Weak Approximation and R-equivalence on Cubic Surfaces

Sir Peter Swinnerton-Dyer

Abstract

Let V be a nonsingular cubic surface defined over an algebraic number field K, and assume that V has points in every completion K_v. There is a long-standing problem of finding the obstructions to the Hasse principle and to weak approximation on V, the conjecture in each case (due to Colliot-Thélène and Sansuc) being that the obstruction is just the Brauer-Manin obstruction. The latter is known to be computable, though the algorithm is somewhat ugly and a heuristic process is usually preferable. Another way of phrasing the same problem is to ask what is the adelic closure of the set $V(K)$.

A partial answer to this question is given by the following theorem: to each place v of bad reduction one can associate a finite disjoint union

$$V(K_v) = \cup W_j^{(v)}$$

which is easily computable in any particular case. The v-adic closure of any R-equivalence class in $V(K)$ is a set U_{iv} which is the union of some of the $W_j^{(v)}$; and the adelic closure of any R-equivalence class is of the form $\prod' U_{iv} \times \prod'' V(K_v)$, where i depends on v, the first product is over all places of bad reduction and the second product is over all places of good reduction for V. Thus the adelic closure of $V(K)$ is a union of sets $\prod' W_j^{(v)} \times \prod'' V(K_v)$. For specific V a search program will give those products which contain a point of $V(K)$ and in which points of $V(K)$ are therefore everywhere dense. For a product which appears not to contain a point of $V(K)$, it is reasonable to hope that there is a Brauer-Manin obstruction. For all V for which this process has been used, it turns out that one can indeed find the exact adelic closure of $V(K)$ in this way. This is illustrated in the final section.

1. *Introduction.* The origin of this paper is a remark of Heath-Brown [2], that for an explicitly given cubic surface defined over $\mathbf{Q}$ it should be possible to show that the Brauer-Manin obstruction is the only obstruction to weak approximation — provided that statement is in fact true. He suggested that this could be done by studying particular parametric solutions — or, which comes to almost the same thing, particular R-equivalence classes; and

we shall see that this is true (and indeed true over an arbitrary algebraic number field), though in general more than one class is needed.

Let V be a nonsingular cubic surface defined over an algebraic number field K; then R-equivalence on V is defined as the finest equivalence relation such that two points given by the same parametric solution are equivalent. Let ℓ be any line not lying in V and meeting V in three points P_1, P_2, P_3, each defined over K but not necessarily distinct. Following Manin, if $\mathcal{C}_i$ is the R-equivalence class of P_i we shall write $\mathcal{C}_3 = \mathcal{C}_1 \circ \mathcal{C}_2$. Let P be a point of an equivalence class $\mathcal{C}$ which does not lie on any of the lines of V, and let Γ be the intersection of V with the tangent plane to V at P. Thus Γ is an irreducible cubic with a singularity at P. Every point P_1 of $\Gamma(K)$ other than P is in $\mathcal{C} \circ \mathcal{C}$, and by taking ℓ to be the tangent to Γ at P_1 we obtain

$$(\mathcal{C} \circ \mathcal{C}) \circ (\mathcal{C} \circ \mathcal{C}) = \mathcal{C} \circ \mathcal{C}. \tag{1}$$

Still following Manin, we define *universal equivalence* to be the finest equivalence relation in $V(K)$ such that $P_1 \sim P_2$ whenever $P \circ P_1 \sim P \circ P_2$ for some P. This is not trivial, because $Q_1 \circ Q_2$ is many-valued if $Q_1 = Q_2$ or if Q_1 and Q_2 lie on the same line of V.

The main object of this paper is to describe the closure of any R-equivalence class $\mathcal{C}$ in the adelic topology on V.

Theorem 1 *Let V be a nonsingular cubic surface defined over an algebraic number field K. There is a finite set $\mathcal{B}$ of places of K and for each v in $\mathcal{B}$ a partition*

$$V(K_v) = U_{1v} \cup \ldots \cup U_{nv}, \tag{2}$$

where the U_{iv} are disjoint open sets in the v-adic topology and n depends on v, with the following property. If $\mathcal{C}$ is any R-equivalence class in $V(K)$ then the closure of $\mathcal{C}$ in the adelic topology has the form $\prod U_{iv} \times \prod V(K_v)$, where the first product is over the places in $\mathcal{B}$, the second product is over the places not in $\mathcal{B}$, and each i depends on v and $\mathcal{C}$.

In more low-brow language, Theorem 1 asserts that for the problem of weak approximation within $\mathcal{C}$ only the places in $\mathcal{B}$ matter and there is no interaction between distinct places. It follows that the first of these statements holds also for weak approximation over K, though it is well known that the second does not. It is implicit in this (and the corresponding local result is

a necessary step in the proof) that if $\mathcal{C}_1$ and $\mathcal{C}_2$ are any two R-equivalence classes their adelic closures are either disjoint or identical. In the former case $\mathcal{C}_1$ and $\mathcal{C}_2$ are easily separated by congruence conditions. Colliot-Thélène has pointed out to me that there are known to be Châtelet surfaces on which there are distinct R-equivalence classes with the same adelic closure, and from these one can derive cubic surfaces with the same property. Indeed except in very special cases it is not even known whether the number of R-equivalence classes is finite.

The set $\mathcal{B}$ in Theorem 1 is actually the set of places v of bad reduction of V in the following sense. Let $\mathfrak{p}$ be a finite prime in K. After multiplying the equation of V by a suitable constant (depending on $\mathfrak{p}$) we can assume that all its coefficients are integers at $\mathfrak{p}$ and at least one of them is a unit at $\mathfrak{p}$. We define $\tilde{V} = \tilde{V}_{\mathfrak{p}}$ to be the surface defined over the residue field $\mod \mathfrak{p}$ whose equation is the reduction $\mod \mathfrak{p}$ of the equation of V. We now say that v is a *place of bad reduction* for V if either

(i) v is finite and $\tilde{V}$ has a singularity or a multiple component, or

(ii) v is a real infinite place and $V(K_v)$ has more than one component.

The set of places of bad reduction for V may be changed if one makes a linear transformation in the ambient space; but clearly this would not affect the smallest set $\mathcal{B}$ for which Theorem 1 holds. There is scope for a more sophisticated approach, which would involve developing a theory of Néron models for cubic surfaces.

In this paper I only give the proof of Theorem 1 when $\mathcal{B}$ is the larger set which also contains the primes of Norm 2,3 or 4; as so often, much of the difficulty in the proof comes from the small primes. This raises the further question: if $\tilde{V}$ is not a cone and does not contain a line of singular points, and if P_1, P_2 are points of $V(K_{\mathfrak{p}})$ whose reductions $\mod \mathfrak{p}$ are nonsingular on $\tilde{V}$, does it follow that they lie in the same component of the partition (2)? This is certainly true except perhaps when $\mathfrak{p}$ is small.

Each element of the partition (2) is either the closure in $V(K_v)$ of some R-equivalence class or the set of points of $V(K_v)$ not in the closure of $V(K)$. I do not know an algorithm for constructing the partition (2); but there is a wholly explicit procedure for constructing a finite refinement of it, and this is good enough for applications. It is probable that the algorithm used does not generally give the actual partition (2); when it does not do so, how to generate the correct coarsening is an interesting and probably difficult

open question. The main complication comes from the possible existence of sporadic parametric solutions. For example, over the algebraic closure $\bar{K}$ there are in general ∞^5 quadrics which touch V at 4 points, and whose intersection with V is therefore a parametrisable curve; but nothing is known about which if any of them are defined over K.

In what follows, if L, Q or C is a polynomial in the coordinates $X_0, \ldots, X_3$ then L will always be linear, Q quadratic and C cubic, and their coefficients will be integral at any relevent prime; but each of these letters is also used for other purposes. All constants implicit in the O notation will be absolute. Except in the purely geometric §2, we shall also adopt the following conventions. If $\mathfrak{p}$ is a finite prime of K, we denote by $\mathfrak{O}_\mathfrak{p}$ the ring of elements of K integral at $\mathfrak{p}$, by k the residue field $\bmod \mathfrak{p}$ and by q the number of elements of k; and a tilde will denote the reduction $\bmod \mathfrak{p}$ of anything defined over K. When we write an equation for V, it will always be assumed that all the coefficients are in $\mathfrak{O}_\mathfrak{p}$. At least one of them will be a unit at $\mathfrak{p}$; so we obtain the equation of $\tilde{V}$ simply by reducing all the coefficients $\bmod \mathfrak{p}$. If we define something over k otherwise than by reduction $\bmod \mathfrak{p}$, we shall denote it by a lower case letter; and the corresponding capital letter will denote some lift of it to K. We use the same conventions occasionally for objects defined over extensions of K and k; but this will always be made clear.

The structure of this paper is as follows. In §2 we prove a miscellany of geometric results which are needed later in the paper; some of them are certainly known but not well known. The next four sections cover the local theory. In §3 we consider the archimedean places, for which the partition (2) is simply into the connected components of $V(K_v)$. For finite primes a crucial weapon in the argument is the process of moving a curve sideways on V; §4 describes this process and provides quantitative estimates of how nearly parallel the new curve is to the old one. The process enables one to show that if $\mathcal{C}$ is an R-equivalence class in $V(K)$ then its closure in the $\mathfrak{p}$-adic topology is open. This, and the fact proved in Lemma 11 that the closures of two R-equivalence classes are either coincident or disjoint, are needed to prove the existence and key properties of the partition (2). In §5 we prove that if $\tilde{V}$ is nonsingular and $V(K)$ is not empty then every point of $\tilde{V}(k)$ is liftable to $V(K)$. At the end of §5 we prove that under the same conditions every point of $\tilde{V}(k)$ is liftable to each class of $V(K)$.

We shall say that a point p of $\tilde{V}(k)$ is *densely liftable* to an R-equivalence class $\mathcal{C}$ if $\mathcal{C}$ is dense in the inverse image of p under the map $V(K_\mathfrak{p}) \to \tilde{V}(k)$; note that to say simply that p is densely liftable means that it is densely

liftable to some class $\mathcal{C}$ and not simply to $V(K)$. In §6, which depends on the techniques of §4, we prove that if $\tilde{V}$ is nonsingular and $V(K)$ is not empty then every point of $\tilde{V}(k)$ is densely liftable. It now follows from the final result of §5 that every point of $\tilde{V}(k)$ is actually densely liftable to each class of $V(K)$; at the end of §6 we give an alternative proof, which contains ideas which may be valuable even when $\tilde{V}$ is singular. Thus the partition (2) is trivial when $\tilde{V}$ is nonsingular. The proof of Theorem 1 is now reduced to the global analogue of Lemma 11; this occupies §7. In the final section of the paper we specialize to the surfaces

$$f = X_1^3 + X_2^3 + X_3^3 - dX_0^3 = 0 \tag{3}$$

which occur for $d = 2, 3$ in Heath-Brown's paper; in particular we show that for Heath-Brown's surfaces the Brauer-Manin obstruction is indeed the only obstruction to weak approximation.

I am indebted to Jean-Louis Colliot-Thélène for a number of valuable comments.

2. *Geometric background.* This section contains various geometric statements which will be needed elsewhere in the paper. Throughout it, W will be an absolutely irreducible cubic surface, not necessarily nonsingular, defined over a field L. We use the language of classical geometry, so that the objects introduced may not all be defined over L.

Lemma 1 *Let Λ be a line on W and Π any plane through Λ. If Π is the tangent to W at more than two points of Λ then Λ contains a singular point of W.*

Proof. Take coordinates so that Λ is $X_2 = X_3 = 0$ and Π is $X_3 = 0$. The equation of W will have the form

$$X_0^2 L_0(X_2, X_3) + X_0 X_1 L_2(X_2, X_3) + X_1^2 L_1(X_2, X_3) + \ldots = 0 \tag{4}$$

where the remaining terms are at most linear in X_0, X_1 together. If Π is the tangent to W at $(x_0, x_1, 0, 0)$ then

$$x_0^2 L_0(1, 0) + x_0 x_1 L_2(1, 0) + x_2^2 L_1(1, 0) = 0.$$

Thus Π can only be the tangent to W at more than two points of Λ if the equation (4) reduces to $X_3 Q(X_0, X_1) + \ldots = 0$; and in this case W has a singular point where $Q(X_0, X_1) = X_2 = X_3 = 0$. □

Let P be a point of W; what can we say about the set of points P_1 on W such that the line PP_1 touches W at P_1? Take coordinates so that the equation of W is $f(X_0, \dots, X_3) = 0$ and P is $(1, 0, 0, 0)$. The points P_1 are those which satisfy $\partial f/\partial X_0 = 0$. If this does not hold identically, it defines a (possibly decomposable) quadric; and the intersection of this with W breaks up into at most six curves, each of which has absolutely bounded genus. In particular, if L is the finite field of q elements then there are only $O(q)$ such points P_1 in $W(L)$.

If $\partial f/\partial X_0$ vanishes identically then the choice of P implies that f cannot contain a term of the form aX_0^3, so we have just two possibilities:

(i) f is independent of X_0, so that W is a cone with vertex P;

(ii) $\operatorname{char} L = 2$ and after a linear transformation on X_1, X_2, X_3 we can take

$$f = X_0^2 X_3 + C(X_1, X_2, X_3).$$

In both these cases P_1 can be any point of W. If (i) holds then P is a singular point of W. If (ii) holds then the singular points of W are given by

$$\partial C/\partial X_1 = \partial C/\partial X_2 = \partial C/\partial X_3 + X_0^2 = 0,$$

so that W has singular points though P is not one of them. In particular we have proved

Lemma 2 *Suppose that W is nonsingular and let P be a point on W. Then the points P_1 on W such that the tangent to W at P_1 passes through P all lie on a certain (possibly decomposable) quadric. If L is the finite field of q elements then there are only $O(q)$ such points in $W(L)$.* □

Lemma 3 *If W is nonsingular, P is on W and ℓ is a line through P on W then ℓ cannot be a multiple component of the intersection of W with the tangent to W at P.*

Proof. If not, take coordinates so that P is $(1, 0, 0, 0)$, ℓ is $X_2 = X_3 = 0$, the tangent to W at P is $X_3 = 0$ and its intersection with W contains the line ℓ with multiplicity at least 2. The equation of W has the form

$$X_3 Q(X_0, \dots, X_3) + X_2^2 L(X_0, X_1, X_2) = 0;$$

and any point $(x_0, x_1, 0, 0)$ with $Q(x_0, x_1, 0, 0) = 0$ is singular on W. □

Recall that an Eckardt point of W is a nonsingular point P of W such that the tangent plane to W at P meets W in three lines through P. If W has a singular point on the tangent plane, these lines need not be distinct.

Lemma 4 *Suppose that W is nonsingular and Λ is a line on W. Then Λ contains at most 5 Eckardt points if $\mathrm{char}(L) = 2$ and at most 2 otherwise.*

Proof. Take coordinates so that Λ is $X_2 = X_3 = 0$ and contains the two Eckardt points $P_0 = (1, 0, 0, 0)$ and $P_1 = (0, 1, 0, 0)$. We need to distinguish two cases, according as the tangents to W at P_0 and P_1 are the same or different. If they are the same, we can take them both to be $X_3 = 0$; it follows that the equation of W must have the form

$$X_3 Q(X_0, \ldots, X_3) + X_2^3 = 0 \tag{5}$$

where the coefficients of X_0^2 and X_1^2 in Q are nonzero. But now the intersection of W with the tangent at P_0 (or P_1) is the line Λ counted three times and this contradicts Lemma 3. If instead the tangents at P_0 and P_1 are distinct then we can take them to be $X_3 = 0$ and $X_2 = 0$ respectively. Now the equation of W must have both the forms

$$X_3 Q_0'(X_0, \ldots, X_3) + C_0(X_1, X_2) = X_2 Q_1'(X_0, \ldots, X_3) + C_1(X_0, X_3) = 0$$

where the coefficients of X_0^2 in Q_0' and X_1^2 in Q_1' are nonzero. Hence the equation of W has the form

$$f = X_3 Q_0(X_0, X_3) + X_2 Q_1(X_1, X_2) + X_2 X_3 L(X_0, \ldots, X_3) = 0 \tag{6}$$

where c_0 and c_1, the coefficients of X_0^2 in Q_0 and of X_1^2 in Q_1, are nonzero. Conversely, P_0 and P_1 are Eckardt points on (6). The tangent to (6) at a point $(a_0, a_1, 0, 0)$ is $c_0 a_0^2 X_3 + c_1 a_1^2 X_2 = 0$; so the line $X_2 = X_3 = 0$ contains no singular points. If $(a_0, a_1, 0, 0)$ is another Eckardt point on Λ, so that a_0, a_1 are nonzero, then we could also write f in the form

$$Y Q_0^*(X_0, Y) + X_2 Q_1^*(a_0 X_1 - a_1 X_0, X_2) + Y X_2 L^*(X_0, \ldots, X_3) \tag{7}$$

where $Y = c_0 a_0^2 X_3 + c_1 a_1^2 X_2$. This forces $\mathrm{char}(L) = 2$, because otherwise (7) would contain a term in $X_0 X_1 X_2$ whereas (6) does not. But if $\mathrm{char}(L) = 2$ then (7) is equivalent to

$$L^* = L^\sharp(a_0 X_1 - a_1 X_0, X_2, X_3), \quad c_0^2 a_0^3 d_1 + c_1^2 a_1^3 d_0 = 0$$

where d_0, d_1 are the middle coefficients of Q_0, Q_1. In general the first condition allows only one value of a_0/a_1, but if $L^* = L^\sharp(X_2, X_3)$ the first condition is identically satisfied. If also d_0, d_1 are both nonzero there are five distinct Eckardt points on $X_2 = X_3 = 0$. If d_0, d_1 both vanish then W has the form

$$c_0 X_0^2 X_3 + c_1 X_1^2 X_2 + C(X_2, X_3) = 0$$

and every point of $X_2 = X_3 = 0$ is an Eckardt point; but now

$$c_0 X_0^2 + \partial C/\partial X_3 = c_1 X_1^2 + \partial C/\partial X_2 = 0$$

determines a line of singular points of W. □

Lemma 5 *Suppose that W is not a cone and does not contain a line of singular points. Then W contains at most 27 lines and at most 4 singular points; it contains at most 45 Eckardt points unless it has the special form (5), and at most 18 Eckardt points if* $\mathrm{char}(L) \neq 2$.

