ACTA ARITHMETICA
XXX (1976)

Algebraic points on cubic hypersurfaces

by

D. F. Coray* (Cambridge, Mass.)

Introduction. The following conjecture was apparently first formulated by Cassels and Swinnerton-Dyer (in the case $n = 3$), and it is closely connected with some of the problems mentioned by B. Segre in [15], p. 2:

Conjecture (CS). *Let $f(x_0, \ldots, x_n)$ be a cubic form with coefficients in a field k. Suppose f has a non-trivial solution in an algebraic extension K/k, of degree d prime to 3. Then f also has a non-trivial solution in the ground field k.*

Of course the crucial condition in this statement is that d should be prime to 3. The case $n \leqslant 2$ was already known to Henri Poincaré [11]; his proof will be given in § 2, since the geometrical ideas it involves are fundamental in the study of the case $n = 3$ and will be used throughout this paper. We begin with a few rather dry lemmas on the rationality of cycles on an algebraic variety (§ 1), which are necessary if we want to proceed on firm ground when using algebraic geometry over an arbitrary field. The use of these lemmas is exemplified in § 2, which therefore gives not only Poincaré's proof, but also a few other applications of the same type of argument. In § 3 we discuss some of the first attempts made at proving the conjecture when $n = 3$, including a very interesting descent argument due to Cassels (unpublished). This result implies in particular that (CS) holds when $n = 3$ and k is a local field. But the argument fails when the characteristic of the residue class field is equal to 2.

At this point, the exposition breaks into two parts: in §§ 4 and 5, we use a different method to prove the conjecture in full generality over any local field (i.e. for all n and without any restriction on the characteristic). This is done by purely arithmetic means, and the reader who is more interested in the geometrical aspect of the problem may proceed

* This paper forms the substance of a dissertation presented to the University of Cambridge [3]. I wish to express my gratitude to the Research Committee of the University of Geneva and to the Société Académique (Turettini Fund) for financial support.

directly to §§ 6, 7 and 8. There he will find, first the simple extension of Poincaré's result to divisors lying on a curve of arbitrary degree and arbitrary genus (§ 6); and then a descent argument on cubic surfaces, which enables us to assume (when $n = 3$) that d is equal to 4 or 10 (§ 7). The final section shows that (CS) holds for *singular* cubic surfaces, and also for those cubic surfaces which contain a k-rational set of 3 or 6 skew lines. The general case of a cubic surface defined over a field like $k = \boldsymbol{Q}$ therefore remains open. By the results of § 4, any counterexample to (CS) must also violate the Hasse principle. Hence, although the conjecture does not look terribly plausible when $n > 3$ and $k = \boldsymbol{Q}$, the problem of actually determining a counterexample appears to be extremely hard.

1. Rationality of cycles. The lemmas introduced in this section are all essentially well-known. We state them in a form that will be sufficient for our purposes; generalizations can be found in the first chapter of Weil's *Foundations* [22]. We begin with a few words on the terminology adopted, since it differs from that of Weil.

We shall be working over a given field of definition k, and by *variety* we mean a projective variety V (not necessarily irreducible) in $\boldsymbol{P}^n(\bar{k})$, $\bar{k}$ being the algebraic closure of k. This will indeed prove more convenient than working in a universal domain. V is called *k-rational* if the homogeneous ideal $I(V)$ associated with it in $\bar{k}[X_0, \ldots, X_n]$ is defined over(1) k. For any field $K \subset \bar{k}$, $V(K)$ denotes the set of points of V with coordinates in K. A *hypersurface* V is the *divisor* $V = V(f)$ of $\boldsymbol{P}^n$ determined by a form f and not the *variety* $V(f)$. This convention enables us to identify forms with hypersurfaces even when they are degenerate. Our conjecture can therefore be restated as follows:

(CS) *Let $V \subset \boldsymbol{P}^n$ be a k-rational cubic hypersurface, and let K be a finite extension of k with degree d prime to 3. Then $V(k) = \emptyset \Rightarrow V(K) = \emptyset$.*

As we shall see later (footnote (9)), there is no loss of generality in assuming that V is absolutely irreducible.

A *Galois automorphism* is an element σ of the group $\mathscr{G} = \mathrm{Gal}(\bar{k}/k)$. There is an obvious action of $\mathscr{G}$ on the points of $\boldsymbol{P}^n(\bar{k})$, but $\mathscr{G}$ also acts on the subvarieties of $\boldsymbol{P}^n$, since(2) $V = V(\mathfrak{b}) \Rightarrow V^\sigma = V(\mathfrak{b}^\sigma)$. We note that a point P of $\boldsymbol{P}^n$ is k-rational if and only if it belongs to $\boldsymbol{P}^n(k)$, and if k is perfect, this is equivalent to saying that P is invariant under the action of $\mathscr{G}$. More generally:

(1) As a trivial example, the point $(1, t^{1/p}) \in \boldsymbol{P}^1(\bar{k})$ is not rational over $k = \boldsymbol{F}_p(t)$, although it can be defined — as a set — by the ideal $(X_1^p - tX_0^p)$; indeed its ideal in $\bar{k}[X_0, X_1]$ is not generated by polynomials with coefficients in k.

(2) We denote by $V(\mathfrak{b})$ the set of zeros in $\boldsymbol{P}^n(\bar{k})$ of the ideal $\mathfrak{b}$; $\mathfrak{b}^\sigma = \{f^\sigma \mid f \in \mathfrak{b}\}$, where σ acts on the coefficients of f; $V^\sigma = \{x^\sigma \mid x \in V\}$.

LEMMA 1.1. *Suppose the variety $V \subset \boldsymbol{P}^n$ is defined over the separable closure $\bar{k}^s$ of k, and let $\mathfrak{a} \subset \bar{k}[X_0, \ldots, X_n]$ be its ideal. Then the following conditions are equivalent:*

(i) *V is k-rational;*
(ii) *V is Zariski-closed (over k);*
(iii) *$V = V^\sigma$ $\forall \sigma \in \mathscr{G}$;*
(iv) *$\mathfrak{a} = \mathfrak{a}^\sigma$ $\forall \sigma \in \mathscr{G}$.*

Proof. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) follow trivially from the definitions. (i) follows easily from (iv); we give the details for the convenience of the reader:

Let $\mathfrak{a} = (f_1, \ldots, f_s)$, where the f_i's are in $K[X_0, \ldots, X_n]$ for some finite Galois extension K/k. Let $\omega_1, \ldots, \omega_d$ be a basis for K over k. Then $f_i = \varphi_1^{(i)}\omega_1 + \ldots + \varphi_d^{(i)}\omega_d$, where the φ's are polynomials with coefficients in k. Since now $\mathfrak{a} = \mathfrak{a}^\sigma$ $\forall \sigma \in \mathrm{Gal}(K/k)$, $\mathfrak{a}$ contains all the conjugates $f_i^\sigma = \varphi_1^{(i)}\omega_1^\sigma + \ldots + \varphi_d^{(i)}\omega_d^\sigma$ of each f_i. Hence $\varphi_1^{(i)}, \ldots, \varphi_d^{(i)} \in \mathfrak{a}$, since the matrix $(\omega_j^\sigma)_{j,\sigma}$ is invertible, and so $\mathfrak{a} = (\varphi_1^{(i)}, \ldots, \varphi_d^{(i)})_{1 \leqslant i \leqslant s}$. ∎

COROLLARY 1.2. *Suppose k is perfect and $V \subset \boldsymbol{P}^n$ has precisely r distinct conjugates V^σ (over k). Then V is defined over a field K of degree $[K : k] = r$.*

Proof. Let $\mathscr{H} = \{\sigma \mid V^\sigma = V\} \subset \mathscr{G}$ and $E^\sigma = \{V^\sigma\}_{\sigma \in \mathscr{G}}$. $\mathscr{G}$ acts transitively on the set E, and $\mathscr{H}$ is the isotropy group $\mathscr{G}_V$ of V; hence

$$[\mathscr{G} : \mathscr{H}] = [\mathscr{G} : \mathscr{G}_V] = \mathrm{card}(\mathscr{G} \cdot V) = \mathrm{card}\, E = r.$$

Let $K = \bar{k}^{\mathscr{H}}$ be the fixed field of $\mathscr{H}$. By Galois theory, $[K : k] = [\mathscr{G} : \mathscr{H}] = r$ and, by Lemma 1.1, V is defined over K (and in fact over no smaller field containing k)(3). ∎

LEMMA 1.3. *The image V^σ of an absolutely irreducible variety $V \subset \boldsymbol{P}^n$ under a Galois automorphism is an absolutely irreducible variety of the same dimension and the same degree.* ∎

This is clear; however, it is interesting to remark that the elements of $\mathscr{G}$ are neither algebraic morphisms nor continuous mappings in the transcendental topology (when $k \subset \boldsymbol{C}$)(4). They are continuous in the Zariski topology (this implies the first assertion about irreducibility), but even so they have more geometrical properties than one would normally expect: for instance they also preserve the genus of a curve.

(3) Using the equivalence (i)$\Leftrightarrow$(iii) of Lemma 1.1, it is easy to see that K is in fact the *least* field of definition containing k: if V is defined both over K and over K', it is also defined over their intersection. The existence of a least field of definition is less easy to prove when the extensions can be inseparable (see [22], chap. I, § 7, Lemma 2).

(4) Consider for example the effect of σ: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ on a sequence of $\boldsymbol{Q}$-rational points tending to $\sqrt{2}$!

A *cycle* $Z = \sum n_i V_i$, where all the $V_i \subset \boldsymbol{P}^n$ are absolutely irreducible varieties, is said to be *k-rational* if $Z = Z^\sigma = \sum n_i V_i^\sigma \ \forall \sigma \in \mathcal{G}$ and if each n_i is divisible by the order of inseparability of V_i over k (see [22], p. 123).

We shall frequently use the following two lemmas:

LEMMA 1.4 (Weil). *If Z_1 and Z_2 are two k-rational cycles, then so is their intersection $Z_1 \cdot Z_2$.*

Proof. If k is perfect, the multiplicities do not come into account and the result follows from Lemma 1.1, since the intersection of two closed sets is closed.

In the general case, this is a non-trivial result, due to André Weil ([22], chap. VIII, § 3, theorem 4). ■

This lemma implies in particular that, when $k = \boldsymbol{F}_p(t)$, any two k-rational curves through $P = (t^{1/p}, 1, 0) \in \boldsymbol{P}^2(\bar{k})$ meet in the point P with multiplicity divisible by p.

COROLLARY 1.5. *If Z_1, Z_2 and Z_3 are three k-rational positive cycles such that $Z_1 \cdot Z_2 \geqslant Z_3$, then the residual intersection $Z_1 \cdot Z_2 - Z_3$ is also k-rational.*

Proof. This evidently follows from Lemma 1.4 and the obvious fact that the sum of two k-rational cycles (not necessarily positive) is still k-rational. ■

A *prime k-rational 0-cycle* Z consists of all the conjugates of a point P, each taken with multiplicity equal to the degree of inseparability of $k(P)/k$.

LEMMA 1.6. *Let Z be a prime k-rational 0-cycle of degree d; then the family of k-rational hypersurfaces $F \subset \boldsymbol{P}^n$, of any given degree l, containing the points of $|Z|$, is determined by d linear conditions (not necessarily independent) on the coefficients of*(5) *F.*

Proof. Let P be any point of $|Z|$ and let $(1, a_1, \ldots, a_n)$ be its coordinates. Then $P \in F \Leftrightarrow F(1, a_1, \ldots, a_n) = 0$, and this clearly represents d linear conditions on the coefficients of the form F, since every monomial $a_1^{\mu_1} \ldots a_n^{\mu_n}$ can be expressed linearly in terms of a basis of $k(P)/k$. Then F, having its coefficients in k, will also contain all the conjugates of P. ■

As an illustration we note that, if $k = \boldsymbol{F}_2(t)$, there is no k-rational plane containing the point $P = (1, t^{1/4}, t^{1/2}, t^{3/4}) \in \boldsymbol{P}^3(\bar{k})$, since there is no linear relation over k between $1, t^{1/4}, t^{1/2}, t^{3/4}$. Everything happens as if P had four distinct conjugates in general position in $\boldsymbol{P}_3$.

