$p = 5;\ 1 \leqslant r \leqslant n \leqslant 25$

1																								
1	1																							
1	3	1																						
1	2	1	1																					
1	0	0	0	1																				
1	1	0	0	0	1																			
1	3	1	0	0	1	1																		
1	2	1	1	0	1	3	1																	
1	0	0	0	1	1	2	1	1																
1	1	0	0	0	2	0	0	0	1															
1	3	1	0	0	2	2	0	0	0	1														
1	2	1	1	0	2	1	2	0	0	1	1													
1	0	0	0	1	2	4	2	2	0	1	3	1												
1	1	0	0	0	3	0	0	0	2	1	2	1	1											
1	3	1	0	0	3	3	0	0	0	3	0	0	0	1										
1	2	1	1	0	3	4	3	0	0	3	3	0	0	0	1									
1	0	0	0	1	3	1	3	3	0	3	4	3	0	0	1	1								
1	1	0	0	0	4	0	0	0	3	3	1	3	3	0	1	3	1							
1	3	1	0	0	4	4	0	0	0	1	0	0	0	3	1	2	1	1						
1	2	1	1	0	4	2	4	0	0	1	1	0	0	0	4	0	0	0	1					
1	0	0	0	1	4	3	4	4	0	1	3	1	0	0	4	4	0	0	0	1				
1	1	0	0	0	0	0	0	0	4	1	2	1	1	0	4	2	4	0	0	1	1			
1	3	1	0	0	0	0	0	0	0	0	0	0	0	1	4	3	4	4	0	1	3	1		
1	2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	1	2	1	1	
1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

References

[1] L. Carlitz, *A problem in partitions related to the Stirling numbers*, Bull. Amer. Math. Soc. 70 (1964), pp. 275-278.

[2] — *Single variable Bell polynomials*, Collectanea Mathematica 14 (1962), pp. 13-25.

[3] E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier*, Bull. Soc. Math. France 6 (1878), pp. 49-54.

[4] J. Riordan, *Combinatorial Analysis*, New York 1958.

[5] J. Touchard, *Propriétés arithmétiques de certains nombres recurrents*, Ann. Soc. Sci., Bruxelles, A 53 (1933), pp. 21-31.

Reçu par la Rédaction le 11. 5. 1964

ACTA ARITHMETICA
X (1965)

Systems of three quadratic forms

by

B. J. Birch (Manchester) and D. J. Lewis (Ann Arbor, Mich.)*

1. Introduction. Artin conjectured that a set of forms $f_1, \ldots, f_r$ of degrees $d_1, \ldots, d_r$ respectively, in n variables over a $\mathfrak{p}$-adic field k has a common non-trivial zero in k provided that $n > \sum d_i^2$. This conjecture has been verified in the following cases: (i) one quadratic form ([9]), (ii) one cubic form ([7], [11], [6], [14]), (iii) two quadratic forms ([8], [2]), (iv) one quintic form ([1]) and (v) one form of degree 7 or 11 ([10]), provided in cases (iv) and (v) that the residue class field is large enough.

As Artin has shown, it is sufficient for the proof of the conjecture to show that it holds for the case of a single form of arbitrary degree. On the other hand, for example, if $N(x)$ is the reduced norm form of a division algebra of degree two over k, then N is a quadratic form over k in four variables that has only the trivial zero in k; and if $f_1, \ldots, f_4$ are quadratic forms over k then $f = N(f_1, \ldots, f_4)$ is a quartic form whose zeros in k are precisely the common zeros in k of $f_1, \ldots, f_4$. Thus, in examining the truth of the conjecture for a single quartic we need to know whether the conjecture is valid for a system of quadratics. It is this last problem which we shall investigate in this note. Many of our results hold for any system of quadratics, but eventually the work becomes so involved that we restrict ourselves to three quadratics. Our arguments are in essence very similar to those used in [2]; however, our proof is far more involved, because in contrast to the case of two quadratics there does not seem to be any elegant utilizable property of a system of three quadratics which has only singular zeros (compare Lemma 2 of [2]). For reasons which will become clear later, our proof will work only if the residue class field is not too small and has odd characteristic.

Throughout this note, k will denote a $\mathfrak{p}$-adic field with ring of integers $\mathfrak{O}$ with maximal prime ideal $\mathfrak{p}$. The residue class field $\mathfrak{O}/\mathfrak{p}$ will be denoted by k^*. We denote the characteristic of k^* by p and the number

* This paper was begun during a period in which the authors received support from the National Science Foundation under Grant GP88.

of elements by q. The homomorphism of $\mathfrak{O}$ to k^* may be extended in a natural way to a homomorphism of the polynomial ring $\mathfrak{O}[x_1, \ldots, x_n]$ to $k^*[x_1, \ldots, x_n]$; we denote the image of $f(\boldsymbol{x})$ by $f^*(\boldsymbol{x})$. When we speak of a zero of a set of forms, we will always mean a nontrivial zero; when we speak of a point we will normally mean projective point. A vector $\boldsymbol{z}$ is a *nonsingular* zero of a set $f_1, \ldots, f_r$ if $f_1(\boldsymbol{z}) = \ldots = f_r(\boldsymbol{z}) = 0$ and the matrix $(\partial f_i/\partial x_j)$ evaluated at $\boldsymbol{z}$ has rank r.

We say that a system $f_1, \ldots, f_r$ of forms over a given field has *order* t provided we can express these forms in terms of t linear forms and no fewer, i. e.

$$f_\nu = \sum_{i,j=1}^{t} a_{ij}^{(\nu)} L_i L_j,$$

where the $a_{ij}^{(\nu)}$ and the coefficients of the L_i are in a given field. The order of a system depends only on the minimal field containing the coefficients of the system; for relative to a field K, t is less than n if and only if the relations

$$\sum_{i=1}^{n} z_i \frac{\partial f_\nu}{\partial x_i} = 0 \qquad (\nu = 1, \ldots, r)$$

have a nontrivial solution with the z_i in K. But these equations are equivalent to a system of linear equations in the z_i with coefficients in the minimal field of the system, and hence are solvable in K if and only if they are solvable in the minimal field.

A system of forms in n variables is said to be *nondegenerate* if its order is n.

2. Well known lemmas. We need to quote a number of well known results.

Lemma 1. *A set of r quadratic forms in $n > 2r$ variables with coefficients in a finite field k^* has a zero in k^* and the number of such projective points is congruent to* 1 *modulo the characteristic of k^*.*

This is but a special case of theorems of Chevalley [5] and Warning [15]. Note that both parts of the conclusion may break down if $n \leqslant 2r$.

Lemma 2. *Let f be a non-degenerate quadratic form over the finite field k^*. If the order of f is at least* 3 *then every zero of f is nonsingular and the zeros of f do not lie in a hyperplane.*

This is essentially Lemma 1 of [2].

Lemma 3. *Let $f_1, \ldots, f_r$ be quadratic forms in n variables over the finite field k^*. Then there are at least $n-2r$ linearly independent zeros in k^* which are common zeros of $f_1, \ldots, f_r$.*

This is easily derived from Lemma 1 using induction.

Lemma 4. *If f is a nonzero form of degree d in n variables over the finite field k^* with q elements then f has at most dq^{n-1} zeros in k^*.*

Proof. There is nothing to prove if $d \geqslant q$. Suppose $d < q$. Since f is not the zero polynomial there is a point not on $f = 0$. So we may suppose that $f(\boldsymbol{e}_1) \neq 0$. Then

$$f = b_0 x_1^d + b_1(x_2, \ldots, x_n) x_1^{d-1} + \ldots + b_d(x_2, \ldots, x_n),$$

where $b_0 \neq 0$ and the b_ν are forms of degree ν in $x_2, \ldots, x_n$. For each choice of $x_2, \ldots, x_n$ there are at most d values of x_1 for which $f = 0$. Hence the conclusion follows.

Lemma 5. *Let f and g be forms of degree* 2 *and d, respectively, over a finite field k^* and suppose the order of f is at least* 3. *If every nonsingular zero of f in k^* is a zero of g then f is a factor of g provided k^* contains sufficiently many elements.*

Proof. Since f has order at least 3, it has a nonsingular zero in k^*. Hence the quadric $f = 0$ can be mapped birationally over k^* onto a hyperplane. Consequently the quadric $f = 0$ has approximately q^{n-2} nonsingular points over k^*. On the other hand f is absolutely irreducible and if g is not a multiple of f then the locus $f = g = 0$ has projective dimension $n-3$ and so has $O(q^{n-3})$ points in k^*. If q is sufficiently large this contradicts the hypothesis that each nonsingular zero of f is on $g = 0$.

