Proc. Camb. Phil. Soc. (1969), **66**, 323
PCPS 66–38
Printed in Great Britain

Cubic forms over algebraic number fields

By C. RYAVEC
University of Michigan

(*Received* 8 *June* 1967)

In 1935 Tartakowski (7) proved that, in general, a cubic form in sufficiently many variables with coefficients in an algebraic number field K has a non-trivial zero in that field; and in the case when K is the rational field 57 variables suffice. Here, 'in general' means that the coefficients of the form do not lie in a proper subvariety of the coefficient space. Hence, Tartakowski's result holds for almost all cubic forms. Later, Lewis (5) proved that if K is any algebraic number field such that $[K: Q] = n$, then there exists a function $\psi(n)$ such that *every* cubic form over K in $m \geqslant \psi(n)$ variables has a non-trivial zero in K. His bound, $\psi(n)$, is extremely large; e.g. when K is the rational field, $\psi(1) > 500$.

The above bound was greatly reduced when Davenport (2) proved that a homogeneous, cubic form in m variables with rational coefficients always represents 0 non-trivially if $m \geqslant 32$. Employing the methods of (2), Ramanujam (6) showed that any homogeneous, cubic form over any algebraic number field represents 0 non-trivially in that field provided the number of variables is at least 54.

Subsequently, Davenport (3) proved that any homogeneous, cubic form in $m \geqslant 17$ variables over the rational field represents 0 non-trivially; and this condition was later relaxed (4) to $m \geqslant 16$. The object of this paper is to show that it is possible to adopt the methods of Davenport (3) and some of those of Ramanujam (6) to prove that the condition $m \geqslant 54$ for cubic forms over any algebraic number field can also be relaxed to $m \geqslant 17$.

The distinguishing feature of Davenport's paper (2) is that it marks the first time that the Hardy–Littlewood Circle Method (which was also used in (3) and (4)) was successfully applied to Diophantine equations of non-additive type. Davenport found that with the assumption that the cubic form $C(X_1, \ldots, X_m)$ does not represent 0 non-trivially and $m \geqslant 32$ the number of solutions, $N(P)$, of $C(X_1, \ldots, X_m) = 0$ with X_i an integer and $|X_i| < P$ satisfies

$$N(P) = cP^{m-3} + o(P^{m-3}) \quad \text{as} \quad P \to \infty, \tag{1}$$

where c is a positive constant. From (1) he deduced that $C(X)$ does indeed represent 0 non-trivially; so that the original assumption that $C(X)$ does not represent 0 non-trivially is false. Thus, Davenport showed that $C(X)$ did represent 0 non-trivially if $m \geqslant 32$, although the asymptotic formula (1) was not valid.

The same logical structure is employed by Davenport in (4) and by Ramanujam in (6) and by myself in this paper. I also use the same general line of proof in this paper as that which is used in (3) and (6). The changes I have made consist of (*a*) appropriately

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

modifying the arguments of (3) to suit the number field case and (*b*) adding some lemmas and remarks of my own to make the proof clear.

The question is still open as to whether or not the methods used by Davenport in (4) to obtain the bound 16 can be modified to prove the same result for the number field case. This would require, among other things, the extension of certain results in the geometry of numbers over the rational integers to similar results over algebraic number fields. Only partial results have been obtained in this direction so far.

Finally, it has been shown that there exist cubic forms in nine variables which do not represent 0 non-trivially (see (3), p. 108). On the other hand, Lewis has shown that every cubic form in ten or more variables with coefficients in an algebraic number field K possesses a non-trivial zero in $K_{\mathfrak{P}}$ for every prime $\mathfrak{P}$ of K. It appears likely, then, that any cubic form over any algebraic number field in $m \geqslant 10$ variables has a non-trivial zero in that field. No counter example to this conjecture has been found as yet, while the results of Davenport (4) and of this paper are the best that are known in this direction.

We prove:

THEOREM. *Let K be an algebraic number field and $\mathfrak{O}_K$ its ring of integers. Let*

$$C(X) = \sum_{1 \leqslant i,j,k \leqslant m} c_{ijk} X_i X_j X_k$$

be a homogeneous, cubic form with coefficients in $\mathfrak{O}_K$. Then $C(X)$ represents 0 non-trivially in $(\mathfrak{O}_K)^m$ provided $m \geqslant 17$.

If $C(X)$ is degenerate over K, then one can easily prove that $C(X)$ represents 0 non-trivially in $(\mathfrak{O}_K)^m$, the mth Cartesian product of $\mathfrak{O}_K$. So without loss of generality it may be assumed that $C(X)$ is non-degenerate over K.