Proof. Let $X_0 = X_1 = 0$ be a line on W; the general plane Π through it has the form $\mu X_0 = \lambda X_1$, so we can write $X_0 = \lambda X_4$, $X_1 = \mu X_4$ and use X_2, X_3, X_4 as coordinates in Π. The residual intersection of Π with W is obtained by substituting for X_0, X_1 in the equation of W and dividing by X_4, so its equation has the form

$$a_{22} X_2^2 + a_{23} X_2 X_3 + a_{33} X_3^2 + a_{24} X_2 X_4 + a_{34} X_3 X_4 + a_{44} X_4^2 = 0 \qquad (8)$$

where a_{22}, a_{23}, a_{33} are linear in λ and μ, a_{24} and a_{34} are quadratic and a_{44} is cubic. This equation defines a union of lines if and only if its discriminant vanishes, and the latter is of degree 5 in λ, μ. Thus either there are at most 5 planes through $X_0 = X_1 = 0$ whose intersection with W is a union of lines or every such plane has this property — the latter being the case when the discriminant vanishes identically.

Suppose first that the discriminant does vanish identically. We distinguish five cases, according as for general λ, μ the equation (8) represents

(i) two distinct lines whose common point is not on $X_4 = 0$,

(ii) two distinct lines meeting on $X_4 = 0$, neither being $X_4 = 0$,

(iii) a double line other than $X_4 = 0$,

(iv) the line $X_4 = 0$ and another line,

(v) the line $X_4 = 0$ taken twice.

In case (i) let P be the point of intersection of the two lines; then in the original coordinates P has the form $(\lambda f_1, \mu f_1, f_2, f_3)$ where the f_i are in $L[\lambda, \mu]$ and f_1 does not vanish identically. Let C be the locus of P as λ/μ varies; Π is transversal to C when P is not on $X_4 = 0$, so C is nonsingular at P and the tangent line to C at P does not lie in Π. Thus P is a singular point of W and C is a curve of singular points of W; since the join of any two singular points of W lies in W and W is irreducible, C must be a line, contrary to hypothesis. In case (ii) the discriminant of $a_{22}X_2^2 + a_{23}X_2X_3 + a_{33}X_3^2$ must vanish; but this form cannot vanish identically since we are not in case (iv) or (v). There are now two alternatives: either the form is the product of a linear form in $L[\lambda, \mu]$ and the square of a linear form in $L[X_2, X_3]$ or $\mathrm{char}(L) = 2$, $a_{23} = 0$ and a_{22}/a_{33} is not constant. If the first alternative holds, then by a linear transformation on X_2, X_3 with constant coefficients we can make $a_{23} = a_{33} = 0$, whence the fact that (8) is a pair of lines implies $a_{34} = 0$; now the equation of W does not involve X_3, so that W is a cone. If the second alternative holds, then (8) can only factorize if $(a_{24}X_2 + a_{34}X_3)^2$ is proportional to $a_{22}X_2^2 + a_{33}X_3^2$; this requires $a_{24} = a_{34} = 0$ and we would be in case (iii). In case (iii) we have the same alternatives as in case (ii), and the reason for rejecting the first alternative remains valid; hence as above we can assume that $\mathrm{char}(L) = 2$ and that the equation of W has the form

$$X_0X_2^2 + aX_1X_3^2 = f(X_0, X_1)$$

for some $a \neq 0$. But now every point of the ambient space with

$$X_2^2 = \partial f/\partial X_0, \quad aX_3^2 = \partial f/\partial X_1$$

is a singular point of W; so we have a curve of singular points, and as before this is impossible. In cases (iv) and (v) $a_{22} = a_{23} = a_{33} = 0$, so every point of the line $X_0 = X_1 = 0$ is singular on W.

Henceforth we can assume that given any line ℓ on W there are at most 5 planes through ℓ whose intersection with W is a union of lines; and there is at least one such plane. Among the planes which meet W in a union of lines, let Π_0 be one which involves the smallest number $n \leq 3$ of distinct lines. Any line ℓ which lies in W but not in Π_0 meets Π_0 in a point which lies on some line ℓ_0 in $\Pi_0 \cap W$; and we have already seen that there are at most 8 lines on W which meet ℓ_0 but do not lie in Π_0. Hence there are altogether

at most $8n + n \leq 27$ lines on W. Except in the special case (5), an Eckardt point on W lies on at least n distinct lines of W, and there are at most 5 Eckardt points on any line, and at most 2 if $\mathrm{char}(L) \neq 2$. Hence there are at most $5(9n)/n = 45$ Eckardt points on W, and at most $2(9n)/n = 18$ if $\mathrm{char}(L) \neq 2$. I have no reason to think that either of these estimates is best possible.

If W has more than one singular point, then we can take coordinates so that two of them are $P_0 = (1, 0, 0, 0)$ and $P_1 = (0, 1, 0, 0)$. Thus none of the monomials which appear in the equation of W is of degree greater than 1 in X_0 or in X_1, and the entire line P_0P_1 lies in W. If the equation of W contains a term $aX_0X_1X_2$ or $aX_0X_1X_3$, no other point of P_0P_1 is singular; otherwise every point of P_0P_1 is singular. Thus under the hypotheses of the Lemma W cannot contain three collinear singular points. If W contained four coplanar singular points $P_0, \ldots, P_3$ the plane of these points would meet W in at least the six distinct lines P_iP_j, which is impossible. Finally, suppose that W contains five singular points $P_0, \ldots, P_4$ no four of which are coplanar. The point Q at which the line P_3P_4 meets the plane $P_0P_1P_2$ cannot for example lie on P_1P_2 because that would imply that $P_1, \ldots, P_4$ are coplanar; so W meets the plane $P_0P_1P_2$ in three lines and at least one additional point Q, which again is impossible. □

If P is a nonsingular point of $W(L)$, we shall need various constructions for generating further such points. The importance of the first one is that it works even if P is an Eckardt point and none of the three lines through it is defined over L. Note that though we assume $\mathrm{char}(L) = 0$ for the conclusion of the Lemma, we do not use this in the construction. Indeed, we are also interested in using this construction when L is a finite field; see Lemma 12 and the end of the proof of Theorem 5. However we then need to assume or demonstrate the existence of a line ℓ defined over L and having the properties stated in the second sentence of the proof; and we need to show that ℓ_1 can be chosen so that the resulting point R is not simply P. The proof follows a remark of Manin ([3], p2). The idea goes back to Richmond and in principle to Ryley; see the notes to §13.6 in [1].

Lemma 6 *Suppose that W is not a cone, that there is a point P of $W(L)$ nonsingular on W and that* $\mathrm{char}(L) = 0$*; then $W(L)$ is Zariski dense in W, and the same holds for each R-equivalence class in $W(L)$.*

Proof. We may assume that W does not contain a line of singular points;

for if $X_0 = X_1 = 0$ were such a line then the equation of W would be inhomogeneous linear in X_0, X_1 together and it would be trivial to parametrize W. By hypothesis, the general line ℓ through P does not lie on or touch W, and it does not meet any line of W except perhaps at P. Since L is infinite we can find such a line ℓ which is defined over L. Denote by P', P'' the other points where ℓ meets W, so that P', P'' are distinct and distinct from P. Both P' and P'' are nonsingular on W, because they have multiplicity one in $\ell \cdot W$. They are either each defined over L or each defined over a quadratic extension of L and conjugate over L. Let Π' be the tangent plane to W at P' and Γ' the intersection of Π' with W, and similarly for Π'', Γ''; by hypothesis Γ', Γ'' are absolutely irreducible cubic curves with singularities at P', P'' respectively. Let ℓ_1 be any line in the ambient space not passing through P' or P'' nor lying on Π' or Π''; and let Q', Q'' be the intersections of ℓ_1 with Π', Π'' respectively. Let R' be the third intersection of $P'Q'$ with Γ' and similarly for R''; we assume ℓ_1 so chosen that neither R' nor R'' is one of the points where $\Pi' \cap \Pi''$ meets W, nor does the line $R'R''$ lie in W. Let R be the third intersection of $R'R''$ with W; if ℓ_1 is defined over L then so are $R'R''$ and R.

Conversely, let R be in general position on W and let Γ_1 be the projection of Γ' from R onto Π''. The intersections of Γ_1 and Γ'' at the points where Π' meets Γ'' contribute only $\deg(\Gamma' \cdot \Gamma'') = 3$ to $\deg(\Gamma_1 \cdot \Gamma'') = 9$; so there are points R' on Γ' and R'' on Γ'' with $R' \neq R''$ and $R'R''$ passing through R. Moreover R', R'' must be in general position on Γ', Γ'' respectively. By taking $R'R''$ to be ℓ_1, we see that the set of R constructed in this way contains a Zariski open subset of W. Hence the same holds for the set of all R obtained when ℓ_1 is in general position. But since L is infinite, the set of lines ℓ_1 defined over L is Zariski dense in the set of all lines. Because the space of lines in $\mathbf{P}^3$ is rational over the prime field, all the points R constructed in the proof of Lemma 6 lie in the same R-equivalence class $\mathcal{C}_0$. Projecting from a point of $\mathcal{C}_0 \circ \mathcal{C}$ now shows that each class $\mathcal{C}$ is Zariski dense on W. $\square$

Remark. Suppose that W and P are defined over an algebraic number field K, and let $\mathfrak{p}$ be a finite prime of K. In the first instance we choose $L = K_\mathfrak{p}$; then provided P' and P'' are each defined over $K_\mathfrak{p}$ we can simplify the description of this construction. For in this case R' and R'' are defined over $K_\mathfrak{p}$. Conversely if R' is any point of $\Gamma'(K_\mathfrak{p})$ other than P', and similarly for R'', then we can find a line ℓ_1 defined over $K_\mathfrak{p}$ which gives rise to this pair R', R''; indeed we can simply take ℓ_1 to be $R'R''$. In this way we obtain a point R in $W(K_\mathfrak{p})$. But we can approximate arbitrarily closely to ℓ and ℓ_1

over K; so we can by this construction obtain a point of $W(K)$ arbitrarily close to R. Moreover, for fixed P the points of $W(K)$ generated in this way as ℓ, ℓ_1 vary all lie in the same R-equivalence class. Now let U be an open subset of $W(K_\mathfrak{p})$. If for fixed P we can generate every point of U in this way, working over $K_\mathfrak{p}$ and requiring that P', P'' are each defined over $K_\mathfrak{p}$, it follows that there is an R-equivalence class of $W(K)$ which is dense in U. We shall make use of this argument in §8.

In the statement and proof of Lemma 7, all P_i will be points of W and all Q_i points of $\mathbf{P}^1$. Let P_0 be a point of W which does not lie on any of the lines on W and let Γ_0 be the intersection of W with the tangent plane to it at P_0; denote by $\phi : \mathbf{P}^1 \to \Gamma_0$ the desingularization of Γ_0. Let $Z \subset W \times \mathbf{P}^1 \times \mathbf{P}^1 \times W$ be the locus of points $P_1 \times Q_2 \times Q_3 \times P_4$ such that $P_1, \phi(Q_2), P_4$ are the three intersections of some line with W and P_4 lies on the tangent plane to W at $\phi(Q_3)$. For P_1 on W, define $Z(P_1)$ by

$$Z \cdot (P_1 \times \mathbf{P}^1 \times \mathbf{P}^1 \times W) = P_1 \times Z(P_1).$$

In other words, $Z(P_1)$ is the fibre of $Z \to W$ at P_1.

Lemma 7 *If W is nonsingular and P_1 is in general position on W, then $Z(P_1)$ is an absolutely irreducible curve in $\mathbf{P}^1 \times \mathbf{P}^1 \times W$.*

Proof. Let Y be the locus of points $P \times P'$ on $W \times W$ such that P lies on the tangent plane to W at P'. By Lemma 2, if $Y \cdot (P \times W) = P \times Y(P)$ then $Y(P)$ is the intersection of W with a quadric. If P is not in Γ_0 then $Y(P)$ does not contain Γ_0 because it does not contain P_0; and if P is in Γ_0 the intersection of $Y(P)$ with Γ_0 consists of P, P_0 and at most two other points, so again $Y(P)$ does not contain Γ_0. Hence $Y(P) \cdot \Gamma_0$ is well-defined and therefore $\deg(Y(P) \cdot \Gamma_0) = 6$. Now suppose that $P_1 \times Q_2 \times Q_3 \times P_4$ is in Z with Q_2 in general position on $\mathbf{P}^1$; then P_1 and Q_2 determine P_4 uniquely and hence $\phi(Q_3)$ must be in $Y(P_4) \cdot \Gamma_0$. Thus $Z(P_1)$ has dimension 1. Moreover P_4 can only lie on Γ_0 if P_4 coincides with $\phi(Q_2)$ and is in $Y(P_1) \cdot \Gamma_0$. We shall subsequently need the fact that Q_3 is not determined by P_1. For otherwise the cone with vertex P_1 and base Γ_0 would contain the intersection of W with the tangent plane at $\phi(Q_3)$, which is impossible.

Let $C(P_1)$ be the projection of $Z(P_1)$ on $\mathbf{P}^1 \times \mathbf{P}^1$. We have already proved that if Q is on $\mathbf{P}^1$ then

$$\deg\{(Q \times \mathbf{P}^1) \cdot C(P_1)\} = \deg\{Y(P') \cdot \Gamma_0\} = 6 \tag{9}$$

where P' is the remaining intersection with W of the line joining P_1 and $\phi(Q)$. The cone with vertex P_1 and base Γ_0 meets W again in the intersection of W with a quadric, on which P_4 lies, so we also have

$$\deg\{(\mathbf{P}^1 \times Q) \cdot C(P_1)\} = 6. \tag{10}$$

These two results determine the class of $C(P_1)$ as a divisor on $\mathbf{P}^1 \times \mathbf{P}^1$.

We next investigate the singularities of $C(P_1)$. Let $Q_2 \times Q_3$ be a point of $C(P_1)$ and let P_4 be the third intersection of W with the line joining P_1 and $\phi(Q_2)$. A necessary and sufficient condition for $Q_2 \times Q_3$ to be a singular point of $C(P_1)$ is that it has multiplicity greater than 1 as a component of both $C(P_1) \cdot (Q_2 \times \mathbf{P}^1)$ and $C(P_1) \cdot (\mathbf{P}^1 \times Q_3)$. By (9), the first of these happens if and only if $Y(P_4)$ touches Γ_0 at $\phi(Q_3)$; so it can only happen if P_4 lies on a certain not necessarily irreducible curve Γ_1 which depends only on P_0. To express the second condition, let C_1 be the intersection of W with the tangent plane to it at $\phi(Q_3)$ and let C_2 be the remaining intersection of W with the cone of vertex P_1 and base Γ_0; then the second condition is equivalent to saying that C_1 and C_2 touch at P_4 — in other words, that the tangent lines to C_1 at P_4 and to Γ_0 at $\phi(Q_2)$ meet. Suppose that both conditions hold for a particular P_4 not on Γ_0; then $\phi(Q_3)$ lies in $Y(P_4) \cdot \Gamma_0$ which is finite, whence $\phi(Q_2)$ belongs to a finite set and therefore so does P_1. Since P_4 lies on Γ_1, this implies that P_1 is not in general position. Hence P_4 must lie on Γ_0, and it now follows from the first condition that $P_4 = \phi(Q_3)$, and from the first paragraph of the proof that $P_4 = \phi(Q_2)$. Moreover P_4 is one of the points of $Y(P_1) \cdot \Gamma_0$. Conversely, any such point is indeed a singularity of $C(P_1)$.

We have therefore shown that, for P_1 in general position, the singularities of $C(P_1)$ are precisely at the points where $C(P_1)$ meets Δ, the diagonal of $\mathbf{P}^1 \times \mathbf{P}^1$. There are just six of these points, because they correspond to the points where $Y(P_1)$ meets Γ_0. On the other hand, (9) and (10) imply $\deg\{C(P_1) \cdot \Delta\} = 12$; so each point occurs with intersection multiplicity 2 and is therefore an ordinary double point or a cusp. But, using (9) and (10) again, the only way that $C(P_1)$ can be reducible and yet have only six singularities, each of which is a double point or a cusp, is if it has just 2 components and one of them has the form $Q \times \mathbf{P}^1$ or $\mathbf{P}^1 \times Q$; and this is impossible because the singularities lie on Δ and hence cannot all lie on a component of this form. □

When the context makes it necessary, we shall require that every point which we introduce has a fixed coordinate representation $(X_0, \ldots, X_3)$ in

which the X_i are all integers at $\mathfrak{p}$ and at least one of them is a unit there. Using this representation, we write arithmetic operations on such quadruplets as the associated arithmetic operations on points. Let $f(X_0, \ldots, X_3) = 0$ be the equation of W, where the coefficients of f are in $\mathfrak{O}_\mathfrak{p}$ and not all divisible by $\mathfrak{p}$; and for any points T_1, T_2 in $\mathbf{P}^3$ write

$$f_2(T_1, T_2) = \sum_{i=0}^{3} X_i(T_1) \frac{\partial f(T_2)}{\partial X_i}. \tag{11}$$

The value of $f_2(T_1, T_2)$ here depends on the coordinate representations of T_1, T_2. If T_1, T_2 lie in W and T_2 is nonsingular then $f_2(T_1, T_2) = 0$ if and only if T_1 is on the tangent to W at T_2. Now let ℓ be a line which does not touch W and let T_1, T_2, T_3 be the three points of intersection of ℓ and W; thus

$$a_1 T_1 + a_2 T_2 + a_3 T_3 = 0 \tag{12}$$

for some nonzero a_1, a_2, a_3. Because f_2 is linear in its first argument

$$a_1 f_2(T_1, T_3) + a_2 f_2(T_2, T_3) = -a_3 f_2(T_3, T_3) = 0;$$

and because f is homogeneous cubic and vanishes at T_1 and T_2

$$3a_1 a_2^2 f_2(T_1, T_2) + 3a_1^2 a_2 f_2(T_2, T_1) = f(-a_3 T_3) = 0.$$

Hence

$$-\frac{a_1}{a_2} = \frac{f_2(T_2, T_3)}{f_2(T_1, T_3)} = \frac{f_2(T_1, T_2)}{f_2(T_2, T_1)} \tag{13}$$

and in particular

$$f_2(T_1, T_3) f_2(T_1, T_2) = f_2(T_2, T_3) f_2(T_2, T_1). \tag{14}$$

We shall only need these results when $\mathrm{char}(L) = 0$. The proof above fails when $\mathrm{char}(L) = 3$, but because (13), (14) are identities which we have already shown hold when $\mathrm{char}(L) = 0$, they must hold always.

3. *Approximation at an infinite prime.* In this section v will denote an infinite place of K, so that K_v is either $\mathbf{C}$ or $\mathbf{R}$. Our object is to prove

Theorem 2 *If v is an infinite place of K and $V(K)$ is not empty then each R-equivalence class of $V(K)$ is contained in a connected component of $V(K_v)$ and is dense in it.*

Proof. R-equivalence is the finest equivalence relation such that if $\phi : \mathbf{P}^1 \to V$ is defined over K as are Q_1, Q_2 on $\mathbf{P}^1$, then $\phi(Q_1)$ is R-equivalent to $\phi(Q_2)$. Each R-equivalence class lies in a connected component of $V(K_v)$ because $\mathbf{P}^1(K_v)$ is connected and hence so is its image. To complete the proof it is enough to show that if $\mathcal{C}$ is any R-equivalence class then the closure of $\mathcal{C}$ is open in $V(K_v)$.

