre is again the union of two irreducible conics each defined over L_τ^0. A similar argument works if $f_\tau \| (d_{14}^2 - d_{12}d_{13})$.

If finally $f_\tau \| (d_{23}^2 + 4d_{24}d_{34})$ then at $\xi_\tau \times 1$ every linear combination of the two equations (61) must be absolutely irreducible, because otherwise $\alpha_2 U_2^2 + \alpha_3 U_3^2 + 2\alpha_4 U_2 U_3$ and $\beta_2 U_2^2 + \beta_3 U_3^2 + 2\beta_4 U_2 U_3$ would be proportional at $\xi_\tau \times 1$ and so $f_\tau | (d_{23}^2 + 4d_{24}d_{34})^2$. Hence the singular fibre is absolutely irreducible (though it will be singular) and we can take $L_\tau^0 = K_\tau$. □

In all these cases the condition that Γ' is soluble in $k_\mathfrak{p}$ at each point in some neighbourhood of $\alpha_\mathfrak{p} \times \beta_\mathfrak{p}$, where $\mathfrak{p} | f_\tau(\alpha_\mathfrak{p}, \beta_\mathfrak{p})$, is that $\mathfrak{P}$ splits in L_τ^0. A more exhaustive list of possibilities, under a hypothesis weaker than Condition 1, may be found in Lemma 5 of [1].

We also need to know when the curves (57) and (58) are not locally soluble at $\mathfrak{p} = \mathfrak{p}_\tau$, which is the same as evaluating $W'_\mathfrak{p}$ and $W''_\mathfrak{p}$. Here we adopt a somewhat weaker hypothesis than Condition 1.

Lemma 22 *Suppose that c and d are in $\mathfrak{o}$ and let $\mathfrak{p}$ be an odd prime ideal of k which divides one but not both of d and $c^2 - d$. Then $W'_\mathfrak{p}$ and $W''_\mathfrak{p}$ are as in the following table, in which v denotes the normalized additive valuation associated with $\mathfrak{p}$:*

$$\begin{array}{cc}
v(c^2-d) \text{ odd} & m' \in k_\mathfrak{p}^{*2}, \text{ any } m''; \\
v(c^2-d) > 0 \text{ even}, 2c \in k_\mathfrak{p}^{*2} & m' \in k_\mathfrak{p}^{*2}, \text{ any } m''; \\
v(c^2-d) > 0 \text{ even}, 2c \notin k_\mathfrak{p}^{*2} & v(m') \text{ and } v(m'') \text{ even}; \\
v(d) \text{ odd} & m'' \in k_\mathfrak{p}^{*2}, \text{ any } m'; \\
v(d) > 0 \text{ even}, -c \in k_\mathfrak{p}^{*2} & m'' \in k_\mathfrak{p}^{*2}, \text{ any } m'; \\
v(d) > 0 \text{ even}, -c \notin k_\mathfrak{p}^{*2} & v(m') \text{ and } v(m'') \text{ even}.
\end{array}$$

If $\mathfrak{p}$ divides m'' to an odd power but does not divide $c^2 - d$, then (58) *is insoluble in $k_\mathfrak{p}$; similarly if $\mathfrak{p}$ divides m' to an odd power but does not divide d, then* (57) *is insoluble in $k_\mathfrak{p}$.*

Proof The last sentence follows from the earlier ones. For the first three lines, consider the equations (57). In the first line of the table, if $v(X_1^2) < v(c^2-d)$ then m' is a square by the second equation (57); if not, then $v(m')$ is odd and the first equation gives a contradiction. Hence m' is a square, and by the pairing (62) there is no constraint on m''. In the second and third lines, if $v(X_1^2) < v(c^2 - d)$ then m' must be a square; if not, then $2cm'$ must be a square. Using (62) as before, this gives the second line. We can choose X_1 so that $v(X_1^2) = v(c^2 - d)$ and $2c(X_1^2 + 4(d - c^2))$ is a square; so m' can be in the class of $2c$. Using (62) again, this gives the third line. The remaining lines now follow by duality. □

Lines 2 and 3 in this table will not be needed, in view of Condition 1 and the formula for $c^2 - d$; but their duals (which are lines 5 and 6) are needed, and lines 2 and 3 are included for completeness.

(ii) *Local solubility of $\Gamma^1(\alpha, \beta)$ at $\mathfrak{p}_\tau$.* In §5 we used Lemma 13 to relate local solubility of Γ' to local solubility of the C_{ij}; similarly here we relate local solubility of Γ' to local solubility of each of the two equations (61). By the results of §4, the latter requires

> Condition 2. *There is a non-empty open set $\mathcal{A} \subset \mathcal{N}$ in which Γ' is locally soluble at each place in $\mathcal{S}$ and the following conditions*

hold:

$$\begin{aligned}
&\textit{if } f_\tau \| (d_{04}^2 - d_{02}d_{03}) \textit{ then } L(\mathcal{S}; -d_{01}d_{02}, f_\tau; \alpha, \beta) = 1;\\
&\textit{if } f_\tau \| (d_{14}^2 - d_{12}d_{13}) \textit{ then } L(\mathcal{S}; d_{01}d_{12}, f_\tau; \alpha, \beta) = 1;\\
&\textit{if } f_\tau \| d_{01} \textit{ then } L(\mathcal{S}; d_{04}^2 - d_{02}d_{03}, f_\tau; \alpha, \beta) = 1.
\end{aligned}$$

Thus Condition 2 is necessary for solubility. Note that

$$L(\mathcal{S}; d_{14}^2 - d_{12}d_{13}, f_\tau; \alpha, \beta) = L(\mathcal{S}; d_{04}^2 - d_{02}d_{03}, f_\tau; \alpha, \beta)$$

if $f_\tau | d_{01}$, so symmetry between U_0 and U_1 in (61) is preserved.

If α, β are chosen so as to meet the requirements of Lemma 2, then each Legendre-Jacobi function in Condition 2 reduces to a single Hilbert symbol, taken at $\mathfrak{p}_\tau$; so in each of the three cases listed, the condition implies that $\mathfrak{P}$ splits in L_τ^0 in the notation of the proof of Lemma 21. In other words, $\Gamma'(\alpha, \beta)$ is soluble in $k_\mathfrak{p}$. The argument in the case $f_\tau \| (d_{23}^2 + 4d_{24}d_{34})$ is even simpler.

(iii) *Independence of* α, β. The argument here is exactly the same as in §6. If $\mathcal{B}$ is the union of $\mathcal{S}$ and all the $\mathfrak{p}_\tau$, by abuse of language we can now describe $\mathbf{W}'_\mathcal{B}$ as the union of $\mathbf{W}'_\mathcal{S}$ and spaces $\mathbf{W}'_\tau$ associated with f_τ. The space $\mathbf{W}'_\tau$ is one-dimensional if (57) is soluble with $\mathfrak{p}_\tau \| m'$ and trivial otherwise; the former case corresponds to lines 4 and 5 of the table in Lemma 22. A similar remark holds for $\mathbf{W}''_\mathcal{B}$; and we can provide similar descriptions of $\mathbf{U}'_\mathcal{B}$ and $\mathbf{U}''_\mathcal{B}$.