2. Motivations. Conjecture (CS) is essentially motivated by the following three propositions:

(5) It is convenient to use the same symbol for the hypersurface and for the form defining it. Note also that we do not say that F contains Z, but only that F contains the support of Z; it is only when taking intersections that we shall recover the multiplicities (in view of Lemma 1.4). Thus the point $P = (t^{1/2}, 0)$ is simple on the line $y = 0$ (over $k = \boldsymbol{F}_2(t)$), but the line is tangent at P to any k-rational curve containing P as a simple point.

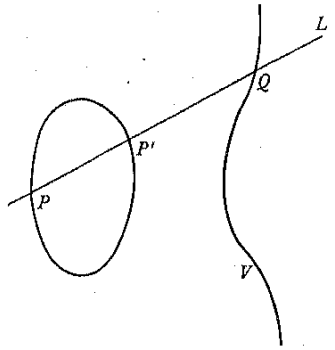
PROPOSITION 2.1. *Let $f(x_0, \ldots, x_n)$ be a quadratic form with coefficients in k, and let K/k be an algebraic extension of odd degree d. Then f represents zero in K if and only if it does so in k.*

PROPOSITION 2.2. *Let $f(x_0, \ldots, x_n)$ be a cubic form with coefficients in k, and let K be a quadratic extension of k. Then if f represents zero in K, it also represents zero in k.*

PROPOSITION 2.3. (CS) *holds for cubic curves (i.e. when $n = 2$).*

We recall that, by definition, a form f *represents zero* (non-trivially) in a field K if it admits a non-trivial solution with coordinates in K. The first two propositions appear as an exercise(6) in Lang's *Algebra* ([8], chap. 7, ex. 7), and Proposition 2.3 follows from a more general result of Poincaré on elliptic curves (see Corollary 6.3). The method used by Poincaré in [11] enables us to prove all three propositions in a unified way, and is both intuitive and rigorous. It will recur later in more complicated situations.

Proof of 2.2. Let P be a point of the cubic hypersurface $V = V(f)$ with coordinates in $K = k(\eta)$, say $P = (1, a_1 + b_1\eta, \ldots, a_n + b_n\eta)$. Without



loss of generality, $b_i \neq 0$ for some i, and so the locus of $(1, a_1 + b_1 t, \ldots, a_n + b_n t)$ is a straight line L containing P and defined over k. Hence L also contains the conjugate P' of P (by Lemma 1.1)(7). Clearly we may assume that $L \not\subset V$, and then $V \cdot L$ is a cycle of degree 3; the residual intersection Q is a k-rational point (by Corollary 1.5)(8). ■

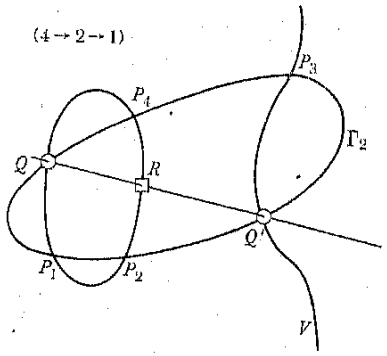
(6) It seems that the only published proof of 2.1 is that of T. A. Springer (C. R. Acad. Sci. Paris, 234 (1952), pp. 1517–1519), although Skolem ([18], p. 297) applied the Poincaré argument to the case $n = 2$.

(7) If K/k is inseparable, then $P' = P$, but — by Lemma 1.4 — $V \cdot L$ then contains P with multiplicity 2, so that the proof is unchanged!

(8) In this proof all the lemmas have been used in trivial situations, and it is just as easy to write a purely arithmetic proof!

Proof of 2.1. The argument is the same as for Proposition 2.2, but we shall use a curve Γ of degree $m \leqslant d-1$ instead of a straight line. Let us suppose the proposition true for all $d' < d$, over any ground field. Let $P = (1, \alpha_1, \ldots, \alpha_n)$ be a point of the quadric $V = V(f)$ with coordinates in K; w.l.o.g. one of the coordinates of P, α_1 say, is not in k. We can therefore assume that α_1 is a generator of K, since otherwise $k(\alpha_1)$ would be a field intermediate to k and K, and we could apply the induction hypothesis (both over k and over $k(\alpha_1)$). Let us write $P = (1, \theta, p_2(\theta), \ldots, p_n(\theta))$, where the p_i's are polynomials of degree $\leqslant d-1$ with coefficients in k. Then the locus of $(1, t, p_2(t), \ldots, p_n(t))$ is a k-rational curve $\Gamma \subset \boldsymbol{P}^n$ of degree $m \leqslant d-1$; and we may assume that $\Gamma \not\subset V$, since $\Gamma(k) \neq \emptyset$. Then $\Gamma \cap V$ consists of finitely many points, since Γ is absolutely irreducible (being given as a locus!). Thus $\Gamma \cdot V$ is a cycle of degree $2m$ (theorem of Bezout [13], chap. III, § 2.2, and chap. IV, § 2.1), containing the prime rational 0-cycle Z of degree d generated by P. The residual intersection is a k-rational positive 0-cycle (Corollary 1.5) of degree $2m-d \leqslant d-2$. Since $2m-d$ is odd, V also contains a prime k-rational 0-cycle of odd degree $d' \leqslant d-2$; i.e. the form f has a solution in an extension K'/k with odd degree $d' \leqslant d-2$, which completes the induction argument. ■

Proof of 2.3. Let P be a point of the plane cubic curve V with coordinates in K; w.l.o.g. $K = k(P)$. Let Z be the prime k-rational 0-cycle, with degree $d = 3r+\varrho$ ($\varrho = 1$ or 2), generated by P. By Lemma 1.6, the family of k-rational curves Γ_l of degree $l = r+1$ containing the conjugates of P is a vector space of dimension $\geqslant \binom{l+2}{2} - d$; this includes the family of k-rational curves Γ_l containing V as a component, whose dimension is $\binom{(l-3)+2}{2}$. Since $\binom{l+2}{2} - d > \binom{l-1}{2}$, there exists a k-rational curve Γ of degree l which does not contain V as a component. Then $\Gamma \cdot V$



is a k-rational 0-cycle(9) of degree $3l = 3r+3$, containing Z, and there is a residual cycle of degree $3-\varrho = 1$ or 2. In the former case, the proposition is proved (in view of Lemma 1.5); in the latter, we need only apply Proposition 2.2. ■

We now derive a few easy corollaries:

Corollary 2.4. (CS) *holds for all C_1 fields*(10), *in particular for finite fields.*

Proof. (CS) is valid when $n \leqslant 2$, by Proposition 2.3. But if k is a C_1 field, there is nothing more to prove, since $n > 2 \Rightarrow V(k) \neq \emptyset$. ■

Corollary 2.5. *Proposition 2.2 is also true for a normal extension K/k of degree $d = 2^s$.*

Proof. The Galois group $\mathrm{Gal}(K/k)$ is a 2-group; hence it is supersolvable, and the result follows by repeated use of Proposition 2.2. ■

Corollary 2.6(11). *Let $V \subset \boldsymbol{P}^n$ be a cubic hypersurface defined over k. If V contains a k-rational divisor D of degree d prime to 3, then $V(k) \neq \emptyset$.*

Proof. Take a generic k-rational 2-plane Π; then $\Pi \cap V$ is a k-rational curve of degree 3 containing $\Pi \cap D$, which is a k-rational 0-cycle of degree d. Since $3 \nmid d$, we can apply Proposition 2.3 to deduce the existence of k-rational points on $\Pi \cap V$. ■

Theorem 2.7. *Let $V \subset \boldsymbol{P}^n$ be a quadric hypersurface, defined over k and such that $V(k) = \emptyset$. Then any k-rational r-cycle Z lying on V, of any dimension r, has even degree.*

Proof. The proof is almost identical with that of the preceding corollary; one uses a linear space Π of codimension r and applies Proposition 2.1. ■

* * *

Having proved Propositions 2.1 and 2.3, it is reasonable to ask whether the analogue of (CS) for curves of degree 4 may also be true. That this is not the case is best shown by an example (cf. also Corollary 6.5):

Example 2.8. *The form $f(x_0, x_1, x_2) = x_0^4 - 3x_1^4 + 2x_2^4 - 3x_1^2x_2^2$ does not represent zero in $\boldsymbol{F}_5$ (and hence in $\boldsymbol{Q}_5$ and in $\boldsymbol{Q}$), although it has the solution*

(9) W. l. o. g. we may assume that V is k-irreducible. Then, even if V is absolutely reducible, $\Gamma \cap V$ consists of a finite number of points, for both Γ and V are k-rational. When $n \geqslant 3$, the case of reducible cubics becomes trivial, since they always have at least one k-rational point!

(10) We recall that a field k is C_1 (or: *quasi-algebraically closed*) if every form of degree d in $d+1$ variables has a non-trivial zero in k. Finite fields are C_1, in virtue of the well-known theorem of Chevalley–Warning.

(11) When $n = 3$, this is contained in a result of B. Segre ([15], theorem 3 (p. 4 and p. 41)).

$(1, \theta, \theta^2)$ *in* $\boldsymbol{Q}(\theta)$ (*and hence in* $\boldsymbol{Q}_5(\theta)$ *and in* $\boldsymbol{F}_5(\theta)$), *where* $\theta^3-\theta^2-1=0$. *In particular, even Corollary* 2.4 *cannot be extended to quartics.*

Hint. $x^4 \equiv 0$ or $1 \pmod 5$; $x^2 \equiv 0$ or $\pm 1 \pmod 5$. ■

It may be worth mentioning that f actually represents zero in some extension of $\boldsymbol{Q}$ of degree d for every value of $d>1$. Indeed, there is the solution $(\sqrt{2}, 1, 1)$ in $\boldsymbol{Q}(\sqrt{2})$ and $(\sqrt[4]{3}, 1, 0)$ in $\boldsymbol{Q}(\sqrt[4]{3})$, which deals with the cases $d=2$ and 4. Now if we want to find a solution of degree 5 (say), we can take a suitably generic conic containing the three conjugates of $(1, \theta, \theta^2)$. It will meet the quartic $\Gamma = V(f)$ residually in a set of five points; with reasonable luck, this set should be $\boldsymbol{Q}$-irreducible. Similarly for all values of d. A rigorous proof proceeds by reduction to Hilbert's irreducibility theorem (see [7], chap. VIII), as follows:

The curve Γ contains at least one positive $\boldsymbol{Q}$-rational divisor D of degree d. The vector space $L(D)$ is generated by $N+1 := l(D)$ elements $f_0, \ldots, f_N$ of the function-field $\boldsymbol{Q}(\Gamma)$, which define a rational transformation $\Phi = (f_0 : \ldots : f_N) : \Gamma \to \boldsymbol{P}^N$; and $\Gamma^* = \Phi(\Gamma)$ is a curve of degree d, which spans $\boldsymbol{P}^N$ (Φ is even an isomorphism when $d \geqslant 7$ ([13], chap. III, §5.6, cor. 4)). Let π be a projection of $\boldsymbol{P}^N$ onto a plane $\boldsymbol{P}^2$ such that $\Gamma^{**} = \pi(\Gamma^*)$ is still a curve of degree d. We can now apply Hilbert's irreducibility theorem to Γ^{**}: the sections of Γ^{**} by straight lines in the plane $\boldsymbol{P}^2$ are in general $\boldsymbol{Q}$-irreducible. We thus get prime $\boldsymbol{Q}$-rational 0-cycles of degree d on Γ by taking the inverse images $(\pi \circ \Phi)^*(Z)$ of such sections. ■

3. Some typical descent arguments. In this section we shall confine our attention to the case of cubic surfaces (i.e. $n=3$). The following proposition — and its proof — are due to Cassels:

Proposition 3.1 (Cassels). *Let* $n=3$. *Assume* (CS) *is true (over* k *and its finite extensions) for all degrees* $d < 3r+1$ $(3 \nmid d)$. *Then it is true for* $d_1 = 3r+1$ *if and only if it is for* $d_2 = 3r+2$.