The proof of the theorem will be accomplished in the next five sections.

1. *Notation.* Q, R, C will denote the rational, real and complex fields, respectively; K will denote an algebraic number field over Q with $[K: Q] = n$; and Z will denote the rational integers.

Put $\delta^{-1} = \{\xi \in K | S(\lambda\xi) \in Z \text{ for all } \lambda \in \mathfrak{O}_K\}$, so that δ is the different (it is an integral ideal) of K. Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of K, and let $\{\rho_1, \ldots, \rho_n\}$ denote the dual basis of δ^{-1}, determined uniquely by $S(\omega_i \rho_j) = \delta_{ij}$.

Let K_R denote the n-dimensional commutative algebra $R \otimes_Q K$ over R; i.e. the scalar extension of K to a module over R. If we identify an element $x \in K$ with $1 \otimes x$ of K_R, then $\{\omega_1, \ldots, \omega_n\}$ is a basis of K_R over R; and for any $y \in K_R$ we can write $y = \sum_{1 \leqslant i \leqslant n} y_i \omega_i$, where $y_i \in R$. For any $y \in K_R$, $S(y)$ and $N(y)$ will denote the trace and norm, respectively, of y over R.

Define a box $B = B(a_1, b_1, \ldots, a_n, b_n)$ in K_R as the set

$$\{y \in K_R | a_i \leqslant y_i < b_i,\ 1 \leqslant i \leqslant n\},$$

where the a_i, b_i are real numbers such that $0 < b_i - a_i \leqslant 1$. $B^{(0)}$ will denote the box $\{y \in K_R | -1 \leqslant y_i < 1\}$. $(K_R)^m$ will be the mth Cartesian product of K_R, considered as an mn-dimensional space over R. $\mathscr{B}$ will denote the Cartesian product of the

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

$B^{(1)}, \ldots, B^{(m)}$; i.e. $\mathscr{B} = B^{(1)} \times B^{(2)} \times \ldots \times B^{(m)}$, a box in $(K_R)^m$. $\mathscr{B}^{(0)}$ is the special box $B^{(0)} \times \ldots \times B^{(0)}$ in $(K_R)^m$.

For real t we let $e(t) = e^{2\pi i t}$ and let $\|t\|$ be the distance of t from the nearest integer.

2. *General cubic exponential sums.* Let $G(X) = \sum_{1 \leqslant i,j,k \leqslant m} g_{ijk} X_i X_j X_k$ be a cubic form with coefficients g_{ijk} in K_R which are symmetric in all three indices. With $G(X)$ we associate the bilinear forms $B_j(X, Y) = \sum_{1 \leqslant i,k \leqslant m} g_{ijk} X_i Y_k$, which are defined on $(K_R)^{2m}$ with values in K_R. We also put $B_j(X, Y) = \sum_{p=1}^{n} \lambda_{jp}(X, Y)\rho_p$, where the λ_{jp} are bilinear forms defined on $(K_R)^{2m}$ with values in R. Finally, unless otherwise stated, all sums will be over integral $X = (X_1, \ldots, X_m)$, $X_i = \sum_{1 \leqslant j \leqslant n} X_{ij}\omega_j$, with X_{ij} in Z.

LEMMA 2·1. *For $P > 1$, let $T = H(P, \mathscr{B}) = \sum_{X \in P\mathscr{B}} e(S(G(X)))$, where $\mathscr{B}$ is a box in $(K_R)^m$ and $P\mathscr{B}$ is the box obtained from it by enlarging each side by the factor P. Then we have the estimate*

$$|T|^4 \ll P^{mn} \sum_{X, Y \in P\mathscr{B}_0} \prod_{1 \leqslant j \leqslant m} \prod_{1 \leqslant p \leqslant n} \min(P, \|6\lambda_{jp}\|^{-1}). \tag{2}$$

Proof. See (6), Lemma 1·1, p. 684.

LEMMA 2·2. *Assume that $|T| \geqslant P^{n(m-\kappa)}$ for $0 < \kappa < m$. Let N_1 denote the number of distinct pairs of integral points X, Y in $P\mathscr{B}^{(0)}$ satisfying $\|6\lambda_{jp}\| < P^{-1}$ for $1 \leqslant j \leqslant m$, $1 \leqslant p \leqslant n$. Then $N_1 \gg (P^{2m-4\kappa} \log^{-m} P)^n$.*

Proof. See (6), Lemma 1·2, p. 684.