To obtain estimates for how large q must be for Lemma 5 to hold one needs to follow a more tedious approach. Following a change of variables one can assume

$$f = \sum_{i=1}^{s} x_{2i-1} x_{2i} + f',$$

where f' involves variables other than $x_1, \ldots, x_{2s}$ and has order at most 2. Thus $f = 0$ contains many linear spaces over k^* of relatively high dimension. By using this information one can show

Corollary. *If k^* contains at least* 7 *elements the conclusion of Lemma* 5 *holds for the cases $d = 2$ and* 3.

Lemma 6. *There is a constant $\lambda(d, d')$ such that if k^* is a finite field with at least $\lambda(d, d')$ elements and if f, g are forms over k^* of degrees d, d' respectively, with f not of the form ηh^2 (where η is a nonsquare of k^*) then there is a point $\boldsymbol{a}$, with coordinates in k^*, not on $g = 0$ for which $f(\boldsymbol{a})$ is a nonzero square of k^*.*

This lemma is a slight modification of a theorem of Carlitz, see [3], [4], [12], [1]. One can easily show that,

Corollary. $\lambda(6, 4) < 49$.

LEMMA 7. *Let f, g be two quadratic forms over a finite field k^*. If the order of the pair f, g is at least 5 and the order of each form in the pencil $\lambda f+\mu g$ is at least 3 then the pair f, g has a nonsingular zero in k^*.*

The proof of this lemma is straightforward and occurs in the proof of the Theorem of [2].

LEMMA 8. *If $f_1, \ldots, f_r$ are forms with coefficients in $\mathfrak{O}$ such that the system $f_1, \ldots, f_r$ has a nonsingular zero in k^* then the system $f_1, \ldots, f_r$ has a zero in $\mathfrak{O}$.*

This is a well known application of Newton approximation — just a version of Hensel's lemma. See, for example, Lemma 6 in [2].

3. An invariant. In this section we define an invariant of a system of $\mathfrak{p}$-adic quadratic forms; in § 4 we will apply this invariant to obtain a method of reduction. This particular reduction technique was first used by Davenport ([6]); we subsequently used it in [2] and it was also used in [10].

Associated to each quadratic form f in n variables over a field not of characteristic 2 there is a $n\times n$ symmetric matrix F such that

$$f(\boldsymbol{x}) = \boldsymbol{x}'F\boldsymbol{x}.$$

If $f_1, \ldots, f_r$ is a set of quadratic forms, we define

$$P(\lambda) = P(\lambda_1, \ldots, \lambda_r) = \det(\lambda_1 F_1+\ldots+\lambda_r F_r),$$

where F_i is the matrix associated with f_i. Let

$$R_{\lambda_1,\ldots,\lambda_r}\left(\frac{\partial P}{\partial\lambda_1}, \ldots, \frac{\partial P}{\partial\lambda_r}\right) = \vartheta(f_1, \ldots, f_r)$$

be the resultant of the polynomials $\partial P/\partial\lambda_1, \ldots, \partial P/\partial\lambda_r$ with respect to the variables $\lambda_1, \ldots, \lambda_r$. Then ϑ satisfies the following identity:

LEMMA 9. *Let $A = (a_{ij})$ be an $r\times r$ matrix and T be an $n\times n$ matrix, both defined over k. If $f_1, \ldots, f_r$ is a system of quadratic forms over k, then*

$$\vartheta\big(a_{11}f_1(T\boldsymbol{x})+\ldots+a_{1r}f_r(T\boldsymbol{x}), \ldots, a_{r1}f_1(T\boldsymbol{x})+\ldots+a_{rr}f_r(T\boldsymbol{x})\big)$$
$$= (\det A)^{n(n-1)^{r-1}}(\det T)^{2r(n-1)^{r-1}}\vartheta(f_1, \ldots, f_r).$$

This is easy enough, though tedious, to verify. For properties of the function ϑ, see [13].

LEMMA 10. *Let $f_1, \ldots, f_r$ be quadratic forms with coefficients in $\mathfrak{O}$. Then there are sequences $f_\nu^{(m)}$ of forms, all with coefficients in $\mathfrak{O}$, such that*

$$\lim_{m\to\infty} f_\nu^{(m)} = f_\nu, \quad \nu = 1, \ldots, r,$$

and such that for each m

$$\vartheta(f_1^{(m)}, \ldots, f_r^{(m)}) \neq 0.$$

This is essentially obvious, compare step 4 on pp. 114-115 of [2].

LEMMA 11. *If $f_\nu^{(m)}$ and f_ν, for $\nu = 1, \ldots, r$ and $m = 1, \ldots,$ are quadratic forms over k such that $\lim_{m\to\infty} f_\nu^{(m)} = f_\nu$ for each ν and such that for each m the set $f_1^{(m)}, \ldots, f_r^{(m)}$ has a nontrivial zero in k then the set $f_1, \ldots, f_r$ has a nontrivial zero in k.*

If a system of forms over k have a nontrivial zero in k they have a zero whose coordinates are in $\mathfrak{O}$ but not all are in $\mathfrak{p}$. One now uses the compactness of $\mathfrak{O}$ to obtain the Lemma.

COROLLARY. *In order to prove that any set of quadratic forms $f_1, \ldots, f_r$ in $4r+1$ variables over a $\mathfrak{p}$-adic field k has a $\mathfrak{p}$-adic zero it will be sufficient to prove this for sets of quadratic forms over $\mathfrak{O}$ with $\vartheta(f_1, \ldots, f_r) \neq 0$.*

This is clear from Lemmas 10 and 11, since every form over k is a multiple of a form over $\mathfrak{O}$.

4. Reduced sets of quadratic forms. Two sets of quadratic forms $f_1, \ldots, f_r$ and $g_1, \ldots, g_r$ over k are *equivalent* if there is a $r\times r$ nonsingular matrix $A = (a_{\nu\mu})$ and a nonsingular $n\times n$ matrix $T = (t_{ij})$, both with elements in k, such that

$$T'G_\nu T = a_{\nu1}F_1+\ldots+a_{\nu r}F_r \quad (\nu = 1, \ldots, r);$$

here as usual F, G are the matrices of the forms f, g. Clearly this is an equivalence relation on sets of quadratic forms in n variables. Given two equivalent sets of quadratic forms, one set has a zero in k if and only if the other set has a zero in k. Thus in our study of the existence of zeros of a set of quadratic forms, we can always replace a set by an equivalent set. In particular, we will always replace a set by an equivalent set with $\mathfrak{p}$-adic integer coefficients. Clearly $\vartheta(f_1, \ldots, f_r) \neq 0$ if and only if ϑ is nonzero for each set equivalent to $f_1, \ldots, f_r$.

We say two equivalent sets are *unimodular equivalent* if A and T are matrices over $\mathfrak{O}$ with unit determinants. If $f_1, \ldots, f_r$ and $g_1, \ldots, g_r$ are unimodular equivalent sets of forms with coefficients in $\mathfrak{O}$, then $f_1^*, \ldots, f_r^*$ and $g_1^*, \ldots, g_r^*$ are equivalent sets of forms over k^*.

If $f_1, \ldots, f_r$ are forms over $\mathfrak{O}$ with $\vartheta(f_1, \ldots, f_r) \neq 0$, write

$$\vartheta(f_1, \ldots, f_r) = \pi^{I(f_1,\ldots,f_r)};$$

so that $I(f_1, \ldots, f_r)$ is a nonnegative rational integer. I is an invariant of unimodular equivalent sets.

A set $f_1, \ldots, f_r$ with coefficients in $\mathfrak{O}$ will be said to be *reduced* if $\vartheta(f_1, \ldots, f_r) \neq 0$ and if

$$I(f_1, \ldots, f_r) \leqslant I(g_1, \ldots, g_r)$$

for every set of forms $g_1, \ldots, g_r$ with coefficients in $\mathfrak{O}$ equivalent to $f_1, \ldots, f_r$. Note that any set of forms unimodular equivalent to a reduced set is a reduced set. Obviously, each set of forms over k is equivalent to a reduced set of forms over $\mathfrak{O}$.