Proof. (i) Let $P = (1, \theta, \alpha, \beta) \in V(K)$, with $[K : k] = d$ (d stands for either d_1 or d_2). W.l.o.g. we may assume that $K = k(\theta)$, since otherwise $k(\theta)$ would be a field intermediate to k and K, and we could use the induction hypothesis[12]. Hence $\alpha = a_0 + a_1\theta + \ldots + a_{d-1}\theta^{d-1}$ and $\beta = b_0 + \ldots + b_{d-1}\theta^{d-1}$. This already shows that there is a k-rational curve of degree $\leqslant d-1$ that contains all the conjugates of P; but we shall need a curve of degree $m \leqslant 2r+1$.

[12] If we may assume that K/k is separable (e.g. if k is perfect), then we can strike out "and its finite extensions" from the induction hypothesis, because there exists a primitive element θ', which can be expressed as a linear combination $\theta' = \theta + \lambda\alpha + \mu\beta$ (see [8], theorem 14, p. 185; w.l.o.g. k is infinite, by Corollary 2.4) and $(1, \theta', \alpha, \beta)$ is a point of a surface which is projectively equivalent to the original one.

(ii) In order to construct it, let us multiply all the coordinates of P by a polynomial $A_0(\theta) = c_0 + c_1\theta + \ldots + c_{2r}\theta^{2r}$, whose coefficients will be determined later. Then

$$P = \big(A_0(\theta), A_1(\theta), A_2(\theta), A_3(\theta)\big),$$

where

$$A_1(\theta) = \theta A_0(\theta) = c_0\theta + \ldots + c_{2r}\theta^{2r+1},$$
$$A_2(\theta) = \alpha A_0(\theta) = c_0' + c_1'\theta + \ldots + c_{d-1}'\theta^{d-1},$$
$$A_3(\theta) = \beta A_0(\theta) = c_0'' + c_1''\theta + \ldots + c_{d-1}''\theta^{d-1}.$$

This defines two polynomials $A_2(t)$ and $A_3(t)$, whose coefficients depend linearly and homogeneously on those of $A_0(t)$. We can therefore determine the coefficients c_i in such a way that the degrees of $A_2(t)$ and $A_3(t)$ do not exceed $2r+1$, since this amounts to solving (non-trivially) a linear system of $2\big((d-1)-(2r+1)\big) = 2d-4r-4 \leqslant 2r$ homogeneous equations in $2r+1$ unknowns.

(iii) Thus we have found a k-rational curve Γ (the locus of $\big(A_0(t), A_1(t), A_2(t), A_3(t)\big)$ of degree $m \leqslant 2r+1$, passing through all the conjugates of P. Since $\Gamma(k) \neq \emptyset$, we may assume without loss of generality that Γ meets V in a finite number of points. Hence there is a residual cycle of degree $\delta = 3m-d$, which is k-rational by Corollary 1.5. If $d = d_2$ then $\delta \leqslant d_1$; and if $d = d_1$ then $\delta = d_2$ or $\delta < d_1$. Since $3 \nmid \delta$, we can also find a prime k-rational 0-cycle of degree $\delta' \leqslant \delta$ not divisible by 3, and the assertion follows from the induction hypothesis[13]. ■

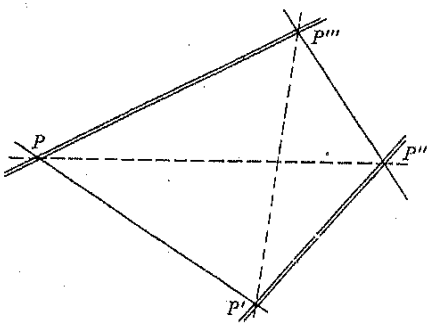
This proposition enables us to concentrate on the case $d \equiv 1 \pmod 3$. The argument, however, does not give the descent from $3r+1$ to $3r-1$, since the number of equations is then equal to that of unknowns. And indeed there is a serious obstruction when $r=1$, since one would have to find a k-rational curve of degree 2 through 4 points:

Example 3.2. *If the point* $P \in \boldsymbol{P}^3$ *is defined over an extension* K/k *with degree* 4 *such that the least normal extension* K'/k *has Galois group* $\mathcal{S}_4$, *and if the four conjugates of* P *are not in a plane, then there are exactly three curves of degree* 2 (*three pairs of lines*) *containing the four points* (see figure overleaf). *None of them is* k*-rational, since they are exchanged by the Galois automorphisms. In fact, each of them is defined over a cubic extension of* k (Corollary 1.2). ■

For degrees higher than 4 — where it is difficult to enumerate all possible curves — the situation is much less clear. For instance, when $r=2$, there exists a k-rational curve Γ of degree 4 through 7 points. It meets the surface in 12 points, with a residual intersection of degree 5;

[13] Since Γ has genus 0, the last part of the proof can be completed without the Bézout theorem, by purely arithmetic means: write $F(t) = f(A_0(t), \ldots, A_3(t)) = P(t) \cdot Q(t)$, where $P(t)$ is the minimal polynomial of θ, and distinguish a few cases.

we thus get the descent from 7 to 5. To show the existence, we note that there are at least ∞^2 quadrics containing the seven points. The intersection of two of them is a curve of degree 4 and genus 1. (It really is a curve, since we may assume that the seven points are not coplanar



and since $\mathcal{G}$ acts transitively on them. The few degenerate cases are readily dealt with (e.g. a twisted cubic and a line).) W.l.o.g., Γ is not contained in V, by Corollary 2.6.

One might think that the reason why Proposition 3.1 did not yield this descent from 7 to 5 lies in the fact that the genus of Γ is equal to 1, while the argument of Cassels works with curves of genus 0. But this is not the right explanation, since —working over an extension of degree 2 — it is possible to replace Γ by a quartic curve of genus 0. Indeed (assuming everything is in general position), take a non-singular quadric Q containing the seven points; by Proposition 2.1, it also contains some k-rational points. It may contain no k-rational line, but there is a quadratic extension L of k such that Q contains two skew lines, D_1 and D_2, defined over L. Then there is an L-rational cubic surface F that contains the seven points and the two lines. This represents only 15 linear conditions; therefore F can be so chosen that it does not contain Q as a component ($20 - 15 > 4$). Hence $Q \cap F = \Gamma' \cup D_1 \cup D_2$, where Γ' is a quartic curve of genus 0, defined over L.

This seems to indicate that the arithmetic proof of 3.1 could be extended. But the geometric approach is often simpler, since we can also use curves of higher genera. Thus the descent from 8 to 7 makes use of a quintic of genus 0, but the geometrical argument using the intersection of two quadrics gives directly a descent from 8 to 4. More generally, this idea of constructing a space curve Γ of degree $2r$, but of arbitrary genus, containing the assigned k-rational set of $d = 3r+1$ points, can be used for a great many values of d. But the details soon become rather complicated, because Γ could be reducible, with a component lying on V.

Furthermore, whenever d is of the form $\frac{3l(l-1)}{2}+1$, this construction proves exceedingly hard, if not impossible (cf. the case $l = 2$ and Example 3.2). In § 7 we shall see how the descent can be performed more simply precisely by studying the curves that lie on the surface.

* * *

Proposition 3.1 has a direct application when k is a *local field*, i.e. when k is complete with respect to a discrete valuation and has a finite residue class field. By *residual characteristic* we mean the characteristic of the residue field.

PROPOSITION 3.3. (CS) *is true (with $n = 3$) for local fields of odd residual characteristic.*

Proof. Write $d = 3r+\varrho$ ($\varrho = 1$ or 2); the proof is by induction on r. By virtue of Proposition 3.1, we may assume that d is even, and greater than 2 (Proposition 2.2). It is clearly sufficient to show that there exists a field intermediate to k and K, and this follows from a more general lemma:

LEMMA 3.4. *Let k be a local field and K a finite extension of k. Suppose that the degree $[K : k]$ is neither a prime nor a power of the residual characteristic p. Then there is a field L intermediate to k and K.*

Proof[14]. We may clearly assume that K/k is either separable or purely inseparable. The latter case is ruled out, since $[K : k]$ would be a power of p (and there would be intermediate fields anyway). We may further assume that K/k is either unramified or totally ramified, since otherwise the maximal unramified subfield of K/k (see e.g. [17], cor. 3, p. 64) is a convenient choice for L. In the former case, the extension is normal with a cyclic Galois group (the residue field being finite), and the result follows from the assumption that $[K : k]$ is not prime. In the latter case, let $q \mid [K : k]$, where q is a prime different from p, and let $\mathfrak{p} = (\pi)$ be the (non-zero) prime ideal of k. We will show that the generator of this prime ideal can be so chosen that it has a qth root ϑ in K; $k(\vartheta)$ will then be the required intermediate field. Now there is an element $\omega \in K$ such that $(\omega)^q = (\pi)$; and π/ω^q is a unit of K. Since K/k is totally ramified, the residue class fields are the same, and so there is a unit $\eta \in k$ such that $v_K(\pi/\omega^q - \eta) > 0$. By Hensel's lemma, the equation $g(X) = \eta X^q - \pi/\omega^q = 0$ has a root ξ in K. Then $\vartheta = \omega\xi$ is a qth root of π/η, as required. ■

(14) I am indebted to Prof. Cassels for suggesting this proof, which is simpler than my original group-theoretic argument.

It is quite clear that Lemma 3.4 expresses a very special property of local fields. In particular, the situation of Example 3.2 can never take place over $\boldsymbol{Q}_p$ ($p \neq 2$), since — by the preceding lemma — any extension of degree 4 of $\boldsymbol{Q}_p$ is biquadratic. Over $\boldsymbol{Q}_2$, however, it is possible to have an extension of degree 4 generated by a polynomial with Galois group $\mathscr{S}_4$ (e.g. x^4-2x-2). This is why we had to assume in Proposition 3.3 that the residual characteristic was not equal to 2. That this restriction is artificial will be seen in the forthcoming section.

4. Quasi-local fields. A field K will be called *quasi-local* if it is complete with respect to a discrete valuation and if its residue class field $k = \mathfrak{O}/\mathfrak{p}$ has property (CS). Any local field is quasi-local, by Corollary 2.4, but the class of quasi-local fields — as a result of our Theorem 4.7 — also includes $C(t)((u_1, \ldots, u_s))$, $\boldsymbol{Q}_p((t_1, \ldots, t_s))$, $\boldsymbol{F}_p((t_1, \ldots, t_s))$, etc. In this section we show that (CS) holds for quasi-local fields.

The proof is based on the following extension of Artin's conjecture for cubics([15]): Any cubic form f with coefficients in K that does not represent zero in K can essentially be written, up to equivalence, in the form $f = \varphi_0 + p\varphi_1 + p^2\varphi_2$, where p is any generator of the ideal $\mathfrak{p}$ and φ_i does not represent zero in k ($i = 0, 1, 2$). The meaning of "essentially" is made precise in the formulation of Theorem 4.5, which will be proved only in §5. In this section we shall see how (CS) follows from that result and we shall derive a few other corollaries.

