ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

PETER SWINNERTON-DYER

Rational points on some pencils of conics with 6 singular fibres

Annales de la faculté des sciences de Toulouse 6e série, tome 8, nº 2 (1999), p. 331-341

<http://www.numdam.org/item?id=AFST_1999_6_8_2_331_0>

Annales de la Faculté des Sciences de Toulouse Vol. VIII, n° 2, 1999
pp. 331–341

Rational points on some pencils of conics with 6 singular fibres [(*)]

SIR PETER SWINNERTON-DYER [(1)]

RÉSUMÉ. — Soient k un corps de nombres et $c \in k$ non carré. Soient f_4, f_2 des polynômes homogènes en X, Y, de degré 4 et 2 respectivement. On donne des conditions nécessaires et suffisantes pour que l'équation

$$U^2 - cV^2 = f_4(X,Y)f_2(X,Y).$$

ait des solutions dans k.

ABSTRACT. — Let k be an algebraic number field, let c be a non-square in k and let f_4, f_2 be homogeneous polynomials in X, Y of degrees 4 and 2 respectively. Necessary and sufficient conditions are obtained for the solubility in k of

$$U^2 - cV^2 = f_4(X,Y)f_2(X,Y).$$

Let $\mathcal{Y} \to \mathbf{P}^1$ be a pencil of conics defined over an algebraic number field k. It is conjectured that the only obstruction to the Hasse principle on $\mathcal{Y}$, and also to weak approximation, is the Brauer-Manin obstruction; and it was shown in [3] that this follows from Schinzel's Hypothesis. Descriptions of the Brauer-Manin obstruction and of Schinzel's Hypothesis can be found in [3]. It is of interest that arguments which show that the Brauer-Manin obstruction is the only obstruction to the Hasse principle for particular classes of $\mathcal{Y}$ normally fall into two parts:

(*) Reçu le 24 décembre 1998, accepté le 27 mai 1999

(1) Isaac Newton Institute, Cambridge University 20 Clarkson Rd., Cambridge, United Kingdom.
E-mail: hpfs100@newton.cam.ac.uk

(i) the proof that some comparatively down-to-earth obstruction is the only obstruction to the Hasse principle;

(ii) the identification of that obstruction with the Brauer-Manin obstruction.

The theorem in this paper is entirely concerned with (i); the equivalence of the obstruction in the theorem with the Brauer-Manin one has already been proved in a much more general context in [1], §2.6b and Chapter 3.

If one does not assume Schinzel's Hypothesis, little is known. The only promising-looking line of attack is through the geometry of the universal torseurs on $\mathcal{Y}$; and these are much easier to study when $\mathcal{Y}$ has the special form

$$U^2 - cV^2 = P(W) \tag{1}$$

where c is a non-square in k and $P(W)$ is a separable polynomial in $k[W]$. By writing $W = X/Y$ we can take the solubility of (1) into the equivalent (though ungeometric) problem of the solubility of

$$U^2 - cV^2 = f(X,Y) \tag{2}$$

in k, where f is homogeneous of even degree; here $\deg f$ is $1+\deg P$ or $\deg P$. The simplest non-trivial case is that of Châtelet surfaces, when $P(W)$ has degree 3 or 4; in this case the conjecture was proved in [2]. The object of this paper is to prove the conjecture when $\deg f = 6$ and $f = f_4 f_2$ over k, where $\deg f_4 = 4$ and $\deg f_2 = 2$.

Until the statement of the main theorem, we make no assumption about (2) other than that $f(X,Y)$ has even degree n and no repeated factor. After multiplying X, Y by suitable integers in k, we can assume that

$$f(X,Y) = a\prod_1^n (X + \lambda_i Y)$$

where a is an integer in k and the λ_i are integers in $\bar{k}$; the λ_i form complete sets of conjugates over k. For convenience we write $\gamma = \sqrt{c}$. We can assume that γ does not lie in any $k(\lambda_i)$; for otherwise $f(X,Y)$ would have a non-trivial factor of the form $F^2 - cG^2$ with F, G in $k[X,Y]$ and we could instead consider the simpler equation

$$U^2 - cV^2 = g(X,Y) = f(X,Y)/(F^2 - cG^2).$$

We can clearly also assume that the λ_i are all distinct; for otherwise we can remove a squared factor from $f(X,Y)$ and reduce to a simpler problem which has already been solved in [2]. To avoid trivialities, we shall also rule out solutions for which each side of (2) vanishes.