(iv) *Effect of introducing* $\mathfrak{p}$. Here again the argument is essentially that of §6. In the description given in (iii), the effect of introducing $\mathfrak{p}$ into f_τ will be as follows. Suppose first that $f_\tau | d$; then if the conditions of lines 4 or 5 of the table in Lemma 22 are satisfied, the new $\mathbf{W}'$ will be the sum of the old $\mathbf{W}'$ and a one-dimensional space $\mathbf{W}'_\mathfrak{p}$, and $\mathbf{W}''$ will be unchanged. Moreover, if m'' represents an element of $\mathbf{U}''$ and $w'_\mathfrak{p}$ is the generator of $\mathbf{W}'_\mathfrak{p}$ then the image of $w'_\mathfrak{p} \times m''$ under the second pairing (64) is 1 if m'' is in $k_\mathfrak{p}^{*2}$ and -1 otherwise. If instead the conditions of line 6 of the table are satisfied, then both $\mathbf{W}'$ and $\mathbf{W}''$ are unchanged. Secondly, suppose that $f_\tau | (c^2 - d)$, so that by Condition 1 we must be in line 1 of the table; then the conclusions are similar to those above for line 4.

(v) *Choice of* $\mathfrak{p}$. It remains to show that if S'_ϕ, S''_ϕ do not satisfy the hypotheses of Lemma 20 then we can choose $\mathfrak{p}$ so as to decrease one of S'_ϕ and S''_ϕ without increasing the other. To achieve this we need to impose two further

conditions, which together serve the same purpose as Condition D in §6. It will be clear from (iv) that we cannot expect symmetry in the treatment of $\mathbf{W}'$ and $\mathbf{W}''$.

Suppose first that m' is in S'_ϕ and is not 1 or d. To remove m' from S'_ϕ we need to introduce $\mathfrak{p}$ satisfying line 1 of the table in Lemma 22; when we do so we shall not increase S''_ϕ because no element of the new $\mathbf{W}''$ not lying in the old $\mathbf{W}''$ can be orthogonal to m'. Thus we must find a first degree prime $\mathfrak{P}$ in K_τ which remains prime in $L_\tau = K_\tau(\sqrt{m'(\xi_\tau, 1)})$; and we already know that it must split in L^0_τ, which is the quadratic extension of K_τ defined in the proof of Lemma 21. Using the convention introduced in (iii), what we need in order to ensure that this is possible is

> Condition 3. *If m' is in $\mathbf{U}'_\mathcal{B}$ and not 1 or d, then there is an $f_\tau | (c^2 - d)$ such that $L_\tau \neq L^0_\tau$.*

If instead m'' is in S''_ϕ and is not in the subgroup generated by $(c^2 - d)$ and $(a^2 - db^2)$, then we have $L_\tau = K_\tau(\sqrt{m''(\xi_\tau, 1)})$. A similar argument now shows that what we need is

> Condition 4. *If m'' is in $\mathbf{U}''_\mathcal{B}$ and not in the subgroup generated by $d_{04}^2 - d_{02}d_{03}$ and $d_{14}^2 - d_{12}d_{13}$ then there exists f_τ such that either $f_\tau | (d_{23}^2 + 4d_{24}d_{34})$ with $m''(\xi_\tau, 1)$ not a square in K_τ or else $f_\tau | d_{01}$ with $K_\tau(\sqrt{m''(\xi_\tau, 1)})$ not contained in $L^0_\tau(\sqrt{-c(\xi_\tau, 1)})$.*

Like Condition D, these can be rewritten in the language of earlier papers; and they can be replaced by weaker but less convenient conditions in just the same way that Condition D can be replaced by Condition E.

8. *Del Pezzo surfaces of degree* 4

Let V be a Del Pezzo surface of degree 4 (that is, the smooth intersection of two quadrics in $\mathbf{P}^4$) defined over an algebraic number field k. Salberger and Skorobogatov [11] have shown that the only obstruction to weak approximation on V is the Brauer-Manin obstruction. More precisely:

Theorem 9 *Suppose that $V(k)$ is not empty. Let $\mathcal{A}$ be the subset of the adelic space $V(\mathbf{A})$ consisting of the points $\prod P_v$ such that*

$$\sum \mathrm{inv}_v(A(P_v)) = 0 \text{ in } \mathbf{Q}/\mathbf{Z}$$

for all A in the Brauer group $\mathrm{Br}(V)$. Then the image of $V(k)$ is dense in $\mathcal{A}$.

In the first part of this section I give a simpler proof of this theorem. What I actually prove is Theorem 10 below, which is equivalent to Theorem 9 because of Lemma 11. Readers who are content with Theorem 10 need not trouble themselves with the Brauer-Manin condition.

Theorem 10 *Let $\mathcal{B}$ be a finite set of places of k, satisfying the conditions for* (68) *analogous to those stated above for* (23).

(i) *For each v in $\mathcal{B}$ let S_v be a point of V defined over k_v, and let λ_v be its image under the projection to $\mathbf{P}^1$. Suppose that all the conditions like*

$$\prod_{v\in\mathcal{B}} \ell^*(v; -a_0a_1, c; \lambda_v) = 1 \tag{65}$$

hold. Then there is a point of $V(k)$ as close as we like to each S_v.

(ii) *Let λ be a point of $\mathbf{P}^1(k)$ such that all the conditions like*

$$L(\mathcal{B}; -a_0a_1, c; \lambda) = 1$$

hold. Then there is a point in $V(k)$ whose projection into $\mathbf{P}^1(k)$ is as close as we like to λ in the topology induced by $\mathcal{B}$.

Since we can find λ arbitrarily close to each λ_v, it follows from the analogue of (10) that the two parts of the theorem are equivalent. In view of the first assertion of Lemma 11 and the fact that weak approximation holds for conics, Theorem 10(ii) is equivalent to Theorem 9. The idea of the proof is that we can use the existence of a point of $V(k)$ to fibre V by conics.

Theorem 2 allows us to find a positive 0-cycle of degree 8 on V defined over k satisfying pre-assigned approximation conditions; and the proof is then completed by a modification of an argument of Coray. Later in this section, we give Coray's full result as Theorem 11.

Write the Del Pezzo surface V as $Q_1 \cap Q_2$ where Q_1, Q_2 are quadrics in $\mathbf{P}^4$. Choose coordinates so that the given point of $V(k)$ is $(1,0,0,0,0)$ and the tangents to Q_1, Q_2 at this point are $X_1 = 0, X_2 = 0$ respectively. Thus the equations of Q_1 and Q_2 can be written

$$X_0X_1 + f_1(X_1, \ldots, X_4) = 0, \quad X_0X_2 + f_2(X_1, \ldots, X_4) = 0 \tag{66}$$

where f_1, f_2 are homogeneous quadratic. The variety (66) is birationally equivalent to the cubic surface $X_2f_1 = X_1f_2$, which is indeed obtained by blowing up the given point of $V(k)$; and this cubic surface is birationally equivalent to the pencil of affine conics

$$Vf_1(U, V, X_3, X_4) = Uf_2(U, V, X_3, X_4), \tag{67}$$

which with some abuse of language can be parametrized by the points (U, V) of $\mathbf{P}^1$. Diagonalizing this equation and then making it homogeneous gives a pencil of projective conics of the form

$$Z_0^2 g_1(U,V) + Z_1^2 g_2(U,V)/g_1(U,V) + Z_3^2 g_5(U,V)/g_2(U,V) = 0,$$

where g_r is homogeneous of degree r. Writing

$$Z_0 = g_2Y_0, \quad Z_1 = g_1Y_1, \quad Z_2 = g_1g_2Y_2$$

and dividing by g_1g_2 we obtain

$$g_2Y_0^2 + Y_1^2 + g_1g_5Y_2^2 = 0. \tag{68}$$

We shall assume that the g_r are coprime in pairs in $k[U, V]$; if not, there is a further simplification of (68) and of the subsequent argument which is left to the reader.

