Mh. Math. 93, 329—348 (1982)

Monatshefte für
Mathematik

On Cubic Polynomials
IV. Systems of Rational Equations

By

Wolfgang M. Schmidt*, Boulder, Colorado

(Received 15 October 1981)

Abstract. It is shown that a system of r homogeneous cubic equations with rational coefficients has a nontrivial solution in rational integers if the number of variables is at least $(10r)^5$. For most such systems, an asymptotic formula holds for the number z_P of solutions whose components have modulus $< P$.

1. Introduction. By a special case of a theorem of BIRCH [1], there is for each r a number $\sigma(r)$ such that a system of r cubic forms with rational coefficients has a nontrivial rational zero when the number of variables exceeds $\sigma(r)$. In what follows, let $\sigma(r)$ be the smallest integer with this property. It appears to be difficult to obtain good bounds for $\sigma(r)$ by BIRCH's method. But DAVENPORT [5] used the Circle Method to obtain $\sigma(1) \leqslant 31$, then [6]

$$\sigma(1) \leqslant 15.$$

There can be no rational zero unless there is a p-adic zero for each prime p. So let $\gamma(r)$ be the smallest integer such that r cubic forms in more than $\gamma(r)$ variables possess a nontrivial p-adic zero for each p. It has been known for some time (DEM'JANOV [10], LEWIS [12]) that

$$\gamma(1) = 9,$$

but no estimates were known for $\gamma(r)$ in general. But LEEP and SCHMIDT [11] could show that a variation of a method of BRAUER [4] yields

$$\gamma(2) \leqslant 320, \tag{1.1}$$

$$\gamma(r) \leqslant (81/2)r^4. \tag{1.2}$$

* Partially supported by NSF contract NSF-MCS-8015356.

0026—9255/82/0093/0329/$04.00

In part III of the present series it was shown that

$$\gamma(r) \leqslant 5300\, r\,(3\,r+1)^2. \tag{1.3}$$

The existence of a nontrivial p-adic zero is usually not enough to obtain a rational zero. In most work to date a nonsingular p-adic zero was required for each p. At the cost of needing a larger number of variables, this difficulty can be overcome:

Theorem 1. *For $r > 1$ we have*

$$\sigma(r) \leqslant 15 + \sum_{t=2}^{r} (8\,t\,\gamma(t) + 2\,t^2 - 2\,t).$$

Combining the theorem with (1.1), (1.2) and (1.3) we get

$$\sigma(2) \leqslant 5139, \tag{1.4}$$

$$\sigma(r) < 66\,(r+1)^6, \tag{1.5}$$

$$\sigma(r) < (10\,r)^5. \tag{1.6}$$

Only the last of these inequalities depends on (1.3) and on the preceding work of this series.

There is no reason to believe that the estimate $\sigma(r) \ll r^5$ is in any way best possible. DAVENPORT and LEWIS [9] showed that for r cubic forms of additive type

$$27\,r^2(\log(9\,r))$$

variables suffice. BIRCH [2] proved (as a special case of a more general theorem) the conditional result that a system of cubic forms has a non-trivial rational zero, provided it has a nonsingular zero in each local field and provided that $s > 8\,r\,(r+1) + \dim V^*$, where V^* is a certain manifold defined in terms of singular points. Conditional results were also proved by TARTAKOVSKY [16], [17].

We will study more general equations

$$\mathfrak{F}_i(\mathbf{x}) = c_i \quad (i = 1, \ldots, r) \tag{1.7}$$

where the $\mathfrak{F}_i$ are cubic forms in $\mathbf{x} = (x_1, \ldots, x_s)$, and where the c_i are constants $(i = 1, \ldots, r)$.

Theorem 2. *Suppose $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ are cubic forms in s variables with rational integer coefficients, and $c_1, \ldots, c_r$ are rational integers. Suppose that no form in the rational pencil, i. e. no form $q_1\mathfrak{F}_1 + \cdots + q_r\mathfrak{F}_r$ with $q_1, \ldots, q_r$ in $\mathbb{Q}$ but not all zero, vanishes on a rational subspace of $\mathbb{Q}^s$ of* *codimension*

$$\leqslant 10r^2 + 6r. \tag{1.8}$$

Given a box $\mathfrak{B} \subset \mathbb{R}^s$ *with sides parallel to the coordinate axes, write* $z_P = z_P(\mathfrak{F}_1, \ldots, \mathfrak{F}_r; c_1, \ldots, c_r)$ *for the number of common integer solutions of* (1.7) *with* $\mathbf{x} \in P\mathfrak{B}$, *i.e. in the box which is obtained from* $\mathfrak{B}$ *by the homothetic map* $\mathbf{x} \to P\mathbf{x}$.

Then as $P \to \infty$,

$$z_P = P^{s-3r}\mathfrak{J}\mathfrak{S} + O(P^{s-3r-\delta}).$$

Here $\delta = \delta(r, s) > 0$, *and the "singular integral"* $\mathfrak{J}$ *depends only on* $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ *and* $\mathfrak{B}$, *whereas the "singular series"* $\mathfrak{S}$ *depends only on* $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ *and* $c_1, \ldots, c_r$.

In view of the condition with (1.8), the hypothesis implies that $s > 10r^2 + 6r$. We may infer the existence of solutions only if $\mathfrak{J} > 0$ and $\mathfrak{S} > 0$. Hence two additional facts are of importance.

First Supplement. *We have* $\mathfrak{J} > 0$ *if the manifold* $M_{\mathfrak{B}}$ *of common real zeros of* $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ *in the interior of* $\mathfrak{B}$ *has dimension* $\geqslant s - r$. *In particular we have* $\mathfrak{J} > 0$ *if* $\mathfrak{B}$ *contains* $\mathbf{0}$ *in its interior.*

Second Supplement. *We have* $\mathfrak{S} > 0$ *if either*

(a) $c_1 = \ldots = c_r = 0$ *and no form of the rational pencil vanishes on a rational subspace of codimension*

$$\leqslant 8r\gamma(r) + 2r^2 - 2r,$$

or if

(b)
$$s > 5300r(3r+1)^2, \tag{1.9}$$

the system $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ *is "bottomed" in a sense to be explained below, and each* $c_i \in m\mathbb{Z}$ *where* $m = m(\mathfrak{F}_1, \ldots, \mathfrak{F}_r) > 0$ *and* $\mathbb{Z}$ *is the ring of rational integers.*

It is easy to deduce Theorem 1. In view of $\sigma(1) \leqslant 15$ it is enough to show that

$$\sigma(r) \leqslant \sigma(r-1) + 8r\gamma(r) + 2r^2 - 2r. \tag{1.10}$$

Suppose then that

$$s > \sigma(r-1) + 8r\gamma(r) + 2r^2 - 2r. \tag{1.11}$$

We will try to apply Theorem 2. We know that $\mathfrak{J} > 0$ if $\mathfrak{B}$ is chosen properly. Further $\mathfrak{S} > 0$ if the condition of part (a) of the Second

Supplement holds. In this case Theorem 2 itself applies, since $\gamma(r) \geqslant 9r$ (a well known fact, since the Artin conjecture, if true, would be best possible). If not, then we may suppose that $\mathfrak{F}_r$ vanishes on a large subspace S. The restrictions of $\mathfrak{F}_1, \ldots, \mathfrak{F}_{r-1}$ to S are $r-1$ forms in

$$\geqslant s - (8r\gamma(r) - 2r^2 + 2r) > \sigma(r-1)$$

variables. Hence $\mathfrak{F}_1, \ldots, \mathfrak{F}_{r-1}$ possess a nontrivial rational zero in S. Thus there is a common rational zero of $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ if the number s of variables satisfies (1.11), and (1.10) follows.