Let $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ be a set of representatives for the ideal classes in k; then it is enough to look for solutions u, v, x, y of (2) for which x, y are integers whose highest common factor is some $\mathfrak{a}_m$. (To move from rational to integral solutions may appear unnatural; but in fact it greatly simplifies the argument which follows, because it means that our intermediate equations do not have to be homogeneous.)

LEMMA 1.— *There is a finite computable list of n-tuples $(\alpha_1^{(r)}, \dots, \alpha_n^{(r)})$ not depending on u, v, x, y, where $\alpha_i^{(r)}$ is in $k(\lambda_i)$ and conjugacy between λ_i and λ_j extends to conjugacy between $\alpha_i^{(r)}$ and $\alpha_j^{(r)}$, with the following property. If (2) has a solution with x, y integers whose highest common factor is some $\mathfrak{a}_m$, then for some r the system*

$$u_i^2 - cv_i^2 = \alpha_i^{(r)}(x + \lambda_i y) \quad (1 \leqslant i \leqslant n) \tag{3}$$

has solutions with u_i, v_i in $k(\lambda_i)$ for each i.

Proof.— We postulate once for all that the manipulations which follow are to be carried out in such a way as to preserve conjugacy. A prime factor $\mathfrak{p}$ of $x + \lambda_i y$ in $k(\lambda_i)$ which also divides $f(x,y)/(x + \lambda_i y)$ must divide

$$a\prod\nolimits_{j \neq i}(-\lambda_i y + \lambda_j y) = y^5 a \prod\nolimits_{j \neq i}(\lambda_j - \lambda_i),$$

and for similar reasons it must divide

$$a\prod\nolimits_{j \neq i}(\lambda_i x - \lambda_j x) = -x^5 a \prod\nolimits_{j \neq i}(\lambda_j - \lambda_i).$$

Hence it divides $a\mathfrak{a}_m \prod_{j \neq i}(\lambda_j - \lambda_i)$ and must therefore belong to a finite computable list; and any prime ideal not in this list which divides some $x + \lambda_i y$ to an odd power must split or ramify in $k(\lambda_i, \gamma)/k(\lambda_i)$. As ideals, $(x + \lambda_i y) = \mathfrak{b}_i \mathfrak{c}_i$ where $\mathfrak{b}_i$ only contains the prime ideals which either lie in the finite computable list above or ramify in $k(\lambda_i, \gamma)/k(\lambda_i)$, and every prime ideal which occurs to an odd power in $\mathfrak{c}_i$ must split in $k(\lambda_i, \gamma)/k(\lambda_i)$. By transferring squares from $\mathfrak{b}_i$ to $\mathfrak{c}_i$ we can assume that each $\mathfrak{b}_i$ is square-free. Each $\mathfrak{b}_i$ belongs to a finite list independent of x, y, and conorm $\mathfrak{c}_i = \mathfrak{C}_i . \sigma \mathfrak{C}_i$ where $\mathfrak{C}_i$ is an ideal in $k(\lambda_i, \gamma)$ and σ is the non-trivial automorphism of $k(\lambda_i, \gamma)$ over $k(\lambda_i)$. Let $\mathfrak{A}_1, \dots, \mathfrak{A}_H$ be a set of representatives for the ideal classes in $k(\lambda_i, \gamma)$; then for some $\mathfrak{A}^{(i)}$ from this list $\mathfrak{A}^{(i)}\mathfrak{C}_i$ is principal, say $\mathfrak{A}^{(i)}\mathfrak{C}_i = (\xi_i + \gamma \eta_i)$ with ξ_i, η_i in $k(\lambda_i)$. Thus

$$(\xi_i^2 - c\eta_i^2) = \mathfrak{b}_i^{-1} \mathfrak{A}^{(i)} \sigma \mathfrak{A}^{(i)} (x + \lambda_i y)$$

as ideals. This implies $\xi_i^2 - c\eta_i^2 = \alpha_i(x + \lambda_i y)$ where the ideal (α_i) belongs to a finite computable list; and as we can clearly vary α_i by any squared factor, this ensures the same property for α_i. □