In principle, the idea of the proof of Theorem 10 is to construct a sequence of positive 0-cycles defined over k of decreasing degrees, each satisfying the conditions like (27), until we obtain a point P_0 in $V(k)$ satisfying the given local conditions; and indeed this is what we shall do in the last part of the proof. But it is not obvious how the local descriptions of successive elements

of the sequence are related. So although the application of Theorem 2 to (68) shows that there is a positive 0-cycle of degree 8 satisfying any assigned local conditions, we do not yet know what local conditions to impose on it for P_0 to be close in the topology induced by $\mathcal{B}$ to the adelic point which is our target. To cope with this, we first run the process backwards.

From now on, any $\mathfrak{b}^r$ or $\mathfrak{b}_v^r$ will be a positive 0-cycle on V, defined over k or k_v respectively, and $\mathfrak{a}^r$ or $\mathfrak{a}_v^r$ will be its projection on $\mathbf{P}^1$. For each v in $\mathcal{B}$ we choose two distinct hyperplanes H'_v and H''_v, each defined over k_v and passing through S_v. Choose H', a hyperplane defined over k and close to each H'_v, and similarly for H''. The intersection $H' \cap H'' \cap V$ is a positive 0-cycle $\mathfrak{b}^1$ of degree 4 defined over k; and though $\mathfrak{b}^1$ may be irreducible over k it is reducible over k_v for each v in $\mathcal{B}$ because it has one point close to S_v. Thus we can write $\mathfrak{b}^1 = \mathfrak{b}_v^2 \cup \mathfrak{b}_v^3$ where $\mathfrak{b}_v^2, \mathfrak{b}_v^3$ are positive 0-cycles of degrees $1, 3$ respectively defined over k_v and $\mathfrak{b}_v^2$ is close to S_v. Hence

$$\begin{aligned} 1 =& L^*(\mathcal{B}; -a_0a_1, c; \mathfrak{a}^1) = \prod \ell^*(v; -a_0a_1, c; \mathfrak{a}_v^2 \cup \mathfrak{a}_v^3) \\ =& \prod \ell^*(v; -a_0a_1, c; \mathfrak{a}_v^2) \prod \ell^*(v; -a_0a_1, c; \mathfrak{a}_v^3) \end{aligned}$$

where the products are each taken over all v in $\mathcal{B}$. But the first product in the second line is 1, by continuity applied to (65); hence

$$\prod \ell^*(v; -a_0a_1, c; \mathfrak{a}_v^3) = 1. \tag{69}$$

Now let P_1 and P_2 be two points of $V(k)$; there are ∞^6 curves on V which are the intersection of V with a quadric and have double points at P_1 and P_2. For each v in $\mathcal{B}$, let C'_v and C''_v be two such curves defined over k_v each of which also passes through the three points of $\mathfrak{b}_v^3$, and let Q'_v, Q''_v be quadrics defined over k_v which contain C'_v, C''_v respectively but neither of which contains the whole of V. Choose Q', a quadric defined over k, close to each Q'_v and touching V at P_1 and P_2, and similarly for Q''; since Q' is given by a single equation and the tangency conditions are linear in the coefficients, this is just a matter of weak approximation. The intersection

$$Q' \cap Q'' \cap V = 4\{P_1\} \cup 4\{P_2\} \cup \mathfrak{b}^4.$$

(This fails if Q' and Q'' have a common component; but we can ensure that this does not happen by requiring P_1, P_2 and $\mathfrak{b}^1$ to be in sufficiently general position. Similar remarks are needed at each stage of the proof.)

Much as before, $\mathfrak{b}^4 = \mathfrak{b}_v^5 \cup \mathfrak{b}_v^6$ over k_v for each v in $\mathcal{B}$, where each $\mathfrak{b}_v^5$ has degree 3 and is close to $\mathfrak{b}_v^3$, and each $\mathfrak{b}_v^6$ has degree 5; hence

$$\prod \ell^*(v; -a_0a_1, c; \mathfrak{a}_v^5) = 1$$

follows from (69) by continuity. But

$$L(\mathcal{B}; -a_0a_1, c; \lambda_1) = L(\mathcal{B}; -a_0a_1, c; \lambda_2) = 1$$

where λ_1, λ_2 are the projections of P_1, P_2 on $\mathbf{P}^1$; so

$$\prod \ell^*(v; -a_0a_1, c; \mathfrak{a}_v^6) = 1.$$

Now let P_3, P_4, P_5 be three further points of $V(k)$; then there are ∞^9 curves on V which are the intersection of V with a quadric and pass through P_3, P_4, P_5. For each v in $\mathcal{B}$, let D_v' and D_v'' be two such curves defined over k_v each of which also passes through the five points of $\mathfrak{b}_v^6$, and let R_v', R_v'' be quadrics defined over k_v which contain D_v', D_v'' respectively but neither of which contains the whole of V. Choose R', a quadric defined over k, close to each R_v' and passing through P_3, P_4, P_5, and similarly for R''. The intersection

$$R' \cap R'' \cap V = \{P_3\} \cup \{P_4\} \cup \{P_5\} \cup \mathfrak{b}^7,$$

where $\mathfrak{b}_v^7$ has degree 13. Much as before, $\mathfrak{b}^7 = \mathfrak{b}_v^8 \cup \mathfrak{b}_v^9$ over k_v for each v in $\mathcal{B}$, where each $\mathfrak{b}_v^9$ is close to $\mathfrak{b}_v^6$, so that $\mathfrak{b}_v^8$ has degree 8 and

$$\prod \ell^*(v; -a_0a_1, c; \mathfrak{a}_v^8) = 1.$$

We now have the necessary map of how to go back. By Theorem 2, we can find a positive 0-cycle $\mathfrak{d}^8$ of degree 8 on V, defined over k and arbitrarily near to each $\mathfrak{b}_v^8$. With the same P_3, P_4, P_5 as before, there is a pencil of curves on V which are the intersections of V with a quadric and pass through P_3, P_4, P_5 and the points of $\mathfrak{d}^8$. Let $\mathfrak{d}^5$, of degree 5, be the residual intersection of the curves of this pencil; since the pencil contains a curve close to each D_v' and another close to each D_v'', it follows that $\mathfrak{d}^5$ is close to each $\mathfrak{b}_v^5$. (This time, the curves in the pencil do not all have a common component, because one of them is arbitrarily close to $R' \cap V$ and another to $R'' \cap V$.)

In the same way, we successively generate a 0-cycle $\mathfrak{d}^3$ on V of degree 3 and arbitrarily close to each $\mathfrak{b}_v^3$, and then a point of $V(k)$ arbitrarily close to each S_v. This last is the point which we want. □

The following lemma and theorem are due to Coray [8]. Lemma 23 is weaker than Theorem 11, but appears to be a necessary step in the proof of the latter. Theorem 11 is one of the two ingredients in the approach to the solubility of Del Pezzo surfaces of degree 4 which forms the last part of this section.