We postpone the classification into bottomed and bottomless systems to the last section. Here we only remark that the bottomless systems are rare, in the sense that they form a proper algebraic subset of all systems.

Corollary 1. *Suppose* (1.9) *holds and* $(\mathfrak{F}_1, \ldots, \mathfrak{F}_r)$ *is a bottomed system with integer coefficients. Then for each* $\mathbf{c} \in m\mathbb{Z}^r$ *where* $m = m(\mathfrak{F}_1, \ldots, \mathfrak{F}_r)$, *the equations* (1.7) *have a solution* $\mathbf{x} \in \mathbb{Z}^s$.

Corollary 2. *Suppose* (1.9) *holds and* $(\mathfrak{F}_1, \ldots, \mathfrak{F}_r)$ *is a bottomed system with rational coefficients. Then for each* $\mathbf{c} \in \mathbb{Q}^r$, *the equations* (1.7) *have a solution* $\mathbf{x} \in \mathbb{Q}^s$.

Proof. Set $\mathbf{x} = q^{-1}\mathbf{y}$. Then the equations (1.7) become

$$\mathfrak{F}_i(\mathbf{y}) = q^3 c_i \quad (i = 1, \ldots, r).$$

For suitable $q > 0$, $q \in \mathbb{Z}$, the numbers $q^3 c_i$ will lie in $m\mathbb{Z}$.

In a sense, the condition that the system is bottomed means that it is "general", and results about general systems are due to TARTAKOVSKY and BIRCH. However, in contrast to these works, we do not always impose extra p-adic conditions. We remark that DAVENPORT and LEWIS [8] and WATSON (in work culminating in [18]) obtained results about a single nonhomogeneous cubic equation.

Our presentation will depend on [14] and, to a lesser extent, on [13], [15] and the other papers of the present series.

2. The Singular Integral and the First Supplement. As in [14], we begin with the singular integral and the singular series. Write

$$\psi(y) = \begin{cases} 1 - |y| & \text{if } |y| \leqslant 1, \\ 0 & \text{if } |y| > 1, \end{cases}$$

and for $T > 0$ put

$$\psi_T(y) = T\psi(Ty) = \begin{cases} T(1 - T|y|) & \text{if } |y| \leqslant T^{-1}, \\ 0 & \text{if } |y| > T^{-1}. \end{cases}$$

Further set $\psi_T(\mathbf{y}) = \psi_T(y_1) \cdots \psi_T(y_r)$ when $\mathbf{y} = (y_1, \ldots, y_r)$.

Let

$$\mathbf{F} = (\mathfrak{F}_1, \ldots, \mathfrak{F}_r)$$

be an r-tuple of cubic forms, and put

$$\mathfrak{J}_T = \int_{\mathfrak{B}} \psi_T(\mathbf{F}(\underline{\xi}))\, d\underline{\xi}. \tag{2.1}$$

It will follow in the course of the proof of Theorem 2, that under the condition given in terms of (1.8), the limit

$$\mathfrak{J} = \lim_{T \to \infty} \mathfrak{J}_T \tag{2.2}$$

exists. This limit is the singular integral $\mathfrak{J}$ of Theorem 2.

Lemma 2 of [14] holds in the present context. That is, the singular integral is positive if the manifold $M_{\mathfrak{B}}$ consisting of real zeros of $\mathbf{F}$ in the interior of $\mathfrak{B}$ has real dimension

$$\dim M_{\mathfrak{B}} \geqslant s - r. \tag{2.3}$$

In particular this is true if $\mathbf{F}$ has a nonsingular zero in the interior of $\mathfrak{B}$. It remains for us to show that (2.3) is certainly true if $\mathfrak{B}$ contains the origin in its interior. We first quote the

Borsuk-Ulam Theorem. *Suppose φ is a continuous map from the sphere S^r into $\mathbb{R}^r$. Then there is a pair $\mathbf{x}, -\mathbf{x}$ of antipodal points on S^r with $\varphi(\mathbf{x}) = \varphi(-\mathbf{x})$.*

For a proof see Borsuk [3].

Now $\mathbf{F}$ defines a map from $\mathbb{R}^s$ into $\mathbb{R}^r$. Given a subspace A^{r+1} of $\mathbb{R}^s$ of dimension $r+1$, it contains an r-sphere, and hence an $\mathbf{x} \neq \mathbf{0}$ with $\mathbf{F}(\mathbf{x}) = \mathbf{F}(-\mathbf{x})$, therefore with $\mathbf{F}(\mathbf{x}) = \mathbf{0}$ since $\mathbf{F}$ is cubic. Thus the manifold M of zeros of $\mathbf{F}$ has nonzero intersections with any subspace A^{r+1} of dimension $r+1$.

Thus M is "large" in some sense. We want to show that its dimension is at least $s-r$. Being simple number theorists, we don't want to go into the definition of dimension, etc. We will simply show that there is a subspace A^{s-r} of dimension $s-r$, such that the orthogonal projection of M on A^{s-r} is A^{s-r} itself. The intersection

$M_{\mathfrak{B}} = M \cap \mathfrak{B}$ then has the property that its orthogonal projection on A^{s-r} contains the origin in its interior, and Lemma 2 of [14] clearly may be applied. Hence it will suffice to prove the following

Lemma 1. *Let M be a subset of $\mathbb{R}^s$ which is "homogeneous" in the sense that $\lambda \mathbf{x} \in M$ whenever $\mathbf{x} \in M$ and $\lambda \in \mathbb{R}$. Suppose that $M \cap A \neq \{\mathbf{0}\}$ for every subspace A of dimension $> r$. Then there is a subspace A^{s-r} such that the orthogonal projection of M on A^{s-r} is A^{s-r} itself.*

Proof. When $r = 0$, then $M = \mathbb{R}^s$. In the step from $r - 1$ to r we may suppose that $M \cap A \neq \{\mathbf{0}\}$ when $\dim A > r$, but that there is a subspace B with $\dim B = r$ and $M \cap B = \{\mathbf{0}\}$. We further may suppose that B is the subspace $x_1 = \ldots = x_{s-r} = 0$. Let A^{s-r} be the subspace $x_{s-r+1} = \ldots = x_s = 0$, and let $\mathbf{u} \neq \mathbf{0}$ be in A^{s-r}. We have $M \cap A \neq \{\mathbf{0}\}$ for the subspace A spanned by B and $\mathbf{u}$. Since $M \cap B = \{\mathbf{0}\}$, some $\mathbf{b} + \lambda \mathbf{u} \in M$, where $\mathbf{b} \in B$ and $\lambda \neq 0$. Thus $\lambda \mathbf{u}$, and hence $\mathbf{u}$, lie in the orthogonal projection of M on A^{s-r}. Since $\mathbf{u}$ was an arbitrary nonzero element of A^{s-r}, the lemma follows.

3. The Singular Series and the Second Supplement. Write $e(x) = e^{2\pi i x}$ and

$$S(\mathbf{a}, q) = \sum_{\mathbf{x} \,(\mathrm{mod}\, q)} e(q^{-1} \mathbf{a} \mathbf{F}(\mathbf{x})) \tag{3.1}$$

where $\mathbf{a} = (a_1, \ldots, a_r)$, $\mathbf{x} = (x_1, \ldots, x_s)$ and $\mathbf{a}\mathbf{F}$ is the inner product $a_1 \mathfrak{F}_1 + \ldots + a_r \mathfrak{F}_r$. Further write

$$A(q, \mathbf{c}) = \sum_{\substack{\mathbf{a} \,(\mathrm{mod}\, q) \\ (\mathbf{a}, q) = 1}} q^{-s} S(\mathbf{a}, q) e(-q^{-1} \mathbf{a} \mathbf{c}) \tag{3.2}$$

where $(\mathbf{a}, q)$ is the greatest common divisor of $a_1, \ldots, a_r, q$, and where $\mathbf{a}\mathbf{c} = a_1 c_1 + \ldots + a_r c_r$.