LEMMA 2·3. *With the assumption of Lemma 2·2, let N_2 denote the number of distinct pairs of integral points X, Y in $P^\theta\mathscr{B}^{(0)}$ satisfying $\|6\lambda_{jp}\| < P^{-3+2\theta}$, where $0 < \theta < 1$ is fixed. Then $N_2 \gg (P^{2m\theta-4\kappa} \log^{-m} P)^n$.*

Proof. See (6), Lemma 1·3, p. 685.

Henceforth, $\mathscr{S}(G)$ will denote the set of integral pairs (X, Y) satisfying the conditions of Lemma 2·3; thus $N_2 = |\mathscr{S}(G)|$.

3. *Special cubic exponential sums.* We now apply Lemma 2·3 to the particular cubic form

$$G(X) = \sum_{1 \leqslant i,j,k \leqslant m} \alpha c_{ijk} X_i X_j X_k, \tag{3}$$

where $\alpha = \sum_{1 \leqslant i \leqslant n} \alpha_i \rho_i$ and c_{ijk} is in $\mathfrak{O}_K$, and α and c_{ijk} are considered in K_R.

LEMMA 3·1. *Let $0 < \theta < 1$, where θ is independent of P, and let $G(X)$ be the form (3). Then for any fixed $\epsilon > 0$, there is a $P(\epsilon)$ such that for all $P > P(\epsilon)$. Either (A) There are more than $P^{mn\theta+\epsilon}$ pairs of integral points X, Y in $P^\theta\mathscr{B}^{(0)}$ satisfying $B_j(X, Y) = 0$, $1 \leqslant j \leqslant m$. Or (B) The hypothesis $|T| \geqslant P^{n(m-\frac{1}{4}m\theta+\epsilon)}$ implies there exists a non-zero integer μ in $\mathfrak{O}_K$ and a ν in δ^{-1} such that*

$$\mu\alpha - \nu = \sum_{1 \leqslant i \leqslant n} \beta_i \rho_i, \tag{4}$$

$$\beta_i \in R, \quad |\beta_i| < P^{-3+2\theta}, \tag{5}$$

$$\mu \in P^{2\theta+\epsilon} B^{(0)}. \tag{6}$$

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

Proof. Apply Lemma 2·3 to $G(X)$ with $\kappa = \frac{1}{4}m\theta - \epsilon$, where ϵ is chosen very small compared with $\frac{1}{4}m\theta$. Then we have

$$6\alpha B_j(X, Y) = 6 \sum_{1 \leqslant p \leqslant n} \lambda_{jp}\rho_p,$$

where $\|6\lambda_{jp}\| < P^{-3+2\theta}$, and where the bilinear forms $B_j(X, Y)$ are now those associated with $C(X)$ and not with $G(X)$.

Now if for all integral X, Y in $\mathscr{S}(G)$ and for all j, $1 \leqslant j \leqslant m$, we have $B_j(X, Y) = 0$, then we have Alternative (A). Otherwise, the hypothesis $|T| \geqslant P^{n(m-m\theta/4+\epsilon)}$ implies that for some j $(1 \leqslant j \leqslant m)$, and for some pair X, Y in $\mathscr{S}(G)$, we have

$$\begin{aligned} 6\alpha B_j(X, Y) &= \sum_{1 \leqslant p \leqslant n} 6\lambda_{jp}\rho_p \\ &= \sum_{1 \leqslant p \leqslant n} r_p\rho_p + \sum_{1 \leqslant p \leqslant n} 6\lambda'_{jp}\rho_p, \end{aligned}$$

where r_j is in Z and $|6\lambda'_{jp}| < P^{-3+2\theta}$ and $B_j(X, Y) \neq 0$. Therefore, choosing $\mu = 6B_j(X, Y)$ and $\nu = \sum_{1 \leqslant p \leqslant n} r_p\rho_p$, and noticing that B_j is in $P^{2\theta+\epsilon}B^{(0)}$, we have (4), (5), (6) satisfied.

It should be noted that Lemma 3·1 holds for any fixed $\epsilon > 0$ and all $P > P(\epsilon)$. Henceforth, in any application of Lemma 3·1, it will be assumed that $P > P(\epsilon)$, although this will not be explicitly stated.

4. *Alternative* (A). In this section it will be shown that Alternative (A) of Lemma 3·1 implies that $C(X)$ represents 0 non-trivially in $(\mathfrak{O}_K)^m$.