Lemma 23 *Let V be a Del Pezzo surface of degree 4, defined over a field L of characteristic 0. If V contains a positive 0-cycle of degree 2 and a positive 0-cycle of odd degree n, both defined over L, then $V(L)$ is not empty.*

Proof We can suppose V embedded in $\mathbf{P}^4$ as the intersection of two quadrics. We proceed by induction on n. If the given 0-cycle of degree 2 consists of the two points P' and P'' then we can suppose that they are conjugate over L and distinct, because otherwise the lemma would be trivial. By a standard result, there are infinitely many points on V defined over $L(P')$ and hence infinitely many positive 0-cycles of degree 2 defined over L. Choose d so that

$$2d(d+1) > n > 2d(d-1)$$

and let $\{P'_i, P''_i\}$ be $\frac{1}{2}\{2d(d+1)-n-1\}$ distinct pairs of points of V, the points of each pair being conjugate over L. The hypersurfaces of degree d cut out on V a system of curves of dimension $2d(d+1)$; hence there is at least a pencil of such curves passing through the P'_i and P''_i and the points of the given 0-cycle of degree n, and this pencil is defined over L. We have accounted for $2d(d+1)-1$ of the $4d^2$ base points of the pencil; so the remaining ones form a positive 0-cycle of degree $2d(d-1)+1$ defined over L. This completes the induction step unless $n = 2d(d-1)+1$.

In this latter case we must have $d > 1$ because if $d = 1$ then $n = 1$ and the lemma is already proved; hence $2d(d+1)-n-1 = 4d-2 \geq 6$. Instead of the previous construction we now choose our pencil of curves to have double points at P'_0 and P''_0 and to pass through $\frac{1}{2}\{2d(d+1)-n-7\}$ other pairs P'_i, P''_i as well as through the points of the given 0-cycle of degree n. In this case each of P'_0 and P''_0 is a base point of the pencil with multiplicity 4; so we have accounted for $2d(d+1)+1$ of the base points of the pencil, and the remaining ones form a positive 0-cycle of degree $2d(d-1)-1$ defined over L. This completes the induction step in this case. □

Theorem 11 *Let V be a del Pezzo surface of degree 4, defined over a field L of characteristic 0. If V contains a 0-cycle of odd degree defined over L then $V(L)$ is not empty.*

Proof By decomposing the 0-cycle into its irreducible components, we can assume that V contains a positive 0-cycle $\mathfrak{a}$ of odd degree defined over L. We can write V as the intersection of two quadrics, each defined over L; let W be one of them. We can find a field $L_1 \supset L$ with $[L_1 : L] \leq 2$ and a point P on W defined over L_1. The lines on W through P are parametrised by the points of a conic, so we can find a field $L_2 \supset L_1$ with $[L_2 : L_1] \leq 2$ and a line ℓ on W, passing through P and defined over L_2. The intersection of this line with another quadric containing V cuts out on V a positive 0-cycle of degree 2 defined over L_2. Applying Lemma 23 to $\mathfrak{a}$ and this 0-cycle, we obtain a point P_2 on V defined over L_2. Repeating this argument for $\mathfrak{a}$ and the positive 0-cycle of degree 2 consisting of P_2 and its conjugate over L_1, we obtain a point P_1 on V defined over L_1; and one further repetition of the argument gives us a point on V defined over L. □

The main theorem of §7.2 provides a promising approach to the problem of finding the obstruction to the Hasse principle for Del Pezzo surfaces of degree 4. One such obstruction is that of Brauer-Manin, and the classical conjecture (due to Colliot-Thélène and Sansuc) is that it is the only one. But the reader is warned that I have not yet been able to push this argument through to a successful conclusion.

The starting point is the following question. Let V be a nonsingular Del Pezzo surface of degree 4, defined over an algebraic number field k and everywhere locally soluble; can we exhibit a family of hyperplane sections of V which is of the form considered in §7.2? It turns out that, after a field extension of odd degree, we can exhibit such a family parametrised by the points of $\mathbf{P}^3$ blown up along a certain curve and at four other points. The construction is as follows.

The surface V is the base locus of a pencil of quadrics; because V is nonsingular, the pencil contains exactly 5 cones defined over $\bar{k}$ and these are all distinct. Hence one at least of them is defined over a field k_1 which is of odd degree over k; and by Theorem 11 it is enough to ask whether V contains points defined over k_1. Henceforth we work over k_1. After a change of variables, we can assume that the singular quadric just described has vertex $(1, 0, 0, 0, 0)$ and therefore an equation of the form $f(X_1, X_2, X_3, X_4) = 0$. By absorbing multiples of the other X_i into X_0, we can now assume that V has the form

$$f(X_1, X_2, X_3, X_4) = 0, \quad aX_0^2 + g(X_1, X_2, X_3, X_4) = 0 \tag{70}$$

with $a \neq 0$.

Now let P be any point on $X_0 = 0$, let Q be the quadric of the pencil (70) which passes through P, and let Π be the tangent hyperplane to Q at P. I claim that the curve of genus 1 in which Π meets V is of the type considered in §7.2. For this it is enough to show for general P that its equation can be put in the form (61). But provided that P does not lie on $f = 0$, by a further change of variables we can take P to be $(0, 1, 0, 0, 0)$ and require

$$f(X_1, X_2, X_3, X_4) = bX_1^2 + f_1(X_2, X_3, X_4).$$

The equation of Q has no term in X_1^2, so by a further change of variables we can take it to have the form

$$aX_0^2 + cX_1X_4 + h(X_2, X_3, X_4) = 0 \tag{71}$$

with $c \neq 0$; this is equivalent to requiring the equation of Π to be $X_4 = 0$. Since V is given by $f = 0$ and (71), its intersection with $X_4 = 0$ has the required form.

This construction breaks down if P lies on V or is the vertex of one of the other singular quadrics of the pencil, because then Π is no longer well-defined. To remedy this, what we do is to choose a point P on $X_0 = 0$ together with a hyperplane Π which touches at P some quadric of the pencil (70). Thus P should be considered as a point of the variety W obtained by blowing up $X_0 = 0$ (which can be identified with $\mathbf{P}^3$) along the curve $V \cap \{X_0 = 0\}$ and at the vertices of the other four singular quadrics of the pencil.

Denote by U the variety over W whose fibres are the curves $V \cap \Pi$ in the construction above; then what we have obtained is a diagram

$$W \longleftarrow U \longrightarrow V$$

in which the left hand map is a fibration. The right hand map here is not a fibration, and it seems unlikely that there is even a subvariety of U on which the restriction of the map is a fibration. But this is not important. What matters is the existence of a section — that is, a map $V \to U$ such that the composite map $V \to U \to V$ is the identity; and for this we only need the map $V \to U$ to be rational rather than everywhere defined. In the notation of (70) let $P_0 = (x_0, \ldots, x_4)$ be a point of V with $x_0 \neq 0$, and choose $P = (0, x_1, x_2, x_3, x_4)$. The equation of Π has no term in X_0; hence since P lies on Π so does P_0. This defines the rational map $V \to U$. Provided V is everywhere locally soluble, so is U. If we can find a field extension k_2/k_1 of

odd degree such that U is soluble in k_2, then V will also be soluble in k_2 and two applications of Theorem 11 will show that V is soluble in k.

We cannot apply the last sentence of Theorem 8 as it stands, because W is too big; but it is simple enough to find a line L defined over k_1 in the $\mathbf{P}^3$ which underlies W such that

- L is in sufficiently general position, and
- the inverse image of L in U is everywhere locally soluble.