Associated with any set of forms $f_1, \ldots, f_r$ over $\mathfrak{O}$ is the order ϱ of the set $f_1^*, \ldots, f_r^*$ over k^*. To each set of quadratic forms $f_1, \ldots, f_r$ in n variables, with coefficients in $\mathfrak{O}$, we associate two other integers, H and h. H will denote the maximal number of linearly independent zeros in k^* of the set $f_1^*, \ldots, f_r^*$, while $h-1$ will denote the maximal dimension of the linear projective subspaces over k^* contained in the set of zeros of $f_1^*, \ldots, f_r^*$. Clearly $H \geqslant h \geqslant n-\varrho$. Two unimodular equivalent sets have the same ϱ, H and h.

LEMMA 12. *Let $f_1, \ldots, f_r$ be a reduced set of forms in n variables over $\mathfrak{O}$. Let Λ be the $\mathfrak{O}$-module generated by the f_ν. Let $g_1, \ldots, g_s$ be a subset of Λ for which $g_1^*, \ldots, g_s^*$ are linearly independent over k^*. Let ϱ, H and h be defined for the set $g_1, \ldots, g_s$. Put*

$$\sigma = h-(n-\varrho), \qquad \Sigma = H-(n-\varrho). \tag{1}$$

Then

$$h \leqslant n(1-s/2r), \tag{2}$$

$$\varrho \geqslant \sigma+sn/2r, \tag{3}$$

$$\Sigma \geqslant \sigma+1, \quad \text{if} \quad n \geqslant 4r+1. \tag{4}$$

Proof. Clearly $s \leqslant r$. We can choose $g_{s+1}, \ldots, g_r$ from Λ so that the set $g_1, \ldots, g_r$ is unimodular equivalent to $f_1, \ldots, f_r$. Hence $g_1, \ldots, g_r$ is a reduced set. We make a unimodular change of variable so that $g_1^*, \ldots, g_s^*$ involve the variables $x_1, \ldots, x_\varrho$ exactly and so that

$$\lambda_1 \boldsymbol{e}_1+\ldots+\lambda_\sigma \boldsymbol{e}_\sigma+\lambda_{\varrho+1}\boldsymbol{e}_{\varrho+1}+\ldots+\lambda_n \boldsymbol{e}_n$$

is a maximal linear subspace contained in the set of zeros of $g_1^*, \ldots, g_s^*$ in k^*. Let W be the linear transformation,

$$W\boldsymbol{e}_\nu = \pi \boldsymbol{e}_\nu \quad (\nu = \sigma+1, \ldots, \varrho), \qquad W\boldsymbol{e}_\nu = \boldsymbol{e}_\nu \quad (\nu = 1, \ldots, \sigma, \varrho+1, \ldots, n).$$

W is a nonsingular linear transformation over k, and the set

$$\pi^{-1}g_1(W\boldsymbol{x}), \ldots, \pi^{-1}g_s(W\boldsymbol{x}), g_{s+1}(W\boldsymbol{x}), \ldots, g_r(W\boldsymbol{x})$$

has integral coefficients and is equivalent to the reduced set $g_1, \ldots, g_r$. But

$$I\big(\pi^{-1}g_1(W\boldsymbol{x}), \ldots, g_r(W\boldsymbol{x})\big) = [2r(\varrho-\sigma)-sn](n-1)^{r-1}+I(g_1, \ldots, g_r)$$

and since $g_1, \ldots, g_r$ is a reduced set we have

$$2r(\varrho-\sigma) \geqslant sn,$$

and hence

$$2r(n-h) \geqslant sn.$$

These two relations yield (3) and (2), respectively.

If $n \geqslant 4r+1$, then (3) implies $\varrho \geqslant \sigma+2s+1$ and then (4) follows directly from Lemma 3.

COROLLARY. *Let $f_1, \ldots, f_r$ be a reduced set of forms in $n \geqslant 4r+1$ variables over $\mathfrak{O}$. Then no form in the linear system*

$$\lambda_1 f_1^*+\ldots+\lambda_r f_r^*$$

can be expressed as

$$a(L_1L_2-L_3L_4),$$

where $a \in k^*$ and $L_1, \ldots, L_4$ are linear forms over k^*.

Proof. Suppose such a form exists, say

$$g_1 = a(L_1L_2-L_3L_4) = \lambda_1 f_1^*+\ldots+\lambda_r f_r^*.$$

Applying Lemma 12 with $s = 1$ gives $h \leqslant n\left(1-\dfrac{1}{2r}\right)$; on the other hand $h = n-2$. These two statements imply $n \leqslant 4r$, contrary to the hypothesis.

LEMMA 13. *Let $f_1, \ldots, f_r$ be a reduced set of quadratic forms in $n \geqslant 4r+1$ variables. Then the order ϱ of $f_1^*, \ldots, f_r^*$ is at least $2r+2$ and $\Sigma \geqslant 3$.*

Proof. It follows from (3) that $\varrho \geqslant 2r+1$ and hence, by Lemma 1, we have $\sigma \geqslant 1$. But then (3) implies $\varrho \geqslant 2r+2$ and (4) implies $\Sigma \geqslant 2$. It follows from the second part of Lemma 1 that the set $f_1^*, \ldots, f_r^*$ has at least $1+p$ projective zeros in k^* (p is the characteristic of k^*). Consequently, if $\Sigma = 2$ then the surfaces $f_\nu^* = 0$ would have a common line of zeros, whence $\sigma = 2$ contrary to (4). Therefore $\Sigma \geqslant 3$.

LEMMA 14. *If $f_1, \ldots, f_r$ is a reduced set of quadratic forms in $n \geqslant 4r+1$ variables over $\mathfrak{O}$, then either $\Sigma \geqslant 4$ or $\sigma \geqslant 2$.*

Proof. From Lemma 13 we have $\varrho \geqslant 2r+2$ and $\Sigma \geqslant 3$. Following a unimodular change of variable we may assume that $f_1^*, \ldots, f_r^*$ is a set of forms in $x_1, \ldots, x_\varrho$, that $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_\Sigma$ are zeros of $f_1^*, \ldots, f_r^*$, and that any zero of $f_1^*, \ldots, f_r^*$ lies in the linear space

$$\lambda_1 \boldsymbol{e}_1+\ldots+\lambda_\Sigma \boldsymbol{e}_\Sigma.$$

Let M denote the number of points over k^* on the locus $f_1^* = \ldots = f_r^* = 0$ which lie on the hyperplane $x_1 = 0$. Then M is the number of points on the locus $f_1^* = \ldots = f_r^* = x_0^2-\eta x_1^2 = 0$, where η is a nonsquare of k^*. This is a set of $r+1$ forms in $2r+3$ variables and hence by Lemma 1, $M \equiv 1 (\mathrm{mod}\, p)$. If $\Sigma = 3$ then $M \geqslant 2$ and consequently $M \geqslant 3$. But then there is a point on $\lambda_2 e_2 + \lambda_3 e_3$ other than e_2 and e_3 on $f_1^* = \ldots = f_r^* = 0$. Consequently the line $\lambda_2 e_2 + \lambda_3 e_3$ is on $f_1^* = \ldots = f_r^* = 0$, and hence $\sigma \geq 2$.

5. Three quadratics. We now restrict our attention to the case of three quadratic forms.

From now on, k will always be a $\mathfrak{p}$-adic field whose residue class field k^* has odd characteristic and contains at least 49 elements, i.e. $p \geq 3$, $q \geq 49$. We consider a reduced set of three quadratic forms f_1, f_2, f_3 over $\mathfrak{O}$ in at least 13 variables. We let ϱ denote the order of f_1^*, f_2^*, f_3^*, over k^*. We may suppose (passing to a unimodular equivalent set, if necessary) that f_1^*, f_2^*, f_3^* are forms in the variables $x_1, x_2, \ldots, x_\varrho$. Then the equations $f_1^* = f_2^* = f_3^* = 0$ determine a locus V^* in $(\varrho-1)$ dimensional k^* space. In our work we can always pass to a unimodular equivalent set of forms and such passage will not affect our normalization so long as the change of variable is restricted to the variables $x_1, \ldots, x_\varrho$.

We shall let Λ denote the linear system $\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$ over k and Λ^* shall denote the linear system $\lambda_1 f_1^* + \lambda_2 f_2^* + \lambda_3 f_3^*$ over k^*.

LEMMA 15. *If V^* has a nonsingular point then f_1, f_2, f_3 have a nontrivial common zero in k.*

This is immediate from Lemma 8.