Strictly speaking, the elements of our list consist of equivalence classes of n-tuples (where the formulation of the equivalence relation is left to the reader); but we shall need to fix which representatives we choose. However, in what follows we shall also need to know that we can take the u_i, v_i to be integers without thereby imposing an uncontrolled extra factor in the $\alpha_i^{(r)}$. For this purpose we need the following result:

LEMMA 2.— *Let K be an algebraic number field and C a non-square in $\mathfrak{O}_K$. Then there exists $A = A(K, C)$ in $\mathfrak{O}_K$ such that if D is in $\mathfrak{O}_K$ with*

$$U^2 - CV^2 = D \tag{4}$$

soluble in K, and if $A^2 | D$, then (4) is soluble with U, V in $\mathfrak{O}_K$.

Proof. — Write $L = K(\sqrt{C})$, let σ be the non-trivial automorphism of L/K and let $\mathfrak{A}_1, \dots, \mathfrak{A}_H$ be a set of integral representatives for the ideal classes of L. Let d be any non-zero integer of K such that $u^2 - Cv^2 = d$ for some u, v in K, and write

$$(u + C^{1/2}v) = \mathfrak{m}/\mathfrak{n}$$

where $\mathfrak{m}, \mathfrak{n}$ are coprime ideals in L. Thus $(u - C^{1/2}v) = \sigma\mathfrak{m}/\sigma\mathfrak{n}$, so that $\sigma\mathfrak{n}|\mathfrak{m}$. Choose r so that $\mathfrak{A}_r\mathfrak{n}$ is principal — say equal to (B). If u_1, v_1 are defined by

$$u_1 + C^{1/2}v_1 = B(u + C^{1/2}v)/\sigma B$$

then the denominator of $u_1 + C^{1/2}v_1$ divides $\sigma\mathfrak{A}_r$ and $u_1^2 - Cv_1^2 = d$. If A in K is divisible by $2C^{1/2}\mathfrak{A}_r.\sigma\mathfrak{A}_r$ for every r, then $A^2d = (Au_1)^2 - C(Av_1)^2$ where Au_1 and Av_1 are integers. □

Since we can multiply each $\alpha_i^{(r)}$ by the square of any nonzero integer in $k(\lambda_i)$, subject to the preservation of conjugacy, we can assume that $\alpha_i^{(r)}$ is divisible by $(A(k(\lambda_i), c))^2$ in the notation of Lemma 2; thus if (3) is soluble at all for given integers x, y then it is soluble in integers. Moreover

$$\prod_{i=1}^n \alpha_i^{(r)} = \left(a \prod_{i=1}^n (u_i^2 - cv_i^2) \right) / (u^2 - cv^2),$$

so that $\prod \alpha_i^{(r)} = a(u_{(r)}^2 - cv_{(r)}^2)$ for some $u_{(r)}, v_{(r)}$ in k. Conversely, any solution of (3) gives rise to a solution of (2); and for this we do not require any condition on (x, y).

If the system (3) has solutions at all, it has solutions for which conjugacy between λ_i and λ_j extends to conjugacy between u_i, v_i and u_j, v_j; such solutions have the form

$$u_i = \lambda_i^{n-1}\xi_0 + \ldots + \xi_{n-1}, \quad v_i = \lambda_i^{n-1}\eta_0 + \ldots + \eta_{n-1} \tag{5}$$

for some ξ_ν, η_ν in k. Thus we can replace (3) by the system

$$(\lambda_i^{n-1}X_0 + \ldots + X_{n-1})^2 - c(\lambda_i^{n-1}Y_0 + \ldots + Y_{n-1})^2 = \alpha_i^{(r)}(X + \lambda_i Y) \tag{6}$$

which is to be solved in k. If we eliminate X, Y these become $n-2$ homogeneous quadratic equations in $2n$ variables, which give a variety $\mathcal{Y}^{(r)}$ defined over k. In the special case $n = 4$ it was shown in [2], §7 that the $\mathcal{Y}^{(r)}$ are factors of the universal torseurs for (1); and the same argument works for all even $n > 2$. However, we shall not need to know this.