It will be shown (Lemma 8 below) that under the hypotheses of Theorem 2,

$$|S(\mathbf{a}, q)| \ll q^{s-r-1-(\varrho/2)}$$

where $\varrho = (10 r)^{-1}$. It then follows that

$$|A(q, \mathbf{c})| \ll q^{-1-(\varrho/2)}, \tag{3.3}$$

and the sum

$$\mathfrak{S} = \mathfrak{S}(\mathbf{c}) = \sum_{q=1}^{\infty} A(q, \mathbf{c}) \tag{3.4}$$

is absolutely convergent, uniformly in $\mathbf{c}$. This sum is the "singular series" of Theorem 2. By the absolute convergence, and since $A(q, \mathbf{c})$ is multiplicative in q,

$$\mathfrak{S}(\mathbf{c}) = \prod_p \chi(p, \mathbf{c}) \tag{3.5}$$

where for each prime p,

$$\chi(p, \mathbf{c}) = 1 + A(p, \mathbf{c}) + A(p^2, \mathbf{c}) + \dots .$$

We have the well known relation

$$1 + A(p, \mathbf{c}) + \dots + A(p^l, \mathbf{c}) = p^{-(s-r)l} \nu_l(\mathbf{c})$$

where $\nu_l(\mathbf{c})$ is the number of solutions $\mathbf{x} \,(\operatorname{mod} p^l)$ of

$$\mathbf{F}(\mathbf{x}) \equiv \mathbf{c} \,(\operatorname{mod} p^l), \tag{3.6}$$

i. e. of $\mathfrak{F}_i(\mathbf{x}) \equiv c_i \,(\operatorname{mod} p^l)$ $(i = 1, \dots, r)$.

Write $\nu_l = \nu_l(\mathbf{0})$, so that ν_l is the number of solutions of

$$\mathbf{F}(\mathbf{x}) \equiv \mathbf{0} \,(\operatorname{mod} p^l), \tag{3.7}$$

and write π_l for the number of *primitive* solutions, i. e. solutions $\mathbf{x} \not\equiv \mathbf{0} \,(\operatorname{mod} p)$.

Lemma 2. $\pi_l \gg p^{l(s-\gamma(r))}$.

Proof. The integer points $\mathbf{x} \,(\operatorname{mod} p^l)$ form a group X under addition, which is the sum of s cyclic groups of order p^l. The primitive integer points are the elements of X of order p^l. The letter H will stand for subgroups of X which are the sum of

$$g = \gamma(r) + 1$$

cyclic groups of order p^l. Introduce

α_1 = number of subgroups H of X,

α_2 = number of subgroups H of X which contain a given $\mathbf{x}$ of X of order p^l,

β_1 = number of elements of order p^l in X,

β_2 = number of elements of order p^l in a given H.

Then

$$\frac{\alpha_1}{\alpha_2} = \frac{\beta_1}{\beta_2} = \frac{p^{ls} - p^{(l-1)s}}{p^{lg} - p^{(l-1)g}} = p^{l(s-g)} \frac{1 - p^{-s}}{1 - p^{-g}} .$$

By definition of $\gamma(r)$ and of g, a system of r forms in g variables possesses a nontrivial p-adic zero, hence possesses a zero $\mathbf{x}$ whose components are p-adic integers, in fact possesses a primitive zero whose components are not all divisible by p. Hence a congruence (3.7) in g variables possesses a primitive solution. Then it must possess at least $p^l - p^{l-1}$ primitive solutions. It follows that in every subgroup H of X there are $p^l - p^{l-1}$ primitive solutions of (3.7). We obtain

$$\pi_l \geqslant (p^l - p^{l-1}) \frac{\alpha_1}{\alpha_2} = p^{l(s-\gamma(r))}(1-p^{-1})(1-p^{-s})(1-p^{-g})^{-1}$$
$$\gg p^{l(s-\gamma(r))}.$$

As a consequence of Lemma 2 we have

$$1 + A(p,\mathbf{0}) + \ldots + A(p^l,\mathbf{0}) = p^{-(s-r)l}\nu_l \geqslant p^{-(s-r)l}\pi_l \gg p^{-l(\gamma(r)-r)}. \tag{3.8}$$

It will be shown in Lemma 8 below that under the hypotheses of part (a) of the Second Supplement,

$$|S(\mathbf{a},q)| \ll q^{s-\gamma(r)-(\varrho/2)},$$

where $\varrho = (10r)^{-1}$. Then

$$|A(q,\mathbf{0})| \ll q^{r-\gamma(r)-(\varrho/2)}$$

and

$$|A(p^{l+1},\mathbf{0}) + A(p^{l+2},\mathbf{0}) + \ldots| \ll p^{-l(\gamma(r)-r+(\varrho/2))}.$$

This relation contradicts (3.8) if $\chi(p,\mathbf{0}) = 0$. Hence each $\chi(p,\mathbf{0})$ is positive and the singular series $\mathfrak{S}$ is positive. So much about part (a) of the Second Supplement. For part (b) see the last section of this paper.

4. *A Lemma with Three Alternatives.* To each cubic form $\mathfrak{F}(\mathbf{x})$ there belongs a unique symmetric trilinear form $\mathfrak{F}(\mathbf{x}|\mathbf{y}|\mathbf{z})$ with $\mathfrak{F}(\mathbf{x}) = \mathfrak{F}(\mathbf{x}|\mathbf{x}|\mathbf{x})$. To our given r-tuple $\mathbf{F} = (\mathfrak{F}_1, \ldots, \mathfrak{F}_r)$ of cubic forms there belongs an r-tuple

$$\mathbf{F}(\mathbf{x}|\mathbf{y}|\mathbf{z}) = (\mathfrak{F}_1(\mathbf{x}|\mathbf{y}|\mathbf{z}), \ldots, \mathfrak{F}_r(\mathbf{x}|\mathbf{y}|\mathbf{z}))$$

of symmetric, trilinear forms. The forms $\mathfrak{F}_i$ in Theorem 2 are supposed to have integer coefficients. We may interpret this to mean that each associated trilinear form has integer coefficients (sneaky!), or else we can force this by multiplying $\mathbf{F}$ by a factor 6 and by noting that if the theorem is true for $6\mathbf{F}$, then it is also true for $\mathbf{F}$.

Given $\underset{\sim}{\alpha} = (\alpha_1, \ldots, \alpha_r) \in \mathbb{R}^r$, write

$$\underset{\sim}{\alpha}\,\mathbf{F}(\mathbf{x}) = \alpha_1 \mathfrak{F}_1(\mathbf{x}) + \ldots + \alpha_r \mathfrak{F}_r(\mathbf{x})$$

and

$$\underset{\sim}{\alpha}\,\mathbf{F}(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z}) = \alpha_1 \mathfrak{F}_1(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z}) + \ldots + \alpha_r \mathfrak{F}_r(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z}).$$

Let $\mathfrak{U}_r$ be the unit cube $0 \leqslant \alpha_i < 1$ $(i = 1, \ldots, r)$, and put

$$S(\underset{\sim}{\alpha}) = \sum_{x \in P\mathfrak{B}} e(\underset{\sim}{\alpha}\,\mathbf{F}(\mathbf{x})).$$

Then the number z_P of Theorem 2 is given by

$$z_P = \int_{\mathfrak{U}_r} S(\underset{\sim}{\alpha})\, e(-\underset{\sim}{\alpha}\,\mathbf{c})\, d\underset{\sim}{\alpha}. \tag{4.1}$$

In proving Theorem 2 we may suppose without loss of generality that $\mathfrak{B}$ has sides at most 1. Besides the cube $\mathfrak{U}_r$ introduced above we will need the cube $\mathfrak{C}_s$ consisting of $\mathbf{x}$ with $-1 < x_i < 1$ $(i = 1, \ldots, s)$.