LEMMA 16. *If V^* contains a line defined over k^* then V^* has a nonsingular point.*

Proof. In this and later proofs we assume that all the points in V^*, with coordinates in k^*, are singular zeros of f_1^*, f_2^*, f_3^*. We gradually accumulate more and more information about the forms until we obtain a contradiction.

The dimension of the largest linear space contained in V^*, defined over k^*, is $\sigma-1$. By hypothesis $\sigma \geq 2$. We can therefore suppose, after possibly applying a unimodular linear transformation on $x_1, \ldots, x_\varrho$, that V^* contains the linear space

$$x_{\sigma+1} = \ldots = x_\varrho = 0.$$

Then

$$f_\nu^* = x_1 L_{\nu 1} + \ldots + x_\sigma L_{\nu\sigma} + g_\nu \quad (\nu = 1, 2, 3),$$

where the L's are linear forms and the g's are quadratic forms in $x_{\sigma+1}, \ldots, x_\varrho$. Since all the points of V^* are singular, there are a_1, a_2, a_3 in k^* (not all 0) so that

$$a_1 L_{1\mu} + a_2 L_{2\mu} + a_3 L_{3\mu} = 0 \quad (\mu = 1, \ldots, \sigma).$$

Upon making a unimodular change in basis of the linear system Λ, we may assume that f_3^* is free of $x_1, \ldots, x_\sigma$.

Now suppose the identical rank of the matrix

$$\mathscr{L} = \begin{pmatrix} L_{11} & L_{12} & \ldots & L_{1\sigma} \\ L_{21} & L_{22} & \ldots & L_{2\sigma} \end{pmatrix}$$

were 2; renumbering variables, we may suppose that

$$L_{11}L_{22} - L_{12}L_{21} = \Delta$$

is not identically 0. By the Corollary to Lemma 12, f_3^* and Δ are not proportional and so by Lemma 5 there is a nonsingular zero of f_3^* with $\Delta \neq 0$. We may solve for x_1, x_2 to obtain a nonsingular point of V^*; a contradiction. Hence the identical rank of $\mathscr{L}$ cannot be 2. Neither can it be 0, for if it were then ϱ would not be the order of f_1^*, f_2^*, f_3^*. Therefore the rank of $\mathscr{L}$ is 1. Changing the basis for Λ, we may now suppose that f_2^* and f_3^* are free of $x_1, \ldots, x_\sigma$. Furthermore $L_{11}, \ldots, L_{1\sigma}$ must be linearly independent over k^*, for otherwise the order of f_1^*, f_2^*, f_3^* would be less than ϱ.

Let τ be the order of the pair f_2^*, f_3^*. Following a unimodular transformation leaving $x_1, \ldots, x_\sigma, x_{\varrho+1}, \ldots, x_n$ fixed, we may assume that f_2^*, f_3^* are forms in $x_{\sigma+1}, \ldots, x_{\sigma+\tau}$. Since V^* contains a $\sigma-1$ dimensional linear space, it follows from Lemma 12 that $\varrho \geq \sigma+7$. Hence V^* contains a point $\boldsymbol{a}$ which lies on $x_1 = \ldots = x_\sigma = 0$. If $\boldsymbol{a}$ also lies on $x_{\sigma+1} = \ldots = x_{\sigma+\tau} = 0$ then V^* would contain a σ dimensional linear space; contrary to the definition of σ. Hence some one of the coordinates $a_{\sigma+1}, \ldots, a_{\sigma+\tau}$, is not 0, say $a_{\sigma+1} \neq 0$. Replacing x_ν $(\nu \neq \sigma+1)$ by $x_\nu + a_\nu a_{\sigma+1}^{-1} x_{\sigma+1}$, we see that we may assume $e_{\sigma+1}$ is on V^*.

If $e_{\sigma+1}$ were a singular point of $f_2^* = f_3^* = 0$, we could, following a unimodular change of basis of the pencil $\lambda_2 f_2 + \lambda_3 f_3$, assume that $f_2^* = x_{\sigma+1}M + g_2$, $f_3^* = g_3$, where M, g_2, g_3 are forms in $x_{\sigma+2}, \ldots, x_{\sigma+\tau}$ and M is not identically 0. By Lemma 12, the order of g_3 is at least 3.

Put $L_{11}(0, x_{\sigma+2}, \ldots, x_\varrho) = L'_{11}$. If L'_{11} is not identically zero, then by Lemma 5 and its Corollary there is a zero of g_3 with $L'_{11}M \neq 0$, and this leads to a nonsingular point on V^*. If L'_{11} is identically zero, then L_{11} is a multiple of $x_{\sigma+1}$. It would then follow from Lemma 5 and its Corollary that there is a nonsingular zero of g_3 for which $Mg_2 \neq 0$, and again this leads to a nonsingular point of V^*.

Finally suppose $e_{\sigma+1}$ is a nonsingular point on $f_2^* = f_3^* = 0$ but is a singular point on V^*. The forms $L_{11}, \ldots, L_{1\sigma}$ must all vanish at $e_{\sigma+1}$, for otherwise it is easy to demonstrate the existence of a nonsingular point on V^*. Hence

$$f_1^* = x_1 L_{11} + \ldots + x_\sigma L_{1\sigma} + x_{\sigma+1} M_1 + h_1,$$

$$f_2^* = x_{\sigma+1} M_2 + h_2,$$

$$f_3^* = x_{\sigma+1} M_3 + h_3,$$

where the L's, M's and h's are forms in $x_{\sigma+2}, \dots, x_\varrho$. But then we see that the linear space $x_1 = \dots = x_\sigma = x_{\sigma+1} = 0$ is on V^*; contrary to the definition of σ.

This completes the proof of Lemma 16.

LEMMA 17. *If V^* contains a planar conic defined over k^*, then V^* has a nonsingular point.*

Proof. We assume each point on V^* with coordinates in k^* is a singular point and obtain a contradiction. By Lemma 16 we may suppose that V^* does not contain a line. By unimodular transformation, we may suppose that the conic with equation $x_2^2 = x_1x_3$ lying in the plane $\lambda_1e_1 + \lambda_2e_2 + \lambda_3e_3$ is contained in V^*; then each of the forms $f^*(x_1, x_2, x_3, 0, \dots, 0)$ is proportional to $x_2^2 - x_1x_3$, so by a unimodular change of basis for the linear system Λ, we may suppose that

$$f_1^* = x_2^2 - x_1x_3 + x_1L_1 + x_2L_2 + x_3L_3 + g_1,$$
$$f_2^* = x_1M_1 + x_2M_2 + x_3M_3 + g_2,$$
$$f_3^* = x_1N_1 + x_2N_2 + x_3N_3 + g_3,$$

where the L_ν, M_ν, N_ν are linear forms and the g are quadratic forms in $x_4, \dots, x_\varrho$.

For all s, t in k^*, $(s^2, st, t^2, 0, \dots, 0)$ is a point of V^* which must be singular; hence there exist a, b in k^* such that $aN_\nu + bM_\nu = 0$, for $\nu = 1, 2, 3$. Again changing our basis for Λ, we may suppose that N_1, N_2, N_3 are identically zero, so that f_3^* is free of x_1, x_2, x_3. By Lemma 12, $g_3 = f_3^*$ has order at least 4. It is now convenient to make a further transformation on x_1, x_2, x_3 leaving the other variables fixed so that the conic becomes $x_1x_2 + x_2x_3 + x_3x_1 = 0$. Our forms are thus normalized to the shape

$$f_1^* = x_1x_2 + x_2x_3 + x_3x_1 + x_1L_1 + x_2L_2 + x_3L_3 + g_1,$$
$$f_2^* = x_1M_1 + x_2M_2 + x_3M_3 + g_2, \qquad f_3^* = g_3.$$

If f_2^* is free of x_1, x_2, x_3 then by Lemmas 12 and 7 the pair f_2^*, f_3^* have a nonsingular common zero $(a_4, \dots, a_\varrho)$. Choose a_1 so that $a_1 + L_3(a_4, \dots, a_\varrho) \neq 0$, then we can choose a_2 and a_3 so that $\boldsymbol{a}$ is a nonsingular point of V^*; a contradiction. So at least one of M_1, M_2, M_3 is not identically zero.