In the following theorem all the statements about (2) can be trivially translated into statements about (1).

THEOREM 1.— *Suppose that $n = 6$ and that $f(X,Y)$ in (2) has the form*

$$f(X,Y) = f_4(X,Y)f_2(X,Y) \tag{7}$$

where f_4, f_2 are defined over k and have degrees $4, 2$ respectively. Assume also that $f(X,Y)$ has no repeated factor. If there is a $\mathcal{Y}^{(r)}$ which is soluble in every completion of k then that $\mathcal{Y}^{(r)}$ is soluble in k; and if this holds for some $\mathcal{Y}^{(r)}$ then (2) contains a Zariski dense set of points defined over k.

Proof. — We first rewrite the equations for $\mathcal{Y}^{(r)}$ in a form which makes better use of the decomposition (7). We can suppose that the linear factors of f_4 are the $X + \lambda_i Y$ with $i = 1,2,3,4$. The system (6) is equivalent to (3); but instead of (5) we now make the substitution

$$\begin{aligned} u_i &= \lambda_i^3\xi_0 + \ldots + \xi_3, \qquad & v_i &= \lambda_i^3\eta_0 + \ldots + \eta_3 \qquad & (i = 1,2,3,4),\\ u_i &= \lambda_i\xi_4 + \xi_5, & v_i &= \lambda_i\eta_4 + \eta_5 & (i = 5,6) \end{aligned}$$

in (3). Correspondingly we replace (6) by

$$U_i^2 - cV_i^2 = \alpha_i^{(r)}(X + \lambda_i Y) \qquad (i = 1,2,3,4), \tag{8}$$
$$(\lambda_i X_4 + X_5)^2 - c(\lambda_i Y_4 + Y_5)^2 = \alpha_i^{(r)}(X + \lambda_i Y) \qquad (i = 5,6), \tag{9}$$

where we have written

$$U_i = \lambda_i^3 X_0 + \ldots + X_3, \ V_i = \lambda_i^3 Y_0 + \ldots + Y_3 \quad (i = 1,2,3,4).$$

By eliminating X, Y between the four equations (8), we obtain two homogeneous quadratic equations in the eight variables U_i, V_i; we treat these as defining a projective variety $\mathcal{X}_1 \subset \mathbf{P}^7$. The U_i, V_i are not defined over k, but it is clear how $\mathrm{Gal}(\bar{k}/k)$ acts on them.

We can now outline the proof of the theorem. It falls naturally into three steps.

(i) $\mathcal{X}_1$ contains a large enough supply of lines defined over k.

(ii) We can choose a Zariski dense set of lines each of whose inverse images in $\mathcal{Y}^{(r)}$ is everywhere locally soluble.

(iii) $\mathcal{Y}^{(r)}$ contains a Zariski dense set of points defined over k.

The map $\mathcal{Y}^{(r)} \to \mathcal{Y}$ then gives the theorem.

By hypothesis, $\mathcal{X}_1$ has points in every completion of k; hence as in [2], Theorem A, there is a point P_0 in $\mathcal{X}_1(k)$, and we can take P_0 to be in general position on $\mathcal{X}_1$. Indeed, we have weak approximation on $\mathcal{X}_1$ because $\mathcal{X}_1$ contains two conjugate $\mathbf{P}^3$ given by

$$X_i \pm \gamma Y_i = 0 \quad (i = 1, 2, 3, 4)$$

for either choice of sign, and these have no common point. To a general k-point P of $\mathcal{X}_1$ we can in an infinity of ways find a k-plane which contains P_0 and P and which meets both these $\mathbf{P}^3$; for we need only choose a k-point P' on PP_0 and note that since P' does not lie on either $\mathbf{P}^3$ there is a unique transversal from P' to the two $\mathbf{P}^3$. Conversely, a general k-plane through P_0 which meets both these $\mathbf{P}^3$ will meet $\mathcal{X}_1$ in just one more point, which must therefore be defined over k. In this way we obtain a map $\mathbf{P}^6(k) \to \mathcal{X}_1(k)$ which is surjective, and this implies weak approximation.