Lemma 3. *Suppose $K > 0$, $\varepsilon > 0$, $\theta > 0$. Given $\underset{\sim}{\alpha}$, we have either*

(i) $$|S(\underset{\sim}{\alpha})| \leqslant P^{s-K},$$

or

(ii) *there are rational approximations $(a_1/q, \ldots, a_r/q)$ to $\underset{\sim}{\alpha} = (\alpha_1, \ldots, \alpha_r)$ satisfying*

$$1 \leqslant q \leqslant P^{2r\theta}, \tag{4.2}$$

$$(\mathbf{a}, q) = 1, \tag{4.3}$$

$$|q\alpha_i - a_i| < P^{-3+2r\theta} \quad (i = 1, \ldots, r), \tag{4.4}$$

or

(iii) *there are*

$$\gg P^{2\theta s - 4K - \varepsilon}$$

pairs of integer points $\mathbf{x}, \mathbf{y}$ in $P^\theta \mathfrak{C}_s$ for which

$$\operatorname{rank}\left(\mathfrak{F}_i(\mathbf{x} \mid \mathbf{y} \mid \mathbf{e}_j)\right)_{1 \leqslant i \leqslant r,\, 1 \leqslant j \leqslant s} < r. \tag{4.5}$$

Here $\mathbf{e}_1, \ldots, \mathbf{e}_s$ are the basis vectors, and the constant in $\gg$ may depend on $r, s, K, \theta, \varepsilon$.

Proof. This is essentially the case $d = 3$ of Lemma 2.5 of Birch [2].

5. Trilinear and Fourlinear Forms. We shall have to deal with fourlinear forms

$$\mathfrak{B}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}\,|\,\mathbf{w}) = w_1 \mathfrak{F}_1(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}) + \ldots + w_r \mathfrak{F}_r(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}). \qquad (5.1)$$

We are not able to deal with such forms directly, but need to examine trilinear forms first.

Lemma 4. *Let* $\mathfrak{T}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z})$ *be a trilinear form with rational coefficients in vectors* $\mathbf{x} \in \mathbb{Q}^s$, $\mathbf{y} \in \mathbb{Q}^t$, $\mathbf{z} \in \mathbb{Q}^t$, *which is symmetric in* $\mathbf{y}$, $\mathbf{z}$. *For given* $\mathbf{x}$, *let* $Y(\mathbf{x})$ *be the subspace of* $\mathbb{Q}^t$ *consisting of* $\mathbf{y}$ *having* $\mathfrak{T}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}) = 0$ *identically in* $\mathbf{z}$.

Suppose that a is an integer in $1 \leqslant a \leqslant s$, *that* $R \geqslant 1$ *and that there are more than*

$$A R^{a-1}$$

integer points $\mathbf{x}$ *with** $|\mathbf{x}| \leqslant R$ *and* $\dim Y(\mathbf{x}) \geqslant d$, *where* $A = A(s,t)$.

Then there are subspaces X *of* $\mathbb{Q}^s$ *and* Y *of* $\mathbb{Q}^t$ *with*

$$\dim X \geqslant a, \quad \dim Y \geqslant d,$$

such that

$$\mathfrak{T}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}) = 0 \quad \text{for } \mathbf{x} \in X,\ \mathbf{y} \in Y,\ \mathbf{z} \in Y. \qquad (5.2)$$

It will be crucial for the applications that A does not depend on the coefficients of $\mathfrak{T}$. A special version is Lemma 3 of DAVENPORT [6]. Another version was proved by DAVENPORT and LEWIS [7] in the context of forms over finite fields. Here we will indicate a proof in the terminology of Lemma 4 of [14].

Proof. Let $\mathfrak{X}$ be the given set of integer points $\mathbf{x}$ with $|\mathbf{x}| \leqslant R$ and $\dim Y(\mathbf{x}) \geqslant d$. When $d = t$, then $\mathfrak{X}$ is a subspace of $\mathbb{Q}^s$ and the conclusion follows easily.

Suppose then that $d < t$. Consider the matrix

$$\mathfrak{T}(\mathbf{x}\,|\,\mathbf{e}_i\,|\,\mathbf{e}_j) \quad (1 \leqslant i,j \leqslant t). \qquad (5.3)$$

Just as in [14]** we may suppose without loss of generality that for $\mathbf{x} \in \mathfrak{X}$ we have $\dim Y(\mathbf{x}) = d$, the matrix (5.3) has rank $t - d$, and the submatrix with $1 \leqslant i,j \leqslant t - d$ is nonsingular.

Again, as in [14], let $D_1(\mathbf{x}), \ldots, D_N(\mathbf{x})$ be the $(t - d + 1)$-subdeterminants of (5.3), arranged in some order. Write $\mathbf{D}(\mathbf{x}) = (D_1(\mathbf{x}), \ldots, D_N(\mathbf{x}))$. As in [14], there exist points $\mathbf{x}$ of $\mathfrak{X}$ for which

* We set $|\mathbf{x}| = \max(|x_1|, \ldots, |x_s|)$.

** But our roles of $\mathbf{y}, \mathbf{z}$ are interchanged from the ones in [14].

at most $s-a$ of the vectors

$$\partial \mathbf{D}/\partial x_1, \ldots, \partial \mathbf{D}/\partial x_s \tag{5.4}$$

are independent. This is a consequence of DAVENPORT's Lemma 2 in [6] (reproduced as Lemma 4 in [14]). It is important to note that the constant A in DAVENPORT's Lemma does not depend on the coefficients of the polynomials.

Construct vectors $y^{(1)} = y^{(1)}(\mathbf{x}), \ldots, y^{(d)} = y^{(d)}(\mathbf{x})$ of $\mathbb{Q}^t$ as in [14]. The components of these vectors are polynomials, and for $\mathbf{x} \in \mathfrak{X}$, they are linearly independent. The identity (7.7) of [14] holds, i. e. we have identically in $\mathbf{x}, \mathbf{z}$ that

$$\mathfrak{T}(\mathbf{x} \mid \mathbf{y}^{(i)}(\mathbf{x}) \mid \mathbf{z}) = \mathfrak{B}^{(i)}(\mathbf{z} \mid D(\mathbf{x})) \quad (i = 1, \ldots, d), \tag{5.5}$$

where each $\mathfrak{B}^{(i)}$ is a bilinear form, in the vector $\mathbf{z}$ with t components and the vector $\mathbf{D}$ with N components. Taking the partial derivate with respect to x_l, we obtain

$$\mathfrak{T}(\mathbf{e}_l \mid \mathbf{y}^{(i)}(\mathbf{x}) \mid \mathbf{z}) + \mathfrak{T}\left(\mathbf{x} \,\middle|\, \frac{\partial}{\partial x_l} \mathbf{y}^{(i)}(\mathbf{x}) \,\middle|\, \mathbf{z}\right) = \mathfrak{B}^{(i)}\left(\mathbf{z} \,\middle|\, \frac{\partial}{\partial x_l} \mathbf{D}(\mathbf{x})\right) \tag{5.6}$$