To do this, we choose any P_1 on $X_0 = 0$ and defined over k_1. The fibre above P_1 is locally soluble except at a finite set $\mathcal{S}$ of places. For each of these places there is a point of U in the corresponding local field, and this maps down to a point of $\mathbf{P}^3$. Using weak approximation on $\mathbf{P}^3$ we can therefore find a point P_2 in $\mathbf{P}^3$ such that the fibre above P_2 is locally soluble at each place in $\mathcal{S}$. We can now take L to be the line P_1P_2 and apply Theorem 8 to the inverse image of L in U.

To obtain a satisfactory theorem for V, we have to translate Conditions 1 to 4 of §7.2 into conditions on V. A tedious calculation, which can be found in [1], shows that Conditions 1, 3 and 4 are satisfied provided L is in sufficiently general position. The difficulty is with Condition 2, or more precisely with the continuous conditions in the sense of §3 which are generated by Condition 2. It ought to be true that these come from the continuous conditions on the two pencils of conics each of which is given by one of the two equations (61) — and which are known to be Brauer-Manin. It ought also to be true that they correspond to the Brauer-Manin conditions on V. But as yet I have been unable to prove either of these assertions.

9. *Diagonal quartic surfaces.*
We now apply the ideas of §6 to K3 surfaces defined over $\mathbf{Q}$ whose equation has the form

$$a_0X_0^4 + a_1X_1^4 + a_2X_2^4 + a_3X_3^4 = 0. \tag{72}$$

We shall always assume that (72) is everywhere locally soluble and the a_i are integral. The surfaces (72) are very special within the family of nonsingular quartic surfaces for at least two reasons: they are Kummer surfaces, and their Néron-Severi groups over $\mathbf{C}$ have maximal rank, which is 20. But this is probably the simplest family of K3 surfaces that can be written down explicitly.

We can take $\mathcal{B}$, the set of bad places for (72), to consist of $\infty, 2$ and the odd primes which divide $a_0a_1a_2a_3$. It is known that the Néron-Severi group of (72) over $\mathbf{C}$ is generated by the 48 lines on the surface. However, what is equally important for our purposes is the Néron-Severi group over $\mathbf{Q}$. There are now 282 possibilities for the Galois group over $\mathbf{Q}$ of the least field of definition of the 48 lines; these have been tabulated by Martin Bright in his Cambridge Ph.D. thesis, which can be found at

http://www.boojum.org.uk/maths/quartic-surfaces/

together with a good deal of other relevent material. We shall be interested in the special case when

$$a_0a_1a_2a_3 \text{ is a square,} \tag{73}$$

because then the surface contains a pencil of curves of genus 1 of the kind considered in §6. There are some other special cases in which the surface (72) contains such a pencil; but this is not true in general and it seems unlikely that one can apply the methods expounded in these notes to the general surface (72).

There is an obvious map from (72) to the quadric surface

$$a_0Y_0^2 + a_1Y_1^2 + a_2Y_2^2 + a_3Y_3^2 = 0. \tag{74}$$

We have assumed that (72), and therefore (74), is everywhere locally soluble; so (74) is soluble in $\mathbf{Q}$. The reason why the case (73) is more tractable than the general case is that if (73) holds then each of the two pencils of lines on (74) is defined over $\mathbf{Q}$, and a general line of either pencil pulls back to a

curve of genus 1 on (72) which is a 2-covering of its Jacobian. It turns out that these curves are of the kind considered in §§5 and 6. More generally, consider a quadric of the form

$$A(Y)D(Y) = B(Y)C(Y) \tag{75}$$

where $A(Y) = \alpha_0 Y_0 + \alpha_1 Y_1 + \alpha_2 Y_2 + \alpha_3 Y_3$ and so on. This quadric is the image of the K3 surface

$$A(X^2)D(X^2) = B(X^2)C(X^2) \tag{76}$$

in an obvious notation, and the pull-backs of the two pencils of lines on (75) can be written

$$yA(X^2) = zB(X^2), \quad yC(X^2) = zD(X^2) \tag{77}$$

and

$$yA(X^2) = zC(X^2), \quad yB(X^2) = zD(X^2). \tag{78}$$

For the time being, we work with (77). Eliminating each of the four variables X_ν in turn, we obtain four equations of the form

$$d_{i\ell}X_i^2 + d_{j\ell}X_j^2 + d_{k\ell}X_k^2 = 0, \tag{79}$$

only two of which are linearly independent. Here i, j, k, ℓ is any permutation of $1, 2, 3, 4$ and $d_{\mu\nu}$ is the value of the determinant formed by columns μ and ν of the matrix

$$\begin{pmatrix} \alpha_0 y - \beta_0 z & \alpha_1 y - \beta_1 z & \alpha_2 y - \beta_2 z & \alpha_3 y - \beta_3 z \\ \gamma_0 y - \delta_0 z & \gamma_1 y - \delta_1 z & \gamma_2 y - \delta_2 z & \gamma_3 y - \delta_3 z \end{pmatrix}.$$

We note the identity

$$d_{01}d_{23} + d_{02}d_{31} + d_{03}d_{12} = 0,$$

which is frequently useful. The Jacobian of the curve (77) has the form

$$E : Y^2 = (X - c_1)(X - c_2)(X - c_3)$$

where

$$c_1 - c_2 = d_{03}d_{21}, \quad c_2 - c_3 = d_{01}d_{32}, \quad c_3 - c_1 = d_{02}d_{13},$$

and the map from the curve (77) to its Jacobian is given by

$$Y = d_{12}d_{23}d_{31}X_1X_2X_3/X_0^3, \quad X - c_i = d_{ij}d_{ki}X_i^2/X_0^2$$

where i, j, k is any permutation of $1, 2, 3$. Although everything so far is homogeneous in y, z, we have to work in $\mathbf{Q}(y, z)$ rather than $\mathbf{Q}(y/z)$, for reasons which are already implicit in §3.

Up to this point, the formulae hold for any nonsingular quartic surface which can be written in the form (76). For the diagonal quartic surface (72) we have the unexpected result that each $d_{k\ell}$ is a constant multiple of d_{ij}, where i, j, k, ℓ is any permutation of $0, 1, 2, 3$. For it follows from the solubility of (74) and the fact that $a_0a_1a_2a_3$ is a square that $-a_1$ is represented by $a_2Y_2^2 + a_3Y_3^2$ over $\mathbf{Q}$. In other words, there exist integers r_1, r_2, r_3 and h such that

$$a_1r_1^2 + a_2r_2^2 + a_3r_3^2 = 0, \quad h^2 = a_0a_1a_2a_3.$$

After rescaling the equation (72) if necessary, we can take

$$\begin{aligned}
A(X^2) =& hr_2X_0^2 + a_1a_3(r_3X_1^2 - r_1X_3^2),\\
B(X^2) =& hr_3X_0^2 - a_1a_2(r_2X_1^2 + r_1X_2^2),\\
C(X^2) =& a_3hr_3X_0^2 - a_1a_2a_3(r_2X_1^2 - r_1X_2^2),\\
D(X^2) =& -a_2hr_2X_0^2 - a_1a_2a_3(r_3X_1^2 + r_1X_3^2);
\end{aligned}$$

and the d_{ij} are given by

$$\begin{aligned}
d_{23} &= a_1^2a_2a_3r_1^2(a_3y^2 + a_2z^2), \quad d_{01} = (h/a_2a_3)d_{23},\\
d_{31} &= a_1^2a_2a_3r_1(a_3r_2y^2 - 2a_3r_3yz - a_2r_2z^2), \quad d_{02} = (h/a_3a_1)d_{31},\\
d_{12} &= a_1^2a_2a_3r_1(a_3r_3y^2 + 2a_2r_2yz - a_2r_3z^2), \quad d_{03} = (h/a_1a_2)d_{12}.
\end{aligned}$$

These choices do not preserve the symmetry, but that loss appears to be unavoidable. Changing the r_i corresponds to a linear transformation on y, z; changing the sign of h gives the pencil (78) instead of (77).