Now let Λ_0, which is a $\mathbf{P}^5$, be the tangent space to $\mathcal{X}_1$ at P_0, and write $\mathcal{X}_2 = \mathcal{X}_1 \cap \Lambda_0$, so that $\mathcal{X}_2$ is a cone whose vertex is P_0 and whose base $\mathcal{X}_3$ is a Del Pezzo surface of degree 4. (The fact that there are 16 lines on a nonsingular Del Pezzo surface, and the incidence relations between them, can be read off from [4], Theorem 26.2.) We can give a rather explicit description of $\mathcal{X}_3$, and in particular we can identify the 16 lines on it, which turn out to be distinct. Drawing on Cayley's exhaustive classification of singular cubic surfaces, a sufficiently erudite reader can derive a painless proof that $\mathcal{X}_3$ is actually nonsingular. (What we actually use is the much weaker statement that $\mathcal{X}_3$ is absolutely irreducible and not a cone, which is not hard to verify.) For $\mathcal{X}_2$ contains the line which is the intersection of

$$U_i - \epsilon_i \gamma V_i = 0 \quad (i = 1, 2, 3, 4) \tag{10}$$

with Λ_0, where each ϵ_i is ± 1. (This intersection is proper because P_0 is in general position.) We denote this line by $L^*(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$ and its projection onto $\mathcal{X}_3$ by $L(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$. The latter clearly meets the four lines which are obtained by changing just one sign, because this already happens for the corresponding lines in $\mathcal{X}_2$; so by symmetry the fifth line which it meets must be obtained by changing all four signs. This can be checked directly; for if we temporarily drop the notation of (3) and write

$$P_0 = (u_1, v_1, u_2, v_2, u_3, v_3, u_4, v_4) \text{ in } \mathcal{X}_0 \subset \mathbf{P}^7,$$

then the join of the two points $(\epsilon_1 cv_1 \pm \gamma u_1, \epsilon_1 u_1 \pm \gamma v_1, \ldots)$ passes through P_0, and each point lies on the corresponding $L^*(\pm\epsilon_1, \pm\epsilon_2, \pm\epsilon_3, \pm\epsilon_4)$. Since

$$u_i(\epsilon_i cv_i \pm \gamma u_i) - cv_i(\epsilon_i u_i \pm \gamma v_i) = \pm\gamma(u_i^2 - cv_i^2)$$

and the equations for $\mathcal{X}_1$ are given by the vanishing of linear combinations of the $U_i^2 - cV_i^2$, these two points also lie on Λ_0. The point

$$P_1 = (\epsilon_1 cv_1, \epsilon_1 u_1, \epsilon_2 cv_2, \epsilon_2 u_2, \epsilon_3 cv_3, \epsilon_3 u_3, \epsilon_4 cv_4, \epsilon_4 u_4),$$

lies on the join of these two points; P_1 is distinct from P_0 unless P_0 lies on the $\mathbf{P}^3$ given by (10) or the $\mathbf{P}^3$ derived from it by changing the sign of γ. Because P_0 is in general position, we can assume that neither of these happens. Now a straightforward calculation, using the fact that we can describe $\mathcal{X}_1$ by equations which express $U_1^2 - cV_1^2$ and $U_2^2 - cV_2^2$ as linear combinations of $U_3^2 - cV_3^2$ and $U_4^2 - cV_4^2$, shows that P_1 is nonsingular on $\mathcal{X}_2$ unless P_0 lies on one of 12 lines, a typical one of which is given by

$$U_1 = V_1 = U_2 = V_2 = 0,\ U_3 = \epsilon_3\gamma V_3,\ U_4 = -\epsilon_4\gamma V_4.$$

Under the same condition, the point induced on $\mathcal{X}_3$ is nonsingular.