Now suppose that there is a nonsingular zero $\boldsymbol{a} = (a_4, \dots, a_\varrho)$ of g_3 such that $M_1(\boldsymbol{a}) = 0$ and $M_2(\boldsymbol{a}) \neq M_3(\boldsymbol{a})$. Choose a_2, a_3 such that

$$a_2 + a_3 + L_1(\boldsymbol{a}) = 1, \qquad a_2M_2(\boldsymbol{a}) + a_3M_3(\boldsymbol{a}) + g_2(\boldsymbol{a}) = 0.$$

Finally put $a_1 = -a_2a_3 - a_2L_2(\boldsymbol{a}) - a_3L_3(\boldsymbol{a}) - g_1(\boldsymbol{a})$. The point $(a_1, a_2, \dots, a_\varrho)$ would be a nonsingular point on V^*. Hence our system has the property:

(I) *Any nonsingular zero of g_3 on $M_i = 0$ is also on $M_j = M_k$, where i, j, k is a permutation of 1, 2, 3.*

We now split our proof into cases, according to how many of M_1, M_2, M_3 are linearly independent.

(A) *Suppose M_1, M_2, M_3 are a linearly independent set.*

Following a unimodular change of variable on $x_4, \dots, x_\varrho$, we may suppose $M_1 = x_4$, $M_2 = x_5$, and $M_3 = x_6$. Write $g_3 = x_4S_1 + h$, where S_1 and h are forms in $x_5, x_6, \dots, x_\varrho$. By Lemma 12 the order of g_3 is at least 4, hence the order of h is at least 2. If the order of h were at least 3 then there would exist a nonsingular zero $(a_5, \dots, a_\varrho)$ of h not on $M_2 - M_3$; contrary to (I). Hence the order of h is 2 and the Corollary to Lemma 12 shows that h cannot split in k^*. Thus

$$h = aS_2^2 - bS_3^2,$$

where $ab \neq$ square and x_4, S_1, S_2, S_3 are linearly independent forms. Now there are points on $x_4 = S_2 = S_3 = 0$, $S_1 = 1$ and they are nonsingular zeros of g_3 which are on $M_1 = 0$. By (I) these points are on $M_2 - M_3 = x_5 - x_6 = 0$. Consequently

$$M_2 - M_3 = x_5 - x_6 = \alpha x_4 + \beta S_2 + \gamma S_3.$$

Since x_4, x_5, x_6 are linearly independent, one of β and γ is nonzero. Hence

$$g_3 = x_4T_1 + c(x_5 - x_6 + dT_2)^2 - eT_2^2,$$

where $ce \neq$ square and x_4, $x_5 - x_6$, T_1, T_2 are linearly independent forms.

Temporarily, let g_3', T_1', T_2', etc. denote the result of replacing x_5 by 0 in g_3, T_1, T_2, etc. Clearly T_2' and $-x_6 + dT_2'$ are not both 0. Let δ denote the order of $c(-x_6 + dT_2')^2 - e(T_2')^2$. If $\delta = 1$ then T_2 is a linear combination of x_5 and x_6 and T_1 is linearly independent of x_4, x_5 and x_6. If $\delta = 2$ then T_2 is linearly independent of x_5 and x_6. Thus, when $\delta = 1$, $g_3' = x_4T_1 + \beta x_6^2$, where $\beta \neq 0$, and hence we can find a nonsingular zero on g_3 which is on $M_2 = x_5 = 0$ and not on $M_1 - M_3 = x_4 - x_6 = 0$; contrary to (I). If $\delta = 2$ and T_1 is not proportional to x_5 then g_3' has order at least 3 and we can find a nonsingular zero of g_3 which is on $x_5 = M_2 = 0$ and which is not on $M_4 = M_6$; contrary to (I). If $\delta = 2$ and T_1 is proportional to x_5 then we can find a nonsingular zero of g_3 which is on $M_3 = x_6 = 0$ and is not on $M_1 - M_2 = 0$; contrary to (I).

(B) *Suppose M_1, M_2, M_3 generate a linear space of dimension 2.*

We may suppose M_1, M_3 are linearly independent and that $M_2 = \alpha M_1 + \beta M_3$. We shall now show that we can assume

$$M_2 = \lambda M_1 \quad \text{with} \quad \lambda \neq 0, 1.$$

If u is any unit of k, the transformation

(5) $x_i = -x_i', \quad x_j = u^{-1}(1+u)x_i'+u^{-1}x_j, \quad x_k = (1+u)x_i'+ux_k',$

with i, j, k some permutation of 1, 2, 3, is an automorph of $x_1x_2+x_2x_3+ +x_3x_1$ and it carries $x_1M_1+x_2M_2+x_3M_3$ into $x_1'M_1'+x_2'M_2'+x_3'M_3'$ where

$$M_i' = -M_i+u^{-1}(1+u)M_j+(1+u)M_k, \quad M_j' = u^{-1}M_j, \quad M_k' = uM_k.$$

Thus the unimodular transformation (5) does not change the shape of the forms f_1^*, f_2^*, f_3^*.

If $\beta \neq 1$, choose u so that $u^* = \beta-1$, and with $i = 2, j = 1, k = 3$ we obtain M_2' proportional to M_1'. If $\beta = 1 \neq \alpha$, on interchanging x_1 and x_3 and applying (5) we also obtain M_2' proportional to M_1'. If $\alpha = \beta = 1$, we have $M_2 = M_1+M_3$. On interchanging x_1 and x_2 we get that $\beta = -1$ and so again we can get M_2' proportional to M_1'. If $M_2 = M_1$, choose $u^* \neq \pm 1$, $i = 3$, $j = 1$, $k = 2$; then $M_2' = \lambda M_2'$ with $\lambda \neq 0, 1$.

We can, therefore, assume M_1, M_3 are linearly independent and $M_2 = \lambda M_1$ with $\lambda \neq 0, 1$. Make a unimodular transformation leaving x_1, x_2, x_3 fixed and such that $M_1 = x_4$, $M_3 = x_5$. Set

$$g_3 = x_4L+h,$$

where L, h are free of x_4. The order of h is at least 2. If the order of h is at least 3 there is a nonsingular zero of h with $x_5 \neq 0$ and hence there is a nonsingular zero of g_3 on $M_1 = 0$ and not on $M_2 - M_3 = 0$; contrary to (I).

If the order of h is 2, by the Corollary to Lemma 12, h cannot split in k^* and hence $h = aU^2-bV^2$, where $ab \neq$ square and U, V are linear forms. By (I), any point on $x_4 = U = V = 0$ not on $L = 0$ must be a point on $M_3 = 0$. Hence

$$M_3 = x_5 = \alpha x_4+\beta U+\gamma V,$$

where at least one of β and γ is nonzero. Then

$$g_3 = x_4T_1+c(x_5+dT_2)^2-eT_2^2,$$

with $ec \neq$ square, and x_4, x_5, T_1, T_2 are linearly independent forms. In this case, we see that there is a nonsingular zero of g_3 which is on $x_5 = M_3 = 0$ and not on $M_2-M_1 = (\lambda-1)x_4 = 0$; contrary to (I).

(C) *Suppose M_1, M_2 and M_3 span a linear space of dimension* 1.

As we saw earlier, at least one of the M_ν is not identically 0. Suppose M_2 and M_3 were identically 0, then since g_3 has order at least 4 by Lemma 4 we can find a nonsingular zero of g_3 not on $M_1 = 0$; contrary to (I). When M_3 is identically 0 and $M_2 = \lambda M_1$, we can use the transformation (5) with $i = 3, j = 1, k = 3$ to obtain a form where none of the M_ν is identically 0. Thus we may suppose that $M_2 = aM_1$, $M_3 = bM_1$, with $ab \neq 0$. To simplify later computation, we make the unimodular transformation

$$\begin{aligned} x_1 &= x_1'+\tfrac{1}{2}L_1-\tfrac{1}{2}L_2-\tfrac{1}{2}L_3, \\ x_2 &= x_2'+\tfrac{1}{2}L_2-\tfrac{1}{2}L_3-\tfrac{1}{2}L_1, \\ x_3 &= x_3'+\tfrac{1}{2}L_3-\tfrac{1}{2}L_1-\tfrac{1}{2}L_2, \\ x_\nu &= x_\nu' \quad (\nu \geq 4). \end{aligned}$$

This transformation takes f_1^* into $x_1'x_2'+x_2'x_3'+x_3'x_1'+g_1'$, f_2^* into $x_1'M_1+ +x_2'M_2'+x_3'M_3+g_2'$, and leaves f_3^* fixed. Hence we may suppose L_1, L_2, L_3 are identically 0. On making a further unimodular change of variable we may also assume $M_1 = x_4$. Thus we have

$$\begin{aligned} f_1^* &= x_1x_2+x_2x_3+x_3x_1+g_1, \\ f_2^* &= x_4(x_1+ax_2+bx_3)+g_2, \\ f_3^* &= g_3, \end{aligned}$$

where g_1, g_2, g_3 are forms in $x_4, \ldots, x_\varrho$.