The 2-covering of E given by the triple (m_1, m_2, m_3) with $m_1m_2m_3 = 1$ is

$$m_iZ_i^2 = X - c_i \text{ for } i = 1, 2, 3 \quad \text{and} \quad Y^2 = Z_1Z_2Z_3.$$

As in §6, values associated with the particular 2-covering given by (77) will be denoted by a superfix 0; the 2-covering itself is given by

$$m_1^0 = -d_{21}d_{31}, \quad m_2^0 = -d_{12}d_{32}, \quad m_3^0 = -d_{13}d_{23}.$$

We shall also need to know the 2-coverings corresponding to the 2-division points. That corresponding to $(c_1, 0)$, for example, is given by

$$m_1 = -a_0 a_1, \quad m_2 = d_{03} d_{21}, \quad m_3 = d_{02} d_{31}, \tag{80}$$

which can alternatively be written

$$m_1 = -a_0 a_1, \quad m_2 = -h/a_1 a_2, \quad m_3 = h/a_3 a_1.$$

It follows from the expressions for the d_{ij} that, up to a squared factor, the discriminant of d_{ij} is equal to $-a_i a_j$; thus in particular d_{ij} has no repeated linear factor and it is a product of two linear factors over $\mathbf{Q}$ if and only if $-a_i a_j$ is in $\mathbf{Q}^{*2}$. If i, j, k is a cyclic permutation of $1, 2, 3$ then

$$d_{0i}/d_{jk} = a_0 a_i / h = h/a_j a_k.$$

Moreover the resultant of d_{ij} and d_{ik} is $-4a_i^2 a_j a_k$, so that d_{ij} and d_{ik} cannot have a common root. The pencil (77) has six singular fibres, given by the roots of $d_{01} d_{02} d_{03} = 0$, and each singular fibre consists of four lines which form a skew quadrilateral. Thus each of the 48 lines on (72) is part of a singular fibre of either (77) or (78).

Martin Bright's thesis contains a dictionary which gives the Néron-Severi group of (72) over any field k. This group has rank at least 2 whenever (73) holds; subject to (73), it has rank greater than 2 if and only if up to fourth powers there is a relation of the form $a_j = 4a_i$ or $a_j = -a_i$ or $a_i a_j = a_k a_\ell$.

In order to apply the results in §6, we must know when Condition D holds, and we must evaluate the relevent Legendre-Jacobi functions. This is where a splitting of cases becomes necessary. In what follows, we confine ourselves to the cases when none of the $-a_i a_j$ is in $\mathbf{Q}^{*2}$, which is equivalent to requiring that all the d_{ij} are irreducible over $\mathbf{Q}$.

Lemma 24 *Suppose that no $-a_i a_j$ is in $\mathbf{Q}^{*2}$. Then for any m which does not satisfy Condition D, one of m and mm^0 can be chosen to be independent of y and z. Moreover the group of such m has order exactly 8 (and consists of the inescapable part of the 2-Selmer group) if and only if $a_0 a_1 a_2 a_3$ is not a fourth power and no $a_i a_j$ is a square.*

Proof A boring calculation shows that the primitive 4-division points satisfy $(X - c_1)^2 = -a_0 d_{12}^2 d_{13}^2 / a_1$ and so on; so under our hypothesis none of them are rational. Now suppose that the triple m does not satisfy Condition D.

As was pointed out at the beginning of §6, we can confine ourselves to those triples m for which the value of m_3 lies in the group generated by

$$-1, 2, d_{23}, d_{31} \text{ and the odd primes in } \mathcal{B};$$

and similarly for m_1 and m_2. In the notation of the first part of §6 each of the p_{ij} has only a single irreducible factor $f_{k\tau}$ in $\mathbf{Q}[y,z]$ and $f_{k\tau}^2 \| p_{ij}$; so we can drop the subscript τ which appears there. Let ξ_3 satisfy $d_{03}(\xi_3, 1) = 0$; then

$$\xi_3 = (-a_2 r_2 \pm r_1\sqrt{-a_1 a_2})/a_3 r_3$$

and therefore

$$\begin{aligned} d_{23}(\xi_3,1) &= -2a_1^2 a_2^2 r_1^3 r_3^{-2}(a_1 r_1 \pm r_2\sqrt{-a_1 a_2}), \\ d_{31}(\xi_3,1) &= -2a_1^3 a_2 r_1^3 r_3^{-2}(a_2 r_2 \mp r_1\sqrt{-a_1 a_2}) = \mp d_{23}(\xi_3,1)\sqrt{-a_1/a_2}. \end{aligned}$$

Here $K_3 = \mathbf{Q}(\xi_3) = \mathbf{Q}(\sqrt{-a_2/a_1})$ and

$$L_3^0 = K_3(\sqrt{d_{31}(\xi_3,1)d_{23}(\xi_3,1)}, \sqrt{-h/a_2 a_3}) = \mathbf{Q}(\sqrt[4]{-a_1 a_2}, \sqrt{-h/a_2 a_3})$$

in the notation of §6. Now suppose for example that m_3 is divisible to the first power by d_{23} but not by d_{31}. Because $L_3 \supset K_3(\sqrt{m_3})$ and we have assumed $L_3 \subset L_3^0$, it follows that $\sqrt{m_3}$ is in L_3^0, which is a biquadratic extension of K_3. Hence one of

$$m_3,\ m_3\sqrt{-a_1/a_2},\ (-h/a_2 a_3)m_3,\ (-h/a_2 a_3)m_3\sqrt{-a_1/a_2}$$

is in K_3^{*2}. But the norm of m_3 for $K_3/\mathbf{Q}$ is $-a_1 a_3$ times an element of $\mathbf{Q}^{*2}$, so this would require $-a_1 a_3$ or $-a_2 a_3$ to be in $\mathbf{Q}^{*2}$, contrary to hypothesis. A similar argument works if m_3 is divisible to the first power by d_{31} but not by d_{23}. It follows that m_3 must contain both or neither of d_{23} and d_{31} as factors. Applying a similar argument to m_1 and m_2, and remembering that $m_1 m_2 m_3$ must be a square, we find that either m or mm^0 must be independent of y/z. It is enough to consider the former case; now as elements of $\mathbf{Q}^*/\mathbf{Q}^{*2}$,

$$\begin{aligned} m_1 &\text{ is in } \{1, -a_2 a_3, h a_0 a_3, -h a_0 a_2\}, \\ m_2 &\text{ is in } \{1, -a_3 a_1, h a_0 a_1, -h a_0 a_3\}, \\ m_3 &\text{ is in } \{1, -a_1 a_2, h a_0 a_2, -h a_0 a_1\}. \end{aligned}$$

In general this allows us only four choices for the m_i such that $m_1m_2m_3$ is a square; these correspond to the origin and the three 2-division points on E. Additional possibilities happen only when at least one of

$$h,\ ha_0a_1,\ ha_0a_2,\ ha_0a_3,\ a_1a_2,\ a_2a_3,\ a_3a_1$$

is in $\pm\mathbf{Q}^{*2}$. But if ha_0a_1 is in $\pm\mathbf{Q}^{*2}$ for example, then all we obtain is a new way of describing triples m which are already known to lie in the inescapable part of the 2-Selmer group; so these cases can be ignored. The others give the exceptions listed.