We first introduce some definitions: throughout this section, K will denote a complete field with a discrete valuation, $\mathfrak{p}$ its (non-zero) prime ideal, and p a fixed generator of $\mathfrak{p}$. An *integral form* is a homogeneous *cubic* polynomial $f(x_1, \ldots, x_n)$ with coefficients in $\mathfrak{O}$. We shall use Dem'janov's notation: a_i, a_{ij}, a_{ijk} are the coefficients of x_i^3, $x_i^2x_j$, $x_ix_jx_k$ respectively; we do not distinguish between a_{ijk}, a_{jik}, etc., but there is a difference between a_{ij} and a_{ji}, which is sanctioned by the following definition: f is called *triangular* if $a_{ij} = 0$ whenever $i < j$.

The coefficients a_i will be called the *principal coefficients* of f. As usual, two forms f and g are said to be *equivalent* if there exists a non-singular projective transformation that carries one into the other. Finally, a principal coefficient a_i of an integral form will be called *admissible* if it is not divisible by p^3, and the form itself will be called *admissible* if all of its principal coefficients are. The following lemma plays a key role in the theory; roughly speaking, it says that one can very often decide whether a form represents zero by merely looking at its coefficients. (Theorem 4.5 will enable us to replace 'very often' by 'always' after a suitable normalization.)

([15]) The original conjecture was proved, among others, by Dem'janov [4] (when the residual characteristic χ is not equal to 3) and by T. A. Springer [19] in the general case. These two proofs are short and elegant. More complicated arguments were also found by Lewis, Davenport, etc.

LEMMA 4.1([16]). *Suppose the integral form $f(x_1, \ldots, x_n)$ does not represent zero in K. Then if p divides a_h for some h, p also divides a_{hi}, a_{ih} and a_{hij} for all i and j.*

Proof. It will simplify the notation to assume for each of these three assertions that $h = 1$, $i = 2$ and $j = 3$.

(i) $p \mid a_{hi}$ $\forall i$. Suppose $p \nmid a_{12}$ and let $x_1 = 1$, $x_i = 0$ $\forall i > 1$. Then

$$f(x) \equiv a_1 x_1^3 \equiv 0 \ (\mathfrak{p}) \quad \text{and} \quad \frac{\partial f}{\partial x_2}(x) \equiv a_{12}x_1^2 \not\equiv 0 \ (\mathfrak{p}),$$

and an application of Hensel's lemma would yield a non-trivial solution of f in K, which is contradictory.

(ii) $p \mid a_{ih}$ $\forall i$. Suppose $p \nmid a_{21}$ and let $x_1 = -a_2/a_{21}$, $x_2 = 1$, $x_i = 0$ $\forall i > 2$. Then, using (i), we see that:

$$f(x) \equiv a_{21}x_1x_2^2 + a_2x_2^3 \equiv 0 \ (\mathfrak{p}) \quad \text{and} \quad \frac{\partial f}{\partial x_1}(x) \equiv a_{21}x_2^2 \not\equiv 0 \ (\mathfrak{p}),$$

a contradiction.

(iii) $p \mid a_{hij}$ $\forall i, j$. Suppose $p \nmid a_{123}$ and let $x_1 = -\dfrac{a_2 + a_3 + a_{23} + a_{32}}{a_{123}}$, $x_2 = x_3 = 1$, $x_i = 0$ $\forall i > 3$. Then, using (i) and (ii), we get:

$$f(x) \equiv a_2x_2^3 + a_{23}x_2^2x_3 + a_{32}x_2x_3^2 + a_3x_3^3 + a_{123}x_1x_2x_3 \equiv 0 \ (\mathfrak{p})$$

and

$$\frac{\partial f}{\partial x_1}(x) \equiv a_{123}x_2x_3 \not\equiv 0 \ (\mathfrak{p}),$$

a contradiction. ∎

COROLLARY 4.2. *If $p^2 \mid a_h$, then p^2 also divides a_{hi} $\forall i$.*

Proof. If $f(x_1, \ldots, x_n)$ does not represent zero, then $f(x_1, x_2, 0, \ldots, 0)$ has the same property. So it is enough to prove this corollary for a form in two variables, say

$$f(x_1, x_2) = a_1x_1^3 + a_{12}x_1^2x_2 + a_{21}x_1x_2^2 + a_2x_2^3.$$

Let $x_1 = y_1/p$, $x_2 = y_2$; then

$$g(y_1, y_2) := pf(x_1, x_2) = \frac{a_1}{p^2}y_1^3 + \frac{a_{12}}{p}y_1^2y_2 + a_{21}y_1y_2^2 + pa_2y_2^3$$

([16]) A special case of this lemma was already proved by Dem'janov; T. A. Springer ([19], p. 513) also uses a version of this result.

is integral, by the lemma. But since now the coefficient of y_2^3 is a multiple of p, another application of the lemma shows that a_{12}/p also is, hence $p^2 | a_{12}$. ■

COROLLARY 4.3. *If $p^2 | a_h$ and $p^2 | a_i$, then $p^2 | a_{hij}$ $\forall j$.*

Proof. As in the foregoing corollary we may assume that f is a form in three variables. Apply the transformation

$$x_1 = \frac{y_1}{p}, \quad x_2 = \frac{y_2}{p}, \quad x_3 = y_3$$

and multiply by p. Again, using Corollary 4.2, we see that f is transformed into an integral form g such that the coefficient of y_3^3 is pa_3 and that of $y_1y_2y_3$ is a_{123}/p. Hence, by Lemma 4.1, $p^2 | a_{123}$. ■

The next corollary is a trivial consequence of the lemma:

COROLLARY 4.4. *If $p^2 | a_h$ and $p | a_i$, then $p^2 | a_{ih}$. If, moreover, $p | a_j$ then $p^2 | a_{hij}$.* ■

THEOREM 4.5. *If $f(x_1, \ldots, x_n)$ does not represent zero in K, then f is, equivalent to an admissible form*

$$\varphi_0(x_1, \ldots, x_r) + p\varphi_1(x_1, \ldots, x_r, x_{r+1}, \ldots, x_s, x_{s+1}, \ldots, x_n) + p^2\varphi_2(x_1, \ldots, x_n),$$

where

$$p \nmid a_1, \ldots, a_r, \quad p \| a_{r+1}, \ldots, a_s, \quad p^2 \| a_{s+1}, \ldots, a_n,$$

and where

$$\varphi_0(x_1, \ldots, x_r), \quad \sigma_1(x_{r+1}, \ldots, x_s) := \varphi_1(0, \ldots, 0, x_{r+1}, \ldots, x_s, 0, \ldots, 0)$$

and

$$\sigma_2(x_{s+1}, \ldots, x_n) := \varphi_2(0, \ldots, 0, x_{s+1}, \ldots, x_n)$$

do not represent zero in the residue class field(17) *k. Furthermore, if*

$$\tau_1(x_1, \ldots, x_n) := \varphi_1(x_1, \ldots, x_n) - \sigma_1(x_{r+1}, \ldots, x_s),$$

we may arrange for each term of τ_1 to involve ***at least*** *one variable x_i with $i \leqslant r$ and* ***at most*** *one with $i > s$, counting multiplicities.*

We defer the proof of this theorem until the next section, but we may already note that the assertions about τ_1 are easy consequences of the corollaries proved above. Indeed, if we know that f is equivalent to an admissible form as described in the first part of the theorem, we may clearly shift into $p^2\varphi_2$ any term of $p\tau_1$ whose coefficient is a multiple of p^2. After this operation, each term of τ_1 involves at most one variable with $i > s$ (by Corollaries 4.2 & 4.3) and at least one with $i \leqslant r$ (by Corollaries 4.2 & 4.4), as asserted.

(17) With the usual convention that the form which is identically zero does not represent zero!

The whole point about the condition on τ_1 is that it is precisely what is needed to prove the converse of the theorem:

PROPOSITION 4.6. *If $f(x_1, \ldots, x_n)$ is of the form described in Theorem 4.5, then it does not represent zero in K.*

Proof. By the usual argument, $x_i = p\xi_i$ $\forall\, i \leqslant r$, and hence

$$p^2\varphi_0(\xi_1, \ldots, \xi_r) + \varphi_1(x_1, \ldots, x_n) + p\varphi_2(x_1, \ldots, x_n) = 0.$$

Now $\varphi_1 = \sigma_1 + \tau_1$ and since each term of τ_1 involves at least one variable x_i with $i \leqslant r$, τ_1 is a multiple of p; hence σ_1 also is. Thus $x_i = p\xi_i$ $\forall i \leqslant s$; and since each term of τ_1 involves at most one variable x_i with $i > s$, τ_1 is then a multiple of p^2 (square!); hence we can divide by p, and the result follows. ■

It is now easy to prove (CS):

THEOREM 4.7. *Let $F(x_1, \ldots, x_n)$ be a cubic form defined over the quasi-local field K, and let L/K be an algebraic extension of degree d prime to 3. Then F represents zero in K if and only if it does so in L.*

Proof. Suppose F does not represent zero in K; then, by Theorem 4.5, we may assume that F is of the form $\varphi_0 + p\varphi_1 + p^2\varphi_2$. Let π be a generator

$$\begin{array}{ccc} L & \xleftarrow{4.6} & l = \mathfrak{O}_L/(\pi) \\ \uparrow d & & \uparrow f \\ K & \xrightarrow{4.5} & k = \mathfrak{O}_K/(p) \end{array}$$

of the prime ideal of L. Then $p = \eta \cdot \pi^e$, where η is a unit of L, and the residue class field l of L is an extension of degree f of k. Since $3 \nmid d = ef$ ([17], prop. 3, p. 38, & cor. 1, p. 39), we have $3 \nmid e$ and $3 \nmid f$; and we can write $F = \varphi_0 + \eta\pi^e\varphi_1 + \eta^2\pi^{2e}\varphi_2$.

We know that φ_0, σ_1 and σ_2 do not represent zero in k, and hence they do not represent zero in l either (since K is quasi-local and $3 \nmid f$). Let $e = 3e + \varrho$, with $\varrho = 1$ or 2, and write:

$$y_i = x_i \text{ if } i \leqslant r; \quad y_i = \pi^e x_i \text{ if } r < i \leqslant s; \quad y_i = \pi^{2e} x_i \text{ if } s < i \leqslant n.$$

Clearly, this transformation does not affect solvability in L, and we have:

$$\pi^e\sigma_1(x_{r+1}, \ldots, x_s) = \pi^\varrho\sigma_1(y_{r+1}, \ldots, y_s),$$
$$\pi^{2e}\sigma_2(x_{s+1}, \ldots, x_n) = \pi^{2\varrho}\sigma_2(y_{s+1}, \ldots, y_n),$$

and also (considering the special shape of τ_1):

$$\pi^e\tau_1(x_1, \ldots, x_n) = \pi^\varrho\tau_1^*(y_1, \ldots, y_n),$$
$$\pi^{2e}\tau_2(x_1, \ldots, x_n) = \pi^{2\varrho}\tau_2^*(y_1, \ldots, y_n),$$

where τ_1^* and τ_2^* are integral forms (over L) retaining the general shape of τ_1 and $\tau_2 := \varphi_2 - \sigma_2$. In particular, the last sentence of Theorem 4.5 applies also to τ_1^*.