$$(1 \leqslant i \leqslant d,\ 1 \leqslant l \leqslant s).$$

By construction, the vectors $\mathbf{y}^{(j)}(\mathbf{x})$ lie in $Y(\mathbf{x})$ for $\mathbf{x} \in \mathfrak{X}$. Since $\mathfrak{T}$ is symmetric in the last two arguments, $\mathfrak{T}(\mathbf{x} \mid \mathbf{w} \mid \mathbf{y}^{(j)}(\mathbf{x})) = 0$ identically in $\mathbf{w}$ when $\mathbf{x} \in \mathfrak{X}$. Substituting $\mathbf{z} = \mathbf{y}^{(j)}(\mathbf{x})$ in (5.6) we obtain

$$\mathfrak{T}(\mathbf{e}_l \mid \mathbf{y}^{(i)}(\mathbf{x}) \mid \mathbf{y}^{(j)}(\mathbf{x})) = \mathfrak{B}^{(i)}(\mathbf{y}^{(j)}(\mathbf{x}) \mid \frac{\partial}{\partial x_l} \mathbf{D}(\mathbf{x})) \quad (1 \leqslant i,j \leqslant d,\ 1 \leqslant l \leqslant s),$$

for $\mathbf{x} \in \mathfrak{X}$. We substitute $\mathbf{x} = \mathbf{a}$ where $\mathbf{a}$ is an element of $\mathfrak{X}$ for which at most $s-a$ of the vectors (5.4) are independent. Let X be the subspace of $\mathbb{Q}^s$ consisting of $\mathbf{u} = (u_1, \ldots, u_s)$ with

$$u_1 \frac{\partial}{\partial x_1} \mathbf{D}(\mathbf{a}) + \ldots + u_s \frac{\partial}{\partial x_s} \mathbf{D}(\mathbf{a}) = 0.$$

Then $\dim X \geqslant a$, and for $\mathbf{u} \in X$ we have

$$\mathfrak{T}(\mathbf{u} \mid \mathbf{y}^{(i)}(\mathbf{a}) \mid \mathbf{y}^{(j)}(\mathbf{a})) = 0 \quad (1 \leqslant i,j \leqslant d).$$

The assertion of the lemma holds with the space X, and the space Z spanned by $\mathbf{y}^{(1)}(\mathbf{a}), \ldots, \mathbf{y}^{(d)}(\mathbf{a})$.

Lemma 5. *There is a constant $B = B(s)$ as follows. Let $\mathfrak{T}(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z})$ be a symmetric trilinear form in vectors $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{Q}^s$. Let b be an integer in $s < b \leqslant 2s$, and let $R \geqslant 1$. Suppose there are more than*

$$B R^{b-1}$$

pairs $(\mathbf{x}, \mathbf{y})$ of integer points with $|\mathbf{x}| \leqslant R$, $|\mathbf{y}| \leqslant R$ for which

$$\mathfrak{T}(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z}) = 0$$

identically in $\mathbf{z}$. Then there is a subspace S of $\mathbb{Q}^s$ with

$$\dim S \geqslant b - s$$

such that $\mathfrak{T}(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z}) = 0$ for $\mathbf{x}, \mathbf{y}, \mathbf{z} \in S$.

Proof. For given $\mathbf{x}$, let again $Y(\mathbf{x})$ be the subspace consisting of $\mathbf{y}$ for which $\mathfrak{T}(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z}) = 0$ identically in $\mathbf{z}$. In a subspace Y of dimension d, there are at most $c_1(s) R^d$ integer points $\mathbf{y}$ with $|\mathbf{y}| \leqslant R$. Thus if $\lambda(d)$ is the number of $\mathbf{x}$ with $\dim Y(\mathbf{x}) = d$ and $|\mathbf{x}| \leqslant R$, then our hypothesis yields

$$c_1(s) \sum_{d=0}^{s} \lambda(d) R^d \geqslant B R^{b-1}.$$

Hence there is a d with $\lambda(d) \geqslant c_2(s) B R^{b-d-1}$. If B is so large that $c_2(s) B > A$, then the preceding lemma may be applied with $a = b - d$, and we obtain subspaces X and Y with (5.2) having $\dim X \geqslant b - d$, $\dim Y \geqslant d$. The intersection $S = X \cap Y$ has the properties enunciated in the lemma.

Lemma 6. *Suppose $\mathfrak{B}(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z} \mid \mathbf{w})$ with $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{Q}^s$ and $\mathbf{w} \in \mathbb{Q}^r$ is a fourlinear form which is symmetric in $\mathbf{x}, \mathbf{y}, \mathbf{z}$. Let $s > 2r^2 - 2r$, and let c be an integer with*

$$s + 2r^2 - 2r < c \leqslant 2s. \tag{5.7}$$

There is a constant $C = C(\mathfrak{B})$ as follows. Suppose that $R \geqslant 1$ and that there are

$$\geqslant C R^{c-1}$$

pairs $(\mathbf{x}, \mathbf{y})$ of integer points with $|\mathbf{x}| \leqslant R$, $|\mathbf{y}| \leqslant R$ for which there is a nonzero $\mathbf{w}$ in $\mathbb{Q}^r$ such that $\mathfrak{B}(\mathbf{x} \mid \mathbf{y} \mid \mathbf{z} \mid \mathbf{w}) = 0$ identically in $\mathbf{z}$.

Then there is a nonzero $\mathbf{w}_0 \in \mathbb{Q}^r$ and there is a subspace S of $\mathbb{Q}^s$ with

$$\dim S \geqslant c - s - 2r^2 + 2r$$

such that $\mathfrak{B}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}\,|\,\mathbf{w}_0) = 0$ *for* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in S$.

Proof. Let $(\mathbf{x}, \mathbf{y})$ be a typical pair in the hypothesis of the lemma. The condition that $\mathfrak{B}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}\,|\,\mathbf{w}) = 0$ identically in $\mathbf{z}$ is a linear condition on $\mathbf{w}$, and since a nontrivial such $\mathbf{w} \in \mathbb{Q}^r$ exists, the condition must amount to not more than $r - 1$ linear homogeneous equations in $w_1, \ldots, w_r$. The coefficients of each of these equations are $\leqslant c_3(\mathfrak{B}) R^2$ in absolute value, since $|\mathbf{x}|, |\mathbf{y}| \leqslant R$. Hence these linear equations have a nonzero solution $\mathbf{w} = \mathbf{w}(\mathbf{x}, \mathbf{y})$ whose components are integers not exceeding $c_4(\mathfrak{B}) R^{2(r-1)}$ in absolute value. The number of possibilities for such vectors $\mathbf{w}$ does not exceed $c_5(\mathfrak{B}) R^{2r^2 - 2r}$. Since there are at least $C R^{c-1}$ pairs in the hypothesis, there must be a $\mathbf{w}_0$ having $\mathbf{w}_0 = \mathbf{w}(\mathbf{x}, \mathbf{y})$ for at least $(C/c_5) R^{c - 2r^2 + 2r - 1}$ of these pairs. Now if C is so large that $C/c_5 \geqslant B$, then the preceding lemma may be applied with $\mathfrak{T}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}) = \mathfrak{B}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}\,|\,\mathbf{w}_0)$ and with $b = c - 2r^2 + 2r$. The coefficients of $\mathfrak{T}$ here depend on R and may be quite large, but fortunately the constant B of Lemma 5 does not depend on the coefficients.

6. *The Minor Arcs.* Let $\mathfrak{B}$ be the fourlinear form (5.1). For every pair $(\mathbf{x}, \mathbf{y})$ with (4.5) there is a $\mathbf{w} \neq \mathbf{0}$ such that $\mathfrak{B}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}\,|\,\mathbf{w}) = \mathbf{w}\mathbf{F}(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}) = 0$ identically in $\mathbf{z}$. In other words, $W(\mathbf{x}, \mathbf{y}) \neq \mathbf{0}$.