If for example a_2a_3 is a square then $(1, -a_1a_2, -a_1a_2)$ does not satisfy Condition D. Again, if h is in $-\mathbf{Q}^{*2}$ then (a_1a_3, a_1a_2, a_2a_3) does not satisfy Condition D, whereas if h is in $\mathbf{Q}^{*2}$ then (a_1a_2, a_2a_3, a_3a_1) does not satisfy Condition D. In each of these cases, the group of inescapable elements of the 2-Selmer group acquires one extra generator which is the m just listed. If both a_2a_3 and one of $\pm h$ is a square, then we acquire two extra generators in this way. □

We can now state the main result of this section, which is simply the specialization of Theorem 6 to our case, and which therefore requires no further proof. If $\mathcal{N}^2$ is as at the beginning of §3, we shall denote by $\mathcal{A}$ the closure of the set of points $\alpha \times \beta$ in $\mathcal{N}^2$ at which (77) is locally soluble for $y = \alpha, z = \beta$ at each place of $\mathcal{B}$ and all the Legendre-Jacobi conditions associated with any pencil of conics (79) hold.

Theorem 12 *Assume Schinzel's Hypothesis and Hypothesis* Ш. *Let* (72) *be everywhere locally soluble and such that $a_0a_1a_2a_3$ is a square. Suppose also that no $-a_ia_j$ is in $\mathbf{Q}^{*2}$. If $\mathcal{A}$ is not empty and Condition D holds, then* (72) *contains rational points.*

As was remarked at the end of §6, we can here replace Condition D by the weaker Condition E. This will hold unless a relevent one of the m listed at the end of the proof of Lemma 24 corresponds to an everywhere locally soluble 2-covering. It turns out that solubility in $\mathbf{R}$ is automatic. Lemma 13 provides a simple test, which is not always satisfied, for solubility at odd primes. But to test for solubility in $\mathbf{Q}_2$ is more tedious.

By the results of §4, the solubility of the pencil of conics (79) is equivalent to three Legendre-Jacobi conditions, of which a typical one is

$$L(\mathcal{B}; -d_{i\ell}d_{j\ell}, d_{k\ell}) = 1. \tag{81}$$

There are twelve conditions of this kind, but they are not all independent. Indeed in the notation of Lemma 9 the continuous conditions, which form a subgroup there called Λ_0, are all Brauer-Manin; and Bright's table shows that in the most general case satisfying (73) there is only one Brauer-Manin condition. This gives us advance assurance that the algebra on which we now embark will be fruitful. Since as an element of $\mathbf{Q}^*/\mathbf{Q}^{*2}$ the discriminant of $d_{k\ell}$ is equal to $-a_k a_\ell$,

$$(-a_k a_\ell, d_{k\ell}(\alpha,\beta))_p = 1 \text{ for } \alpha \times \beta \text{ in } \mathcal{A} \text{ and } p \text{ not in } \mathcal{B}.$$

Since $d_{i\ell}d_{j\ell}/d_{ik}d_{jk}$ is also equal to $-a_k a_\ell \bmod \mathbf{Q}^{*2}$,

$$L(\mathcal{B}; -d_{i\ell}d_{j\ell}, d_{k\ell}; \alpha, \beta) = L(\mathcal{B}; -d_{ik}d_{jk}, d_{\ell k}; \alpha, \beta).$$

We shall denote either of these last two expressions by F_{ij}. Again,

$$L(d_{ij}, d_{ki})L(d_{ki}, d_{ij}) = \prod_{p \text{ not in } \mathcal{B}} (d_{ij}, d_{ki})_p = \prod_{v\in\mathcal{B}} (d_{ij}, d_{ki})_v$$

from which it follows that

$$F_{ij}F_{jk}F_{ki} = \prod_{v\in\mathcal{B}} \{(d_{ij}, d_{jk})_v (d_{jk}, d_{ki})_v (d_{ki}, d_{ij})_v\}.$$

We know that (79) is locally soluble at each place v in $\mathcal{B}$. The local solubility condition for (23) is (24); applying this to (79) we obtain

$$(d_{i\ell}, -d_{j\ell})_v (d_{j\ell}, -d_{k\ell})_v (d_{k\ell}, -d_{i\ell})_v = (-1,-1)_v.$$

Taking the product of this equation over all v in $\mathcal{B}$ and using the Hilbert product formula, we obtain

$$\begin{aligned} F_{ij}F_{jk}F_{ki} &= \prod_{v\in\mathcal{B}} \{(d_{jk}, -a_j a_k)_v (d_{ki}, -a_k a_i)_v (d_{ij}, -a_i a_j)_v\} \\ &= \prod_{p \text{ not in } \mathcal{B}} \{(d_{jk}, -a_j a_k)_p (d_{ki}, -a_k a_i)_p (d_{ij}, -a_i a_j)_p\} = 1, \end{aligned}$$

because for example $-a_j a_k$ is up to a squared factor the discriminant of d_{jk} and is therefore a square mod p for any prime p outside $\mathcal{B}$ which divides $d_{jk}(\alpha,\beta)$. One now deduces that

$$F_{i\ell}F_{j\ell}F_{k\ell} = F_{i\ell}F_{jk} = F_{j\ell}F_{ki} = F_{k\ell}F_{ij}$$

on $\mathcal{A}$, whence all the $F_{i\ell}F_{j\ell}F_{k\ell}$ are equal on $\mathcal{A}$.

The explicit formulae which follow (19) show that, in the notation of §3, the value of θ associated with $L(\mathcal{B}; \pm d_{i\ell}, d_{k\ell})$ is $-a_ia_k$; so the value of θ associated with F_{ij} is a_ia_j. It follows from the calculations in the previous paragraph that in general there is only one non-trivial continuous condition, which can be written $F_{12}F_{23}F_{31} = 1$. If however one of the a_ia_j is a square then the corresponding condition $F_{ij} = 1$ is also in Λ_0. The remarks at the end of the proof of Lemma 24 show that Condition D cannot then hold, but Condition E may still hold in some part of $\mathcal{A}$.

The easiest way to evaluate the one condition which is non-trivial and continuous even in the general case involves dropping the symmetry; we have for example

$$\begin{aligned} F_{01}F_{23} &= L(-d_{03}d_{13}, d_{23})L(-d_{02}d_{03}, d_{01}) = L(d_{02}d_{13}, d_{23}) \\ &= L(-ha_1a_3, d_{23}) = \prod_{p \text{ not in } \mathcal{B}} (-ha_1a_3, d_{23})_p = \prod_{v \in \mathcal{B}} (-ha_1a_3, d_{23}(\alpha, \beta))_v. \end{aligned}$$

Of the surfaces (72) satisfying (73) and with each $|a_i| < 16$, there are just two which are everywhere locally soluble but are not known to have a solution in $\mathbf{Q}$. They are

$$2X_0^4 + 9X_1^4 = 6X_2^4 + 12X_3^4 \quad \text{and} \quad 4X_0^4 + 9X_1^4 = 8X_2^4 + 8X_3^4.$$

It turns out that both of them are insoluble in $\mathbf{Q}$: the first fails the condition $F_{01}F_{23} = 1$ and the second has a_0a_1 square and fails the condition $F_{01} = 1$. We give the details for the first one. The calculations for the second one are more tedious, since to evaluate F_{01} one needs to use the formulae which follow (19).