The lines $L(++++)$ and $L(----)$ are defined over $k(\gamma)$ and conjugate over k; thus their intersection is defined over k and $\mathcal{X}_3$ does contain a point defined over k. Moreover the $u_i^2 - cv_i^2$ cannot all vanish because γ is not in any $k(\lambda_i)$; so P_1 is nonsingular on $\mathcal{X}_2$ and k-points are Zariski dense on $\mathcal{X}_3$. (See [4], Theorems 30.1 and 29.4.) Henceforth $P_2 \neq P_0$ will always denote a point on $\mathcal{X}_2$ defined over k and P_3 will denote the corresponding point on $\mathcal{X}_3$.

Once we have chosen P_2, the general point of the line P_0P_2 is given by setting the X_i, Y_i for $i = 0, 1, 2, 3$ equal to linear forms in Z_1, Z_2; and we can suppose that P_0 corresponds to (1,0) and P_2 to (0,1). The equations for $\mathcal{X}_1$ are then satisfied identically, and (8) expresses X, Y as quadratic forms in Z_1, Z_2. There remain the equations (9), which now take the form

$$(\lambda_i X_4 + X_5)^2 - c(\lambda_i Y_4 + Y_5)^2 = \phi_i(Z_1, Z_2) \quad (i = 5, 6) \qquad (11)$$

for certain quadratic forms ϕ_5, ϕ_6. In view of the remarks in the previous paragraph we can certainly assume that ϕ_5, ϕ_6 are linearly independent and each has rank 2. We need to check that we can choose the line P_0P_2 so that the system (11) is everywhere locally soluble. This is of course the crucial step in the proof of the Theorem; but in order not to disrupt the flow of the argument, we postpone the proof of it and of an auxiliary result to Lemma 3 below. Given this, we would like to conclude the argument by appealing to Theorem A of [2]; but unfortunately we are in the exceptional case (E_5) of that theorem. Some discussion of this exceptional case can already be found in the literature (for example in [2]); but it is not clear that any published result meets our needs. We therefore proceed as follows.

Suppose first that λ_5, λ_6 are in k and write

$$U_i = \lambda_i X_4 + X_5, \ V_i = \lambda_i Y_4 + Y_5 \quad (i = 5, 6).$$

The equation (11) for $i = 5$ is $U_5^2 - cV_5^2 = \phi_5(Z_1, Z_2)$, which is everywhere locally soluble, and therefore soluble by the Hasse-Minkowski theorem. Its general solution is given by homogeneous quadratic forms in three variables W_1, W_2, W_3. The equation (11) with $i = 6$ now reduces to

$$U_6^2 - cV_6^2 = g(W_1, W_2, W_3) \tag{12}$$

where g is quartic. This is everywhere locally soluble; so all we have to do is to set W_3 equal to $e_1W_1 + e_2W_2$ where e_1, e_2 are integers in k such that

$$U_6^2 - cV_6^2 = g(W_1, W_2, e_1W_1 + e_2W_2) \tag{13}$$

is everywhere locally soluble and has no Brauer-Manin obstruction. This is not difficult. Let $\mathcal{S}$ consist of the places in k which are either infinite or divide $6c$ or either of the polynomials $g(W_1, 0, W_3)$ or $g(0, W_2, W_3)$; by means of a linear transformation on the W_i if necessary, we can assume that neither of these expressions vanishes identically and hence $\mathcal{S}$ is finite. Solubility of (13) at the places in $\mathcal{S}$ can be ensured by local conditions on e_1, e_2. Choose e_1 to satisfy all these local conditions and also $g(1, 0, e_1) \neq 0$. For the local solubility of (13) all we now have to consider are the primes in $\mathcal{S}$ and the primes $\mathfrak{p}$ which divide $g(1, 0, e_1)$. For the former, we need only impose local conditions on e_2; for the latter it is enough to ensure that $\mathfrak{p} \nmid g(0, 1, e_2)$, which we can do because Norm $\mathfrak{p} > 3$. Finally, $g(W_1, W_2, W_3)$ is the product of two absolutely irreducible quadratic forms defined over $\bar{k}$ which correspond to the linear factors of ϕ_6; so it is irreducible over k by Lemma 3. By Hilbert irreducibility we can ensure that $g(W_1, W_2, e_1W_1 + e_2W_2)$ is irreducible over k; so the Châtelet equation (13) is soluble, by Theorem B of [2].