Suppose the third alternative of Lemma 3 holds for certain arbitrarily large values of P. Put

$$c = 2s - [4K/\theta]$$

where [ ] denotes the integer part. We have

$$2\theta s - 4K - \varepsilon = \theta(2s - (4K/\theta) - (\varepsilon/\theta)) > \theta(c - 1)$$

if $\varepsilon > 0$ is sufficiently small. Hence Lemma 6 may be applied with $R = P^\theta$ (we don't have to check (5.7), since the lemma is trivially true if this condition is violated). There is then a rational $\mathbf{w}_0 \neq \mathbf{0}$ and a subspace S of $\mathbb{Q}^s$ with

$$\dim S \geqslant c - s - 2r^2 + 2r \geqslant s - (4K/\theta) - 2r^2 + 2r$$

such that $\mathbf{w}_0 F(\mathbf{x}\,|\,\mathbf{y}\,|\,\mathbf{z}) = 0$ for $\mathbf{x}, \mathbf{y}, \mathbf{z} \in S$. The form $\mathbf{w}_0 \mathbf{F}$ of the rational pencil vanishes on a space S with

$$\operatorname{codim} S \leqslant (4K/\theta) + 2r^2 - 2r.$$

We now set either

$$K = K_1 = \theta(2r^2 + 2r + (1/5)),$$

or

$$K = K_2 = \theta(2r\gamma(r) + (1/5)).$$

Suppose the hypotheses of Theorem 2 hold. Applying what we just said with $K = K_1$, we see that the form $\mathbf{w}_0\mathbf{F}$ would vanish on a rational subspace of codimension $\leqslant 10r^2 + 6r$, which is impossible. Hence the third alternative of Lemma 3 is ruled out.

On the other hand, suppose that the stronger hypotheses of part (a) of the Second Supplement hold. Putting $K = K_2$, we see that the form $\mathbf{w}_0\mathbf{F}$ would vanish on a rational subspace of codimension $\leqslant 8r\gamma(r) + 2r^2 - 2r$, which is impossible. Again the third alternative of Lemma 3 is ruled out.

We now put $\Delta = 2r\theta$ and $\varrho = (10r)^{-1}$, so that $K_1 = \Delta(r + 1 + \varrho)$, $K_2 = \Delta(\gamma(r) + \varrho)$. Our conclusions may be summarized as follows.

Lemma 7. *Suppose the hypotheses of Theorem 2 hold. Then for large P, each $\underline{\alpha}$ either has*

(i) $$|S(\underline{\alpha})| \leqslant P^{s-\Delta(r+1+\varrho)},$$

or

(ii) *$\underline{\alpha}$ lies in the set $\mathfrak{N}(\Delta)$, consisting of r-tuples which have approximations $(a_1/q, \ldots, a_r/q)$ with*

$$1 \leqslant q \leqslant P^{\Delta}, \tag{6.1}$$

$$(\mathbf{a}, q) = 1, \tag{6.2}$$

$$|q\alpha_i - a_i| < P^{-3+\Delta} \quad (i = 1, \ldots, r). \tag{6.3}$$

Moreover, if the hypotheses of part (a) *of the Second Supplement hold, then* (i) *may be replaced by*

(i′) $$|S(\underline{\alpha})| \leqslant P^{s-\Delta(\gamma(r)+\varrho)}.$$

Next we have

Lemma 8. *Suppose* $\mathbf{a} = (a_1, \ldots, a_r)$ *and* q *have* $(\mathbf{a}, \mathbf{q}) = 1$. *Then the sum* $S(\mathbf{a}, q)$ *given by* (3.1) *has*

$$|S(\mathbf{a}, q)| \ll q^{s-r-1-(\varrho/2)}$$

if the conditions of Theorem 2 hold. It even has

$$|S(\mathbf{a}, q)| \ll q^{s-\gamma(r)-(\varrho/2)}$$

if the conditions of part (a) *of the Second Supplement hold.*

Let $\mathfrak{n}(\Delta)$ be the complement of $\mathfrak{N}(\Delta)$ in $\mathfrak{U}_r$.

Lemma 9. *For* $0 < \Delta < 3r/(r+1)$ *we have*

$$\int_{\mathfrak{n}(\Delta)} |S(\underline{\alpha})|\, d\underline{\alpha} \ll P^{s-3r-(\varrho\Delta/2)}.$$

Proofs. Just as for Lemmas 7, 8 in [14].

Now let $\mathfrak{M} = \mathfrak{M}(\Delta)$ consist of $\underline{\alpha}$ in $\mathfrak{U}_r$ for which there are approximations $(a_1 q/, \ldots, a_r/q)$ with (6.1), (6.2) and

$$\left|\alpha_i - \frac{\alpha_i}{q}\right| \leqslant P^{-3+\Delta} \quad (i = 1, \ldots, r). \tag{6.4}$$

Since (6.4) is weaker than (6.3), we have

$$\mathfrak{N}(\Delta) \cap \mathfrak{U}_r \subseteq \mathfrak{M}(\Delta).$$

Then the complement $\mathfrak{m} = \mathfrak{m}(\Delta)$ of $\mathfrak{M} = \mathfrak{M}(\Delta)$ in $\mathfrak{U}_r$ is contained in $\mathfrak{n}(\Delta)$. Following tradition we call $\mathfrak{M}$ the "major arcs" and $\mathfrak{m}$ the "minor arcs". According to Lemma 9, the integral

$$\int_{\mathfrak{m}} S(\underline{\alpha})\, e(-\underline{\alpha}\mathbf{c})\, d\underline{\alpha},$$

which is the part of the integral (4.1) belonging to $\mathfrak{m}$, is small. We therefore may turn to the major arcs.

7. The Major Arcs. Given $\mathbf{a}, q$ with (6.1), (6.2), let $\mathfrak{M}_{\mathbf{a},q} = \mathfrak{M}_{\mathbf{a},q}(\Delta)$ be the set of $\underline{\alpha}$ with (6.4).

Lemma 10. *Suppose* $\underline{\alpha} = q^{-1}\mathbf{a} + \underline{\beta} \in \mathfrak{M}_{\mathbf{a},q}$. *Then*

$$S(\underline{\alpha}) = q^{-s} S(\mathbf{a}, q)\, I(\underline{\beta}) + O(q P^{s-1+\Delta})$$

where

$$I(\underline{\beta}) = \int_{P\mathfrak{B}} e(\underline{\beta}\mathbf{F}(\underline{\xi}))\, d\underline{\xi}.$$

Proof. We proceed as with Lemma 9 in [14], the only exception being that in the formula below (9.3),

$$q|\underline{\beta}|P \ll q P^{-2+\Delta} P$$

is to be replaced by

$$q|\underline{\beta}|P^2 \ll q P^{-3+\Delta} P^2.$$

Lemma 11. *For sufficiently small $\Delta > 0$*

$$\int_{\mathfrak{M}} S(\underline{\alpha})\, e(-\mathbf{c}\,\underline{\alpha})\, d\underline{\alpha} = P^{s-3r}\,\mathfrak{S}(P^{\Delta}, \mathbf{c})\,\mathfrak{J}(P^{\Delta}) + O(P^{s-3r-\delta})$$

for some $\delta > 0$, where

$$\mathfrak{S}(P^{\Delta}, \mathbf{c}) = \sum_{q \leqslant P^{\Delta}} A(q, \mathbf{c})$$

with $A(q, \mathbf{c})$ given by (3.2), *and*

$$\mathfrak{J}(P^{\Delta}) = \int_{|\underline{\gamma}| < P^{\Delta}} \Big(\int_{\mathfrak{B}} e(\underline{\gamma}\,\mathbf{F}(\underline{\xi}))\, d\underline{\xi}\Big)\, d\underline{\gamma}.$$