Let P be a point of $V(K_v)$ in the closure of $\mathcal{C}$ and choose a point Q_0 in $V(K)$ such that the tangent plane to V at Q_0 meets V in an irreducible curve Γ_0 which does not pass through P; this is possible because $V(K)$ is dense in the Zariski topology. For any point Q_1 of $\Gamma_0(K)$ other than Q_0, let Q_1' be the other intersection of PQ_1 with V and let Γ_1 be the residual intersection of V with the cone of vertex Q_1' and base Γ_0; thus Γ_1 is birationally equivalent to $\mathbf{P}^1$ over K_v. It is easy to see that as Q_1 varies on Γ_0 the curves Γ_1 are not all tangent to one another at P. Choose points Q_2, Q_3 of $\Gamma_0(K)$ so that the corresponding curves Γ_2, Γ_3 are not tangent at P; and choose local coordinates ξ, η on V near P so that the tangents to Γ_2, Γ_3 at P are $\eta = 0, \xi = 0$ respectively. By continuity we can choose $\epsilon > 0$ with the following property. Let P' be any point of $V(K_v)$ with $|\xi| < 3\epsilon, |\eta| < 3\epsilon$ and, starting from Q_2, Q_3 and Γ_0, construct curves Γ_2', Γ_3' through P' in the same way as we constructed Γ_2, Γ_3 through P. Near P, Γ_2' is nearly parallel to Γ_2 and similarly for Γ_3'; so for all points of Γ_2', Γ_3' in $|\xi| < 2\epsilon, |\eta| < 2\epsilon$ we have

$$|d\eta/d\xi| < \tfrac{1}{10} \text{ for } \Gamma_2', \quad |d\xi/d\eta| < \tfrac{1}{10} \text{ for } \Gamma_3'. \tag{15}$$

Let $P^* = (\xi^*, \eta^*)$ be a point of $V(K_v)$ with $|\xi^*| < \epsilon, |\eta^*| < \epsilon$; to complete the proof of the theorem it is enough to show that P^* is in the closure of $\mathcal{C}$. Choose $P_0 = (\xi_0, \eta_0)$ in $\mathcal{C}$ with $d(P, P_0) < \frac{1}{2}\epsilon$ and therefore $d(P^*, P_0) < 2\epsilon$, where d is the metric induced by ξ, η. Without loss of generality we can assume that $|\xi^* - \xi_0| \leq |\eta^* - \eta_0|$. Starting with Γ_0 and Q_3 construct $\Gamma_3^\sharp$ passing through P_0 in the same way as we constructed Γ_3 passing through P. There is a non-constant map $\mathbf{P}^1 \to \Gamma_3^\sharp$ defined over K, and $\Gamma_3^\sharp$ is almost parallel to Γ_3. Hence there is a point of $\Gamma_3^\sharp$ at which $\eta = \eta^*$; so we can find a point $P_1 = (\xi_1, \eta_1)$ in $\Gamma_3^\sharp(K)$, and therefore R-equivalent to P_0, such that $|\eta^* - \eta_1| \leq \frac{1}{10}|\eta^* - \eta_0|$. It follows from (15) that

$$|\xi_0 - \xi_1| \leq \tfrac{1}{10}|\eta_0 - \eta_1| \leq \tfrac{1}{9}|\eta^* - \eta_0|;$$

hence $|\xi^* - \xi_1| \leq |\xi^* - \xi_0| + \frac{1}{9}|\eta^* - \eta_0|$ and so $d(P^*, P_1) \leq \frac{4}{5} d(P^*, P_0)$. Iterating this construction, we obtain a sequence of points $P_0, P_1, \ldots$ in $\mathcal{C}$ which tend to P^*. $\square$

4. *Approximation at a finite prime.* If $\mathfrak{p}$ is a finite prime of K then $V(K_\mathfrak{p})$ is totally disconnected, so the analogue of Theorem 2 is worthless. The methods which were used to prove Theorem 2 will show that any R-equivalence class of $V(K)$ is dense in some open subset of $V(K_\mathfrak{p})$, but for applications we shall need the more specific statement in Theorem 3 below. In this and the next two sections we shall be concerned with one finite prime $\mathfrak{p}$. We shall denote by v the normalized additive valuation associated with $\mathfrak{p}$ and by π a uniformizing parameter for $\mathfrak{p}$ in K. Expressions such as $O(\mathfrak{p}^n)$ will denote elements of K or $K_\mathfrak{p}$ divisible by $\mathfrak{p}^n$. Note that if Q_1, Q_2 are points of V such that $\widetilde{Q_1} = \widetilde{Q_2}$ is nonsingular on V then $f_2(Q_1, Q_2) = O((Q_1 - Q_2)^2)$ in the notation of (11).

An important procedure in several parts of this paper is the translation of a smooth curvilinear arc in V. Let P_0 be a point of $V(K)$ such that $\widetilde{P_0}$ is nonsingular on $\tilde{V}$ and let $\Gamma_0 \subset V$ be an arc through P_0. Let P_1 be another point of $V(K)$ such that $\widetilde{P_1} = \widetilde{P_0}$. Let R be a point of $V(K)$ such that $\tilde{R}$ is nonsingular on $\tilde{V}$ and not on the tangent plane to $\tilde{V}$ at $\widetilde{P_0}$, and neither P_0 nor P_1 is on the tangent plane to V at R. For $i = 0, 1$ let S_i be the third intersection of $P_i R$ with V. Denote by Γ' the residual intersection of V with the cone of vertex S_0 and base Γ_0, and by Γ_1 the residual intersection of V with the cone of vertex S_1 and base Γ'; thus R lies on Γ' and P_1 on Γ_1. We call Γ_1 a *translation* of Γ_0 from P_0 to P_1. In applications, Γ_0 will be an arc of a rational curve defined over K; then this will also be true of Γ_1. We shall show that Γ_1 is approximately parallel to Γ_0, in a sense made explicit in (22) or (23) below.

Take coordinates such that P_0 is $(1, 0, 0, 0)$, R is $(0, 1, 0, 0)$ and the tangent to V at P_0 is $X_1 = 0$. Let $X = X_2/X_0$ and $Y = X_3/X_0$, so that X, Y are local coordinates at P_0 on V. If $S_0 = aP_0 + bR$ the fact that neither $\tilde{R}$ nor $\widetilde{S_0}$ is equal to $\widetilde{P_0}$ implies that a, b are in $\mathfrak{O}_\mathfrak{p}$ and b is a unit at $\mathfrak{p}$. Normalizing, we can write $S_0 = C_0 P_0 + R$, where $C_0 \neq 0$ because P_0 is not on the tangent to V at R. Write $N = v(C_0)$; thus N is independent of the representations of P_0, R chosen, though C_0 is not. Denote by $\mathcal{N}$ the subset of the inverse image of $\widetilde{P_0}$ in $V(K)$ at which $v(X) \geq N + 1, v(Y) \geq N + 1$. There is a one-one correspondence between the points of the inverse image of $\widetilde{P_0}$ in $V(K_\mathfrak{p})$ and the pairs X, Y in $K_\mathfrak{p}$ with $\pi | X, \pi | Y$. Let A, B be such that $AX + BY = 0$ touches Γ_0 at P_0, where A, B are in $\mathfrak{O}_\mathfrak{p}$ and at least one of them is a unit; and write

$$\xi = AX + BY, \quad \eta = A'X + B'Y \tag{16}$$

for some A', B' in $\mathfrak{O}_\mathfrak{p}$ such that $AB' - A'B$ is a unit at $\mathfrak{p}$. Thus η is a local variable at P_0 on Γ_0 and $v(\eta) \geq N+1$ in $\mathcal{N}$. It follows that on Γ_0 we have a power series expansion $\xi = \sum_2^\infty a_n \eta^n$ convergent in some neighbourhood of $\eta = 0$. We assume Γ_0 so chosen that this series converges in $v(\eta) \geq N+1$ and that $v(a_n) > -(N+1)(n-1)$ for all n; thus ξ is small compared to η on Γ_0 provided $v(\eta) \geq N+1$. This will certainly hold if the arc Γ_0 has good reduction mod $\mathfrak{p}$. In this section, for any variable ζ we shall denote by $\Omega(\zeta)$ a power series of the form $\sum_1^\infty c_n \zeta^n$ which converges in $v(\zeta) \geq N+1$ and satisfies $v(c_n) > -n(N+1)$ for all n; here Ω need not be the same from one occasion to the next. Thus $\xi = \eta\Omega(\eta)$ on Γ_0.

Lemma 8 *If P_1 is in $\mathcal{N}$ then Γ_1 has the form $\xi - \xi_1 = (\eta - \eta_1)\Omega(\eta - \eta_1)$ where ξ_1, η_1 are the values of ξ, η at P_1.*

Proof. Because $\tilde{R}$ is not on the tangent to $\tilde{V}$ at $\widetilde{P_0}$, $f_2(R, P_0)$ is a unit at $\mathfrak{p}$. Since any point of $\mathcal{N}$ has a representation which differs from that of P_0 by $O(\mathfrak{p}^{N+1})$, $f_2(R, P)$ is a unit at $\mathfrak{p}$ for any P in $\mathcal{N}$, and similarly for $f_2(S_0, P)$ and $f_2(S_1, P)$. Now $S_0 = R + C_0 P_0$ can be written

$$S_0 = R - \{f_2(P_0, R)/f_2(R, P_0)\}P_0 = R + \{f_2(P_0, S_0)/f_2(S_0, P_0)\}P_0 \quad (17)$$

in view of (13), so that $v(f_2(P_0, R)) = v(f_2(P_0, S_0)) = N$; hence as above $v(f_2(P, R)) = v(f_2(P, S_0)) = N$ for all P in $\mathcal{N}$. But once we have fixed the representation of P_1 it follows from (13) that we can choose the representation of S_1 to satisfy

$$S_1 = R - \{f_2(P_1, R)/f_2(R, P_1)\}P_1; \quad (18)$$

and as above $v(f_2(P, S_1)) = N$ for all P in $\mathcal{N}$. Now let P_0' be any point of $\mathcal{N} \cap \Gamma_0$ and let R' be the third intersection of $P_0'S_0$ with V and P_1' the third intersection of $R'S_1$ with V; thus P_1' is on Γ_1. We can take

$$R' = S_0 - \{f_2(P_0', S_0)/f_2(S_0, P_0')\}P_0'. \quad (19)$$

It follows from (17) and (19) that

$$R' - R = \frac{f_2(P_0, S_0)}{f_2(S_0, P_0)}P_0 - \frac{f_2(P_0', S_0)}{f_2(S_0, P_0')}P_0'; \quad (20)$$

since the denominators are units, the coordinates of R' differ from those of R by $O(\mathfrak{p}^{N+1})$. A similar result holds for S_0 and S_1. Hence

$$C_0^{-1}(S_1 - R') = C_0^{-1}(S_0 - R) + O(\mathfrak{p}) = P_0 + O(\mathfrak{p})$$

is the coordinate representation of a point of $R'S_1$; since this is close to $\widetilde{P_0}$ the reduction mod $\mathfrak{p}$ of $R'S_1$ is $\widetilde{P_0}\tilde{R}$. Since this line is transversal to $\tilde{V}$ at $\widetilde{P_0}$, it follows from Hensel's Lemma that P_1' is within $O(\mathfrak{p})$ of P_0. Now let a, b be such that $P_1' = -aR' + bS_1$. Using (20) and the analogous estimate for $S_0 - S_1$,

$$P_1' + O(a\mathfrak{p}^{N+1}) + O(b\mathfrak{p}^{N+1}) = -aR + bS_0 = (b-a)R + bC_0P_0. \tag{21}$$

If $v(b) > v(a)$ then $v(b-a) = v(a)$ and (21) is impossible since $(b-a)R$ is strictly larger than any of the other terms except perhaps P_1'; so we can assume that $v(b) \leq v(a)$. Because $\tilde{R} \neq \widetilde{P_0}$ each term on the right must be $O(1) + O(a\mathfrak{p}^{N+1}) + O(b\mathfrak{p}^{N+1})$. Applying this first to bC_0R_0 and remembering that $v(a) \geq v(b)$, we obtain $b = O(\mathfrak{p}^{-N})$; now applying it to $(b-a)R$ we obtain $b - a = O(\mathfrak{p})$ and so $v(b) = v(a) = -N$. Using (17), (18) and (19) in $P_1' = -aR' + bS_1$,

$$P_1' = -aC_0P_0 + a\frac{f_2(P_0', S_0)}{f_2(S_0, P_0')}P_0' - b\frac{f_2(P_1, R)}{f_2(R, P_1)}P_1 + (b-a)R. \tag{22}$$

The coefficients of P_0', P_1 here are $aC_0 + O(\mathfrak{p})$ and $-bC_0 + O(\mathfrak{p})$ respectively, so

$$P_1' = (bC_0 + O(\mathfrak{p}))P_0 + O(\mathfrak{p}^{N+1}) + (b-a)R.$$

Since the term in R does not affect the values of X, Y at P_1', we deduce that P_1' is in $\mathcal{N}$.

We shall repeatedly use the fact that if any of the power series $\sum_1^\infty c_n\eta^n$ which appear in the following argument converges in $v(\eta) \geq N+1$ and has a sum which is $O(\mathfrak{p})$ for all such η, then it has the form $\Omega(\eta)$. To prove this, we note that because of the way in which these properties are proved they hold when η is merely in the maximum unramified extension of $K_\mathfrak{p}$. Since the residue field of this extension is infinite, the bound $\sum c_n\eta^n = O(\mathfrak{p})$ cannot depend on cancellation between terms individually larger; so $c_n\eta^n = O(\mathfrak{p})$ for each n. Now let η_0' be the value of η at P_0'. It follows from (20) that $R' - R$ has a power series expansion in η_0' convergent in $v(\eta_0') \geq N+1$ and with zero constant term. Since it is also $O(\mathfrak{p}^{N+1})$ we deduce $R' - R = C_0\Omega(\eta_0')$. By (18) and (19)

$$f_2(S_1, R') = f_2(R, R') - \frac{f_2(P_1, R)f_2(P_1, R')}{f_2(R, P_1)},$$
$$f_2(R', S_1) = f_2(S_0, S_1) - \frac{f_2(P_0', S_0)f_2(P_0', S_1)}{f_2(S_0, P_0')}.$$

In each of these equations, the first term on the right is $O(\mathfrak{p}^{2N+2})$ and the second is the sum of a constant and an expression of the form $C_0^2\Omega(\eta_0')$. It follows from the first equation that

$$f_2(S_1, R') = f_2(S_1, R) + C_0^2\Omega(\eta_0')$$

where the first term on the right has valuation $2N$ and is independent of η_0'. By the second equation $f_2(R', S_1) - f_2(R, S_1)$ is $O(\mathfrak{p}^{2N+1})$ and has a power series expansion convergent in $v(\eta_0') \geq N+1$; so

$$f_2(R', S_1) = f_2(R, S_1) + C_0^2\Omega(\eta_0')$$

where again the first term on the right has valuation $2N$ and is independent of η_0'. But by (13)

$$-b/a = f_2(S_1, R')/f_2(R', S_1) = c + \Omega(\eta_0')$$

where $c = f_2(S_1, R)/f_2(R, S_1)$ is a unit at $\mathfrak{p}$. Dividing (22) by aC_0, we find that the values of X, Y at P_1' can be expanded as power series in η_0' convergent in $v(\eta_0') \geq N+1$; and they satisfy

$$X(P_1') = X(P_1) + X(P_0') + \Omega(\eta_0') + C_0^{-1}O({\eta_0'}^2) \tag{23}$$

together with a similar equation for Y. It follows that Γ_1 is smooth at P_1 and the tangent there is given by

$$A(X - X(P_1)) + B(Y - Y(P_1)) = 0,$$

so that $\eta - \eta_1$ is a local variable on Γ_1 at P_1. Moreover $\eta(P_1') - \eta_1 = \eta_0' + \Omega(\eta_0')$; inverting this we get $\eta_0' = \eta(P_1') - \eta_1 + \Omega(\eta(P_1') - \eta_1)$, and it follows that

$$\xi(P_1') - \xi_1 = \eta_0'\Omega(\eta_0') = (\eta(P_1') - \eta_1)\Omega(\eta(P_1') - \eta_1)$$

as claimed. □

Theorem 3 *Let P, R be points of $V(K)$ such that $\tilde{P}$ is nonsingular on $\tilde{V}$, $\tilde{R}$ is not on the tangent to $\tilde{V}$ at $\tilde{P}$ and P is not on the tangent to V at R. Let $S = R + C_0P$ be the third intersection of PR with V and write $N = v(C_0)$. Let Γ_0, Γ_1 be arcs of rational curves on V defined over K and passing through P; assume that $\tilde{P}$ is nonsingular on both $\widetilde{\Gamma_0}$ and $\widetilde{\Gamma_1}$ and Γ_0, Γ_1 do not touch at P. Let X, Y be local variables on V at P whose reductions* $\bmod \mathfrak{p}$ *are*

local variables on $\tilde{V}$ at $\tilde{P}$. For $i = 0, 1$ let $A_iX + B_iY = 0$ touch Γ_i at P, where A_i, B_i are in $\mathfrak{O}_\mathfrak{p}$ and at least one of them is a unit at $\mathfrak{p}$; and write $M = v(A_0B_1 - A_1B_0)$. If $\mathcal{C}$ is the R-equivalence class of P then the points of $\mathcal{C}$ are dense in the $\mathfrak{p}$-adic topology in the open neighbourhood

$$v(X) \geq L, \quad v(Y) \geq L \tag{24}$$

where $L = 3M + N + 1$.