If instead λ_5, λ_6 are not in k, it follows from Lemma 3 and the linear independence of ϕ_5 and ϕ_6 that $\phi_5\phi_6$ is irreducible over k. Hence (11) is soluble in k by Theorem 12.1 of [2]. The reader can easily check that the solutions thus constructed are in general position, and therefore Zariski dense on (2).

All that remains to do is to prove the following:

LEMMA 3.— *If $\mathcal{Y}^{(r)}$ is everywhere locally soluble there are lines P_0P_2 such that* (11) *is everywhere locally soluble and $\phi_i(Z_1, Z_2)$ is irreducible over $k(\lambda_i)$ for $i = 5, 6$.*

Proof.— We note first that in general ϕ_i is irreducible over $k(\lambda_i)$. For if we take P_2 to be P_1 and P_0, P_1 to have Z-coordinates $(1, 0)$, $(0, 1)$ respectively, each $U_i^2 - cV_i^2$ with $i = 1, 2, 3, 4$ is a multiple of $Z_1^2 - cZ_2^2$; hence the same is true of X and Y, and therefore of ϕ_5 and ϕ_6. The general assertion now follows from Hilbert's Irreducibility Theorem.

The main complication in the proof of this Lemma is that we cannot assume weak approximation on $\mathcal{X}_3$; indeed weak approximation is probably not even true, since the Brauer group of $\mathcal{X}_3$ is non-trivial. (See [5].) Let $\mathcal{S}_1$ be a finite set of places in k containing the infinite places, all small primes and all primes dividing $2c$, any $\mathfrak{a}_m$, the discriminant of f or any of the $\alpha_i^{(r)}$. Then we can choose P_0 to be in the image of $\mathcal{Y}^{(r)}(k_v)$ under the map $\mathcal{Y}^{(r)} \to \mathcal{X}_1$ for each v in $\mathcal{S}_1$, by weak approximation on $\mathcal{X}_1$. Denote by u_i, v_i, x, y the values of U_i, V_i, X, Y at P_0; these values depend on the particular coordinate representation of P_0 which we choose, so that we can still multiply the u_i, v_i by an arbitrary $\mu \neq 0$ in k and multiply x, y by μ^2. We can therefore ensure that x, y are integers and that the ideal (x, y) is not divisible by the square of any prime ideal outside $\mathcal{S}_1$. We then re-choose the u_i, v_i for $i = 1, 2, 3, 4$ to satisfy (8) and be integral, which we can do by the remark immediately after the proof of Lemma 2. This of course alters P_0, but since it leaves x, y unchanged the equations (9) remain locally soluble at every place in $\mathcal{S}_1$. Because the old P_0 was in general position on $\mathcal{X}_1$, we can assume that the right hand sides of the two equations (9) do not vanish at P_0.

We do not know the quadratic forms ϕ_5 and ϕ_6 until we have chosen P_2. But the values of $\phi_5(1, 0)$ and $\phi_6(1, 0)$ as elements of k^*/k^{*2} only depend on P_0, for they are simply the values of the right hand sides of the two equations (9) at P_0. We can therefore properly involve these values in the argument in advance of the choice of P_2. We now have local solubility of (11) for $i = 5, 6$ for $Z_2 = 0$ except perhaps at primes which are not in $\mathcal{S}_1$ but which divide $\phi_5(1, 0)\phi_6(1, 0)$; let $\mathcal{S}_2$ be the finite set of such primes. We can delete from $\mathcal{S}_2$ any primes for which c is a quadratic residue, for (11) is certainly soluble at such primes. To prove the Lemma, we need only show that we can choose P_2 so that no prime $\mathfrak{p}$ in $\mathcal{S}_2$ divides $\phi_5(0,1)\phi_6(0,1)$.