Therefore it is enough to show that the form

$$\varphi_0(y_1, \ldots, y_r) + \eta\pi^{\varrho}\{\sigma_1(y_{r+1}, \ldots, y_s) + \tau_1^*(y_1, \ldots, y_n)\} + \\ + \eta^2\pi^{2\varrho}\{\sigma_2(y_{s+1}, \ldots, y_n) + \tau_2^*(y_1, \ldots, y_n)\}$$

does not represent zero in L. If $\varrho = 1$, this is just Proposition 4.6 (with K replaced by L), and if $\varrho = 2$, the proof is only slightly more complicated and will be left to the reader. ■

Among the corollaries of Theorem 4.7, we have the following:

PROPOSITION 4.8. *Let k be a global field; then* (CS) *holds for the class of cubic hypersurfaces satisfying the Hasse principle.*

Proof. If $V(k) = \emptyset$ and V satisfies the Hasse principle, there exists a prime $\mathfrak{p}$ such that $V(k_\mathfrak{p}) = \emptyset$. If K/k is an extension of degree d prime to 3, there exists a prime $\mathfrak{P}$ over $\mathfrak{p}$ such that the completion $K_\mathfrak{P}/k_\mathfrak{p}$ has degree prime to 3 (since $d = \sum e_i f_i$). By Theorem 4.7, $V(K_\mathfrak{P}) = \emptyset$, and so $V(K) = \emptyset$. ■

PROPOSITION 4.9. *Let k be a quasi-local field and $V \subset \boldsymbol{P}^n$ a cubic hypersurface defined over k and such that $V(k) = \emptyset$. Then the degree d of any k-rational r-cycle Z lying on V, of any dimension r, is a multiple of* 3.

Proof. The proof is identical with that of Theorem 2.7: take a generic k-rational linear space Π of codimension r; then $\Pi \cap Z$ is a k-rational 0-cycle Z_0, of degree d. By Theorem 4.7, d is a multiple of 3. (Z_0 may be reducible, but the degree of every irreducible component must be divisible by 3.) ■

COROLLARY 4.10. *Let k be a global field and $V \subset \boldsymbol{P}^n$ a cubic hypersurface, defined over k and satisfying the following condition:*

(*) *There exist a k-rational hyperplane H and a prime $\mathfrak{p}$ such that $(V \cap H)(k_\mathfrak{p}) = \emptyset$.*

Then the degree d of any k-rational r-cycle Z lying on V, of any dimension $r \geqslant 1$, is a multiple of 3.

Proof. Without loss of generality we may assume that Z is irreducible. Hence either $|Z| \subset H$, or $Z \cap H$ is an $(r-1)$-cycle of degree d lying on $V \cap H$. In either case, we can apply Proposition 4.9, since $V \cap H$ is a cubic hypersurface in $\boldsymbol{P}^{n-1}$ and $(V \cap H)(k_\mathfrak{p}) = \emptyset$. ■

5. Proof of Theorem 4.5

(i) $\chi \neq 3$ (after Dem'janov). We now proceed to the proof of Theorem 4.5, first under the assumption that the characteristic χ of the residue class field is not equal to 3, since in this case the proof is very simple and entirely constructive. Our argument follows Dem'janov's paper [4] very closely, and we shall borrow two of his lemmas.

LEMMA 5.1. *If $f(x_1, \ldots, x_n)$ does not represent zero in K, then f is equivalent to a triangular form* (char$K \neq 3$).

Proof, see [4], p. 889. ■

We can thus assume without loss of generality that f is triangular; we can also assume that its *principal* coefficients a_i are integral and not divisible by p^3, for we can use transformations of the type $x_i \mapsto p x_i$ to bring it to that shape if necessary. We claim that, as a matter of fact, *all* the coefficients are then integral. Indeed, if some of the other coefficients were not integral, we could multiply the whole form by a suitable power of p so as to obtain an integral form, one of whose coefficients would be a unit. But this would contradict Lemma 4.1, since all the principal coefficients would be divisible by p.

We may therefore assume that f is triangular and admissible. Let us renumber the variables in such a way that

$$p \nmid a_1, \ldots, a_r, \quad p \| a_{r+1}, \ldots, a_s, \quad p^2 \| a_{s+1}, \ldots, a_n,$$

and let

$$\varphi_0(x_1, \ldots, x_r) = f(x_1, \ldots, x_r, 0, \ldots, 0),$$
$$\tilde{\sigma}_1(x_{r+1}, \ldots, x_s) = f(0, \ldots, 0, x_{r+1}, \ldots, x_s, 0, \ldots, 0)$$

and

$$\tilde{\sigma}_2(x_{s+1}, \ldots, x_n) = f(0, \ldots, 0, x_{s+1}, \ldots, x_n).$$

Clearly, the renumbering can be done in such a manner that φ_0, $\tilde{\sigma}_1$ and $\tilde{\sigma}_2$ are triangular.

The form f is now equal to $\varphi_0 + \tilde{\sigma}_1 + \tilde{\sigma}_2 + \varrho$, where ϱ contains all the overlapping terms (like $a_{n1}x_1x_n^2$, $a_{1sn}x_1x_sx_n$, etc.). Let $\tilde{\tau}_2(x_1, \ldots, x_n)$ contain the terms of ϱ whose coefficients are divisible by p^2, and $\tilde{\tau}_1(x_1, \ldots, x_n)$ all the remaining ones. Let $\sigma_1 = \frac{1}{p}\tilde{\sigma}_1$, $\sigma_2 = \frac{1}{p^2}\tilde{\sigma}_2$, $\tau_1 = \frac{1}{p}\tilde{\tau}_1$, $\tau_2 = \frac{1}{p^2}\tilde{\tau}_2$; all these forms are integral, according to Lemma 4.1. Finally, let $\varphi_1 = \sigma_1 + \tau_1$ and $\varphi_2 = \sigma_2 + \tau_2$, so that $f = \varphi_0 + p\varphi_1 + p^2\varphi_2$.

The theorem will be proved if we can show that φ_0, σ_1 and σ_2 do not represent zero modulo p. And this is another lemma of Dem'janov's ([4], p. 891):

LEMMA 5.2. *If $\psi(x_1, \ldots, x_m)$ is a triangular integral form, all the principal coefficients of which are units, then ψ represents zero in K if and only if it does so modulo* p ($\chi \neq 3$). ■

The assumption $\chi \neq 3$ is essential in Lemma 5.2, as the following example shows: $x^3 + 5y^3$ has the solution (1, 1) modulo 3, but there is

no non-trivial solution in $\boldsymbol{Q}_3$. In fact, replacing x by $z+y$, we get $z^3+3z^2y+3zy^2+6y^3$, which clearly does not represent zero in $\boldsymbol{Q}_3$, since it is of the form predicted by Theorem 4.5. In [3] we used this remark to construct an effective proof of Theorem 4.5, valid without any restriction on the characteristic; but the argument is laborious and does not present an immense interest. However, the case of residual characteristic equal to 3 is important, since without it we cannot derive Proposition 4.8. We shall therefore outline an alternative (non-constructive) approach, following T. A. Springer [19].

(ii) χ arbitrary (after Springer). This proof does not differ very much from the preceding one; Lemmas 5.1 and 5.2 are replaced by a maximality condition on the number of variables occurring in φ_0 and in σ_1. But the main idea of Springer was to use the formalism he had developped for the study of quadratic forms in an earlier paper. We write the proof only in outline; the missing details are all in [19].

If $i \in \boldsymbol{Z}$, let $M_i = \{x \in K^n \mid v_{\mathfrak{p}}(f(x)) \geqslant i\}$. The M_i's are $\mathfrak{O}$-modules, and $M_0 \supset M_1 \supset M_2 \supset M_3 = \mathfrak{p}M_0$. Let $E = M_0/M_3$, $E_i = M_i/M_{i+1}$; these are vector spaces over $k = \mathfrak{O}/\mathfrak{p}$. Using the completeness of K, it is not difficult to check that $\dim_k E = n$; also $\sum_{i=0}^{2} \dim_k E_i = n$. We take a basis $\{\bar{e}_1, \ldots, \bar{e}_r\}$ of E_0, $\{\bar{e}_{r+1}, \ldots, \bar{e}_s\}$ of E_1, $\{\bar{e}_{s+1}, \ldots, \bar{e}_n\}$ of E_2, and choose representatives $\{e_1, \ldots, e_n\}$ such that

$$\{e_1, \ldots, e_r\} \subset M_0, \quad \{e_{r+1}, \ldots, e_s\} \subset M_1, \quad \{e_{s+1}, \ldots, e_n\} \subset M_2.$$

Then $\{e_1, \ldots, e_n\}$ is a basis of K^n. We may write each vector $x \in K^n$ in the form $x = \sum \xi_i e_i$, and then

$$f(x) = \sum_{i \leqslant j \leqslant k} a_{ijk}\, \xi_i \xi_j \xi_k.$$

Let us define

$$\sigma_0(x) := \varphi_0(x) = \sum_{i \leqslant j \leqslant k \leqslant r} a_{ijk}\, \xi_i \xi_j \xi_k,$$

$$\sigma_1(x) = \frac{1}{p} \sum_{r < i \leqslant j \leqslant k \leqslant s} a_{ijk}\, \xi_i \xi_j \xi_k, \qquad \sigma_2(x) = \frac{1}{p^2} \sum_{s < i \leqslant j \leqslant k} a_{ijk}\, \xi_i \xi_j \xi_k.$$

Then $f = \varphi_0 + p\sigma_1 + p^2\sigma_2 + \varrho$, where ϱ contains overlapping terms only.

The principal coefficients $\frac{a_{jjj}}{p^i}$ of σ_i are units, by the definition of the M_i's, and therefore the σ_i's and f must have integral coefficients, as in Dem'janov's argument. Finally it is easy to see that the σ_i's do not represent zero modulo p. Indeed, if $\sigma_i(x) \equiv 0 \pmod{\mathfrak{p}}$, with $x = \sum \xi_j e_j$, we can clearly assume that $x \in M_i$. Hence $f(x) = p^i \sigma_i(x) \equiv 0 \ (\mathfrak{p}^{i+1})$.

This implies that $x \in M_{i+1}$, and therefore all the ξ_j's are congruent to zero modulo p, since the $\bar{e}_j$'s form a basis of E_i. ■

6. Curves and divisors. We now revert to the case of an arbitrary ground field k, but we shall restrict our attention to the case of surfaces (i.e. $n = 3$). The main idea we shall be using is to construct curves Γ on the cubic surface V with relatively small genera, and to show that they contain 0-cycles of sufficiently small degrees. In this section we prove a few auxiliary results we shall need in the study of those curves.

(a) Divisors on a curve. For our purposes it is not natural to call divisors only the simple subvarieties of Γ, since a double point of Γ is usually non-singular on V and is thus a perfectly legitimate 0-cycle. We shall therefore adopt the following terminology:

A (k-rational) 0-*cycle* on Γ is what Weil calls a (rational) 0-chain, ([22], p. 206); in other words singular points are tolerated (sometimes welcome!).

A (k-rational) *Weil divisor* on Γ is what Weil simply calls a (rational) divisor; it consists of simple[18] points.

A *k-Divisor* on Γ is a divisor in the sense of the theory of places of $k(\Gamma)$ ([2]).

Every Weil divisor defines a k-Divisor, and every k-Divisor defines a 0-cycle, in such a way that the degrees are preserved; but there is more structure in k-Divisors.

The following theorem generalizes an old result of Poincaré on elliptic curves ([11], chap. IV, pp. 178–180):

THEOREM 6.1. *Let $\Gamma \subset \boldsymbol{P}^n$ be an absolutely irreducible k-rational curve of degree m and geometric genus g (over k)*[19]; *suppose Γ contains a k-Divisor E of degree e, and let $\delta = \gcd(m, e, 2(g-1))$. Then Γ also contains positive k-Divisors of degree $\theta = j\delta$, for every integer j such that $\theta \geqslant g$. (And in fact it contains at least $\infty^{\theta-g}$ of them.)*

Before proceeding to the proof, we may mention a few corollaries:

---

[18] In what follows, the words 'simple', 'absolutely simple', 'smooth' and 'non-singular' are considered synonymous (Jacobian criterion of simplicity). A point is called 'regular' if the local ring at that point is regular. Smooth ⇒ regular, but the converse does not hold, unless k is perfect (cf. [26], pp. 253 ff.).