Proof. Denote the set (24) by $\mathcal{N}$ and let P^* be a point of $\mathcal{N}$ defined over $K_\mathfrak{p}$. To prove the Theorem, it is enough to construct a sequence of points $P_0 = P, P_1, \ldots$ in $\mathcal{C}$ such that $P^* - P_n = O(\mathfrak{p}^{L+n})$. The construction of P_{n+1} from P_n is as follows. Write $\xi_i = A_iX + B_iY$ for $i = 0, 1$ and let A, B in $\mathfrak{O}_\mathfrak{p}$ be such that $AB_i - A_iB$ is a unit for $i = 1, 2$; thus $\eta = AX + BY$ is a local variable at P on each Γ_i and

$$(A_0B_1 - A_1B_0)\eta = (AB_1 - A_1B)\xi_0 - (AB_0 - A_0B)\xi_1. \tag{25}$$

Let ξ_0^*, ξ_1^* be the values of ξ_0, ξ_1 at P^*. Let Γ_{0n} be the translation of Γ_0 from P to P_n, and choose a point Q_n in $\Gamma_{0n}(K)$ with

$$(\eta(Q_n) - \eta(P_n)) - \frac{A_0B - AB_0}{A_0B_1 - A_1B_0}(\xi_1^* - \xi_1(P_n)) = O(\mathfrak{p}^{L+n+1}).$$

The second term on the left is $O(\mathfrak{p}^{L+n-M})$, so it follows from Lemma 8 that

$$\xi_0(Q_n) - \xi_0(P_n) = O(\mathfrak{p}^{2L+2n-2M-N})$$

and therefore $\xi_0^* - \xi_0(Q_n) = O(\mathfrak{p}^{L+n})$. Also (25) implies

$$\xi_1(Q_n) - \xi_1(P_n) = \xi_1^* - \xi_1(P_n) + O(\mathfrak{p}^{L+n+M+1}) + O(\mathfrak{p}^{2L+2n-2M-N}),$$

so that

$$\xi_1^* - \xi_1(Q_n) = O(\mathfrak{p}^{L+n+M+1}).$$

Now let Γ_{1n} be the translation of Γ_1 from P to Q_n and choose P_{n+1} in $\Gamma_{1n}(K)$ with

$$(\eta(P_{n+1}) - \eta(Q_n)) - \frac{AB_1 - A_1B}{A_0B_1 - A_1B_0}(\xi_0^* - \xi_0(Q_n)) = O(\mathfrak{p}^{L+n+1}).$$

Much as before, we have

$$\xi_1^* - \xi_1(P_{n+1}) = O(\mathfrak{p}^{L+n+M+1}),$$
$$\xi_0^* - \xi_0(P_{n+1}) = O(\mathfrak{p}^{L+n+M+1});$$

and these give $P^* - P_{n+1} = O(\mathfrak{p}^{L+n+1})$ by the analogues of (25) for X, Y in terms of ξ_0, ξ_1. □

The statement of Theorem 3 naturally raises the question: if γ is a curve of genus 0 on $\tilde{V}$, under what conditions can it be lifted to an arc of a curve of genus 0 on V? If γ has simply been conjured up, this may well be impossible; but if γ has been constructed it will often be possible to lift the construction. A good example of this is implicit in the proof of Lemma 12. The simplest case is the following, which nevertheless involves certain subtleties.

Lemma 9 *Let P be a point of $V(K)$ such that $\tilde{P}$ is nonsingular on $\tilde{V}$, and suppose that $\tilde{V}$ does not contain a plane through $\tilde{P}$. Let γ be the intersection of $\tilde{V}$ with the tangent to $\tilde{V}$ at $\tilde{P}$, and let p_1 be a point of $\gamma(k)$ which is nonsingular both on γ and on $\tilde{V}$. Then p_1 is liftable to a point P_1 and γ is liftable at p_1 to an arc of a curve Γ of genus 0 passing through P_1.*

Proof. The first step is to show that we can reduce to the case when P is not on any line of V. We proceed step-by-step, at each step replacing P by a less insalubrious point. Suppose first that P lies on a line of V not defined over K; each such line contains at most one point of $V(K)$, so we have only finitely many such P to consider. By Lemma 6 we can find a point R of $V(K)$ which does not lie on any line of V and is such that the tangent to V at R does not contain P; thus the tangent to V at R meets V in an irreducible cubic curve C. If S_0 is a general point of C, the tangent to V at S_0 does not pass through P because otherwise the tangent to V at R would pass through P. Choose such an S_0 in $C(K)$ and then choose S_1 in $C(K)$ close to S_0. Let PS_0 meet V again in T and let TS_1 meet V again in P_2. Then P_2 is close to P but not identical with it; in particular $\widetilde{P_2} = \tilde{P}$ but P_2 does not lie on a line of V not defined over K.

It can still happen that P_2 lies on a line Λ of V defined over K. By the proof of Lemma 5, there are at most 10 points of Λ at which the tangent to V meets V in a union of lines; so we can replace P_2 by a point P_3 which does not have this property but for which $\widetilde{P_3} = \widetilde{P_2}$. The residual part of the intersection of V with the tangent to V at P_3 is an irreducible conic passing

through P_3; we can therefore choose a point P_4 on it and defined over K such that $\tilde{P}_4 = \tilde{P}_3$ but P_4 does not lie on any line of V. We now start again with P_4 in place of P; the advantage of this is that we can now assume that the tangent to V at P meets V in an irreducible cubic curve Γ.

Now choose coordinates so that P is $(1,0,0,0)$ and the tangent to V at P is $X_3 = 0$. The equation of V has the form $X_3X_0^2 + \ldots = 0$, and it contains at least one term not divisible by X_3 whose coefficient is a unit at $\mathfrak{p}$; for otherwise $\tilde{V}$ would contain the plane $X_3 = 0$. So we obtain the equation of γ by setting $X_3 = 0$ and reducing all coefficients mod $\mathfrak{p}$. By Hensel's Lemma we can lift p_1 to a point P_1' in $\Gamma(K_\mathfrak{p})$. Let Λ_1 be a line defined over K, lying in $X_3 = 0$, passing through P and close to PP_1'; then Λ_1 meets Γ again in a point P_1 defined over K and close to P_1', and γ lifts to an arc of Γ. □

Corollary *Let ℓ be a line on $\tilde{V}$ defined over k and such that no point of ℓ is singular on $\tilde{V}$. If there is a point P of $V(K)$ such that $\tilde{P}$ lies on ℓ, then any point p_1 of $\ell(k)$ can be lifted to a point P_1 of $V(K)$, and at p_1 the line ℓ can be lifted to an arc of a curve Γ_1 of genus 0 passing through P_1.*

Proof. If $\tilde{V}$ were not irreducible then ℓ would contain a singular point, contrary to hypothesis. Let γ be the intersection of $\tilde{V}$ with the tangent to $\tilde{V}$ at $\tilde{P}$. It follows from the Lemma that the property holds for any p_1 in $\ell(k)$ except perhaps the singular points of γ on ℓ, which are $\tilde{P}$ and at most one other point. Since $\ell(k)$ consists of $q+1$ points, we can find at least one p_1 for which the property does hold. Now repeat the argument with P_1 instead of P, noting that if γ_1 is the intersection of $\tilde{V}$ with the tangent to $\tilde{V}$ at p_1 then no point of ℓ can be singular on both γ and γ_1. □

Because of the hypotheses involved, it might appear that Theorem 3 is not always applicable; but we can cope with this by rescaling. Let V be any nonsingular cubic surface and P any point of $V(K)$. By Lemma 6 we can find a point R in $V(K)$ such that the line PR does not lie in or touch V, and R does not lie on any line of V. We can take P to be $(1,0,0,0)$, the tangent to V at P to be $X_3 = 0$ and R to be $(0,0,0,1)$; thus the equation of V can be written

$$f(X_0, \ldots, X_3) = a_{003}X_0^2X_3 + \ldots = 0$$

where the coefficients of f are in $\mathfrak{O}_\mathfrak{p}$ and $a_{003} \neq 0$. Multiply by a_{003} and replace X_0 by $a_{003}^{-1}X_0$; this forces $a_{003} = 1$, so that now $\tilde{P}$ is nonsingular on $\tilde{V}$ and $\tilde{R}$ does not lie on the tangent to $\tilde{V}$ at $\tilde{P}$. To construct the curves Γ_i

let Γ' be the intersection of V with the tangent to V at R and Λ the line of intersection of the tangents at P and R; because R does not lie on a line of V, Γ' is an absolutely irreducible plane cubic. Let T be in general position on Γ'. If PT touched V then this would hold for every point of Γ', whereas it does not hold for R. Let T' be the remaining intersection of PT with V and let Γ be the residual intersection of V with the cone of vertex T' and base Γ'. If the tangent to Γ' at T meets Λ at U then the tangent to Γ at P is PU. Hence as T varies in $\Gamma(K)$, the tangent to Γ at P does vary; so we can take Γ_0, Γ_1 to be the Γ constructed from some T_0, T_1 in $\Gamma(K)$.

We do not yet know the behaviour of the $\widetilde{\Gamma}_i$ at $\tilde{P}$. But let η be a common local variable for each Γ_i at P of the form $(AX_1+BX_2)/X_0$, with A, B in $\mathfrak{O}_\mathfrak{p}$. The coordinates of a point of Γ_i are given by power series in η convergent in some $\mathfrak{p}$-adic neighbourhood of $\eta = 0$. We can choose n so that for $i = 0, 1$ these series converge in $v(\eta) \geq n+1$ and their values are $O(\mathfrak{p})$ there. If we now write $\pi^n X_1, \pi^n X_2$ for X_1, X_2, the effect will be that the $\widetilde{\Gamma}_i$ are nonsingular at $\tilde{P}$.

We have therefore shown that to any P in any class $\mathcal{C}$ there exists an integer $L(P)$ such that if P^* in $V(K_\mathfrak{p})$ satisfies $P^* - P = O(\mathfrak{p}^{L(P)})$ in the original coordinate system then P^* is in the closure of $\mathcal{C}$ in the $\mathfrak{p}$-adic topology. We next show that we can choose an L which is valid for all P. Indeed we can apply the last construction with P^* instead of P, but with R, T_0 and T_1 still defined over K; and these will work for all P near enough to P^*. Thus there is a neighbourhood $\mathcal{N}$ of P^* such that if there is a point of some class $\mathcal{C}$ in $\mathcal{N}$ then points of $\mathcal{C}$ are dense in $\mathcal{N}$. Because $V(K_\mathfrak{p})$ is compact, it is covered by finitely many such neighbourhoods.

It is natural to ask for conditions under which we can assert that if P is in $V(K)$ then $\tilde{P}$ is densely liftable. The most useful result of this kind which I can prove are Theorem 4 and Lemma 10 and its Corollary.

Theorem 4 *Let P, R be points of $V(K)$ such that $\tilde{P}, \tilde{R}$ are nonsingular on $\tilde{V}$ and $\tilde{P}\tilde{R}$ does not lie on or touch $\tilde{V}$.*

(i) *Let Γ_0, Γ_1 be arcs of rational curves on V defined over K such that $\widetilde{\Gamma_0}, \widetilde{\Gamma_1}$ are nonsingular at $\tilde{P}$ and do not touch there. Then $\tilde{P}$ and $\tilde{R}$ are both densely liftable.*

(ii) *Suppose that $\tilde{R}$ does not lie on any line on $\tilde{V}$, and denote by γ the intersection of $\tilde{V}$ with the tangent to $\tilde{V}$ at $\tilde{R}$. Let t_1, t_2 be points of $\gamma(k)$ distinct from each other and from $\tilde{R}$, and such that $\tilde{P}t_i$ does not*

lie in or touch $\tilde{V}$; and suppose that the tangents to γ at t_1, t_2 do not meet on the tangent to $\tilde{V}$ at $\tilde{P}$. Then $\tilde{P}$ and $\tilde{R}$ are both densely liftable.

Proof. These are both special cases of Theorem 3 in which the hypotheses imply $M = N = 0$. If S is the third point of intersection of PR with V then $\tilde{S}$ is distinct from $\tilde{P}$ and $\tilde{R}$; hence $N = 0$. For (i) we can now replace Γ_0 and Γ_1 by their translations to P; Theorem 3 now shows that $\tilde{P}$ is densely liftable, and projection from S gives the same result for $\tilde{R}$. For (ii) we argue as follows. By hypothesis γ is an irreducible cubic; let Γ be the intersection of V with the tangent to V at R. Lift each $\tilde{R}t_i$ to a line through R in the plane of Γ; its third intersection T_i with Γ is a lift of t_i. Let S_i be the third intersection of PT_i with V; by hypothesis $\widetilde{S}_i$ is not equal to $\tilde{P}$ or t_i. If Γ_i is the residual intersection of V with the cone with base Γ and vertex S_i then each $\widetilde{\Gamma}_i$ is nonsingular at $\tilde{P}$ and $\widetilde{\Gamma}_1, \widetilde{\Gamma}_2$ do not touch at $\tilde{P}$; thus $M = 0$. Theorem 3 now shows that $\tilde{P}$ is densely liftable; and again projection from S proves that $\tilde{R}$ is also densely liftable. □

The last part of this argument can be generalized. Let P, R be points of $V(K)$ such that $\tilde{P}, \tilde{R}$ are nonsingular on $\tilde{V}$, $\tilde{P}$ is densely liftable and $\tilde{R}$ is liftable. If $\tilde{P}\tilde{R}$ does not touch $\tilde{V}$ at $\tilde{R}$ then $\tilde{R}$ is also densely liftable.

Suppose that $\tilde{V}$ is not a cone and does not have a line of singularities, and let P be any point of $V(K)$ such that $\tilde{P}$ is nonsingular on $\tilde{V}$. Provided q is large enough, arguments like those of Lemma 12 below show that we can find R, t_1, t_2 satisfying all the conditions of Theorem 4. It follows that if q is large enough, every nonsingular point of $\tilde{V}(k)$ which is liftable is densely liftable. We shall see in Theorem 5 that, without any condition on q, if $\tilde{V}$ is nonsingular then every point of $\tilde{V}(k)$ is liftable; we are therefore motivated to ask what is then the obstruction to every point of $\tilde{V}(k)$ being densely liftable. We consider this question in §6. A similar investigation would be possible though laborious when $\tilde{V}$ is singular but is not a cone and does not have a line of singular points.

If $\tilde{V}$ is a cone or has a line of singular points, I have no reason to believe that every nonsingular point of $\tilde{V}(k)$ which is liftable is densely liftable. However, if $\mathfrak{p} \not| 3$ it is true (though not proved in this paper) that we can always rescale V so that reduction $\bmod \mathfrak{p}$ yields a more tractable surface over k than the original $\tilde{V}$. I believe this to hold even if $\mathfrak{p}|3$. Special cases of this assertion can be found in §8.

In the proof of Theorem 3 the key fact was that, given rational arcs Γ_i through P, through any point P' of $V(K)$ near enough to P we could find

rational arcs Γ_i' whose reductions $\bmod \mathfrak{p}$ are the same as those of Γ_i. We achieved this by translation; but this is not the only method available — and indeed it may cease to be available if $\tilde{V}(k)$ is too small. We shall later need the following result. The construction underlying the proof is the same as that of Theorem 4(i), except that we no longer have to employ translations or mention R because the hypotheses of Lemma 10 provide us with the rational arcs through P which had to be constructed in the proof of Theorem 4(i).

Lemma 10 *Suppose that p is nonsingular in $\tilde{V}(k)$ and liftable, and there are rational arcs γ_1, γ_2 on $\tilde{V}$, defined over k and transversal at p. Suppose that p is liftable and that for every point P in the inverse image of p in $V(K)$ there are rational arcs Γ_1, Γ_2 defined over K, passing through P and such that the reduction $\bmod \mathfrak{p}$ of each Γ_i is γ_i. Then p is densely liftable.* □

Corollary *Suppose that p is nonsingular on $\tilde{V}(k)$ and that the tangent to $\tilde{V}$ at p meets $\tilde{V}$ in a curve γ, not necessarily irreducible, which has an ordinary double point at p. Suppose further that the two tangent directions to γ at p are each defined over k. Then p is densely liftable.*

Proof. Denote by γ_1, γ_2 the two branches of γ at p. In the notation of the Lemma, we can only lift γ_1 and γ_2 over $K_\mathfrak{p}$, because if Γ is the intersection of V with the tangent to V at P then the two points above P on the desingularization of Γ are defined over $K_\mathfrak{p}$ by Hensel's Lemma but need not be defined over K. Denote the branches of Γ by Γ_1 and Γ_2. If P_1^* is a point of $\Gamma_1(K_\mathfrak{p})$ then we can construct P_1 in $\Gamma(K)$ and arbitrarily close to P_1^* by approximating to the line PP_1^* by a line Λ through P and in the plane of Γ, and taking P to be the third intersection of Λ with Γ. (The modification of this argument needed if Γ_1 is a line is obvious.) This is all we need for the successive approximation construction which underlies the proofs of Theorems 3 and 4 to work. □

Lemma 11 *Let $\mathcal{C}_1, \mathcal{C}_2$ be R-equivalence classes in $V(K)$; then their closures in $V(K_\mathfrak{p})$ are either disjoint or identical.*

Proof. It is enough to show that if P^* in $V(K_\mathfrak{p})$ is in the closure of both $\mathcal{C}_1$ and $\mathcal{C}_2$, and Q^* in $V(K_\mathfrak{p})$ is in the closure of $\mathcal{C}_1$, then Q^* is in the closure of $\mathcal{C}_2$. By Lemma 6 we can choose R in $V(K)$ so that neither of RP^* and S^*Q^* lies in or touches V, where S^* in $V(K_\mathfrak{p})$ is the third intersection of RP^* with V. Let the third intersection of S^*Q^* with V be T^* in $V(K_\mathfrak{p})$.

Now let P_1 in $\mathcal{C}_1$ and P_2 in $\mathcal{C}_2$ be arbitrarily close to P^*, and for $i = 1, 2$ let P_iR meet V again in S_i; thus S_i is arbitrarily close to S^* and the class of S_i is $\mathcal{C} \circ \mathcal{C}_i$ where $\mathcal{C}$ is the class of R. Let Q_1 in $\mathcal{C}_1$ be arbitrarily close to Q^* and let Q_1S_1 meet V again in T; thus T is in $\mathcal{C}$ and is arbitrarily close to T^*. If S_2T meets V again in Q_2 then Q_2 is in $\mathcal{C}_2$ and arbitrarily close to Q^*. $\square$

If $\mathcal{C}$ is an R-equivalence class, the closure of $\mathcal{C}$ in $V(K_\mathfrak{p})$ is a union of some of the neighbourhoods constructed in the proof of Theorem 3. This is the partition of $V(K_\mathfrak{p})$ which we claimed in the Introduction that we could construct explicitly. It will follow from Lemma 11 and the arguments of §7 that (2) is the coarser partition in which each set U_{iv} is either the closure of some R-equivalence class or the set of points of $V(K_\mathfrak{p})$ which are not in the closure of $V(K)$.

5. *The lifting process.* This and the next section are concerned with various aspects of the following question: if $\tilde{V}$ is nonsingular and $V(K)$ is not empty, in what circumstances can we lift a point of $\tilde{V}(k)$ to $V(K)$?