Proof. The argument for Lemma 10 of [14] carries over with small changes. For $\underline{\alpha} = q^{-1}\mathbf{a} + \underline{\beta} \in \mathfrak{M}_{\mathbf{a},q}$,

$$e(-\mathbf{c}\,\underline{\alpha}) = e(-q^{-1}\mathbf{a}\mathbf{c})\, e(-\underline{\beta}\,\mathbf{c}) = e(-q^{-1}\mathbf{a}\mathbf{c}) + O(P^{-3+\Delta}),$$

so that by our Lemma 10,

$$S(\underline{\alpha})\, e(-c\,\underline{\alpha}) = q^{-s} S(\mathbf{a}, q)\, e(-q^{-1}\mathbf{a}\mathbf{c})\, I(\underline{\beta}) + O(qP^{s-1+\Delta}).$$

We have to integrate over $\mathfrak{M}_{\mathbf{a},q}$, and take the sum over the sets $\mathfrak{M}_{\mathbf{a},q}$, which are disjoint when Δ is small.

The error term, when integrated over $\mathfrak{M}_{\mathbf{a},q}$, i.e. over $|\underline{\beta}| \leqslant P^{-3+\Delta}$, gives

$$\ll P^{-3r+\Delta r} P^{s-1+2\Delta} = P^{s-3r-1+(r+2)\Delta}.$$

Summation over $\mathbf{a}$ gives a factor $\leqslant q^r$, and summation over $q \leqslant P^{\Delta}$ gives a factor $\leqslant \sum q^r \leqslant P^{\Delta(r+1)}$, so that the total error is

$$\ll P^{s-3r-1+(2r+3)\Delta}.$$

This certainly is $\ll P^{s-3r-\delta}$ when Δ is small.

The main term gives

$$\mathfrak{S}(P^{\Delta}, \mathbf{c}) \int_{|\underline{\beta}| < P^{-3+\Delta}} I(\underline{\beta})\, d\underline{\beta}.$$

With the new variables $\underline{\gamma} = P^3 \underline{\beta}$, the integral becomes

$$P^{-3r} \int_{|\underline{\gamma}| < P^{\Delta}} I(P^{-3}\underline{\gamma})\, d\underline{\gamma} = P^{s-3r}\,\mathfrak{J}(P^{\Delta}),$$

since

$$I(P^{-3}\underline{\gamma}) = \int_{P\mathfrak{B}} e(P^{-3}\underline{\gamma}\,\mathbf{F}(\underline{\xi}))\, d\underline{\xi} = P^s \int_{\mathfrak{B}} e(\underline{\gamma}\,\mathbf{F})\, d\underline{\xi}.$$

8. Completion of the Proof of Theorem 2. Formula (4.1) in conjunction with Lemmas 9 and 11 yields

$$z_P = P^{s-3r} \mathfrak{J}(P^{\Delta}) \mathfrak{S}(P^{\Delta}, \mathbf{c}) + O(P^{s-3r-\delta}).$$

It remains for us to show that $\mathfrak{J}$ (as defined in (2.2)) exists and that

$$|\mathfrak{J} - \mathfrak{J}(P^{\Delta})| \ll P^{-\Delta},$$

as well as that $\mathfrak{S}(\mathbf{c})$ (as defined in (3.4)) exists and that

$$|\mathfrak{S}(\mathbf{c}) - \mathfrak{S}(P^{\Delta}, \mathbf{c})| \ll P^{-\Delta}.$$

The assertions concerning the singular series are immediate consequences of the definitions and of the inequality (3.3), which follows from Lemma 8. To deal with the singular series we follow the procedure in [14]. Put

$$\mathfrak{K}(\underline{\gamma}) = \int_{\mathfrak{B}} e(\underline{\gamma}\mathbf{F}(\underline{\xi}))\, d\underline{\xi}.$$

Lemma 12.

$$|\mathfrak{K}(\underline{\gamma})| \ll \min(1, |\underline{\gamma}|^{-r-1}).$$

Proof. Same as for the corresponding lemma in [14], the only difference being that now we set $\underline{\beta} = P^{-3}\underline{\gamma}$. But still $P = |\underline{\gamma}|^{r+2}$ and $\varphi = (r+2)^{-1}$.

As a consequence of the lemma, the integral

$$\mathfrak{J}_0 = \int \mathfrak{K}(\underline{\gamma})\, d\underline{\gamma}$$

is absolutely convergent, and

$$|\mathfrak{J}_0 - \mathfrak{J}(P^{\Delta})| \ll P^{-\Delta}.$$

Finally, again as in [14],

$$|\mathfrak{J}_0 - \mathfrak{J}_T| \ll T^{-1},$$

so that the limit $\mathfrak{J}$ of $\mathfrak{J}_T$ exists, and $\mathfrak{J} = \mathfrak{J}_0$.

9. Bottomed and Bottomless Systems. We finally come to part (b) of the Second Supplement and to the definition of bottomed systems.

Let k be a field of characteristic 0. To each cubic form $\mathfrak{F}$ with coefficients in k there belongs a unique symmetric trilinear form $\mathfrak{F}(\mathbf{x}|\mathbf{y}|\mathbf{z})$ with $\mathfrak{F}(\mathbf{x}) = \mathfrak{F}(\mathbf{x}|\mathbf{x}|\mathbf{x})$. Let $\mathbf{F} = (\mathfrak{F}_1, \ldots, \mathfrak{F}_r)$ denote an r-tuple of such cubic forms in vectors $\mathbf{x} = (x_1, \ldots, x_s)$. If T, τ are linear transformations respectively of k^r into itself and of k^s into itself, let

$T\mathbf{F}_\tau$ be the r-tuple of cubic forms with

$$T\mathbf{F}_\tau(\mathbf{x}) = T(\mathbf{F}(\tau(\mathbf{x}))).$$

Call systems $\mathbf{F}$ and $\mathbf{F}'$ *equivalent* if there are nonsingular T, τ with $T\mathbf{F}_\tau = \mathbf{F}'$.

Following [13] we call a system *special* if there are nonnegative integers $a_1, \ldots, a_s$ and $b_1, \ldots, b_r$ with

$$3s^{-1}(a_1 + \ldots + a_s) < r^{-1}(b_1 + \ldots + b_r) \tag{9.1}$$

such that

$$\mathfrak{F}_j(\mathbf{e}_{i_1} | \mathbf{e}_{i_2} | \mathbf{e}_{i_3}) = 0$$

for every j and every triple i_1, i_2, i_3 with

$$a_{i_1} + a_{i_2} + a_{i_3} < b_j.$$

Here $\mathbf{e}_1, \ldots, \mathbf{e}_s$ are the basis vectors. We call a system *bottomless* if it is equivalent to a special one. (The reason for this name is more apparent in the case where k is the field $\mathbb{Q}_p$ of p-adic numbers, which was studied in [13].) A system which is not bottomless will be called *bottomed.*

By an *invariant* $\mathfrak{J} = \mathfrak{J}(\mathbf{F})$ we will mean a not identically vanishing form (with coefficients in $\mathbb{Z}$) in the coefficients of the forms $\mathfrak{F}_j$, which has

$$\mathfrak{J}(T\mathbf{F}_\tau) = (\det T)^{\Delta/r}(\det \tau)^{3\Delta/s}\,\mathfrak{J}(\mathbf{F}),$$

where Δ is the total degree of $\mathfrak{J}$. As was pointed out in [15], such an invariant certainly does exist.