Eliminating x_1 from $f_1^* = 0$ and $f_2^* = 0$ gives a form

$$T = x_4(x_2x_3+g_1)-(x_2+x_3)(ax_2x_4+bx_3x_4+g_2),$$

which must vanish at every point of V^*. The discriminant of T, as a quadratic form in x_2, x_3 and 1, is

$$\Delta = \tfrac{1}{4}x_4[g_2^2-g_1x_4^2(a^2+b^2+1-2a-2b-2ab)].$$

If there is a nonsingular zero of g_3 which is not a zero of Δ then $x_4 \neq 0$ and we can find x_2 and x_3 such that $T = 0$ and $\dfrac{\partial T}{\partial x_2} \neq 0$. On choosing x_1 so that $f_2^* = 0$, we obtain a nonsingular zero of V^*; contrary to hypothesis.

So we may assume that each nonsingular zero of g_3 makes Δ vanish. If g_3 is free of x_4, then every nonsingular zero of g_3, as a zero of Δ must be a zero of g_2. It follows from Lemma 5 that g_2 is proportional to g_3 and hence some linear combination of f_2^* and f_3^* has order 2; contrary to the assumption that f_1, f_2, f_3 is a reduced set of forms. If g_3 involves x_4, then by Lemma 2, g_3 has a nonsingular zero with $x_4 \neq 0$. Hence, after a unimodular change of variable leaving x_1, x_2, x_3, x_4 fixed, we have $g_3(e_4) = 0$; i.e. $g_3 = x_4L+h$, where L, h are free of x_4, h has order at least 2 and h is irreducible over k^*. Each point $(x_5, \ldots, x_\varrho)$ for which $L \neq 0$ gives a nonsingular zero of g_3. Thus we deduce that

$$\Delta(-h, Lx_5, \ldots, Lx_\varrho) = S(x_5, \ldots, x_\varrho)$$

vanishes whenever L does not. Hence S has at least $q^{\varrho-5}(q-1)$ zeros. Since $q \geqslant 49$ it follows from Lemma 4 that S is identically 0. Thus we have g_3 dividing Δ. But g_3 is absolutely irreducible, hence there is a quadratic form G and constant c such that

$$g_3 G = g_2^2 - c g_1 x_4^2.$$

Putting $g_2 = x_4 M + H$, where H is free of x_4; we see that h is a factor of H^2. Since h is irreducible over k^* it follows that H is proportional to h. Consequently there is a linear combination of f_2^* and f_3^* with order 2, contrary to f_1, f_2, f_3 being a reduced set.

This completes the proof of Lemma 17.

6. Conclusion. We prove

THEOREM. *Let f_1, f_2, f_3 be three quadratic forms in at least* 13 *variables over a $\mathfrak{p}$-adic field k, where the residue class field k^* has odd characteristic and contains at least* 49 *elements, then f_1, f_2, f_3 have a common nontrivial zero in k.*

Proof. We may suppose by the Corollary to Lemma 11 that f_1, f_2, f_3 have $\vartheta(f_1, f_2, f_3) \neq 0$, and so we may suppose f_1, f_2, f_3 are a reduced set of forms with coefficients in $\mathfrak{O}$. We retain the notations ϱ, V^* defined at the beginning of § 5. By Lemma 15, it will be enough to show that V^* has a nonsingular point. By Lemmas 16 and 17 we may suppose that V^* contains neither a line nor a planar conic defined over k^*. By Lemma 14, V^* has at least 4 linearly independent points. In case the characteristic of k^* is not 3, V^* will contain at least 5 points.

Suppose $\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(5)}$ are 5 points on V^*; and that each of these points is singular and so for each $\nu = 1, 2, \ldots, 5$ there is a linear combination

$$g^{(\nu)} = \lambda_1^{(\nu)} f_1^* + \lambda_2^{(\nu)} f_2^* + \lambda_3^{(\nu)} f_3^*$$

such that all the partial derivatives $\dfrac{\partial g^{(\nu)}}{\partial x_j}$ $(j = 1, 2, \ldots, \varrho)$ vanish at $\boldsymbol{a}^{(\nu)}$. The points $\lambda^{(\nu)} = (\lambda_1^{(\nu)}, \lambda_2^{(\nu)}, \lambda_3^{(\nu)})$ may be viewed as points of a projective plane and three cases arise:

(I) Three of the points $\lambda^{(\nu)}$ are collinear but distinct.

(II) Three of the points $\lambda^{(\nu)}$ coincide.

(III) Three of the points $\lambda^{(\nu)}$ are linearly independent.

We may suppose the relevant three points are $\boldsymbol{a}^{(1)}$, $\boldsymbol{a}^{(2)}$, $\boldsymbol{a}^{(3)}$. Since V^* contains no line, these points are linearly independent. Hence by a unimodular change of variable we may suppose $\boldsymbol{a}^{(1)}$, $\boldsymbol{a}^{(2)}$, $\boldsymbol{a}^{(3)}$ are the points $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, $\boldsymbol{e}_3$. Then for $\nu = 1, 2, 3$, the form $\lambda_1^{(\nu)} f_1^* + \lambda_2^{(\nu)} f_2^* + \lambda_3^{(\nu)} f_3^*$ is free of the variable x_ν. By a unimodular change of basis of the linear system Λ, we may further assume: In case (I) that $\lambda^{(1)} = (1, 0, 0)$, $\lambda^{(2)} = (0, 1, 0)$, $\lambda^{(3)} = (1, 1, 0)$; in case (II) that $\lambda^{(1)} = \lambda^{(2)} = \lambda^{(3)} = (1, 0, 0)$; and in case (III) that $\lambda^{(1)} = (1, 0, 0)$, $\lambda^{(2)} = (0, 1, 0)$, $\lambda^{(3)} = (0, 0, 1)$. Thus we may suppose: In case (I), that f_1^* is free of x_1, f_2^* is free of x_2 and $f_1^* + f_2^*$ is free of x_3; in case (II), that f_1^* is free of x_1, x_2 and x_3; and in case (III), that f_ν^* is free of x_ν for $\nu = 1, 2, 3$. We deal with cases (I), (II) and (III) separately in Lemmas 18, 19, 20.

In case $p = 3$ it may occur that V^* contains only 4 points. These points must be linearly independent and we may suppose each is a singular point. In that event, in addition to the above cases, a fourth case arises:

(IV) The four points $\lambda^{(\nu)}$ coincide in pairs and V^* has no points, with coordinates in k^*, other than $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, $\boldsymbol{e}_3$ and $\boldsymbol{e}_4$.

As above we may suppose that f_1^* is free of x_1 and x_3, f_2^* is free of x_2 and x_4. We treat this case in Lemma 21.

LEMMA 18. *In Case* (I), *V^* has a nonsingular point.*

Proof. In case (I) we may suppose the points $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, $\boldsymbol{e}_3$ are on V^* and that f_1^* is free of x_1, f_2^* is free of x_2 and $f_1^* + f_2^*$ is free of x_3. Thus we see that f_1^* and f_2^* considered as forms in x_1, x_2, x_3 are linear. Hence V^* contains the planar conic $f_3^*(x_1, x_2, x_3, 0, \ldots, 0) = 0$, and so by Lemma 17, V^* has a nonsingular zero.