Lemma 12 *There is an absolute constant q_0 with the following property. Suppose that $\tilde{V}$ is not a cone and does not have a line of singularities, and that P_0 is a point of $V(K)$ such that $\widetilde{P_0}$ is nonsingular on $\tilde{V}$. If $q > q_0$ there is a point of $V(K)$ in general position on V whose reduction* mod $\mathfrak{p}$ *does not lie on any of the lines on $\tilde{V}$.*

Proof. We mimic the construction in Lemma 6. Let P_0 be the given point of $V(K)$. Choose a line ℓ_1, defined over k and passing through $\widetilde{P_0}$, which does not touch $\tilde{V}$ either at $\widetilde{P_0}$ or elsewhere and which does not meet any of the lines on $\tilde{V}$ except perhaps at $\widetilde{P_0}$. This is possible if q is large enough, for there are q^2 lines through $\widetilde{P_0}$ defined over k which do not touch $\tilde{V}$ at $\widetilde{P_0}$; of these only $O(q)$ touch $\tilde{V}$ elsewhere and only $O(q)$ meet one of the lines on $\tilde{V}$ at a point other than $\widetilde{P_0}$. Let p_1' and p_1'' be the other points where ℓ_1 meets $\tilde{V}$; they are distinct and different from $\widetilde{P_0}$, and they are either each defined over k or conjugate over k and defined over k_1, the unique quadratic extension of k. Let π' be the tangent plane to $\tilde{V}$ at p_1' and γ' its intersection with $\tilde{V}$; and define π'', γ'' similarly. By the conditions above, γ' and γ'' are absolutely irreducible; they are also distinct, as are π' and π'', because π' is transversal to ℓ_1. Moreover, $\widetilde{P_0}$ does not lie on π' or π''.

Lift ℓ_1 to a line L_1 containing P_0 and defined over K. Let P_1', P_1'' be the other two intersections of L_1 with V; at worst they are defined over a

quadratic extension K_1 of K and are conjugate over K, and by abuse of language we can say that their reductions are p_1', p_1'' respectively. (It can happen that p_1', p_1'' are defined over k but P_1', P_1'' are not defined over K; now $\mathfrak{p}$ splits in K_1 and we have to take the reductions modulo the appropriate one of its prime factors.) Let Π' be the tangent plane to V at P_1' and Γ' its intersection with V, and similarly for Π'', Γ''.

Let ℓ_2 be a line defined over k and not passing through p_1' or p_1'' nor lying on π' or π''. Let p_2', p_2'' be the intersections of ℓ_2 with π', π'' respectively and p_3', p_3'' the third intersections of $\tilde{V}$ with $p_1'p_2', p_1''p_2''$ respectively. We assume ℓ_2 so chosen that neither p_3' nor p_3'' lies on ℓ_3, the intersection of π' and π'', and that p_2' does not lie on one of the lines having triple contact with γ' at p_1' and similarly for p_2''. This is possible since q is large. We can generate in this way any pair of points p_3' on γ' and p_3'' on γ'' having the same rationality properties with respect to k as p_1' and p_1'' and distinct from p_1', p_1'' respectively and from the points where $\tilde{V}$ meets ℓ_3. We call these pairs p_3', p_3'' *allowable*. The line $p_3'p_3''$ is defined over k and hence so is p_4, the point where it meets $\tilde{V}$ again.

There are only $O(q)$ allowable pairs p_3', p_3'' for which $p_4 = \widetilde{P_0}$, because there are only $O(q)$ lines defined over k which meet γ' and contain $\widetilde{P_0}$. Also p_4 can never be p_1', p_1'' or one of the points at which ℓ_3 meets $\tilde{V}$. I claim that any other point p_4 is generated by at most six allowable pairs. If p_4 is for example on π' then we need p_3' to be p_4 and p_3'' to be one of the three points at which the tangent plane to $\tilde{V}$ at p_4 meets γ''; so assume that p_4 is on neither π' nor π''. Let γ^* be the projection of γ'' from p_4 onto π'; γ^* is different from γ' because the unique singularity of γ'' at p_1'' does not project onto the unique singularity of γ' at p_1'. Hence γ^* and γ' have at most six intersections outside ℓ_3; and these are the only points p_3' which can give rise to p_4. But we have $q^2 - O(q)$ allowable pairs p_3', p_3''; so we generate at least $\frac{1}{6}q^2 - O(q)$ distinct p_4. Hence if $q > q_0$ we can ensure that p_4 does not lie on any of the lines of $\tilde{V}$. Now lift ℓ_2 to any line L_2 defined over K. Let P_2' be the intersection of L_2 with Π' and let P_3' be the third intersection of $P_1'P_2'$ with V; and similarly for P_2'', P_3''. Let Γ' be the intersection of Π' with V, and similarly for Γ''; then $P_3' \times P_3''$ is in general position on $\Gamma' \times \Gamma''$. If P_4 is the third intersection of $P_3'P_3''$ with V, then it is defined over K and is a lift of p_4. An argument like that earlier in this paragraph shows that any point P_4 other than P_0 comes from at most six pairs P_3', P_3''; so P_4 is in general position on V. Here of course the Zariski open set in which P_4 is required to

lie can depend on q. $\square$

Theorem 5 *With the notation of* §1, *if* $\tilde{V}$ *is nonsingular and* $V(K)$ *is not empty then every point of* $\tilde{V}(k)$ *can be lifted to a point of* $V(K)$.

Proof. Let K^* be a large enough extension of K in which $\mathfrak{p}$ remains prime, let k^* be the corresponding residue field mod $\mathfrak{p}$ and let q^* be the number of elements of k^*. The first step is to show that every point of $\tilde{V}(k^*)$ can be lifted to a point of $V(K^*)$ — in other words, that the Theorem holds if q is large enough. Let P be the given point of $V(K)$; after Lemma 12 we can assume that $\tilde{P}$ does not lie on any of the lines on $\tilde{V}$. Now take $W = \tilde{V}$ and $p_0 = \tilde{P}$ in Lemma 7; to say that p_1 is in general position on W is simply to say that it lies outside a certain proper subvariety W_1 of W. Since W_1 is independent of the choice of K^*, we can find a point p_1 in $W(k^*)$ but outside W_1. Let Z, ϕ, γ_0 be as in the proof of Lemma 7. Then $Z(p_1)$ is an absolutely irreducible curve of bounded genus, defined over k^*, and hence it contains a point $q_2 \times q_3 \times p_4$ defined over k^* with p_4 not on γ_0. Since q_3 is not determined by p_1, we can assume that it is not on one of the lines of $\tilde{V}$. By Lemma 9 $\phi(q_2)$ and $\phi(q_3)$ can be lifted to $V(K^*)$, and hence the same is true of p_4 because it lies on the tangent to $\tilde{V}$ at $\phi(q_3)$; and since $p_1, \phi(q_3), p_4$ are collinear points on $\tilde{V}$, this implies that we can lift p_1 also.

To come down from K^* to K, choose a sequence of quadratic extensions

$$K = K_0 \subset K_1 \subset K_2 \subset \dots$$

in all of which $\mathfrak{p}$ remains prime, and let

$$k = k_0 \subset k_1 \subset k_2 \subset \dots$$

be the corresponding sequence of residue fields mod $\mathfrak{p}$. By the previous paragraph, for large enough n every point of $\tilde{V}(k_n)$ can be lifted to a point of $V(K_n)$. Suppose that this holds for $n = N + 1$; we proceed by downward induction, asking what are the obstacles for deducing it for $n = N$. This descent argument will involve a substantial number of cases, according to the rationality properties with respect to k_N of the lines on $\tilde{V}$; these cases fill all the paragraphs of the proof after this one. Write $M = 2^N$, so that k_N contains q^M elements. We are given a point P in $V(K) \subset V(K_N)$; let γ_0 be the intersection of $\tilde{V}$ with the tangent plane to $\tilde{V}$ at $\tilde{P}$. By Lemma 9 every point of $\gamma_0(k_N)$, including the singular point $\tilde{P}$, can be lifted to $V(K_N)$.

Suppose first that there is a line ℓ on $\tilde{V}$ which is defined over k_N; either it is contained in γ_0 or it meets γ_0 in a point defined over k_N and therefore liftable to $V(K_N)$. Using the Corollary to Lemma 9 we see that in either case every point of $\ell(k_N)$ can be lifted to $V(K_N)$.

Next suppose that $\tilde{V}$ contains a pair of skew lines defined, as a pair, over k_N and let p_1 be a point of $\tilde{V}(k_N)$ not lying on either line. Let p_2', p_2'' be the two points at which the unique transversal through p_1 to the two lines meets them. If each of p_2', p_2'' is defined over k_N we can lift them to points P_2', P_2'' of $V(K_N)$ because each of them lies on a line on $\tilde{V}$ defined over k_N; if not, they are defined over k_{N+1} and conjugate over k_N; so we can lift p_2' to a point P_2' of $V(K_{N+1})$ and p_2'' to its conjugate P_2'' over K_N. In either case the line $P_2'P_2''$ is defined over K_N and its third intersection with V is a lift of p_1 to $V(K_N)$. Hence in this case we can lift any point of $\tilde{V}(k_N)$.

Henceforth we can assume that $\tilde{V}$ does not contain such a pair of skew lines. Suppose that p_1 is a point of $\tilde{V}(k_N)$ and let ℓ_1 be a line through p_1, defined over k_N and not touching $\tilde{V}$ at p_1. There are three possibilities for the other intersections of ℓ_1 with $\tilde{V}$:

(i) a point p_2 defined over k_N, counted twice;

(ii) two points p_2 and p_3, each defined over k_N;

(iii) two points p_2', p_2'' conjugate over k_N and defined over k_{N+1}.

Much as above, in case (iii) we can lift p_2', p_2'' to points of $V(K_{N+1})$ conjugate over K_N and thus lift p_1 to a point of $V(K_N)$. Similarly if we can lift p_2, p_3 in case (ii), or p_2 in case (i), to $V(K_N)$ then the same is true for p_1; in case (i) this uses Lemma 9. Hence if p_1 cannot be lifted then on each of the q^{2M} lines ℓ_1 there is another point of $\tilde{V}(k_N)$ which cannot be lifted; in particular, if there are any points of $\tilde{V}(k_N)$ which cannot be lifted, there are at least $q^{2M}+1$ of them.

Suppose first that $\tilde{V}$ contains three coplanar lines each defined over k_N; these lines contain at least $3q^M$ points of $\tilde{V}(k_N)$ all of which are liftable. If there are also unliftable points it follows from the tables in Swinnerton-Dyer [4], partly repeated in Manin [3], pp 176-7, that we are in case C_4 and there are no liftable points outside these three lines. But let p be a point of $\tilde{V}(k_N)$ lying on just one of these lines; p cannot be an Eckardt point because the tables show that there are no more lines of $\tilde{V}$ defined over k_{N+1}. So the tangent plane to $\tilde{V}$ at p meets $\tilde{V}$ again in an irreducible curve, and this

contains at least one point of $\tilde{V}(k_N)$ which is liftable by Lemma 9 and does not lie on any of the three lines. This is a contradiction.

Suppose next that $\tilde{V}$ contains just one line ℓ defined over k_N and does contain unliftable points. Now $\tilde{V}(k_N)$ must contain at least $q^{2M}+q^M+2$ points, so the tables show that we must be in case C_{24}. As in the previous paragraph, no point of $\ell(k_N)$ can be Eckardt; so if p is any point of $\ell(k_N)$ the tangent plane to $\tilde{V}$ at p meets $\tilde{V}$ again in an irreducible conic, which contains at least q^M+1 liftable points. Since there are at least $\frac{1}{2}(q^M+1)$ distinct such conics, no two of which have a point in common, there are at least $\frac{1}{2}(q^M+1)^2$ liftable points on $\tilde{V}$. Counting the total number of points on $\tilde{V}(k_N)$ we obtain

$$q^{2M}+1+\tfrac{1}{2}(q^M+1)^2 \leq q^{2M}+2q^M+1$$

which is impossible.

Henceforth we can assume that $\tilde{V}$ contains no lines defined over k_N; it now follows from the table that the total number of points on $\tilde{V}(k_N)$ is

$$q^{2M}+rq^M+1 \quad \text{with} \quad r \leq 2. \tag{26}$$

Suppose that $\tilde{V}(k_N)$ contains R unliftable points of which E are Eckardt. If p is an unliftable Eckardt point then there are no other points of $\tilde{V}(k_N)$ on the tangent plane to $\tilde{V}$ at p, and every line through p defined over k_N and not in the tangent plane contains one or two more points of $\tilde{V}(k_N)$; moreover, every point of $\tilde{V}(k_N)$ other than p lies on one such line. Hence there are exactly $q^{2M}-rq^M$ such lines which touch $\tilde{V}$ at a point $p_1 \neq p$, and each such p_1 is an unliftable point of $\tilde{V}(k_N)$. Similarly, if p is unliftable but not Eckardt the number of other points of $\tilde{V}(k_N)$ on the tangent plane to $\tilde{V}$ at p is $q^M+\epsilon_p$ where $\epsilon_p = 0$ or ± 1; so the number of points p_1 as above is

$$q^{2M}-(r-1)q^M+\epsilon_p.$$

It follows that the number of pairs p, p_1 with p and p_1 distinct and unliftable and p in the tangent plane to $\tilde{V}$ at p_1 is

$$R(q^{2M}-rq^M)+(R-E)q^M+\sum \epsilon_p.$$

On the other hand, the number of pairs p, p_1 with p and p_1 distinct, p in the tangent plane to $\tilde{V}$ at p_1 and p_1 unliftable is

$$(R-E)q^M+\sum \epsilon_{p_1}.$$

Since the second of these numbers cannot be less than the first, we have $R(q^M - r) \leq 0$; so we can only have $R > 0$ if $q^M = r = 2$. But any $\tilde{V}$ with $q^M = r = 2$ which contains no lines defined over k must be in case C_{12} of [4] and therefore has a triple of conjugate coplanar lines. Since $\mathbf{P}^3(k)$ contains only 8 points outside the plane of these lines and $\tilde{V}(k)$ contains 9 points, these lines must meet in an Eckardt point. It follows that $\tilde{V}$ is

$$X_3(X_0^2 + X_1^2 + X_1X_2 + X_2^2) + X_0X_3^2 + X_1^3 + X_1X_2^2 + X_2^3 = 0.$$

However, the methods which we have already used are enough to show that if one point defined over k_N on this surface is liftable then all of them are. (If the point known to be liftable is the Eckardt point $(1, 0, 0, 0)$ then we have to use the construction in the proof of Lemma 12.) Thus there is no obstruction to the downward induction. □

Corollary *Let $\mathcal{C}$ be a given R-equivalence class in $V(K)$; then under the conditions of the Theorem every point of $\tilde{V}(k)$ can be lifted to $\mathcal{C}$.*

Proof. It is enough to show that there is some class $\mathcal{C}_0$ to which every point of $\tilde{V}(k)$ can be lifted. For let P_1 be a point of $\mathcal{C} \circ \mathcal{C}_0$ and p any point of $\tilde{V}(k)$. If Q is a lift of $p \circ \widetilde{P_1}$ to $\mathcal{C}_0$ then $Q \circ P_1$ is a lift of p to $\mathcal{C}$. We use this idea at each stage of the argument.

In the first part of the proof of the Theorem, for which q^* is large, we exhibited a birational map $\psi : \mathbf{P}^4 \to V$ defined over K^* such that $\psi(V)$ contains lifts of every point of $\tilde{V}(k^*)$. Since all points of $\psi(V)$ are in the same R-equivalence class, this proves the Corollary in this case.

Now let P_2 be a point of $V(K_N)$ and let $\mathcal{C}_2$ be its class as a point of $V(K_{N+1})$. If P', P'' are points of $V(K_{N+1})$ conjugate over K_N and such that P' is in $\mathcal{C}_2$, then by taking conjugates in the linkage between P_2 and P' it follows that P'' is also in $\mathcal{C}_2$. If P in $V(K_N)$ is the third intersection of $P'P''$ with V, then the class $\mathcal{C}_0$ of P in $V(K_N)$ depends only on $\mathcal{C}_2$. (The special cases when $P' \circ P''$ is not singlevalued are not straightforward. But let Γ' be a rational curve defined over K_{N+1} and Γ'' its conjugate over K_N. We can take Q' generic on Γ' over K_{N+1} and therefore defined over a field $K_{N+1} \otimes K_N(s, t)$ where s, t are independent transcendentals over K_N. Let Q'' be the conjugate of Q' over $K_N(s, t)$; then the locus of $Q' \circ Q''$ over K_N is an image of $\mathbf{P}^2$ and there is a value of $P' \circ P''$ in this image. Now we can appeal to Lemma 9.) Replacing P_2 by $P_2 \circ P_2$ and using (1) we can assume that $\mathcal{C}_2 \circ \mathcal{C}_2 = \mathcal{C}_2$; thus some point of $V(K_N)$ in $\mathcal{C}_0$ (and therefore every such point) is in $\mathcal{C}_2$ when

considered as a point of $V(K_{N+1})$. Now the induction argument still works if instead of the set of liftable points of $\tilde{V}(k_N)$ we consider the set of points of $\tilde{V}(k_N)$ liftable to $\mathcal{C}_0$. □

6. *The dense lifting process.* Throughout this section, we assume that $\tilde{V}$ is nonsingular and $V(K)$ is not empty. Everything will be defined over k unless otherwise specified. We shall repeatedly use the fact that the order of $\tilde{V}(k)$ is congruent to 1 mod q. This holds because the characteristic roots of Frobenius in middle dimension are in this case q times roots of unity. Alternatively one may consult the tables in [4] or [3] already cited.

Theorem 5 shows that every point of $\tilde{V}(k)$ is liftable; the object of this section is to show that, with an explicit list of possible exceptions, every point of $\tilde{V}(k)$ is densely liftable. With the possible exception of (42), it follows from the Remark at the end of §5 that if one point of $\tilde{V}(k)$ is densely liftable, then for any prescribed R-equivalence class $\mathcal{C}$ every point of $\tilde{V}(k)$ is densely liftable to $\mathcal{C}$. There is a major bifurcation of the argument, according to whether $\tilde{V}$ contains a line defined over k or not. Until further notice, we suppose that $\tilde{V}$ contains at least one line defined over k.

Suppose first that there is a plane π_0 which meets $\tilde{V}$ in three lines ℓ_1, ℓ_2, ℓ_3 each defined over k (and distinct because $\tilde{V}$ is nonsingular) and that these lines do not meet in an Eckardt point. There are exactly $3q$ points of $\tilde{V}(k)$ on π_0; but the total number of points in $\tilde{V}(k)$ is congruent to 1 mod q, so there is at least one such point p not on π_0. The tangent to $\tilde{V}$ at p cannot pass through all three points like p_{ij} at which ℓ_i, ℓ_j meet; suppose it does not pass through p_{12}. By Theorem 4(i) and the Corollary to Lemma 9, both p_{12} and p are densely liftable. Henceforth we can assume that this configuration does not occur.