Lemma 13. *A bottomless system* $\mathbf{F}$ *has*

$$\mathfrak{F}(\mathbf{F}) = 0$$

for any invariant $\mathfrak{J}$.

In [13] this was proved for $k = \mathbb{Q}_p$.

Proof. We may suppose without loss of generality that $\mathbf{F}$ is special. Adjoin a variable Z to the field k, and define linear transformations T, τ by

$$T\mathbf{e}_i = Z^{b_i}\mathbf{e}_i \quad (i = 1, \ldots, r),$$

$$\tau\mathbf{e}_j = Z^{a_j}\mathbf{e}_j \quad (j = 1, \ldots, s),$$

and put $\mathbf{F}' = T^{-1}\mathbf{F}_\tau$. Then

$$\mathfrak{F}'_j(\mathbf{e}_{i_1} | \mathbf{e}_{i_2} | \mathbf{e}_{i_3}) = Z^{a_{i_1}+a_{i_2}+a_{i_3}-b_j}\,\mathfrak{F}_j(\mathbf{e}_{i_1} | \mathbf{e}_{i_2} | \mathbf{e}_{i_3})$$

is zero when $a_{i_1} + a_{i_2} + a_{i_3} < b_j$, hence in each case it lies in the polynomial ring $k[Z]$. So each coefficient of $\mathbf{F}'$ lies in $k[Z]$, and so does $\mathfrak{J}(\mathbf{F}')$. But

$$\mathfrak{J}(\mathbf{F}') = Z^{-(b_1 + \cdots + b_r)(\Delta/r) + (a_1 + \cdots + a_s)(3\Delta/s)} \mathfrak{J}(\mathbf{F}),$$

and comparison with (9.1) shows that $\mathfrak{J}(\mathbf{F}')$ cannot lie in $k[Z]$ unless $\mathfrak{J}(\mathbf{F}) = 0$.

As a direct consequence of the lemma we see that *the bottomless systems lie in a proper algebraic subset of the space of all systems of cubic forms.* In fact it would not be hard to show that the bottomless systems themselves form a proper algebraic subset, and that this subset has a dimension quite a bit smaller than the set of all systems, at least when r and s are large. In [13, Theorem 3] we gave another result which shows that bottomlessness is rather rare, namely: *If* $\mathbf{F}$ *is bottomless, then there is a* t *in* $1 \leqslant t \leqslant r$ *and there are* t *independent forms in the pencil generated by* $\mathbf{F}$ *which vanish on a subspace of* k^s *of dimension* $\geqslant 1 + (r - t)[s/t]$.

Now in the context of the Second Supplement, we call $\mathbf{F}$ (which has coefficients in $\mathbb{Q}$) bottomed or bottomless if it so with respect to the field $\mathbb{C}$ of complex numbers. A bottomed system then is also bottomed in each p-adic field $\mathbb{Q}_p$. So by Theorem 2 of [14], if $\mathbf{F}$ has coefficients in $\mathbb{Z}$ and is bottomed, and if (1.9) holds, then there is a positive integer $m_p = m_p(\mathbf{F})$ such that the number $\nu_l(\mathbf{c})$ of solutions of the congruence (3.6) satisfies $\nu_l(\mathbf{c}) \gg p^{l(s-r)}$ when $\mathbf{c} \in m_p \mathbb{Z}^r$. Since $\chi(p, \mathbf{c})$ as defined in § 3 is the limit (as $l \to \infty$) of $\nu_l(\mathbf{c}) p^{-l(s-r)}$, we have $\chi(p, \mathbf{c}) > 0$. Now under the hypotheses of Theorem 2, the product (3.5) for $\mathfrak{S} = \mathfrak{S}(\mathbf{c})$ is convergent uniformly in $\mathbf{c}$, and hence $\chi(p, c) > 0$ for each $\mathbf{c} \in \mathbb{Z}^r$ when $p > p_0$. Hence certainly $\chi(p, \mathbf{c}) > 0$ for each prime p if $\mathbf{c} \in m\mathbb{Z}^r$ where

$$m = \prod_{p < p_0} m_p .$$

In this situation $\mathfrak{S} = \mathfrak{S}(\mathbf{c}) > 0$, as asserted.

References

[1] Birch, B. J.: Homogeneous forms of odd degree in a large number of variables. Mathematika **4**, 102—105 (1957).

[2] Birch, B. J.: Forms in many variables. Proc. Royal Soc. A **265**, 245—263 (1962).

[3] Borsuk, K.: Drei Sätze über die n-dimensionale Euklidische Sphäre. Fund. Math. **20**, 177—190 (1933).

[4] BRAUER, R.: A note on systems of homogeneous algebraic equations. Bull. Amer. Math. Soc. **51**, 749—755 (1945).

[5] DAVENPORT, H.: Cubic forms in 32 variables. Phil. Trans. Royal Soc. London A **251**, 193—232 (1959).

[6] DAVENPORT, H.: Cubic forms in 16 variables. Proc. Royal Soc. A **272**, 285—303 (1963).

[7] DAVENPORT, H., LEWIS, D. J.: Exponential sums in many variables. Amer. J. Math. **84**, 649—665 (1962).

[8] DAVENPORT, H., LEWIS, D. J.: Non-homogeneous cubic equations. J. London Math. Soc. **39**, 657—671 (1964).

[9] DAVENPORT, H., LEWIS, D. J.: Simultaneous equations of additive type. Phil. Trans. Royal Soc. London A **264**, 557—595 (1969).

[10] DEM'JANOV, V. B.: On cubic forms in discretely normed fields. Akad. Nauk SSSR. (NS) **74**, 889—891 (1950).

[11] LEEP, D., SCHMIDT, W. M.: Systems of homogeneous equations. (In preparation.)

[12] LEWIS, D. J.: Cubic homogeneous polynomials over p-adic number fields. Ann. Math. (2) **56**, 473—478 (1952).

[13] SCHMIDT, W. M.: Simultaneous p-adic zeros of quadratic forms. Mh. Math. **90**, 45—65 (1980).

[14] SCHMIDT, W. M.: Simultaneous rational zeros of quadratic forms. Progress Math. (In print.)

[15] SCHMIDT, W. M.: On cubic polynomials III. Systems of p-adic equations. Mh. Math. **93**, 211—223 (1982).

[16] TARTAKOVSKII, V. A.: The number of representations of large numbers by a form of "general type" with many variables. (Russian). I. Vestnik Leningrad Univ. **13**, no. 7, 131—154 (1958), and II. ibid. **14**, no. 7, 5—17 (1959).

[17] TARTAKOVSKII, V. A.: On representability of large numbers by forms of "general type" with a large number of variables. (Russian). Izv. Vysš. Učebn. Zaved. Matematika **1959**, no. 1 (2), 161—173 (1959).

[18] WATSON, G. L.: Non-homogeneous cubic equations. Proc. London Math. Soc. (3) **17**, 271—295 (1967).

Prof. Dr. W. M. SCHMIDT
Mathematics Department
University of Colorado
Boulder, CO 80309, U.S.A.

Verleger: Springer-Verlag, Mölkerbastei 5, A-1010 Wien. — Herausgeber: Prof. Dr. Hans Reiter, Institut für Mathematik der Universität, Strudlhofgasse 4, A-1090 Wien. — Redaktion: Strudlhofgasse 4, A-1090 Wien. — Hersteller: Ernst Becvar, Lichtgasse 10, A-1150 Wien. — Verlagsort: Wien. — Herstellungsort: Wien. — Printed in Austria.