[19] The theorem becomes false if we replace g by the *absolute* genus. The conclusion of Corollary 6.2, for instance, does not hold for the curve $t^2y^2z^3 = x^5 + t^2y^5 + tz^5$, which has no point defined over $\boldsymbol{F}_5((t))$, although the absolute genus is zero [20].

[20] As these assertions may not appear quite obvious, we briefly sketch the proofs: (i) Since the equation is homogeneous, it is enough to look for solutions in $\boldsymbol{F}_5[[t]]$; then use the p-adic argument of Proposition 4.6 ($\mathfrak{p} = (t)$). (ii) Write $X = x + t^{2/5}y + t^{1/5}z$, $Y = ty$, $Z = z$; the affine equation becomes $Y^2 = X^5$, and this is the locus of (u^2, u^5), with $u = Y/X^2$. ■ The relative genus is actually equal to 6, since all the points are regular.

COROLLARY 6.2 (Hilbert & Hurwitz [5]). *Every curve of genus 0 and odd (resp. even) degree has infinitely many k-rational points (resp. k-rational pairs of points).* ■

COROLLARY 6.3 (Poincaré). *A curve of genus 1 and degree m, containing a k-rational set of e non-singular points, also contains a k-rational set of* $\delta = \gcd(m, e)$ *points.* ■

Note that Proposition 2.3 follows easily from this result. The next corollary can be proved by a direct argument (consider the canonical class!):

COROLLARY 6.4. *A k-rational curve of genus 2 always contains points with coordinates in k or in a quadratic extension of k.* ■

COROLLARY 6.5. *Let Γ be an absolutely irreducible plane curve of degree 4, defined over k. Suppose Γ contains a k-rational set of d non-singular points, with d odd. Then Γ also contains a k-rational set of 3 points.* ■

The last corollary is in a sense the extension of (CS) to quartic curves. We already know (Example 2.8) that it cannot be substantially improved.

Proof of Theorem 6.1. (i) Assume first that Γ is non-singular. Let K be a divisor in the canonical class, and M a k-rational divisor of degree m, obtained by taking the complete intersection of Γ with a generic k-rational hyperplane in $\boldsymbol{P}^n$. It is known that K can be chosen k-rational ([23], p. 13). Let $D = \mu M + \varepsilon E + \varkappa K$, where $\mu m + \varepsilon e + \varkappa(2g-2) = \delta$, and let $j \in \boldsymbol{N}^*$. By the Riemann inequality, $l(jD) \geqslant j\delta + 1 - g$ is positive as soon as $\theta = j\delta \geqslant g$. Hence the divisor jD, which is k-rational, is linearly equivalent to a *k-rational* positive divisor Θ of degree θ, by [23], prop. 2, pp. 5–6. The family of such divisors has dimension $l(jD) - 1 \geqslant \theta - g$, by [22], cor. 1, p. 265. This proves all the assertions of the theorem when Γ is non-singular. Note, however, that in Weil's theory the genus (of a *non-singular* curve) does not depend on the ground field k; but in this case, g is equal to the absolute genus ([21]).

(ii) Let us now consider the general case of a curve Γ which may be singular; but for simplicity we shall assume that E is a Weil divisor. Then the obvious thing to do is to take a non-singular model Γ^* of Γ ([13], chap. II, § 5.4, theorem 10); this comes equipped with a finite morphism $\Gamma^* \xrightarrow{p} \Gamma$, which is also a birational equivalence. Therefore we can lift the divisor E to a divisor $p^*(E)$ on ([22]) Γ^*, and similarly a Weil divisor M of degree m to ([23]) $p^*(M)$, and then use part (i) of the proof: the required

([21]) This is an expression of the fact that the genus can change only in the presence of regular points that are not smooth (see [12], corollary, p. 182; cf. also [26], pp. 4–5, 254–255).

([22]) and $\deg p^*(E) = \deg E$, since E is a Weil divisor!

([23]) A trivial remark: the degree of Γ^* (which anyway depends on the choice of an embedding) is usually different from that of Γ (e.g. there is no non-singular quartic of genus 2 in $\boldsymbol{P}^n$!). That is why we also have to lift a divisor M from Γ to Γ^*.

positive 0-cycle is the projection of Θ into Γ. However, this argument is valid only if k is perfect, since the existence of a non-singular model Γ^* *defined over k*, equipped with a morphism $p\colon \Gamma^* \to \Gamma$ also defined over k, is not guaranteed otherwise (see [22], Appendix I, cor. 2, p. 346 and the remark that follows([24])).

(iii) When k is imperfect, we therefore need another argument. Since we know (footnote([19])) that we have to use the relative genus, it is natural to employ the Riemann–Roch theorem for function fields([25]). We can proceed as in (i), using the Riemann inequality for function fields ([2], p. 22), except that there is no need to assume Γ non-singular. The reason why this approach is successful, is that, in an example like $y^2 = x^p - t$, the local ring at the singular point $(t^{1/p}, 0)$ is regular of dimension 1; hence it is a discrete valuation ring as for the non-singular points of Γ. ■

(b) Curves on a surface. The next result we need is a theorem of Max Noether, which appeared in a famous memoir to the Berlin Academy ([10], § 6):

PROPOSITION 6.6 (M. Noether). *Let Γ be a divisor of degree m, lying on a non-singular surface* $F_\mu \subset \boldsymbol{P}^3$ *of degree μ. The arithmetic genus of Γ satisfies the inequality*

$$p_a(\Gamma) \leqslant \tfrac{1}{2}(\beta-1)(\beta-2) + \tfrac{1}{2}(l\mu - 2\beta)(l+\mu-4),$$

where $m = l\mu - \beta \quad (0 \leqslant \beta < \mu)$.

Proof. The modern proof makes use of the formula

$$p_a(\Gamma) = \frac{\Gamma(\Gamma+K)}{2} + 1$$

(see [16], chap. IV, no. 8, or [13], chap. VI, § 1.4, theorem 4), where $K = (\mu-4)H$ is the canonical class, and H a plane section, of F_μ ([13], chap. III, § 5.4). Hence

$$(**) \qquad p_a(\Gamma) = \tfrac{1}{2}(\Gamma)^2 + \tfrac{1}{2}m(\mu-4) + 1.$$

Suppose for example that $\beta = 0$ (the only case we shall require). Let Γ_0 be a complete intersection with degree $l\mu$; then $(\Gamma_0)^2 = (lH)^2 = l^2\mu$, so that $p_a(\Gamma_0) = \tfrac{1}{2}l\mu(l+\mu-4)+1$, and all one needs to show is that —

([24]) Weil gives the standard example $y^2 = x^p - t$ $(p > 2)$, where the singularity at $(t^{1/p}, 0)$ cannot be resolved over $k = \boldsymbol{F}_p(t)$.

([25]) One has to check that the field of constants is k, in other words that k is algebraically closed in $k(\Gamma)$. This follows from the assumption that Γ is absolutely irreducible and from [22], chap. I, § 6, theorem 3, and § 7, theorem 5. I am grateful to Dr U. Bartocci for many useful comments on this section, and also for drawing my attention to the nice example of an $\boldsymbol{R}$-irreducible curve for which the above condition is not satisfied: in $\boldsymbol{R}(x)[y]/(x^2+y^2)$, one has $(y/x)^2 + 1 = 0$ (!).

for a fixed degree $m = l\mu$ — the genus is maximal on complete intersections. This follows at once from the Hodge Index Theorem ([9], lecture 18): $\deg(\Gamma - \Gamma_0) = 0$ and therefore $(\Gamma - \Gamma_0)^2 \leqslant 0$. Hence

$$(\Gamma)^2 \leqslant 2(\Gamma \cdot \Gamma_0) - (\Gamma_0)^2 = 2lm - l^2\mu = (\Gamma_0)^2. \blacksquare$$

In the case of a cubic surface $V = F_3$, the above formula yields $p_a(\Gamma_0) = \frac{3l(l-1)}{2} + 1$, for a complete intersection $\Gamma_0 = V \cap F_l$. More generally, for any divisor Γ of degree m, one has $p_a(\Gamma) \leqslant \left[\frac{m(m-3)}{6}\right] + 1$. This could also be found by using the plane representation([26]) of V, or by computing the intersection numbers in the Néron–Severi group of V (cf. [20]).

Unfortunately we shall also require an estimate for the genus of a curve lying on a *singular* surface. As a matter of fact, Noether's proof works for *normal* surfaces $F_\mu \subset \boldsymbol{P}^3$. But the "modern" argument indicated above does not even make sense in that case (there is no good intersection theory for singular surfaces)! In addition, there are serious difficulties due to the fact that Γ may not be a Cartier divisor. It is therefore preferable to go back to the old proof, using Weil divisors:

LEMMA 6.7. *The geometric genus of an irreducible curve Γ of degree $3l$, lying on an irreducible cubic surface V with only finitely many singular points*([27]), *does not exceed*

$$g_{\max} = \frac{3l(l-1)}{2} + 1.$$

Proof. For complete intersections, one still has

$$p_a(\Gamma) = \frac{3l(l-1)}{2} + 1$$

([16], chap. IV, no. 7). Hence the proof given in [10], § 6, is still valid: Noether shows that, for any given degree $m = l\mu$, the genus is maximal on complete intersections; for this he uses only the basic properties of the genus and the fact that the plane sections of F_μ ($= V$) are in general non-singular (this is why we assume that there are only finitely many singular points!). It may be worth mentioning that his argument depends on an auxiliary result on non-singular plane curves, which is rather long to prove but which is fortunately trivial in the case of cubics: indeed all it asserts is that, for positive divisors D of a fixed degree d, the index of speciality is maximal on complete intersections; and since the canonical class of an elliptic curve is 0, there is nothing to prove! ($l(K-D)$ is always zero.) ■

([26]) see [21], pp. 12–17; and also [15], pp. 29–31 for an explicit description.

([27]) For any surface $V \subset \boldsymbol{P}^3$, this condition is equivalent to saying that V is normal, as follows from [25], cor. 12.12 and prop. 12.13.

7. The descent on cubic surfaces. We now have all the necessary tools to prove the following extension of Proposition 3.1:

THEOREM 7.1. *Let $V \subset \boldsymbol{P}^3$ be a non-singular cubic surface defined over the perfect field k and containing a point P with coordinates in an algebraic extension K/k of degree d prime to 3. Then there is an extension L/k, with degree 1, 4 or 10, such that $V(L) \neq \emptyset$.*

Proof. In view of Corollary 2.4, we may assume that k is infinite. The argument is by induction on the degree d. Let Z be the k-rational cycle generated by the conjugates of P; w.l.o.g. $k(P) = K$, and so Z consists of d distinct points (Corollary 1.2). Let l be the integer for which

$$\frac{3l(l-1)}{2} + 1 \leqslant d < \frac{3l(l+1)}{2} + 1.$$

In what follows, we shall denote by F_l any k-rational surface of degree l containing Z and such that $V \not\subset F_l$; by Lemma 1.6, we know that such surfaces do exist, since

$$\binom{l+3}{3} - \binom{l}{3} = \frac{3l(l+1)}{2} + 1 > d.$$

Let $f = 3l(l+1)/2 - d$ be the extra freedom, i.e. the number of conditions we can further impose on the system of surfaces $|F_l|$. The idea of the proof is to apply Theorem 6.1 to a divisor $\Gamma = V \cap F_l$ of the linear system cut out by $|F_l|$. In a first stage (A), we shall assume throughout the argument that Γ is an absolutely irreducible curve, even when we impose additional constraints on the system $|F_l|$. The reducible case will be considered separately (B); as a matter of fact it is essentially simpler!