LEMMA 4·1. *Let ϵ be any fixed, positive number. Assume that for some arbitrarily large $\Gamma > 0$ there exist more than $\Gamma^{mn+\epsilon}$ distinct pairs X, Y of integral points in $(\mathfrak{O}_K)^m$ such that $0 < |X|, |Y| < \Gamma$ and $B_j(X, Y) = 0$ for $1 \leqslant j \leqslant m$, where $0 < |X| < \Gamma$ means that $0 < |X_{ij}| < \Gamma$, $X_i = \sum_{1 \leqslant j \leqslant n} X_{ij}\omega_j$, $X_{ij} \in Z$, $X = (X_1, \ldots, X_m)$. Then $C(X)$ represents 0 non-trivially in $\mathfrak{O}_K$.*

Proof. This lemma is a generalization to cubic forms over algebraic number fields of Lemma 4 of (4), which gives the result for cubic forms over the rationals. The main step in proving Lemma 4 of (4) is provided by Lemma 3 of (4), and the proofs of both these lemmas (as given in (4)) carry over almost word for word to the number field case. In proving these lemmas a result is used concerning the existence of a non-singular integral solution of a system of polynomial equations with integral coefficients. This result is given as Lemma 2 of (4) and its proof uses methods of algebraic geometry. In the number field case the corresponding result is required when the coefficients and variables are integers of a given algebraic number field; and here again the proof given in (4) is applicable in these more general circumstances with very little modification.

5. *Alternative* (B). Henceforth it will be assumed that Alternative (B) holds; i.e. the assumption that $|T(\alpha)| \geqslant P^{n(m-m\theta/4+\epsilon)}$ implies that there is a $\mu \neq 0$, $\mu \in \mathfrak{O}_K$, and a $\nu \in \delta^{-1}$ satisfying (4), (5), and (6), where

$$T(\alpha) = \sum_{X \in P\mathscr{B}} e(S(\alpha C(X))), \quad \alpha = \sum_{1 \leqslant i \leqslant n} \alpha_i\rho_i, \ \alpha_i \in R.$$

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

For the remainder of this section, we let

$$\mathscr{R} = \{\alpha \in K_R | 0 < \alpha_i \leqslant 1;\ \alpha = \sum_{1 \leqslant i \leqslant n} \alpha_i \rho_i\}. \tag{7}$$

If $N(P)$ denotes the number of solutions of $C(X) = 0$, with $X \in P\mathscr{B}$, we have

$$N(P) = \int_{\mathscr{R}} T(\alpha)\, d\alpha, \quad d\alpha = d\alpha_1 d\alpha_2 \dots d\alpha_n. \tag{8}$$

For $\gamma \in K$, let $a(\gamma)$ denote the denominator of the ideal $(\gamma)\delta$; i.e. $a(\gamma)$ is the integral ideal $((1), (\gamma)\delta)^{-1}$. For those $\gamma \in K$ which satisfy Norm $(a(\gamma)) = N(a(\gamma)) \leqslant P^{2\theta}$, and for any θ such that $0 < \theta < 1$, we let

$$B(\gamma) = B(\gamma, \theta) = \left\{\alpha \in K_R | \alpha - \gamma = \sum_{1 \leqslant i \leqslant n} \beta_i \rho_i;\ |\beta_i| < P^{-3+2\theta} \frac{1}{N(a(\gamma))}\right\}. \tag{9}$$

We define the union of the major arcs to be

$$\mathfrak{M} = \bigcup_{\substack{\gamma \,(\mathrm{mod}\, \delta^{-1}) \\ N(a(\gamma)) \leqslant P^{2\theta}}} B(\gamma), \tag{10}$$

where θ will be specified later. The totality of minor arcs is defined to be

$$\mathfrak{m} = \{\alpha \in \mathscr{R} | \alpha \not\equiv \mu \,(\mathrm{mod}\, \delta^{-1}), \quad \forall\, \mu \in \mathfrak{M}\}. \tag{11}$$

It follows from the periodicity $(\mathrm{mod}\, \delta^{-1})$ of the function $T(\alpha)$ that

$$\int_{\mathfrak{M}} T(\alpha)\, d\alpha = \int_{\mathscr{C}\mathfrak{m}} T(\alpha)\, d\alpha,$$

where $\mathscr{C}\mathfrak{m}$ denotes the complement of $\mathfrak{m}$ with respect to $\mathscr{R}$.