Suppose next that there is a plane π_0 which meets $\tilde{V}$ in three lines ℓ_1, ℓ_2, ℓ_3 each defined over k and all meeting in an Eckardt point p_0. It was shown in the proof of Lemma 5 that there are at most 5 planes through ℓ_1 which meet $\tilde{V}$ in a union of lines. If there is a plane π_1 through ℓ_1 and defined over k which meets $\tilde{V}$ residually in an irreducible conic γ_1 (which certainly happens if $q > 4$), then we can usually find a point p' on γ_1 but not on ℓ_1 such that the tangent to γ_1 at p' does not pass through p_0. Indeed this can only fail if $q = 3$; for there are 0 or 2 points of $\gamma_1(k)$ at which the tangent to γ_1 passes through p_0, and 0 or 2 other points of $\ell_1 \cap \gamma_1(k)$. By Theorem 4(i) and the Corollary to Lemma 9, p_0 and p' are densely liftable. By the remark after the proof of Theorem 4, any point of $\pi_0 \cap \tilde{V}(k)$ not on the tangent to $\tilde{V}$ at

p' is densely liftable; and clearly there are such points on at least two of the lines ℓ_i.

We must still identify those $\tilde{V}$ for which the argument fails. Take coordinates so that p_0 is $(1,0,0,0)$, π_0 is $X_3 = 0$ and the ℓ_i are $X_2 = 0$, $X_1 = 0$ and $X_1 + X_2 = 0$ respectively. The equation of $\tilde{V}$ has the form

$$X_1X_2(X_1 + X_2) + X_3Q(X_0, \ldots, X_3) = 0 \tag{27}$$

where the coefficient of X_0^2 in Q is nonzero. There are two reasons why the argument of the previous paragraph might break down: because there is no suitable π_1 or because there is no suitable p'. Suppose first that there is no suitable π_1. Let p_1 be a point of $\ell_1(k)$ other than p_0. Because we have ruled out the previous case, p_1 must be Eckardt; so by Lemma 4 $q = 2$ or 4. If $q = 4$ the proof of Lemma 4 shows that $\tilde{V}$ has the form

$$\begin{aligned} X_3(c_0X_0^2 + c_0^2X_0X_3 + e_0X_3^2) + X_2(c_1X_1^2 + c_1^2X_1X_2 + e_1X_2^2) \\ + X_2X_3L(X_2, X_3) = 0. \end{aligned}$$

But it must also have the corresponding form with X_1 and X_2 interchanged, as well as having the form (27); so it must actually have the form

$$X_1X_2(X_1 + X_2) + X_3(c_0X_0^2 + c_0^2X_0X_3 + e_0X_3^2) = 0.$$

If the last factor on the left splits, then we can use the argument of the previous paragraph, taking for p' any point with $X_2 = 0$, $X_3 \neq 0$. If it does not split, then after writing $c_0^{-1}X_3$ for X_3 we are reduced to the two surfaces

$$X_1X_2(X_1 + X_2) + X_3(X_0^2 + X_0X_3 + \omega X_3^2) = 0 \quad (\omega^2 + \omega + 1 = 0) \tag{28}$$

over $\mathbf{F}_4$. If $q = 2$ the proof of Lemma 4 shows that $\tilde{V}$ has the form

$$X_0X_3(X_0 + X_3) + X_1X_2(X_1 + X_2) + bX_2X_3(X_0 + X_1) + C(X_2, X_3) = 0.$$

But it must also have the corresponding form with X_1, X_2 interchanged; so $b = 0$ and $C(X_2, X_3)$ is simply a multiple of X_3^3. Using an argument like that just before (28), we are reduced to the surface

$$X_1X_2(X_1 + X_2) + X_3(X_0^2 + X_0X_3 + X_3^2) = 0. \tag{29}$$

over $\mathbf{F}_2$. Suppose instead that γ_1 exists but contains no suitable p'; thus $q = 3$. We have excluded the previous case, and if γ_1 touches ℓ_1 then the

argument above shows that a suitable p' exists. So the argument can only fail if one of the 3 points of ℓ_1 other than p_0 is Eckardt and γ_1 is a conic through the remaining two points of $\ell_1(k)$. Moreover, the remaining plane through ℓ_1 must meet $\tilde{V}$ residually in a pair of lines not individually defined over k; for if it met $\tilde{V}$ in an irreducible conic that conic would contain a point which could serve as p'. Thus in particular there must be just three points of $\tilde{V}(k)$ outside π_0. Much as before, $\tilde{V}$ must have the form (6) and also the corresponding form with the roles of X_1 and X_2 interchanged; and it must also have the form (27). Thus it can be written

$$X_1X_2(X_1+X_2)+X_3Q_0(X_0,X_3)+bX_1X_2X_3=0.$$

But it also needs to have a second Eckardt point on $X_1+X_2=X_3=0$, so $b=0$. Thus $\tilde{V}$ can only be

$$X_1X_2(X_1+X_2)+X_3(X_0^2+X_3^2)=0;$$

and this is not a counterexample because we can take $p'=(1,1,1,2)$.

Suppose next that $\tilde{V}$ contains two skew lines ℓ_1,ℓ_2 each defined over k. These account for $2q+2$ points of $\tilde{V}(k)$; since the order of $\tilde{V}(k)$ is congruent to 1 mod q, there must be such points not on ℓ_1 or ℓ_2. Let p be one of them, and let the unique transversal through p to ℓ_1 and ℓ_2 meet these lines in p_1 and p_2 respectively. By Lemma 9 we can lift each p_i to a point P_i of $V(K)$ and each ℓ_i to an arc Γ_i of genus 0 through P_i. Let P be the third intersection of P_1P_2 with V, and let Γ_2' be the residual intersection of V with the cone of base γ_2 and vertex P. Apply Theorem 4(i) to the curves Γ_1,Γ_2' and the line PP_2 through P_1; thus P,P_1,P_2 are all densely liftable.

We now suppose that $\tilde{V}$ contains a line ℓ defined over k, but does not contain any of the configurations discussed above. Let p be a point of ℓ such that the tangent to $\tilde{V}$ at p meets $\tilde{V}$ in ℓ and an irreducible conic γ which meets ℓ in two distinct points p and p'. By the Corollary to Lemma 10, p and p' are densely liftable. This argument only fails if for every p_1 of $\tilde{V}(k)$ outside $\ell\cup\gamma$ the tangent at p_1 to $\tilde{V}$ contains ℓ. This implies that any point p_0 on ℓ other than p or p' must be Eckardt; so $q=2,3$ or 4. Moreover, we have now accounted for all $q+1$ planes through ℓ, so $\tilde{V}(k)$ contains just one point outside $\ell\cup\gamma$. The tables already cited show that this cannot happen for $q=4$. Now take ℓ to be $X_2=X_3=0$, p and p' to be $(1,0,0,0)$ and $(0,1,0,0)$, the unique point p_1 of $\tilde{V}(k)$ outside $\ell\cup\gamma$ to be $(0,0,0,1)$ and γ to be $X_3=0$, $X_0X_1+X_2^2=0$; thus $\tilde{V}$ has the form

$$X_2(X_0X_1+X_2^2)+cX_2X_3^2+X_3Q(X_0,X_1,X_2)=0,$$

where $Q(X_0, X_1, 0)$ is irreducible over k. Direct calculation now yields the following two possibilities:

$$X_2(X_0X_1 + X_2^2) + X_3(X_0^2 + X_0X_1 + X_1^2) + X_2X_3(X_0 + X_1 + X_2 + X_3) = 0 \tag{30}$$

over $\mathbf{F}_2$, and

$$X_2(X_0X_1 + X_2^2) + X_3(X_0^2 + X_1^2 + X_2^2 - X_2X_3) = 0 \tag{31}$$

over $\mathbf{F}_3$.

Still supposing that $\tilde{V}$ contains a line ℓ defined over k, we can now assume that if p is any point of $\ell(k)$ then either p is Eckardt or the tangent to $\tilde{V}$ at p meets $\tilde{V}$ residually in an irreducible conic γ which touches ℓ. Thus the tangent planes at the $q+1$ points of $\ell(k)$ are distinct and therefore exhaust the planes through ℓ. Take coordinates so that the line ℓ is $X_2 = X_3 = 0$; thus $\tilde{V}$ has the form

$$X_2Q_2(X_0, X_1, X_2) + X_3Q_3(X_0, X_1, X_3) + X_2X_3L(X_0, \ldots, X_3) = 0.$$

By considering the tangent planes at the points of ℓ, we see that each equation

$$\lambda Q_2(X_0, X_1, 0) + \mu Q_3(X_0, X_1, 0) = 0$$

(with λ, μ in k and not both zero) has exactly one root. Hence $\mathrm{char}(k) = 2$ and Q_2, Q_3 have no terms in X_0X_1. Suppose there are points p_1, p_2 on ℓ such that the residual intersection of $\tilde{V}$ with the tangent to $\tilde{V}$ at p_i is an irreducible conic γ_i; and suppose further that there are points r_i on γ_i but not on ℓ such that r_1r_2 does not touch $\tilde{V}$ and the tangents to γ_1 at r_1 and to γ_2 at r_2 do not meet. (All this is certainly possible if $q \geq 8$. For we can find p_1, p_2 because there are at most 5 Eckardt points on ℓ; and there are at most $4q$ pairs r_1, r_2 which fail the first condition and none which fail the second.) Denote by r_0 the third intersection of r_1r_2 with $\tilde{V}$ and by γ_0 the residual intersection of $\tilde{V}$ with the cone of base γ_2 and vertex r_0. By Lemma 9 each γ_i is liftable at r_i and hence γ_0 is also liftable at r_1. Hence by Theorem 4(i) r_1 and r_2 are densely liftable.

We must still find the $\tilde{V}$ for which this argument fails. We know already that $q = 2$ or 4. The first possibility is that all the points of $\ell(k)$ are Eckardt and that there are no points of $\tilde{V}(k)$ outside ℓ. The tables already cited show

that this cannot happen for $q = 4$; for $q = 2$ calculations based on the proof of Lemma 4 show that $\tilde{V}$ must be

$$X_0X_3(X_0 + X_3) + X_1X_2(X_1 + X_2) + X_2^3 + X_2^2X_3 + X_3^3 = 0 \qquad (32)$$

over $\mathbf{F}_2$. Again, if $q = 4$ the proof of Lemma 4 shows that $\ell(k)$ cannot contain exactly 4 Eckardt points; but a calculation starting from (6) shows that $\ell(k)$ can have exactly 2 Eckardt points if $\tilde{V}$ is

$$X_3(X_0^2 + X_0X_3 + X_3^2) + X_2(X_1^2 + X_1X_2 + X_2^2) + X_0X_2X_3 = 0 \qquad (33)$$

over $\mathbf{F}_2$. Leaving these two cases aside, after a change of coordinates we can take p_1 to be $(1, 0, 0, 0)$ with tangent $X_3 = 0$ and p_2 to be $(0, 1, 0, 0)$ with tangent $X_2 = 0$; and by a further change of coordinates we can reduce $\tilde{V}$ to the form

$$c_2X_2(X_1^2 + X_0X_2) + c_3(X_0^2 + X_1X_3) + X_2X_3L(X_0, \ldots, X_4) = 0$$

where c_2, c_3 are nonzero. Straightforward calculation shows that for $q = 2$ the argument fails only for the two surfaces

$$X_2(X_1^2 + X_0X_2) + X_3(X_0^2 + X_1X_3)X_2X_3^2 = 0, \qquad (34)$$
$$X_2(X_1^2 + X_0X_2) + X_3(X_0^2 + X_1X_3)X_2X_3(X_0 + X_1 + X_3) = 0, \qquad (35)$$

in both cases over $\mathbf{F}_2$. But if $q = 4$ there are no cases when the argument fails.

Now we can assume that $\tilde{V}$ contains no lines defined over k. Thus if p is in $\tilde{V}(k)$ and not Eckardt, the tangent to $\tilde{V}$ at p meets $\tilde{V}$ in an irreducible cubic γ. Suppose first that there is a point p such that γ has an ordinary double point with tangent directions defined over k. By the Corollary to Lemma 10, p is densely liftable. Thus henceforth we can assume there is no such point p.

Suppose however that there is a point p such that γ has a cusp or an ordinary double point at which the tangent directions are not defined over k. Let p_1 be any other point of $\gamma(k)$ and denote by γ_1 the intersection of $\tilde{V}$ with the tangent to $\tilde{V}$ at p_1; then the third intersection p_2 of γ and γ_1 is also the third intersection of γ with the tangent to γ at p_1. Take coordinates so that p is $(1, 0, 0, 0)$ and the plane of γ is $X_3 = 0$; then γ has the form

$$X_0Q(X_1, X_2) + C(X_1, X_2) = 0, \qquad (36)$$

and the general point on it is $(-C(\lambda,\mu), \lambda Q(\lambda,\mu), \mu Q(\lambda,\mu))$. In particular the three points given by (λ_i, μ_i) for $i = 1, 2, 3$ are collinear if and only if the determinant whose i^{th} row is

$$-C(\lambda_i,\mu_i) \quad \lambda_i Q(\lambda_i,\mu_i) \quad \mu_i Q(\lambda_i,\mu_i)$$

vanishes. Write $C = a_0X_1^3 + \ldots + a_3X_2^3$. If p is an ordinary double point, by working over $\mathbf{F}_{q^2}$ we can take $Q = X_1X_2$ and now the collinearity condition becomes

$$a_0\lambda_1\lambda_2\lambda_3 + a_3\mu_1\mu_2\mu_3 = 0;$$

here a_0, a_3 are nonzero because (36) is nonsingular. In particular there are at most 3 points at which the tangent has triple contact with γ. But if γ has a cusp we can take $Q = X_2^2$ and now the collinearity condition becomes

$$a_0(\lambda_1\mu_2\mu_3 + \lambda_2\mu_1\mu_3 + \lambda_3\mu_1\mu_2) + a_1\mu_1\mu_2\mu_3 = 0,$$

where $a_0 \neq 0$ because (36) is nonsingular, and where $\mu = 0$ corresponds to p. There is just one point of triple contact when $\mathrm{char}(k) \neq 3$; when $\mathrm{char}(k) = 3$ there are no points of triple contact when $a_1 \neq 0$ and every point is a point of triple contact when $a_1 = 0$. Also if $\mathrm{char}(k) = 2$ all tangents meet γ again in the same point, given by $a_0\lambda = a_1\mu$.

Suppose in the notation of the previous paragraph that we can choose p_1 so that $p_2 \neq p_1$; this is certainly possible unless $q = 2$ or $\mathrm{char}(k) = 3$ and γ has a cusp. Then γ and γ_1 are transversal at p_2. If also there is a line through p_2 which meets $\tilde{V}$ at three distinct points, then p_2 is densely liftable. This is certainly possible, using a line in the plane of γ, unless $q < 4$ or $\mathrm{char}(k) = 2$ and γ has a cusp; for there are at most 4 points $p_3 \neq p_2$ on γ such that p_2p_3 touches γ, and at most 3 such points if $q = 4$.

We have still to list the $\tilde{V}$ for which this argument fails. Take coordinates such that p is $(1,0,0,0)$ and the tangent there is $X_3 = 0$. If $q = 2$ direct calculation shows that the argument only fails for

$$X_0^2X_1 + X_1^2X_2 + X_2^2X_0 + X_0X_1X_2 + X_3^3 = 0, \tag{37}$$

and

$$\begin{aligned} X_0^2X_1 + X_1^2X_2 + X_2^2X_0 + X_0X_1X_2 + X_3(X_0X_1 + X_1X_2 + X_2X_0) \\ + X_3^2(X_0 + X_1 + X_2 + X_3) = 0, \end{aligned} \tag{38}$$

with $k = \mathbf{F}_2$ in both cases. Next suppose that $q = 3$ and p is not a cusp. The two possibilities for γ are

$$X_0(X_1^2 + X_2^2) + X_1X_2(X_1 + X_2) = 0 \quad \text{or} \quad X_0(X_1^2 + X_2^2) + X_1^2X_2 = 0;$$

but in the first case we can take p_1 to be $(2, 1, 1, 0)$ and in the second case we can take it to be $(0, 0, 1, 0)$. There remains the possibility that $\mathrm{char}(k) = 2$ or 3 and every point of $\tilde{V}(k)$ is either an Eckardt point or a cusp. Suppose first that $\mathrm{char}(k) = 2$; we can take the equation of γ to be $X_0X_2^2+X_1^3+aX_1^2X_2 = 0$. Thus p_2 is $(0, a, 1, 0)$ whatever choice of p_1 we make. But now the points of $\tilde{V}$ at which the tangent passes through p_2 are the points of γ and of one other plane, and this second plane must pass through p. Because we can assume that γ_1 has a cusp at p_1, if this second plane contains a point of γ_1 then it contains the whole of γ_1. Since $q \geq 4$ it is now easy to see that there is a point p_3 of $\tilde{V}(k)$ not in either of these planes nor in the tangent at p_2; and p_2p_3 is the line through p_2 which we need to complete the proof. Finally suppose that $\mathrm{char}(k) = 3$ and that the equation of γ is $X_0X_2^2 + X_1^3 = 0$; thus $p_2 = p_1$ whatever p_1 we choose. Now $\tilde{V}$ has the form

$$X_0X_2^2 + X_1^3 + X_3Q(X_0, X_1, X_2) + X_3^2L(X_0, \ldots, X_3) = 0,$$

where the coefficient of X_0^2 in Q is nonzero and can be made 1 by rescaling. The coefficients of X_0X_2 and X_2^2 in Q can be reduced to 0 by adding suitable multiples of X_3 to X_0, X_2. The condition that $(\lambda^3, -\lambda, 1)$ is a cusp for every λ is equivalent to $Q = X_0^2 + aX_0X_1 - aX_1^2$ for some a. Applying the same argument with $(0, 0, 1, 0)$ in place of p gives $a = 0$ because the equation of $\tilde{V}$ cannot contain a term in $X_1^2X_3$, and also shows that L is simply a multiple of X_2. Rescaling and using the uniqueness of cube roots, we find that $\tilde{V}$ must be

$$X_0X_2^2 + X_2X_3^2 + X_3X_0^2 + X_1^3 = 0.$$

But this has a singular point at $(1, 0, 1, 1)$.