(A) There are three subcases:

(i) $d > \frac{3l(l-1)}{2} + 1$, $f \geqslant 3$: In this case, let Σ be a k-rational set of three points Q_1, Q_2, Q_3 on V (e.g. the intersection of V with a k-rational line). Since $f \geqslant 3$, we can require F_l to contain them as well. The curve Γ will therefore contain a k-Divisor of degree 1([28]), so that $\delta = \gcd(m = 3l,$

([28]) Since Γ contains a divisor of degree d and one of degree 3 (the only reason for introducing the set Σ is to avoid difficulties with g.c.d.'s). We may clearly assume that Z is a Weil divisor, for if P were a multiple point of Γ, then all of its conjugates would also be, and the genus would be negative ($p_a(\Gamma) < d$). A standard geometrical argument shows that we can also arrange for Σ to be a Weil divisor: the family of surfaces F_l containing the points of Z defines a rational transformation Φ: $V \to \boldsymbol{P}^N$

$e=1,\ 2(g-1)\big)=1$. Since the geometric genus of Γ does not exceed $p_a(\Gamma)=3l(l-1)/2+1$ (Proposition 6.6), we can find on V a k-rational positive 0-cycle of degree $3l(l-1)/2+1<d$ (Theorem 6.1). One at least of its k-irreducible components has degree d' prime to 3, and there is an extension K'/k with degree $d'<d$ such that $V(K')\neq\emptyset$.

(ii) $d>\dfrac{3l(l-1)}{2}+1$, $f<3$: The argument is the same as in case (i), except that there is no need to introduce an additional set of three points: $\delta=\gcd(3l,d,2g-2)\,|\,l$, so that one can choose $\theta=j\delta$ in Theorem 6.1 in such a way that it does not exceed ([29])

$$(g-1)+2\delta\leqslant(g-1)+2l\leqslant\frac{3l(l-1)}{2}+2l=\frac{3l(l+1)}{2}-l<d$$

(providing $f<l$, which is certainly the case if $l\geqslant 3$; the case $l=2$ is easily disposed of).([30])

(iii) $d=\dfrac{3l(l-1)}{2}+1$, $f\geqslant 9$: In this case the genus of Γ can be as large as $3l(l-1)/2+1$ and we need a further trick to bring it down; unfortunately, the method works only when $f\geqslant 9$, and this is where the descent breaks down when d is equal to 4 or 10.

We take a k-rational set of three points Q_1,Q_2,Q_3 and impose on F_l the further condition that it should meet V at Q_1,Q_2 and Q_3 with multiplicity at least 2 (in other words the tangent space to F_l at each point Q_i must contain the tangent plane to V at Q_i). This represents nine linear constraints (three for each Q_i), and they can be satisfied since $f\geqslant 9$. The curve Γ' thus acquires three double points, and so its geometric genus does not exceed $3l(l-1)/2-2$. Since

$$\delta=\gcd(3l,d,2g-2)\,|\,\gcd\left(l,\ d=\frac{3l(l-1)}{2}+1\right)=\begin{cases}1 \text{ if } l\not\equiv 2\ (4),\\ 2 \text{ if } l\equiv 2\ (4),\end{cases}$$

we obtain a descent from d to

$$d'=\frac{3l(l-1)}{2}-2 \quad\text{or}\quad \frac{3l(l-1)}{2}-1.$$

This completes the proof under the assumption that Γ is absolutely irreducible. This is more or less the general case, because in view of the second theorem of Bertini (see e.g. [24], § I.6) we may assume that the surface F_l is irreducible([31]), and one might hope to prove that the divisor cut out by F_l on V can also be chosen irreducible. Unfortunately, it is not very easy to show that there are no fixed components. However, when Γ is reducible, the genus of each component is quite small and the preceding argument should continue to apply. We use this idea to complete the proof:

(B) We assume that Γ is absolutely reducible and that the cycle Z is contained in a k-irreducible component $C=C_1\cup\ldots\cup C_r$, which itself consists of r absolutely irreducible components C_j. We now have two subcases:

(i) $r=1$. Without loss of generality, the degree m of C is a multiple of 3 (by Corollary 2.6), say $m=3\lambda$ with $\lambda<l$; now the genus of C does not exceed $3\lambda(\lambda-1)/2+1$ and the descent again follows from Theorem 6.1: $\delta=\gcd(3\lambda,d,2g-2)$ divides λ, and so there is always a $j\not\equiv 0\ (3)$ such that ([29])

$$g\leqslant j\delta\leqslant\frac{3\lambda(\lambda-1)}{2}+2\delta<\frac{3\lambda(\lambda-1)}{2}+3\lambda\leqslant\frac{3l(l-1)}{2}<d.$$

(ii) $r\geqslant 2$. Since the action of the Galois group $\mathcal{G}$ on the C_j's is transitive, each of the components C_j contains an equal number ν of conjugates of P. Let us assume that $P\in C_1$; we know that C_1 is defined over an extension L/k of degree r (Corollary 1.2). If C_1 is the only component containing P, then none of the conjugates of P belongs to more than

---

(cf. the remark made after Example 2.8), where $N\geqslant f>4$ (since $3\nmid f$). Φ may not be one-to-one, but it is easy to see that its image is a surface, which spans $\boldsymbol{P}^N$. Since there is some freedom in the choice of Σ, we may also assume that $\Phi(Q_i)$ is non-singular ($i=1,2,3$). The sections $V\cap F_l$ are carried into hyperplane sections $\Phi(V)\cap H$ in $\boldsymbol{P}^N$. If the linear space H spanned by $\Phi(Q_1)$, $\Phi(Q_2)$ and $\Phi(Q_3)$ does not contain the tangent plane T_1 at $\Phi(Q_1)$, then there is a k-rational hyperplane H that contains H but not T_1; and therefore Q_1 — hence also Q_2 and Q_3 — are simple for the corresponding F_l. Therefore it suffices to show that we can choose Σ in such a way that $H\neq T_1$.

Let $G_{m,n}$ be the grassmannian of m-planes in $\boldsymbol{P}^n$, and consider the variety $W\subset(V\times G_{2,N})\times G_{1,3}$ consisting (generically) of triples (Q_1,H,L) such that $Q_1\in\Sigma=L\cap V$ and $H\supset\Phi(\Sigma)$. The fibre of the first projection $W\to V\times G_{2,N}$ above (Q_1,H) corresponds to those $L\in G_{1,3}$ which contain Q_1 and at least one other point Q_2 such that $\Phi(Q_2)\in H\cap\Phi(V)$. This last set is at most one-dimensional. Hence the dimension of the fibre does not exceed 1, since the straight line L is entirely determined when the two points Q_1 and Q_2 are given. Now the subset of $V\times G_{2,N}$ consisting of the pairs (Q_1,T_1) is only 2-dimensional. Therefore the family of 'bad' lines (i.e. those which map to $H=T_1$) has dimension at most equal to 3. This shows that it is always possible to choose a k-rational line L in the 4-dimensional space $G_{1,3}$ in such a way that $H\neq T_1$, as required. ■ (I owe this argument to Prof. Zariski.)

([29]) The interval $[g,(g-1)+2\delta]$ contains 2δ integers. Two of them are multiples of δ; one at least is not divisible by 3.

([30]) This argument can thus be used whenever $f<l$. In the case considered here, it is easy to see that δ is actually equal to 1, 2 or 4.

([31]) There is no fixed component, because the family of surfaces with degree l containing Z includes all the reducible surfaces which contain V. Thus only V could be a fixed component, and we know that this is not the case. For essentially the same reason, the system is not composite with a pencil.

one component of C, and so $\nu r = d$. Since $3 \nmid d$, both ν and r are prime to 3; and since P has exactly ν conjugates on C_1, it follows that P is defined over an extension of L with degree ν. The same situation occurs if P belongs to precisely two components of C, except that([32]) $\nu r = 2d$.

We may then assume that the degree μ of C_1 is a multiple of 3, say $\mu = 3\lambda$, since otherwise $V(L) \neq \emptyset$ (Corollary 2.6) and since([33])

$$[L:k] = r \leqslant 3l \leqslant \frac{3l(l-1)}{2} < d;$$

in addition $3l \geqslant r\mu = 3r\lambda$, since all the C_j's have the same degree (Lemma 1.3). We can therefore use the same argument as in case (i): on C_1, we can find an L-Divisor of degree $\theta_1 \geqslant g_1$, where g_1 is the genus of C_1, and this induces a k-Divisor of degree $\theta = r\theta_1$ on C. We need only check that $\theta < d$; but([29])

$$\theta = r\theta_1 \leqslant r(g_1 - 1 + 2\lambda) \leqslant r\left(\frac{3\lambda(\lambda-1)}{2} + 2\lambda\right) = r\lambda\,\frac{3\lambda+1}{2} \leqslant \frac{3l(l-1)}{2} < d.$$

The last inequality but one holds when $\lambda \geqslant 2$; but $\lambda = 1 \Rightarrow \mu = 3$, and then C_1 contains an L-rational point (by Corollaries 6.2 and 6.3).

This completes the proof, because P cannot belong to more than two components of C. Indeed, if P belonged to $s > 2$ distinct components, the total number of intersections $i = \sum_{j<k}(C_j \cdot C_k)$ would be $\geqslant (s-1)d$. On the other hand, it is known that

$$i = p_a(C) - \sum_{j=1}^{r} p_a(C_j) + (r-1);$$

therefore, even if all the $p_a(C_j)$ are zero, the maximum value that i can take is $3l(l-1)/2 + r$. Hence

$$2d \leqslant (s-1)d \leqslant i \leqslant \frac{3l(l-1)}{2} + r < \frac{3l(l-1)}{2} + d,$$

in contradiction with the fact that

$$d \geqslant \frac{3l(l-1)}{2} + 1. \quad \blacksquare$$

If k is not perfect, the theorem remains true, at least in a slightly weaker form:

PROPOSITION 7.2. *If* (CS) *holds* (*with* $n = 3$) *over all finite extensions of* k *when* $d = 4$ *or* 10, *then it holds for all values of* d.

([32]) If we knew that (CS) held over all finite extensions of k when $d = 4$ or 10, we could now complete the proof by induction, instead of using the argument of the following paragraph.

([33]) except when $l = 2$, but this case is trivial.

Sketch of proof. The argument is essentially the same, but one first shows that there is no loss of generality in assuming $k(P)/k$ separable. Indeed we may suppose that $k(P)/k$ is either separable or purely inseparable of prime degree p, since otherwise there exists an intermediate field. If $k(P)/k$ is purely inseparable, we use Proposition 3.1 to replace it by a separable extension with degree equal to $p+1$ or smaller than p.

Then the argument which served to prove Theorem 7.1 can be repeated, with only minor changes: in particular, when $d = p+1 = 3l(l-1)/2+2$, one proceeds as in case (A) (iii) — instead of (A) (i) — in order to get an extension of degree strictly less than p. There is no problem with the relative genus g, which does not exceed the arithmetic genus, though it may be greater than the absolute genus. This follows from [12], Theorem 11, p. 181, which implies that $\pi = g + \delta$ does not depend on the ground field, and from [6], Theorem 2, p. 190, which asserts that — over $\bar{k}$ — $\pi = p_a(\Gamma)$. Cf. [16], p. 81 (note). ■

8. Severi-Brauer varieties. We shall now apply the result of the previous section to prove (CS) in a few special cases. We recall that a non-singular cubic surface is said to have property ϱ_ν if it contains a k-rational set of ν skew lines (terminology of B. Segre). Then we have the following

PROPOSITION 8.1. (CS) *holds for the class of cubic surfaces* V *having properties* ϱ_3 *or* ϱ_6.