Now let $\mathfrak{p}$ be in $\mathcal{S}_2$ and $\mathfrak{P}$ be any prime ideal in $k(\lambda_1,\ldots,\lambda_4,\gamma)$ which divides $\mathfrak{p}$, and use a tilde to denote reduction mod $\mathfrak{P}$; we have $\mathfrak{P}\|\mathfrak{p}$ because all the primes which ramify lie in $\mathcal{S}_1$. The two $\mathbf{P}^3$ given by $U_i \pm \tilde{\gamma}V_i = 0$ $(i = 1,2,3,4)$ are also given by $X_i \pm \tilde{\gamma}Y_i = 0$ $(i = 1,2,3,4)$; so if $\tilde{P}_0$ lies on either of them then $\tilde{\gamma}$ would be equal to the reduction mod $\mathfrak{P}$ of the value of $\mp X_i/Y_i$ at P_0. Since the latter is an element of k, this would mean that c would be a quadratic residue mod $\mathfrak{p}$ — a case which we have already ruled out. Again, if for example $\tilde{u}_1 = \tilde{v}_1 = \tilde{u}_2 = \tilde{v}_2 = 0$ then x, y would be divisible by $\mathfrak{P}^2$ and hence by $\mathfrak{p}^2$; and this too we have ruled out. The calculations following (10) now show that $\tilde{P}_1$ is nonsingular on $\tilde{\mathcal{X}}_2$, where P_1 is as in those calculations.

At most one pair of $\tilde{u}_i, \tilde{v}_i$ vanish; if there is such a pair, we can suppose it is given by $i = 4$. The equations for $\tilde{\mathcal{X}}_2$ are

$$U_1^2 - \tilde{c}V_1^2 = \text{homogeneous quadratic form in } U_3, V_3, U_4, V_4, \tag{14}$$

$$U_1\tilde{u}_1 - \tilde{c}V_1\tilde{v}_1 = \text{linear form in } U_3, V_3, U_4, V_4,$$

and two similar ones involving U_2 and V_2. The equation (14) is equivalent to the vanishing of a quadratic form of rank 6, so it cannot have a hyperplane section which is not absolutely irreducible; and it now follows easily that $\tilde{\mathcal{X}}_2$ is absolutely irreducible. The projection from $\tilde{\mathcal{X}}_2$ to the $\mathbf{P}^3$ with coordinates U_3, V_3, U_4, V_4 is generically onto. Hence there are at most $O(q^2)$ points in $\tilde{\mathcal{X}}_2(\mathbf{F}_q)$ for which the right hand side of (9) vanishes for $i = 5$ or $i = 6$. The implied constant here, like λ below, is absolute because it depends only on the degrees of the various maps and varieties involved. Now let P be the point on $\mathcal{X}_3$ corresponding to P_1 on $\mathcal{X}_2$; thus P is the intersection of two lines on $\mathcal{X}_3$. We have already shown that $\tilde{P}$ is nonsingular for all the $\mathfrak{p}$ which still concern us. The construction in the proof of [4], Theorem 30.1 specifies a non-constant map $\psi : \mathbf{P}^1 \to \mathcal{X}_3$; and the reduction mod $\mathfrak{p}$ of the image of ψ is obtained by carrying out the corresponding construction using $\tilde{\psi}$ and $\tilde{\mathcal{X}}_3$, so this image has good reduction. Hence there is a point Q in the image of ψ, defined over k and such that $\tilde{Q}$ is nonsingular on $\tilde{\mathcal{X}}_3$ and does not lie on any of the lines of $\tilde{\mathcal{X}}_3$. Repeating this process using this time the construction in the proof of [4], Theorem 29.4, we obtain a map $\mathbf{P}^2 \to \mathcal{X}_3$ which has good reduction mod $\mathfrak{p}$ for all relevent $\mathfrak{p}$. This lifts back to a map $\mathbf{P}^3 \to \mathcal{X}_2$ which is generically onto and has good reduction mod $\mathfrak{p}$ for all relevent $\mathfrak{p}$. Hence there exists an absolute constant $\lambda > 0$ such that $\tilde{\mathcal{X}}_2$ has at least λq^3 points which can be lifted back to points of $\tilde{\mathcal{X}}_0(\mathbf{F}_q)$. Provided that q is large enough, which we ensure by putting all small primes into $\mathcal{S}_1$,