LEMMA 19. *In case* (II), *V^* has a nonsingular point.*

Proof. In this case we may suppose that $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, $\boldsymbol{e}_3$ are on V^* and that f_1^* is free of x_1, x_2, x_3. If any linear combination of f_2^* and f_3^* is linear in the variables x_1, x_2, x_3, then V^* contains a planar conic and hence, by Lemma 17, V^* has a nonsingular point. Furthermore, if neither f_2^* nor f_3^* contains the term $x_1 x_2$ with a nonzero coefficient then the line $\lambda \boldsymbol{e}_1 + \mu \boldsymbol{e}_2$ is on V^* and hence, by Lemma 16, V^* has a nonsingular point. A similar result holds regarding the terms $x_2 x_3$ and $x_3 x_1$. Thus we are left with the case where each of the terms $x_1 x_2$, $x_2 x_3$, $x_3 x_1$ appear in one or the other of f_2^* and f_3^* and each linear combination of f_2^*, f_3^* contains at least one of these terms. On making a unimodular change of basis of the linear system Λ, we may suppose that

$$f_1^* = g_1,$$

$$f_2^* = x_1 x_2 + a x_2 x_3 + x_1 L_1 + x_2 L_2 + x_3 L_3 + g_2,$$

$$f_3^* = x_1 x_3 + b x_2 x_3 + x_1 M_1 + x_2 M_2 + x_3 M_3 + g_3,$$

where the L's, M's and g's are free of x_1, x_2 and x_3, and at least one of a and b is nonzero. By replacing x_2 by $x_2 - L_1$ and x_3 by $x_3 - M_1$, we may suppose that L_1 and M_1 are identically 0. Then g_2 is not proportional to f_1^*, since otherwise a linear combination of f_1^* and f_2^* is of the shape excluded by the Corollary to Lemma 12. Similarly g_3 and f_1^* are not proportional.

Suppose now that L_3 and M_2 are not both identically 0, say L_3 is not identically 0. Since f_1, f_2, f_3 is a reduced set of forms, f_1^* has order at least 4 and hence we can find a nonsingular zero of f_1^* for which $L_3 \neq 0$. If at this point we also have $g_2 \neq 0$ then on taking $x_2 = 0$, $x_3 = -g_2/L_3$, $x_1 = -M_3 - g_3/x_3$, we obtain a nonsingular point on V^*. If on the other hand, every nonsingular zero of f_1^* is a zero of $L_3 g_2$ then, by Lemma 5, f_1^* is a factor of $L_3 g_2$ and since f_1^* is absolutely irreducible it follows that g_2 and f_1^* are proportional; an impossibility.

There remains the possibility that L_3 and M_2 are both identically 0. Eliminating x_1 from $f_2^* = f_3^* = 0$ gives

$$C = ax_2x_3^2 - bx_2^2x_3 + x_2x_3(L_2 - M_3) + x_3g_2 - x_2g_3.$$

Put $x_2 = t$, $x_3 = st$ so that

$$C = t[(as^2 - bs)t^2 + s(L_2 - M_3)t + sg_2 - g_3].$$

Write $D(s) = s^2(L_2 - M_3)^2 - 4(as^2 - bs)(sg_2 - g_3)$. $D(s)$ is the discriminant for the quadratic polynomial $t^{-1}C$. We have seen earlier that one of a and b is nonzero, say $a \neq 0$, and that g_2 is not proportional to f_1^*. Hence by Lemma 5 we can find a nonsingular zero of f_1^* for which $g_2 \neq 0$. Then, at this point, $D(s)$ is a cubic polynomial in s and so by Lemma 6, there is an s such that $D(s)$ is a nonzero square. Note that $s \neq 0$. Next choose t to be a nonzero root of $C = 0$. Finally take $x_1 = -ast - L_2 - g_2/t$. The point so obtained is a nonsingular point on V^*.

This completes the proof of Lemma 19.

LEMMA 20. *In case* (III), *V^* has a nonsingular point.*

Proof. In this case we may suppose e_1, e_2, e_3 are on V^* and f_ν^* is free of x_ν ($\nu = 1, 2, 3$). If the term x_2x_3 does not appear in f_1^* with a nonzero coefficient the line $\lambda_1 e_1 + \lambda_2 e_2$ is on V^* and, by Lemma 16, V^* would contain a nonsingular point. Hence we may suppose that x_2x_3 appears with nonzero coefficient in f_1^*, x_1x_3 appears with nonzero coefficient in f_2^* and x_1x_2 appears with nonzero coefficient in f_3^*. We may multiply f_1, f_2, f_3 by appropriate units and assume these coefficients to be 1. Thus we have

$$f_1^* = x_2x_3 + x_2M_1 + x_3N_1 + g_1,$$
$$f_2^* = x_3x_1 + x_3M_2 + x_1N_2 + g_2,$$
$$f_3^* = x_1x_2 + x_1M_3 + x_2N_3 + g_3,$$

where the M's, N's and g's are free of x_1, x_2 and x_3. On replacing x_1 by $x_1 - N_3$, x_2 by $x_2 - N_1$, and x_3 by $x_3 - N_2$ we see that we can suppose further that N_1, N_2 and N_3 are identically 0. We deduce from Lemma 12 that g_1, g_2 and g_3 each have rank at least 2, and by the Corollary to Lemma 12 we see that g_1, g_2, g_3 are irreducible over k. Furthermore, no two of g_1, g_2 and g_3 are proportional, since otherwise the linear system Δ would contain a form of the shape prohibited by the Corollary to Lemma 12.

Eliminating x_1 from $f_2^* = f_3^* = 0$, we get

$$h = (x_3M_2 + g_2)(x_2 + M_3) - g_3x_3 = 0.$$

Eliminating x_2 from $h = f_1^* = 0$, we get

$$(6)\quad x_3^2(g_3 - M_2M_3) + x_3(g_3M_1 - g_2M_3 + g_1M_2 - M_1M_2M_3) + g_2(g_1 - M_1M_3) = 0.$$

This last form is a quadratic in x_3 whose discriminant is

$$(7)\quad \Delta = (g_3M_1 + g_1M_2 + g_2M_3 - M_1M_2M_3)^2 - 4g_1g_2g_3.$$

By eliminating in a different order, we see that x_1 and x_2 satisfy similar quadratic equations with the same discriminant Δ. Furthermore, at any point of V^* the value of the Jacobian $\left(\frac{\partial f_\nu^*}{\partial x_\mu}\right)$, $\nu = 1, 2, 3$, $\mu = 1, 2, 3$, is $\Delta^{1/2}$. Hence, if we can find $x_4, \ldots, x_\varrho$ so that Δ is equal to a nonzero square and so that at least two of

$$(8)\quad g_1 - M_1M_3,\qquad g_2 - M_2M_1,\qquad g_3 - M_3M_2$$

do not vanish, then we can find a nonsingular point on V^*.

We observe that Δ is not identically 0, for if it were then either two of the g_ν would be proportional or at least one of the g_ν would factor over k^*; either situation being contrary to earlier observations. Furthermore, none of the forms in (8) are identically 0, since each g_ν is irreducible over k^*. It follows from Lemma 6 and its Corollary that V^* has a nonsingular point except possibly when Δ is of the form ηh^2, where η is a nonsquare of k^* and h is a cubic form over k^*.

We now verify that V^* has a nonsingular point when Δ has the form ηh^2. We have

$$4g_1g_2g_3 = (g_1M_2 + g_2M_3 + g_3M_1 - M_1M_2M_3)^2 - \eta h^2.$$

Since the right hand side splits over a quadratic extension of k^* and since no two g_ν's are proportional, it must be the case that each g_ν splits over this extension. Since each g_ν has rank at least 2 and does not factorize over k^*, there are nonzero linear forms $P_1, Q_1, P_2, Q_2, P_3, Q_3$ over k^* such that

$$g_\nu = P_\nu^2 - \eta Q_\nu^2\qquad (\nu = 1, 2, 3).$$

We then have

$$\Delta = \eta(P_1P_2Q_3+P_2P_3Q_1+P_3P_1Q_2+\eta Q_1Q_2Q_3)^2,$$

and

$$(9) \quad g_1M_2+g_2M_3+g_3M_1-M_1M_2M_3 = 2(P_1P_2P_3+\eta P_1Q_2Q_3+\eta P_2Q_3Q_1+\eta P_3Q_1Q_2),$$

identically.