It only remains to find those $\tilde{V}$ for which every point of $\tilde{V}(k)$ is Eckardt and there are no lines on $\tilde{V}$ defined over k. Under these conditions, a line on $\tilde{V}$ cannot contain two Eckardt points defined over k, so the order of $\tilde{V}(k)$ is at most 9. Suppose first that this order is 1; then $k = 2$ and $\tilde{V}$ must be

$$\begin{aligned} X_2^3 + X_2^2X_3 + X_3^3 + X_1^2X_2 + X_1X_3^2 + X_1^3 + X_1X_2X_3 \\ + X_0(X_1^2 + X_2^2 + X_3^2) + X_0^2(X_1 + X_2 + X_3) = 0 \end{aligned} \tag{39}$$

over $\mathbf{F}_2$. Any line of $\mathbf{P}^3(k)$ through two Eckardt points meets $\tilde{V}$ in a third distinct point, and this limits the configurations of $\tilde{V}(k)$. If $\tilde{V}(k)$ has order 3 then $q = 2$ and $\tilde{V}$ must be

$$\begin{aligned} X_2^3 + X_2^2X_3 + X_3^3 + (X_0 + X_1)(X_0X_1 + X_2^2 + X_3^2) \\ + (X_2 + X_3)(X_0^2 + X_1^2) = 0 \end{aligned} \tag{40}$$

over $\mathbf{F}_2$. The next possible configuration consists of 7 coplanar points, and this can only occur when $\mathrm{char}(k) = 2$; the corresponding $\tilde{V}$ is

$$X_1^2X_2 + X_1X_2^2 + X_1^2X_3 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2 + X_0^3 = 0 \tag{41}$$

over $\mathbf{F}_2$. Finally, if the order of $\tilde{V}(k)$ is 9 then $\tilde{V}$ must be (42).

We have now achieved the objective stated in the first paragraph of this section: to show that unless $\tilde{V}$ belongs to one of a small number of exceptional cases every point of $\tilde{V}$ is densely liftable. These are in fact only exceptions to the method of proof and not to the conclusion; and for each of them the conclusion can be proved by exploiting the construction in Lemma 6. We illustrate this by considering the surface $\tilde{V}$ given by (29). Let ω in $\mathbf{F}_4$ be such that $1 + \omega + \omega^2 = 0$. The line $X_0 = X_1 = X_3$ meets $\tilde{V}$ in the three points

$$p_0 = (0, 0, 1, 0), \quad p_1' = (1, 1, \omega, 1), \quad p_1'' = (1, 1, \omega, 1).$$

The tangent to $\tilde{V}$ at p_1' is $X_0 + \omega^2X_1 + X_2 = 0$, which meets $\tilde{V}$ in the line $X_1 = X_3$ and the irreducible conic

$$C' : X_0^2 + X_0X_1 + X_0X_3 + X_1^2 + X_1X_3 + X_3^2 = 0.$$

The tangent to C' at $p_2' = (1, \omega, 0, 0)$ is $X_0 + \omega^2X_1 + X_2 = X_2 + \omega X_3 = 0$; so the plane through $p_3 = (1, 0, 0, 0)$ and this tangent, which is $X_2 + \omega X_3 = 0$, is transversal to its conjugate. Now choose any lift P_0 of p_0 to K, and any lift L of $p_1'p_1''$ to K passing through P_0. Let P_1', P_1'' be the other intersections of L with V; they are defined over a quadratic extension K_1 of K, and the prime $\mathfrak{p}$ in K is inert in K_1/K because its residue field in K is $\mathbf{F}_2$ and its residue field in K_1 contains $\mathbf{F}_4$. Let Γ' be the intersection of V with the tangent at P_1'; its reduction mod $\mathfrak{p}$ consists of a line and a conic, but the point p_2' is nonsingular on it. Now let R be any lift of p_3 to $K_\mathfrak{p}$; by the geometric form of Hensel's Lemma and the transversality proved above, there is a unique

line L_1 through R which meets Γ' at a point S' whose reduction is p_2' and which meets Γ'' at a point whose reduction is p_2''. Since this line is unique, it is defined over $K_{\mathfrak{p}}$; hence S' and S'' are conjugate over $K_{\mathfrak{p}}$. Let T' be a point on Γ' defined over K_1 and arbitrarily close to S', and let T'' be its conjugate over K. Since T'' is arbitrarily close to S'', the line $T'T''$ meets V again in a point defined over K and arbitrarily close to R, and its R-equivalence class does not depend on the choice of T'. Hence p_3 is densely liftable, and the result for the other points of $\tilde{V}(k)$ follows immediately.

It now follows from the Corollary to Theorem 5 that, subject to the unproved cases listed earlier in this section, if $\mathcal{C}$ is an R-equivalence class of $V(K)$ then every point of $\tilde{V}(k)$ is densely liftable to $\mathcal{C}$. We now give an alternative proof of this result. It follows from Lemma 11 that if p in $\tilde{V}(k)$ is densely liftable to $\mathcal{C}_1$ and liftable to $\mathcal{C}_2$ then it is densely liftable to $\mathcal{C}_2$. We shall say that two points of $\tilde{V}(k)$ are *lift-equivalent* if they can be lifted to the same R-equivalence class in $V(K)$ — which is the same as saying that they can be densely lifted to the same class; and we shall say that two R-equivalence classes are *closure-equivalent* (in the v-adic topology) if their closures are the same. Clearly two points of $\tilde{V}(k)$ are lift-equivalent if and only if they can be lifted to the same closure-equivalence class.

The definition of universal equivalence was given at the end of §2. The main theorem of [5] states that, with the exception of the surface

$$X_0^3 + X_1^3 + X_2^3 + \omega X_3^3 = 0 \quad (\omega^2 + \omega + 1 = 0) \tag{42}$$

over $\mathbf{F}_4$, there is only one class for universal equivalence in $\tilde{V}(k)$ provided $\tilde{V}$ is nonsingular. Clearly two points of $\tilde{V}(k)$ which are universally equivalent are also lift-equivalent; and since there is only one universal equivalence class in $\tilde{V}(k)$, there is also only one lift-equivalence class. When $\tilde{V}$ is given by (42), it is not hard to give a direct proof that there is only one lift-equivalence class, using the construction in the proof of Lemma 6; on the other hand, the proof of R-equivalence in [5] is not obviously liftable.

7. *Adelic results.* In this section we prove Theorem 1. Let $\mathcal{B}$ consist of the places of bad reduction of V, together with the primes that divide 6. The proof of Theorem 5 and the calculations in §6, taken together, show that if $\mathfrak{p}$ is not in $\mathcal{B}$ any point of $\tilde{V}(k)$ is densely liftable to each R-equivalence class. (The reader who does not wish to rely on heavy calculations will notice that this can be proved much more simply when q is large; see the remark at the

end of §4.) If v is in $\mathcal{B}$ we define the set $U_v(\mathcal{C})$ for any R-equivalence class $\mathcal{C}$ to be the closure of $\mathcal{C}$ in $V(K_v)$ and we define U_v^* to be the complement of the closure of $V(K)$ in $V(K_v)$. By Lemma 11 the $U_v(\mathcal{C})$ as $\mathcal{C}$ varies are either disjoint or identical, and by the remarks after the proof of the Corollary to Lemma 9 there are only finitely many distinct $U_v(\mathcal{C})$ for fixed v. Hence we have defined a suitable partition (2) of $V(K_v)$.

The closure of $\mathcal{C}$ is clearly contained in the appropriate $\prod U_{iv} \times \prod V(K_v)$, so we have only to prove that the two are equal. For this it is enough to show that if $P = \prod P_v$ is in the adelic closure of $\mathcal{C}$ and we obtain P^* by replacing one P_{v_0} by a $P_{v_0}^*$ in the same U_{iv_0} or $V(K_{v_0})$, then P^* is also in the closure of $\mathcal{C}$. Fix adelic neighbourhoods $\mathcal{N} = \prod \mathcal{N}_v$ of P and $\mathcal{N}^* = \prod \mathcal{N}_v^*$ of P^*, where we can assume that $\mathcal{N}_v = \mathcal{N}_v^*$ for $v \neq v_0$, and let $\mathcal{S}$ be the finite set of places such that $\mathcal{N}_v = V(K_v)$ for v outside $\mathcal{S}$. Let $Q = \prod Q_v$ be in $\mathcal{C} \cap \mathcal{N}$. Since P_v^* is in the v-adic closure of $\mathcal{C}$, there is a point $Q_{v_0}^*$ in $\mathcal{C} \cap \mathcal{N}_{v_0}^*$; so there are finite sequences of points R_i in $\mathcal{C}$ and curves γ_i of genus 0 on V and defined over K such that

(i) $R_0 = Q_{v_0}$ and $R_n = Q_{v_0}^*$;

(ii) if $\phi_i : \mathbf{P}^1 \to \gamma_i$ is the desingularization of γ_i then R_{i-1} and R_i are both in $\phi_i(\mathbf{P}^1(K))$.

By downward induction on i we choose v_0-adic neighbourhoods $\mathcal{N}_{iv_0}$ of each R_i such that $\mathcal{N}_{nv_0} = \mathcal{N}_{v_0}^*$ and if T_i is in $\mathcal{N}_{iv_0}$ then the image of R_{i+1} under the translation of γ_{i+1} from R_i to T_i lies in $\mathcal{N}_{(i+1)v_0}$; that we can do this follows from the fact that, for fixed auxiliary points, translation is continuous in T_i and R_{i+1}. By upward induction on i, we now define a sequence of points S_i in $\mathcal{C}$ and curves γ_i' of genus 0 on V defined over K such that

(i) $S_0 = R_0$ and S_i is in $\mathcal{N}_{iv_0}$ for $i > 0$;

(ii) S_i is in $\mathcal{N}_v$ for each $v \neq v_0$;

(iii) if $\psi_i : \mathbf{P}^1 \to \gamma_i'$ is the desingularization of γ_i' then S_{i-1} and S_i are both in $\psi_i(\mathbf{P}^1(K))$.

Then S_n will be in $\mathcal{N}^*$ and Theorem 1 will be proved.

The case $i = 1$ is slightly special; we take γ_1' to be the same as γ_1 and, using weak approximation on $\mathbf{P}^1(K)$, choose S_2 in $\mathcal{N}_{2v_0}$ and in $\mathcal{N}_v$ for each $v \neq v_0$. (This last condition is trivial for v outside $\mathcal{S}$.) If $i > 1$ we can suppose

that we have already chosen S_i and γ_i' to satisfy the conditions above. Take γ_{i+1}' to be the translation of γ_{i+1} from R_i to S_i, and using weak approximation on $\mathbf{P}^1(K)$ choose S_{i+1} to be in $\mathcal{N}_{(i+1)v_0}$ and in $\mathcal{N}_v$ for each $v \neq v_0$.

8. *Surfaces* $X_1^3 + X_2^3 + X_3^3 - dX_0^3 = 0$. In this section we suppose for simplicity that $K = \mathbf{Q}$; our aim is to prove results for the special case where V is given by (3), though some of our results are more general. In (3) we can assume that d is a cube-free integer. The primes of bad reduction are those which divide $3d$; and it follows from the results of §6 that if p is not a prime of bad reduction then every point of $\tilde{V}(k)$ is densely liftable to any R-equivalence class. For any d, the surface (3) contains three obvious points such as $(0, 1, -1, 0)$; but these are all Eckardt points. Non-Eckardt points can be found by the methods of Lemma 6; the first such example was given by Ryley in 1825. The simplest non-Eckardt solution known to me is

$$(3(1 - 3d + 9d^2),\ 1 + 27d^3,\ -1 + 9d - 27d^3,\ 9d - 27d^2), \tag{43}$$

due to Richmond; see the notes to §13.6 in [1]. But in order to prove results about lifting at bad primes we make use of parametric solutions over $\mathbf{Q}_p$ generated by the construction in Lemma 6, and apply the Remark which follows that Lemma; because of the very simple form of the equation for V, this turns out to be simpler than using the methods of Theorems 3 and 4. By analogy with the notation introduced just before Lemma 8, we shall in this section denote by Ω a double power series in the variables A, B which

(i) converges whenever A, B are both integral at p,

(ii) has zero constant term,

(iii) has all its coefficients integral at p;

Ω need not be the same from one appearance to the next, even within the same equation.

If $p \neq 3$ is a prime of bad reduction for V, then $\tilde{V}$ is a cone whose base

$$\gamma :\ X_1^3 + X_2^3 + X_3^3 = 0$$

is a nonsingular cubic curve defined over $\mathbf{F}_p$; and the vertex of $\tilde{V}$ is not liftable even to $\mathbf{Q}_p$. It is now convenient to generalize the previous definition of *densely liftable*. There is a map $\Phi :\ V(\mathbf{Q}_p) \to \gamma(\mathbf{F}_p)$ obtained by forgetting

the value of X_0 and then reducing mod p. We shall say that a point r of $\gamma(\mathbf{F}_p)$ is *densely liftable* to an R-equivalence class $\mathcal{C}$ of $V(\mathbf{Q})$ if $\mathcal{C}$ is dense in $\Phi^{-1}(r)$. This definition can be extended to the general case when $\tilde{V}$ is a cone whose base is a nonsingular cubic, though it is probably only valuable when the vertex of $\tilde{V}$ is not liftable. The ideas behind the following proofs can also probably be extended to the general case, but the calculations required become considerably more tiresome.

Lemma 13 *Let V be given by (3) and let $p \neq 3$ be a prime of bad reduction for V. Let $\mathcal{C}$ be the R-equivalence class of $P = (0, 1, -1, 0)$. Then the point $(1, -1, 0)$ on γ is densely liftable to $\mathcal{C}$.*

Proof. We use the notation of Lemma 6 with $L = \mathbf{Q}_p$; the mysterious powers of 3 in the following formulae have been inserted so that the same formulae can be used in the proofs of Lemmas 15 and 16. Take ℓ to be

$$X_0 = 3A(X_1 + X_2), \quad X_3 = -(1 + pB)(X_1 + X_2)$$

where A, B are elements of $\mathbf{Z}_p$. The points P', P'' where ℓ meets V again satisfy

$$X_1X_2 = -(X_1 + X_2)^2(9dA^3 + pB + p^2B^2 + \tfrac{1}{3}p^3B^3).$$

By Hensel's Lemma this is soluble in $\mathbf{Q}_p$, so that the Remark which follows Lemma 6 is applicable. Denote the solutions by

$$X_1/X_2 = \theta \text{ or } \theta^{-1} \quad \text{where} \quad \theta = -9dA^3(1 + p\Omega) - pB(1 + p\Omega).$$

Thus we can take P' to be given by

$$P' = (-3A(1 + \theta),\ -1,\ -\theta,\ (1 + pB)(1 + \theta));$$

for P'' we simply interchange X_1 and X_2. The tangent to V at P' is

$$9dA^2(1 + \theta)^2X_0 - X_1 - \theta^2X_2 - (1 + pB)^2(1 + \theta)^2X_3 = 0. \qquad (44)$$

Choose the line $P'R'$ to be the intersection of (44) and $X_2 = \theta X_1$, so that the general point on $P'R'$ can be written

$$(-3A(1 + \theta) + s(1 + pB)^2,\ -1,\ -\theta,\ (1 + pB)(1 + \theta) + 9sdA^2)$$

for some s. Substituting into the equation for V and noting that the resulting cubic in s has $s = 0$ as a double root, we find that R' is given by

$$s = \frac{9A(1+\theta)(1+pB)^4 + 243dA^4(1+pB)(1+\theta)}{(1+pB)^6 - 729d^2A^6} = 9A(1+p\Omega).$$

In contrast, choose $P''R''$ to be the intersection of $X_0 = 3A(1+\theta)X_2$ with the tangent to V at P'', so that the general point on $P''R''$ can be written

$$(-3A(1+\theta),\ -\theta + t(1+pB)^2(1+\theta)^2,\ -1,\ (1+pB)(1+\theta) - t\theta^2)$$

for some t. Substituting into the equation for V, we find that R'' is given by

$$t = \frac{3\theta(1+pB)^4(1+\theta)^4 - 3(1+pB)(1+\theta)\theta^4}{(1+pB)^6(1+\theta)^6 - \theta^6} = 3\theta(1+p\Omega).$$

In the notation of (3) and (12), and removing a factor 3, we have

$$R = \tfrac{1}{3}\{f_2(R'', R')R'' - f_2(R', R'')R'\}.$$

But direct clculation gives

$$\begin{aligned}\tfrac{1}{3}f_2(R'', R') &= 1 + 2\theta(1+p\Omega) + 270dA^3(1+p\Omega),\\ \tfrac{1}{3}f_2(R', R'') &= 1 - \theta(1+p\Omega) + 27dA^3(1+p\Omega),\end{aligned}$$

whence

$$R = (-9A(1+p\Omega),\ 1+p\Omega,\ -1+p\Omega,\ -3\theta(1+p\Omega) - 324dA^3(1+p\Omega)). \tag{45}$$

It now follows from Hensel's Lemma that we can obtain in this way any point in $U = \Phi^{-1}((1,-1,0))$. Using the approximation process described in the Remark after Lemma 6, we obtain a set of points of $V(\mathbf{Q})$ dense in U and all belonging to the same R-equivalence class $\mathcal{C}_1$. But the closure of $\mathcal{C}_1$ contains P, which is in $\mathcal{C}$; so by Lemma 11 the closure of $\mathcal{C}$ contains U. □

Corollary *Any point of $\gamma(\mathbf{F}_p)$ which is liftable to V is densely liftable to V.*

Proof. Let R be a point of $V(\mathbf{Q})$; we have to show that $\Phi(R)$ is densely liftable. We can assume that $\Phi(R)$ is not one of the three points like $(1,-1,0)$.

Because $d \neq 1$ or 3, the tangent to γ at $\Phi(R)$ cannot pass through all these three points; so we can assume that it does not pass through $(1,-1,0)$. Let R_2 be the third intersection of V with the join of R and $(0,1,-1,0)$. We have ensured that $\Phi(R_2)$ is neither $\Phi(R)$ nor $(1,-1,0)$. Now let S be any point of $\mathcal{C} \cap \Phi^{-1}((1,-1,0))$ where $\mathcal{C}$ is as in the Lemma, and let S' be the third intersection of V with SR_2; the points S' obtained in this way are dense in $\Phi^{-1}(R)$ and they all lie in $\mathcal{C} \circ \mathcal{C}_2$ where $\mathcal{C}_2$ is the class of R_2. □

If p is large, we still appear to need a large number of R-equivalence classes — indeed potentially one for each point of $\gamma(\mathbf{F}_p)$. But this is not so, as the following result shows.