For the first surface we have $\mathcal{B} = \{2, 3, \infty\}$, and the surface can be written in the form

$$\begin{aligned} 2(X_0^2 - X_2^2 - 2X_3^2)(X_0^2 + X_2^2 + 2X_3^2) \\ = -(3X_1^2 - 2X_2^2 + 2X_3^2)(3X_1^2 + 2X_2^2 - 2X_3^2); \end{aligned}$$

thus the pencil (77) can be taken to be

$$\begin{aligned} 2y(X_0^2 - X_2^2 - 2X_3^2) + z(3X_1^2 - 2X_2^2 + 2X_3^2) = 0, \\ y(3X_1^2 + 2X_2^2 - 2X_3^2) - z(X_0^2 + X_2^2 + 2X_3^2) = 0, \end{aligned}$$

and the d_{ij} are given by

$$\begin{array}{ll} d_{01} = 3(2y^2 + z^2), & d_{23} = 6(2y^2 + z^2), \\ d_{02} = 2(2y^2 - 2yz - z^2), & d_{31} = -6(2y^2 - 2yz - z^2), \\ d_{03} = -2(2y^2 + 4yz - z^2), & d_{12} = 3(2y^2 + 4yz - z^2). \end{array}$$

It follows that $h = 36$; recall that it is only h^2 that was determined earlier, and the choice of sign was equivalent to the choice between the pencils (77) and (78).

We do not need information about $\mathbf{R}$, but in fact we have $c_2 > c_1 > c_3$, so the curve (77) is soluble in $\mathbf{R}$ if and only if $m_2^0 > 0$. All primitive solutions must have X_0, X_2, X_3 odd and $2 \| X_1$, whence $y + z \equiv 0 \bmod 4$; a full analysis shows that this condition is sufficient for solubility in $\mathbf{Q}_2$ as well as necessary, but we do not need this. The analysis of solubility in $\mathbf{Q}_3$ is more tedious. We must have $3 | X_0$ and X_2, X_3 prime to 3. The three triples like (80) lie in W_3 and therefore generate it; so m_1^0 must be in $\mathbf{Q}_3^{*2}$ or $3\mathbf{Q}_3^{*2}$ and m_3^0 must be in $\mathbf{Q}_3^{*2}$ or $6\mathbf{Q}_3^{*2}$. But

$$m_1^0 = -d_{21}d_{31} = -18\{3y^2 - (y+z)^2\}\{2(y+z)^2 - 3z^2\},$$

so $3 \not| (y + z)$. Thus $2y^2 - 2yz - z^2$ is in $2\mathbf{Q}_3^{*2}$, whence consideration of m_3^0 shows that

$$2y^2 + z^2 \text{ is in } \mathbf{Q}_3^{*2} \text{ or } 6\mathbf{Q}_3^{*2}.$$

It now follows easily that $F_{01}F_{23} = -1$ throughout $\mathcal{A}$.

Subject to our two major hypotheses, Theorem 12 asserts that in general the only obstructions to the Hasse principle for surfaces (72) subject to (73) are the continuous Legendre-Jacobi obstructions or equivalently the Brauer-Manin obstructions. 'In general' here means that no $\pm a_i a_j$ is a square and $a_0a_1a_2a_3$ is not a fourth power. I have not attempted to investigate the exceptional cases, but for them there are additional Brauer-Manin obstructions and the assertion above may well remain true. However, without (73) there is strong numerical evidence that the situation is quite different. First, the special surface

$$X_0^4 + 2X_1^4 = X_2^4 + 4X_3^4$$

appears to contain no rational points other than the two obvious ones. This surface has non-trivial Brauer group, but Brauer-Manin obstructions seem to be incapable of showing that a non-singular surface contains a finite non-zero

number of rational points. Second, Bright has investigated surfaces of the form

$$X_0^4 + cX_1^4 = 4X_2^4 + 2cd^2X_3^4$$

where c is not a square. This is one of the simplest families which have no Brauer-Manin obstruction arising from the arithmetic part of the Brauer group — that is, the part of the Brauer group which is killed by replacing the ground field by its algebraic closure. Surfaces of this form have Nèron-Severi group over $\mathbf{Q}$ of rank 2, but they do not admit pencils of curves of genus 1. There are many surfaces of this form which are everywhere locally soluble but do not appear to have any rational solutions. Presumably therefore, there are further obstructions to the Hasse principle as yet undiscovered.

REFERENCES

[1] A.O.Bender and Sir Peter Swinnerton-Dyer, Solubility of certain pencils of curves of genus 1, and of the intersection of two quadrics in $\mathbf{P}^4$, Proc. London Math.Soc. (3)83(2001), 299-329.
[2] J.W.S.Cassels, Second descent for elliptic curves, J. reine angew. Math. 494(1998), 101-127.
[3] J-L.Colliot-Thélène, Hasse principle for pencils of curves of genus one whose Jacobians have a rational 2-division point, (close variation on a paper of Bender and Swinnerton-Dyer), Progr. Math. 199(2001), 117-161.
[4] J-L.Colliot-Thélène, A.N.Skorobogatov and Sir Peter Swinnerton-Dyer, Double fibres and double covers: paucity of rational points, Acta Arith. 79(1997), 113-135.
[5] J-L.Colliot-Thélène, A.N.Skorobogatov and Sir Peter Swinnerton-Dyer, Rational points and zero-cycles on fibred varieties: Schinzel's Hypothesis and Salberger's device, J. reine angew. Math. 495(1998), 1-28.
[6] J-L.Colliot-Thélène, A.N.Skorobogatov and Sir Peter Swinnerton-Dyer, Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, Invent. Math. 134(1998), 579-650.
[7] J-L.Colliot-Thélène and Sir Peter Swinnerton-Dyer, Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties, J. Reine Angew. Math. 453(1994), 49-112.
[8] D.Coray, Points algébriques sur les surfaces de Del Pezzo, C. R. Acad. Sci. Paris 284(1977), 1531-4.
[9] J.S.Milne, Arithmetic Duality Theorems (Boston, 1986).
[10] P.Salberger, Zero-cycles on rational surfaces over number fields, Invent. Math. 91(1988), 505-524.
[11] P.Salberger and A.N.Skorobogatov, Weak approximation for surfaces defined by two quadratic forms, Duke J. Math. 63(1991), 517-536.
[12] J-J.Sansuc, Descente et principe de Hasse pour certains variétés rationnelles, in *Séminaire de Théorie des Nombres, Paris* $1980-81$ (ed. M-J.Bertin), 253-272 (Progr. Math. 22).
[13] Sir Peter Swinnerton-Dyer, Rational points on pencils of conics and on pencils of quadrics, J. London Math. Soc. (2)50(1994), 231-242.
[14] Sir Peter Swinnerton-Dyer, Some applications of Schinzel's hypothesis to diophantine equations, in Number theory in progress (ed. K.Győry, H.Iwaniec and J.Urbanowicz), 503-530 (Berlin, 1999).

[15] Sir Peter Swinnerton-Dyer, Arithmetic of diagonal quartic surfaces, II, Proc. London Math. Soc. (3)80(2000), 513-544.
[16] Sir Peter Swinnerton-Dyer, The solubility of diagonal cubic surfaces, Ann. Scient. Éc. Norm. Sup. (4)34(2001), 891-912.