Proof. It is enough to prove the proposition when d is equal to 4 or 10. Suppose V contains a k-rational triplet of lines and $d = 4$. Then there is another cubic surface F_3 that contains the lines and the four conjugates of P (this represents only 16 conditions). Let Γ be the residual intersection of V and F_3 with respect to the three lines. Γ is a curve of degree 6 and we claim that its arithmetic genus is equal to 1. Indeed it follows from formula (**), used in the proof of Proposition 6.6, that

$$p_a(\Gamma) = \tfrac{1}{2}(\Gamma)^2 - \tfrac{1}{2}\deg\Gamma + 1 = \tfrac{1}{2}(\Gamma)^2 - 2$$

and it suffices to prove that $(\Gamma)^2 = 6$. But the class of Γ in the Néron–Severi group([34]) of V is

$$\gamma = 3\pi - \lambda_1 - \lambda_2 - \lambda_3 = 9\lambda_0 - 4\sum_{i=1}^{3}\lambda_i - 3\sum_{i=4}^{6}\lambda_i,$$

([34]) We use the notation of [20]: λ_0 is the class of a twisted cubic (corresponding to a generic line in the plane), and $\lambda_1, \ldots, \lambda_6$ are the classes of a set of six skew lines (the exceptional divisors). π denotes the class of a plane section.

The three given lines belong to two sextuplets [1], § 3, p. 70; therefore we are allowed to consider them as generators of the Néron–Severi group. For the same reason, it would be sufficient to deal with the case ϱ_6, working if necessary over a quadratic extension of k.

so that $(\gamma)^2 = 81-3\cdot16-3\cdot9 = 6$. Now, since Γ contains the four conjugates of P and has genus 1, it also contains a rational set of 2 points, by Corollary 6.3. (The reducible, or degenerate, cases are harmless, just as in the proof of Theorem 7.1.)

The other cases can be done similarly and are described in the following table:

ϱ_r	d	F_l	# (conditions)	$(\Gamma)^2$	$\deg\Gamma$	$p_a(\Gamma)$
3	4	3	16	6	6	1
3	10	4	25	21	9	7
6	4	5	40	9	9	1
6	10	6	52	30	12	10

This is very satisfactory, except for the last row, where $p_a(\Gamma) = d$ (!). But the (vector) space of sextics has dimension 84, and it includes 20 reducible surfaces containing V; hence the freedom f is equal to $64-52-1 = 11$. Therefore we can certainly impose 9 additional constraints and require that $V\cap F_6$ should have three assigned double points. Then the geometric genus will not exceed $10-3 = 7$, and this completes the proof. ■

It may be worth mentioning that, when k is a number field, the above result also follows from a theorem of Châtelet on Severi–Brauer varieties (see [21], Theorem 7, pp. 15–16) and from Proposition 4.8. But we have made no assumptions on the field k. Similarly, Skolem's result that singular cubic surfaces verify the Hasse principle [18] has an analogue in our theory:

PROPOSITION 8.2. *Over a perfect field k,* (CS) *holds for the class of singular cubic surfaces.*

Proof. By the known classification of singular cubic surfaces (see [14]), we may assume, without loss of generality, that V has only finitely many singular points, and hence at most four. The cases 1, 2 and 4 are trivial: there is always a k-rational point([35]). Therefore we need only consider the case in which V has exactly three double points.

Suppose first that $d = 4$; then there is a k-rational quartic curve Γ containing the 4 conjugates of P and the 3 double points (e.g. the intersection of two quadrics, passing also through a point not on V, so that $\Gamma\not\subset V$). The intersection of Γ and V has degree 12 and thus contains

([35]) The easiest way to see that in the case 4, is to take any twisted cubic containing the four double points. The residual intersection is a k-rational point. The same argument can be used to prove that a normal cubic surface cannot have more than 4 singular points.

a residual set of 2 points (since each of the double points counts as two intersections). Now suppose $d = 10$; then there is a curve Γ of degree 9 going through the 10 conjugates of P, the 3 double points and an additional set of 3 points (e.g. the intersection of two cubics, passing also through a point not on V, so that $\Gamma\not\subset V$). The intersection of Γ and V has degree 27 and thus contains a residual set of 8 points $(27-10-3\cdot2-3)$.

Thus the two cases $d = 4$ and $d = 10$ are solved. It remains to see whether we can apply Theorem 7.1, since V is singular! Now, we made the assumption of non-singularity only in order to avoid difficulties with the genus. But, in part (A) we used only the formula giving the arithmetic genus of a complete intersection, and we saw in the proof of Lemma 6.7 that this remains valid when V is singular. In the first subcase of part (B), we also required an upper bound on the geometric genus of an irreducible curve of degree $3l$, which was not necessarily a complete intersection, and for this we definitely need Lemma 6.7 (but a weaker estimate would suffice). We also used this result in the second subcase of part (B), but it is simpler to make use of the remark contained in footnote([32]).

Finally, the formula

$$p_a(C) = \sum_j p_a(C_j) + i - (r-1)$$

is a general theorem on non-singular surfaces, and we could have blown up the singularities of V before applying it([36]). ■

What happens in the general case when $d = 4$ or 10? If the conjugates of P lie in a plane or on a quadric respectively, the argument used in § 7 still applies; but otherwise the genus of $V\cap F_l$ cannot be made sufficiently small. This is not unlike the case of quartic curves, for which we know (Example 2.8 and Corollary 6.5) that the most we can get is a descent down to degree 3. Of course, we have seen many examples in which the conjecture depends more on the field k than on the geometry of the surface. And so one may still be of the opinion that (CS) is plausible at least when k is a global field, since the local result holds. But it is not clear how one could prove a globalization theorem.

Added in proof. As I found out recently, Theorem 6.1 has also been discussed by B. Segre in Rendiconti Accad. Naz. Lincei, 13 (1952), pp. 335–340.

Another argument for Proposition 8.2, which in particular avoids the use of Lemma 6.7, will appear shortly in Compositio Mathematica.

It is my pleasant duty to thank Professors Cassels, Swinnerton-Dyer and Zariski for their very generous help while I was engaged in this research.

([36]) Alternatively, we may use the much more general formula established by Hironaka: [6], Theorem 3, p. 190.

References

[1] F. Châtelet, *Points rationnels sur certaines surfaces cubiques*, Coll. Int. CNRS, Clermont–Ferrand (1964), pp. 67–75.

[2] Cl. Chevalley, *Introduction to the Theory of Algebraic Functions of one Variable*, Amer. Math. Soc. 1951.

[3] D. F. Coray, *Arithmetic on cubic surfaces*, thesis; Trinity Coll., Cambridge 1974.

[4] (V. B. Dem'janov) В. Б. Демьянов, *О кубических формах в дискретно нормированных полях*, Докл. АН СССР 74 (1950), pp. 889–891.

[5] D. Hilbert and A. Hurwitz, *Über die diophantischen Gleichungen vom Geschlecht Null*, Acta Math. 14 (1891), pp. 217–224.

[6] H. Hironaka, *On the arithmetic genera and the effective genera of algebraic curves*, Memoirs Coll. of Sc. Univ. Kyoto 30 (1956), pp. 177–195.

[7] S. Lang, *Diophantine Geometry*, Interscience 1962.

[8] — *Algebra*, New York, London 1965.

[9] D. Mumford, *Lectures on curves on an algebraic surface*, Princeton 1966.

[10] M. Noether, *Zur Grundlegung der Theorie der algebraischen Raumcurven*, Abh. Akad. Wissenschaften zu Berlin (1882), 120 p. [also: J. Crelle 93 (1882), pp. 271–318 (extract)].

[11] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, J. Math. Pures Appl. 7 (1901), pp. 161–233.

[12] M. Rosenlicht, *Equivalence relations on algebraic curves*, Ann. of Math. 56 (1952), pp. 169–191.

[13] I. R. Šafarevič, *Basic Algebraic Geometry*, Berlin 1974.

[14] B. Segre, *On arithmetical properties of singular cubic surfaces*, J. London Math. Soc. 19 (1944), pp. 84–91.

[15] — *On the rational solutions of homogeneous cubic equations in four variables*, Math. Notae Univ. Rosario 11 (1951), pp. 1–68.

[16] J.-P. Serre, *Groupes algébriques et corps de classes*, Paris 1959.

[17] — *Corps locaux*, Paris 1962.

[18] Th. Skolem, *Einige Bemerkungen über die Auffindung der rationalen Punkte auf gewissen algebraischen Gebilden*, Math. Zeitschr. 63 (1955), pp. 295–312.

[19] T. A. Springer, *Some properties of cubic forms over fields with a discrete valuation*, Proc. Kon. Ned. Akad. v. Wet. (1955), pp. 512–516.

[20] H. P. F. Swinnerton-Dyer, *The birationality of cubic surfaces over a given field*, Michigan Math. Journ. 17 (1970), pp. 289–295.

[21] — *Applications of Algebraic Geometry to Number Theory*, Proc. Symp. AMS, 20 (1971), pp. 1–52.

[22] A. Weil, *Foundations of Algebraic Geometry*, 2nd ed., Amer. Math. Soc. 1962.

[23] — *Courbes algébriques et variétés abéliennes*, Paris 1971 (= 1948).

[24] O. Zariski, *Introduction to the problem of minimal models in the theory of algebraic surfaces*, Publ. Math. Soc. of Japan, 1958.

[25] — *An Introduction to the Theory of Algebraic Surfaces*, Springer Lect. Not. 83, 1969.

[26] — *Collected Papers I*, Cambridge 1972.

Received on 18. 1. 1975 (662)

ACTA ARITHMETICA
XXX (1976)

Comportement local des fonctions à série de Fourier lacunaire

par

MICHEL BRUNEAU (Le Belvedere, Tunis)

En hommage au professeur A. Zygmund

La propriété la plus remarquable des fonctions à série de Fourier lacunaire est qu'il suffit de connaître leur comportement au voisinage de l'origine pour en déduire leur comportement au voisinage de chaque point. Mais si l'on s'interesse non plus à leur ,,nature'', mais plus précisément à leur ,,allure'', il est nécessaire, pour obtenir une propriété de cet ordre, d'adjoindre à la notion de ,,lacunarité'' celle ,,d'équilibre''.

I. Séries de Fourier lacunaires et équilibrées.

(a) Suites équilibrées. $\boldsymbol{T}$ désigne le tore $\boldsymbol{R}/\boldsymbol{Z}$ identifié à $[0,1[$. $\{\cdot\}$ est la partie fractionnaire. Une suite (μ_n) de nombres réels strictement positifs, tendant vers $+\infty$, est dite *équilibrée* si, pour presque tout $0 \leqslant x < 1$, la suite à valeurs dans $\boldsymbol{T}^{\boldsymbol{N}}$

$$n \to (\{\mu_n x\}, \{\mu_{n+1} x\}, \ldots, \{\mu_{n+k} x\}, \ldots) \tag{1}$$

admet 0 pour valeur d'adhérence; par ailleurs elle est dite *lacunaire* si

$$\inf_{n \in \boldsymbol{N}} \frac{\mu_{n+1}}{\mu_n} > 1 \tag{2}$$

et *à rapports bornés* si

$$\sup_{n \in \boldsymbol{N}} \frac{\mu_{n+1}}{\mu_n} < +\infty. \tag{2'}$$

Pour tout nombre réel $\theta > 1$, la suite (θ^n) est équilibrée (voir [5]). En revanche il existe des suites lacunaires et à rapports bornés qui ne sont pas équilibrées; c'est ainsi le cas de la suite (2^n+1).

(b) Fonctions à série de Fourier équilibrée. Une fonction $f: \boldsymbol{T} \to \boldsymbol{R}$, admettant un développement en série de Fourier

$$\sum_{k=0}^{+\infty} (a_k \cos 2\pi n_k x + \beta_k \sin 2\pi n_k x)$$