Lemma 14 *Let V be given by* (3) *and let $p \neq 3$ be a prime of bad reduction for V. Let G be the group of linear equivalence classes of divisors on γ of the form $3s - \mathfrak{b}$ for some s in $\gamma(\mathbf{F}_p)$, where $\mathfrak{b}$ is the divisor of a linear section of γ. Let P be any point of $V(\mathbf{Q})$ and p_1 any point of $\gamma(\mathbf{F}_p)$ such that $p_1 - \Phi(P)$ is in G. Then p_1 is liftable (and hence densely liftable) to the class of P in $V(\mathbf{Q})$.*

Proof. Let s be such that $p_1 - \Phi(P) \sim 3s - \mathfrak{b}$. We again use the notation and construction of Lemma 6. Let P' defined over $\mathbf{Q}_p$ be in $\Phi^{-1}(s)$ and let P'' be the third intersection of PP' with V; thus $\Phi(P'') \sim \mathfrak{b} - \Phi(P) - s$. Because we can if necessary translate s by $(1,-1,0) - (0,1,-1)$, which corresponds to a 3-division point on the Jacobian, we can assume that $s \neq \mathfrak{b} - \Phi(P) - s$; this implies that $\Phi(P') \neq \Phi(P'')$ and therefore the condition in the Remark is satisfied. To choose the lines $P'R'$ and $P''R''$, let Π be a plane containing PP' but whose reduction mod p does not contain the vertex of $\tilde{V}$. Choose the line $P'R'$ to be the intersection of Π with the tangent to V at P'; thus $\Phi(R') \sim \mathfrak{b} - 2s$. Now write $P'' = (x_0, \ldots, x_3)$; we can assume without loss of generality that x_1 is a unit at p. Let $P''R''$ be the intersection of the tangent to V at P'' with $x_2X_3 = x_3X_2$; this last plane is defined because x_2, x_3 cannot both vanish. Since the coefficient of X_0 in the equation of the tangent is divisible by p, $\Phi(R'') = \Phi(P'') \sim \mathfrak{b} - \Phi(P) - s$. If R is the third intersection of $R'R''$ with V then

$$\Phi(R) \sim \mathfrak{b} - \Phi(R') - \Phi(R'') \sim 3s + \Phi(P) - \mathfrak{b} \sim p_1.$$

It can be shown that the points of $\gamma(\mathbf{F}_p)$ form 9 cosets of G if $p \equiv 1 \bmod 3$ and 3 cosets if $p \equiv 2 \bmod 3$. But it is not implied that all these cosets can be lifted, nor that we need as many distinct R-equivalence classes as there are liftable cosets. □

We have still to consider the case $p = 3$. In principle, the methods which we used to prove Lemma 13 are still applicable, but the results become more complicated because of the appearance of 3 as a binomial coefficient.

Lemma 15 *Let V be given by (3), let $p = 3$ and suppose that $d \equiv \pm 2$ or $\pm 4 \bmod 9$. For a, b in $\mathbf{Z}/(3)$ let $U(a,b)$ be the subset of $V(\mathbf{Q}_3)$ satisfying*

$$X_0 \equiv 3aX_1 \bmod 9, \quad X_3 \equiv 3bX_1 \bmod 9. \tag{46}$$

Then any R-equivalence class is either disjoint from or dense in each $U(a,b)$; and for each $U(a,b)$ there is at least one class which is dense in it.

Proof. The argument in the proof of Lemma 13 remains valid up to and including (45); and for $a = b = 0$ the Lemma follows just as before. Analogously to (46), define subsets $U'(a,b)$, $U''(a,b)$ of $V(\mathbf{Q}_3)$ by

$$\begin{aligned} X_0 \equiv 3aX_2 \bmod 9,\ X_1 \equiv 3bX_2 \bmod 9 \quad &\text{for} \quad U'(a,b), \\ X_0 \equiv 3aX_3 \bmod 9,\ X_2 \equiv 3bX_3 \bmod 9 \quad &\text{for} \quad U''(a,b). \end{aligned}$$

If for example we normalize a point of $U(a,b)$ by setting $X_1 = 1$ then

$$X_2 \equiv -1 - 9b^3 + 9da^3 \bmod 27.$$

Now let P' be in $U'(a',b')$ and P'' in $U''(a'',b'')$, and normalize P' by $X_2 = 1$ and P'' by $X_3 = 1$; then

$$\tfrac{1}{3} f_2(P', P'') \equiv -1 + 3b' \bmod 9, \quad \tfrac{1}{3} f_2(P'', P') \equiv 1 + 3b'' \bmod 9$$

so that (12) and (13) imply that the third intersection of $P'P''$ with V is in $U(-a'-a'', -b'-b'')$. Similarly if P is any point of $U(-a'-a'', -b'-b'')$ and P' any point of $U'(a',b')$ then PP' meets V again in a point P'' in $U''(a'',b'')$; in other words, given such P, P' we can find P'' in $U''(a'',b'')$ such that $P'P''$ meets V again in P. This is a situation akin to translation in the sense defined in §4; and since the Lemma holds for $U'(0,0)$, each class must be either disjoint from or dense in each $U(a,b)$.

It only remains to show that each $U(a,b)$ contains a point of $V(\mathbf{Q})$. The example (43) shows that this is true for $U(1,0)$. Now let $P = (3u, 1, v, 3w)$ in $V(\mathbf{Q})$ with u, w integral at 3. A typical line through P in the tangent to V at P is the locus of

$$(3u\lambda t,\ 1 + 9t(\lambda d u^2 - \mu w^2),\ v,\ 3w + \mu t)$$

as t varies; here the ratio λ/μ determines the line. The third intersection of V with this line is given by

$$t = \frac{9(du\lambda^2 - w\mu^2) - 243(du^2\lambda - w^2\mu)^2}{d\lambda^3 - \mu^3 - 729(du^2\lambda - w^2\mu)^3}.$$

If we take P to be in $U(1,0)$ then u is a unit at 3 and $3|w$; and if we choose $\lambda = 1$, $\mu = d$ then $3\|(d\lambda^3 - \mu^3)$, though this is the best we can do. Thus $3\|t$, so that there is a point of $V(\mathbf{Q})$ in one of $U(2,d)$ and $U(0,-d)$; denote its class by $\mathcal{C}$. By taking $\lambda = 1$, $\mu = 0$ we obtain a point in $U(1,0)$ which is also in $\mathcal{C}$. Being the class of the points on a singular cubic, this class satisfies $\mathcal{C} = \mathcal{C} \circ \mathcal{C}$. Using symmetry and the calculations in the previous paragraph, every $U(a,b)$ meets $V(\mathbf{Q})$; and the R-equivalence classes which meet $U(a,b)$ depend only on $da - b$. □

This Lemma does not exhaust $V(\mathbf{Q}_3)$ when $d \equiv \pm 2 \mod 9$, because we still have to consider the set U of points congruent mod 3 to $(-d,1,1,0)$ and those obtained from them by symmetry. But if we can exhibit one point of $V(\mathbf{Q})$ satisfying this condition, then the "third intersection" construction will show that there is a class dense in U. If for example $d = 2$ then $(1,1,1,0)$ is such a point. We can now complete the argument for $d = 2$.

Theorem 6 *If V is $2X_0^3 = X_1^3 + X_2^3 + X_3^3$ then the adelic closure of $V(\mathbf{Q})$ consists of all points for which one of X_1, X_2, X_3 is divisible by* 6.

Proof. Heath-Brown [2] has shown that for any rational point on V one of X_1, X_2, X_3 is divisible by 6. On the other hand, in Theorem 1 we can take $\mathcal{B} = \{2,3\}$. We have shown that for $p = 2$ we have $n \leq 3$; and because of Heath-Brown's result Theorem 1 can only hold if $n = 3$ and, after renumbering, the set U_{i2} consists of all points with $2|X_i$. For $p = 3$ we do not know the decomposition (2), but we have shown that $V(\mathbf{Q})$ is dense in $V(\mathbf{Q}_3)$, so that there is no summand in (2) which does not meet $V(\mathbf{Q})$. Putting together these facts, we obtain the Theorem. Note that in addition to $(0,1,-1,0)$ and (43), we needed to use the point $(1,1,1,0)$ on V. □

The case when $d \equiv \pm 1 \mod 9$ and is therefore a cube in $\mathbf{Q}_3$ is totally different; for now V contains a pair of skew lines together defined over $\mathbf{Q}_3$ and is therefore birationally equivalent over $\mathbf{Q}_3$ to a plane. We cannot lift this map to $\mathbf{Q}$, but we can imitate it. The lines

$$\ell_0' : d^{-1/3}X_0 - \omega X_3 = X_1 + \omega X_2 = 0,$$
$$\ell_0'' : d^{-1/3}X_0 - \omega^2 X_3 = X_1 + \omega^2 X_2 = 0$$

are conjugate over $\mathbf{Q}_3$, lie in V and do not meet. By Lemma 6 we can choose P in $V(\mathbf{Q})$ to be in general position on V; let ℓ be the unique transversal to ℓ_0', ℓ_0'' through P and let it meet ℓ_0' in P_0'. The tangent to V at P_0' meets V in ℓ_0' and a conic C' through P_0'. Let ℓ_1' be a line defined over $\mathbf{Q}_3(\omega)$, passing through P_0' and lying in the tangent to V at P_0', and suppose it meets C' again in P_1'. Given any point P_2 in $V(\mathbf{Q}_3)$, let ℓ_2 be the transversal to ℓ_0', ℓ_0'' through P_2 and let P_3' be the point where it meets ℓ_0'. Let $P_1'P_3'$ meet V again in P_4', which lies on C', and denote by ℓ_4' the line $P_0'P_4'$ which touches V at P_0'. Now let ℓ^* be a line defined over $\mathbf{Q}$ close to ℓ and passing through P; let R_0', R_0'' be its remaining intersections with V and let L be the quadratic extension of $\mathbf{Q}$ over which R_0' and R_0'' are defined. Then $L \otimes_{\mathbf{Q}} \mathbf{Q}_3 = \mathbf{Q}_3(\omega)$ and we can suppose that R_0' is close to P_0'. Choose lines in the tangent to V at R_0' close respectively to $P_1'P_3'$ and $P_1'P_4'$ and defined over L, and suppose they meet V again in R_3', R_4'. Let R_2' be the remaining intersection of $R_3'R_4'$ with V; thus each R_i' is close to the corresponding P_i'. Now let R_2'' be the conjugate of R_2' over $\mathbf{Q}$ and let R be the third intersection of $R_2'R_2''$ with V. Thus R is in $V(\mathbf{Q})$ and close to P_2. But every point P_2 in $V(\mathbf{Q}_3)$ can be obtained in this way; so the points R are dense in $V(\mathbf{Q}_3)$ and they all belong to the same R-equivalence class. Thus in this case the decomposition (2) contains only one summand.

Lemma 16 *Let V be given by* (3)*, let $p = 3$ and suppose that $3 \| d$. For a, b, c in $\mathbf{Z}/(3)$ define $U(a, b)$ by* (46) *and let $U^*(c)$ be the subset of $V(\mathbf{Q}_3)$ satisfying*

$$X_1 \equiv (1 + 3c)X_3 \mod 9, \quad X_2 \equiv (1 - 3c)X_3 \mod 9.$$

Then any R-equivalence class is either disjoint from or dense in each $U(a, b)$ and $V(\mathbf{Q})$ is either dense in or disjoint from each $U^*(c)$; the $U(a, 0)$ and $U^*(0)$ necessarily contain points of $V(\mathbf{Q})$, and all or none of the $U(a, b)$ with $b \neq 0$ and the $U^*(c)$ with $c \neq 0$ contain points of $V(\mathbf{Q})$.

Proof. If 3 divides one of X_1, X_2, X_3 then also $3|X_0$; so the union of the $U(a, b)$ gives all points of $V(\mathbf{Q}_3)$ for which $3|X_3$. Again, if 3 divides none of X_1, X_2, X_3 then $X_1 \equiv X_2 \equiv X_3 \mod 3$ and $X_1 + X_2 - 2X_3 \equiv 0 \mod 9$; so the union of the $U^*(c)$ gives all points of $V(\mathbf{Q}_3)$ for which none of X_1, X_2, X_3 is divisible by 3. The first two paragraphs of the proof of Lemma 15 remain valid, and as before (43) shows that $U(1, 0)$ is not empty; moreover the third intersection of V with the line joining any point of $U'(0, 0)$ and any point of $U''(1, 0)$ lies in $U(2, 0)$.

We next show how to obtain a point of $U^*(0)$. In the notation of Lemma 6 with $L = \mathbf{Q}_3$, let ℓ be

$$X_0 = \tfrac{1}{2}\epsilon(X_1 + X_2), \quad X_3 = \tfrac{1}{2}(X_1 + X_2)(1 + 3\lambda)$$

where $\epsilon = \pm 1$ is such that $\epsilon d \equiv 3 \mod 9$ and λ will be chosen shortly. Thus ℓ passes through $P = (0, 1, -1, 0)$. The points P', P'' where ℓ meets V again are given by

$$8(X_1^2 - X_1X_2 + X_2^2) = (X_1 + X_2)^2(\epsilon d - (1 + 3\lambda)^3).$$

The discriminant of this equation is $-96(2 + (1 + 3\lambda)^3 - \epsilon d)$; if we define μ by $\epsilon d = 3 + 9\mu$ and set $\lambda = \mu + 3\nu$ then this discriminant is congruent to $-2^5.3^4(\lambda^2 + \lambda^3 + \nu) \mod 3^5$ and we can therefore choose ν so that this is a 3-adic square. Denote the solutions by

$$X_1/X_2 = \theta \text{ or } \theta^{-1} \quad \text{where} \quad \theta \equiv 1 \mod 3;$$

they are in $\mathbf{Q}_3$, so that the Remark which follows Lemma 6 is applicable. We can take P' to be given by

$$P' = (\epsilon(1 + \theta),\ 2,\ 2\theta,\ (1 + \theta)(1 + 3\lambda));$$

for P'' we simply interchange X_1 and X_2. The tangent to V at P' is

$$d(1 + \theta)^2X_0 - 4X_1 - 4\theta^2X_2 - (1 + \theta)^2(1 + 3\lambda)^2X_3 = 0.$$

Choose the line $P'R'$ to be the intersection of this with $X_2 = \theta X_1$, so that the general point of $P'R'$ can be written

$$(\epsilon(1 + \theta) + s(1 + 3\lambda)^2,\ 2,\ 2\theta,\ (1 + \theta)(1 + 3\lambda) + sd)$$

for some s. Substituting into the equation for V, we find that R' is given by

$$s = \frac{3d\epsilon(1 + \theta)(1 + 3\lambda)^4 - 3d^2(1 + \theta)(1 + 3\lambda)}{-d(1 + 3\lambda)^6 + d^3} \equiv 3\epsilon \mod 9.$$

In contrast, choose $P''R''$ to be the intersection of $\theta X_0 = \frac{1}{2}\epsilon(1 + \theta)X_1$ with the tangent to V at P'', so that the general point on $P''R''$ can be written

$$(\epsilon(1 + \theta),\ 2\theta,\ 2 + t(1 + \theta)^2(1 + 3\lambda)^2,\ (1 + \theta)(1 + 3\lambda) - 4t)$$

for some t. Substituting into the equation for V we find that R'' is given by

$$t = \frac{6(1+\theta)^4(1+3\lambda)^4 + 48(1+\theta)(1+3\lambda)}{64 - (1+\theta)^6(1+3\lambda)^6},$$

where the denominator is certainly divisible by 9. Thus

$$R'' \equiv (0,\ 0,\ (1+\theta)^2(1+3\lambda)^2,\ -4) \bmod 9.$$

It follows that

$$\tfrac{1}{3}f_2(R'', R') \equiv -4(1-\theta) \bmod 9, \quad \tfrac{1}{3}f_2(R', R'') \equiv 1 \bmod 3$$

whence R is in $U^*(0)$. Approximating in the usual way gives a point R_0 in $V(\mathbf{Q}) \cap U^*(0)$.

A calculation like that in the second paragraph of the proof of Lemma 15 shows that if Q_1 is in $U(a,b)$ and Q_2 is in $U^*(c)$ then the third intersection of Q_1Q_2 with V is in $U^*(b-c)$. But reduction mod 3 shows that if Q' and Q'' are both congruent to $(\epsilon, 1, 1, 1)$ mod 3 then the third intersection of $Q'Q''$ with V is not of this form, and therefore lies in some U, U' or U''. It follows that if R_1 is in $U^*(0)$ then the third intersection of R_0R_1 with V must be in some $U(a,0), U'(a,0)$ or $U''(a,0)$. Since $V(\mathbf{Q})$ is dense in each of these, it must be dense in $U^*(0)$. The remaining parts of the Lemma follow by very similar arguments. □

Remark. Further straightforward calculations, which are left to the reader, show that any R-equivalence class which meets $U^*(c)$ is dense in it and that for fixed a, b the three sets $U(a,b), U'(a,b)$ and $U''(a,b)$ meet the same R-equivalence classes. This last result is in interesting contrast with the situation in Lemma 15.

We can now complete the argument for $d = 3$.

Theorem 7 *If V is $3X_0^3 = X_1^3 + X_2^3 + X_3^3$ then the adelic closure of $V(\mathbf{Q})$ consists of all points for which either one of X_1, X_2, X_3 is divisible by 9 or $X_1 \equiv X_2 \equiv X_3 \bmod 9$.*

Proof. Heath-Brown [2] has shown that any rational point of V satisfies these conditions. Now the Theorem follows at once from Theorem 1, since by Lemma 16 $V(\mathbf{Q})$ is dense in each $U(a,0)$ and in $U^*(0)$. □

For completeness we now deal with the remaining case for which $p = 3$.

Lemma 17 *Let V be given by* (3)*, let $p = 3$ and suppose that $3^2 \| d$. For a, b in $\mathbf{Z}/(3)$ let $U(a,b)$ be the subset of $V(\mathbf{Q}_3)$ satisfying*

$$X_0 \equiv aX_1 \mod 3, \quad X_3 \equiv 3bX_1 \mod 9.$$

Then any R-equivalence class is either disjoint from or dense in each $U(a,b)$, and each $U(a,b)$ meets $V(\mathbf{Q})$ except perhaps when $\frac{1}{9}d \equiv \pm 1 \mod 9$ and $b \neq 0$.

The proof of this is very similar to the first two paragraphs in the proof of Lemma 13, and is left to the reader. The analogues of (43) are

$$(1 - e + e^2,\ 1 + e^3,\ -1 + 3e - e^3,\ 3e - 3e^2),$$
$$(1 + e + e^2,\ -1 + e^3,\ 1 + 3e - e^3,\ 3e + 3e^2)$$

where $e = \frac{1}{9}d$ and a factor 3 can be taken out in one of the two cases. If $d = 9$, the Brauer-Manin obstruction shows that $V(\mathbf{Q})$ can only meet $U(a,b)$ if $b = 0$; but I do not know of any other cube-free value of d with $3^2 \| d$ for which any of the $U(a,b) \cap V(\mathbf{Q})$ is empty.

REFERENCES

[1] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers* (Oxford, first published 1938).

[2] R. Heath-Brown, The density of zeros of forms for which weak approximation fails, Math. Comp. **59**(1992), 613-622.

[3] Y. Manin, *Cubic Forms, Algebra, Geometry, Arithmetic* (North-Holland, 1974).

[4] H.P.F. Swinnerton-Dyer, The zeta-function of a cubic surface over a finite field, Proc. Cambridge Phil.Soc. **63**(1967), 55-71.

[5] H.P.F. Swinnerton-Dyer, Universal equivalence for cubic surfaces over finite and local fields, Symp. Math. **24**(1981), 111-143.