If the difference between the dimension of the linear space spanned by the M's, P's and Q's and the dimension of the linear space spanned by the P's and Q's is 2 or 3 then the left hand side of (9) is at least of degree 2 over $k^*[P_1, \ldots, Q_3]$. If the difference is 1 then the left hand side of (9) is at least of degree 1 over $k^*[P_1, \ldots, Q_3]$ since no two g_ν's are proportional and no g_ν splits over k^*. Hence, we deduce from the identity (9) that the M's are expressible as linear combinations of the P's and Q's. Further examination of the identity (9) shows that it is impossible for P_1, Q_1, P_2, Q_2, P_3, Q_3 to be a linearly independent set of linear forms. On the other hand the set f_1^*, f_2^*, f_3^* has order at least 8 and these forms are expressible in terms of $x_1, x_2, x_3, P_1, Q_1, P_2, Q_2, P_3, Q_3$; hence the dimension of the linear space spanned by the P's and Q's is exactly 5. Without loss of generality we can assume P_1, Q_1, P_2, Q_2, P_3 are linearly independent. Then Q_3 is expressible as a linear combination of the others and Q_3 is not proportional to P_3. Thus we can write $Q_3 = \lambda P_3+Q_3'$, where Q_3' is a nontrivial linear combination of P_1, Q_1, P_2, Q_2. We can then solve

$$P_3(P_1Q_2+P_2Q_1)+Q_3(P_1P_2+\eta Q_1Q_2) = 0,$$

parametrically by choosing P_1, Q_1, P_2, Q_2 so that

$$(P_1Q_2+P_2Q_1)+\lambda(P_1P_2+\eta Q_1Q_2) \neq 0$$

and then solving a linear equation for P_3. When P_1, Q_1, P_2, Q_2 satisfy further inequalities, we obtain solutions of

$$P_1P_2Q_3+P_2P_3Q_1+P_3P_1Q_2+\eta Q_1Q_2Q_3 = 0$$

with

$$g_1-M_1M_3 \neq 0, \quad g_2-M_2M_1 \neq 0, \quad g_3-M_3M_2 \neq 0.$$

For these points, the equation (6) is a quadratic equation in x_3 (the leading coefficient is not 0) with discriminant 0. The same is true for the analogous quadratic equations for x_1 and x_2. Hence there are unique values of x_1, x_2, x_3, determined as rational functions of P_1, P_2, Q_1, Q_2 which make $f_1^* = f_2^* = f_3^* = 0$. Thus V^* contains a rationally parametrized threefold S.

If any point of S were a nonsingular point of V^* the lemma would be proved; so we may suppose that all points of S are singular points of V^*. Then to each point $\boldsymbol{a}$ of S there is a nonzero triple $(\lambda_1, \lambda_2, \lambda_3)$ such that $\sum \lambda_i f_i^*$ and all its derivatives vanish at $\boldsymbol{a}$. The mapping $\boldsymbol{a} \to (\lambda_1, \lambda_2, \lambda_3)$ maps S into the λ-plane. Consequently since $q \geqslant 49$, there is a point in the λ-plane which is the image of at least q points of S. These points cannot be on a straight line, for otherwise V^* would have a nonsingular point by Lemma 16. Hence there are three linearly independent points $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ of V^* with coordinates in k^* and a linear combination $f = \sum \lambda_i f_i^*$ such that all the partial derivatives $\dfrac{\partial f}{\partial x_\nu}$ vanish at each of $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$. But in that event we are back in case (II) and so may apply Lemma 19.

This concludes the proof of Lemma 20.

LEMMA 21. *In case* (IV), V^* *has a nonsingular point.*

Proof. In this case we may suppose $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, $\boldsymbol{e}_3$, $\boldsymbol{e}_4$ are on V^* and f_1^* is free of x_1 and x_3 while f_2^* is free of x_2 and x_4. We may also suppose f_3^* contains the terms x_1x_2, x_1x_4, x_2x_3 and x_3x_4, since otherwise we would have five points on V^* and one of the other cases would apply. Thus we have

$$f_1^* = \alpha x_2x_4+x_2M_2+x_4M_4+g_1,$$
$$f_2^* = \beta x_1x_3+x_1M_1+x_3M_3+g_2,$$
$$f_3^* = ax_1x_2+bx_1x_4+cx_2x_3+dx_3x_4+sx_2x_4+tx_1x_3+ +x_1N_1+x_2N_2+x_3N_3+x_4N_4+g_3.$$

We may assume that neither α nor β is 0. For suppose $\alpha = 0$ then $f_3^*(0, x_2, x_3, x_4, 0, \ldots, 0) = 0$ is a planar conic on V^* and hence, by Lemma 17, V^* has a nonsingular point. On replacing x_1, x_2, x_3, x_4 by $x_1-\beta M_3$, $x_2-\alpha M_4$, $x_3-\beta M_1$, $x_4-\alpha M_2$ respectively we see that we can assume that the M_ν are identically 0. On multiplying the x_i by suitable units and on making a unimodular change of basis for the linear system Λ we obtain

$$f_1^* = x_2x_4+g_1,$$
$$f_2^* = x_1x_3+g_2,$$
$$f_3^* = x_1x_2+x_1x_4+x_2x_3+x_3x_4+x_1N_1+x_2N_2+x_3N_3+x_4N_4+g_3,$$

where the N_ν and g_ν are forms in $x_5, \ldots, x_\varrho$. By Lemma 12 and its Corollary, g_1 and g_2 are nonproportional irreducible forms over k^*. Two cases arise.

If rank $(g_1, g_2) \geqslant 3$, we can make one of g_1 and g_2 vanish without making the other vanish. Suppose we have solved $g_1 = 0$ with $g_2 \neq 0$. We then choose x_3 so that $x_3(x_3^2-N_2x_3-g_2) \neq 0$. We then set $x_4 = 0$, $x_1 = -g_2/x_3$ and choose x_2 to make $f_3^* = 0$. The resulting point is a fifth point on V^*, contrary to hypothesis.

If rank $(g_1, g_2) = 2$, since $\varrho \geqslant 7$, we may solve $g_1 = g_2 = 0$ with some of $x_5, \ldots, x_\varrho$ not zero. We then set $x_3 = x_4 = 0$ and choose x_1, x_2 so that $f_3^* = 0$. The resulting point is a fifth point on V^*, contrary to the hypothesis. This completes the proof of the Lemma and hence the proof of the Theorem.

References

[1] B. J. Birch and D. J. Lewis, *𝔭-adic forms*, J. Indian Math. Soc. 23 (1959), pp. 11-31.

[2] B. J. Birch, D. J. Lewis and T. G. Murphy, *Simultaneous quadratic forms*, American J. Math. 84 (1962), pp. 110-115.

[3] L. Carlitz, *A problem of Dickson's*, Duke Math. J. 14 (1947), pp. 1139-1140.

[4] — *A problem of Dickson*, Duke Math. J. 19 (1952), pp. 471-474.

[5] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Seminar Hamburg 11 (1935), pp. 73-75.

[6] H. Davenport, *Cubic forms in thirty-two variables*, Phil. Transactions Royal Soc., London, 25 (1959), pp. 193-232.

[7] V. B. Demyanov, *On cubic forms in discretely normed fields*, (Russian), C. R. (Doklady) Acad. Sci., U. S. S. R. 74 (1950), pp. 889-891.

[8] — *Pairs of quadratic forms over a complete field with a finite residue class field*, (Russian), Izv. Akad. Nauk. U. S. S. R. 20 (1956), pp. 307-324.

[9] H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlenkörper*, J. Reine Angew. Math. 153 (1924), pp. 819-827.

[10] R. R. Laxton and D. J. Lewis, *Forms of degree 7 and 11 over 𝔭-adic fields*, To appear, Amer. Math. Soc. Symposium on Number Theory.

[11] D. J. Lewis, *Cubic homogeneous polynomials over 𝔭-adic fields*, Annals of Math. (2), 56 (1952), pp. 473-478.

[12] — *Singular quartic forms*, Duke Math. J. 21 (1954), pp. 39-44.

[13] F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Press 1916.

[14] T. A. Springer, *Some properties of cubic forms over fields with a discrete valuation*, Proc. Kon. Ned. Akad. v. Wet. Amst. 48A (1955), pp. 512-516.

[15] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Seminar Hamburg 11 (1935), pp. 76-83.

THE UNIVERSITY, MANCHESTER, ENGLAND
THE UNIVERSITY OF MICHIGAN

Reçu par la Rédaction le 25. 5. 1964

ACTA ARITHMETICA
X (1965)

Errata to the paper "On the distribution of the k-free integers in residue classes"

(Acta Arithmetica 8 (1963), pp. 283-293)

by

E. Cohen and Richard L. Robinson (Tennessee)

In the line following (2.2) on p. 285, replace Q_h by Q_k; in the last line on p. 288 replace $\overline{\Phi}_k(h)$ by $\Phi_k(h)$; in the first and third sentences of Theorem 3, replace the comma preceding "that is" by a semicolon.