It will now be shown that with a suitable choice of the box $\mathscr{B}$, and under the assumption that $C(X)$ does not represent 0 non-trivially in $(\mathfrak{O}_K)^m$, then for $m \geqslant 17$, we have the asymptotic expression

$$N(P) = J \,.\, \mathfrak{S} \,.\, P^{n(m-3)} + o(P^{n(m-3)}) \tag{12}$$

as $P \to \infty$, where $\mathfrak{S}$ and J are positive constants. But for P sufficiently large we see that (12) implies that $N(P) > 1$, which contradicts the assumption that $C(X)$ does not represent 0 non-trivially. Thus the assumption is false, so $C(X)$ does in fact represent 0 non-trivially. Moreover, the expression (12) is not necessarily valid as it was derived from a false premise.

LEMMA 5·1. *Let* $L_k(t) = \sum_{1 \leqslant i \leqslant n} r_{ik} t_i$ *be* n *linear forms in* n *variables with* r_{ik} *in* R. *To every real* $d > 1$, *there is an integral* $t_0 \neq 0$ *such that* $\|L_k(t_0)\| < d^{-1}$ *and* $|t_{i0}| \leqslant d$ *for* $1 \leqslant i, k \leqslant n$, *where* $t_0 = (t_{10}, t_{20}, \dots, t_{n0})$.

Proof. See (1), Theorem VI, p. 13.

For $0 < \theta < 1$, define

$$\mathscr{R}(\theta) = \{\alpha \in \mathscr{R} | \mu\alpha - \nu = \sum_{1 \leqslant i \leqslant n} \beta_i \rho_i,\ |\beta_i| < P^{-3+2\theta}\}, \tag{13}$$

where $\nu \in \delta^{-1}$ and μ is any non-zero element of $\mathfrak{O}_K$ such that $\mu \in P^{2\theta+\epsilon} B^{(0)}$.

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

LEMMA 5·2. *$\mathscr{R} \subseteq \mathscr{R}(3/4+\epsilon)$ for any $\epsilon > 0$.*

Proof. Put $\mu = \sum_{1\leqslant i\leqslant n} u_i\omega_i$, $\omega_i\rho_j = \sum_{1\leqslant k\leqslant n} A_{ijk}\rho_k$. Then

$$\begin{aligned}\mu\alpha &= \sum_{1\leqslant i,j\leqslant n} u_i\alpha_j\omega_i\rho_j \\ &= \sum_{1\leqslant k\leqslant n}\Big[\sum_{1\leqslant i,j\leqslant n} A_{ijk}u_i\alpha_j\Big]\rho_k \\ &= \sum_{1\leqslant k\leqslant n}\Big[\sum_{1\leqslant i\leqslant n} r_{ik}u_i\Big]\rho_k,\end{aligned}$$

where we have put $r_{ik} = \sum_{1\leqslant k\leqslant n} A_{ijk}\alpha_j$. Now apply Lemma 5·1 to the forms $L_k(u) = \sum_{1\leqslant i\leqslant n} r_{ik}u_i$ with $d = P^{-\frac{3}{2}}$. We conclude that there is a $(u_{10}, \ldots, u_{n0}) \neq (0, \ldots, 0)$ such that for all k, $1 \leqslant k \leqslant n$, we have $\| \sum_{1\leqslant i\leqslant n} r_{ik}u_{i0}\| < P^{-\frac{3}{2}}$ and $|u_{i0}| < P^{\frac{3}{2}}$. Now choose $\nu = \sum_{1\leqslant k\leqslant n} v_k\rho_k$, where v_k is the nearest integer to $\sum_{1\leqslant i\leqslant n} r_{ik}u_{i0}$. Then, for any α in $\mathscr{R}$, there is a non-zero μ in $\mathfrak{O}_K$ (here, $\mu = \sum_{1\leqslant i\leqslant n} u_{i0}\omega_i$) and a ν in δ^{-1} (here, $\nu = \sum_{1\leqslant k\leqslant n} v_k\rho_k$) such that

$$\mu\alpha - \nu = \sum_{1\leqslant i\leqslant n} \beta_i\rho_i,$$

where $|\beta_i| < P^{-\frac{3}{2}}$. Therefore, α is in $\mathscr{R}(\frac{3}{4}+\epsilon)$ for any $\epsilon > 0$ by the definition of $\mathscr{R}(\theta)$ given in (13). Since α in $\mathscr{R}$ was arbitrary, this implies that $\mathscr{R} \subseteq \mathscr{R}(\frac{3}{4}+\epsilon)$.

Q.E.D.

LEMMA 5·3.

$$\left|\int_{\mathfrak{m}} T(\alpha)\,d\alpha\right| = o(P^{n(m-3)}) \quad as \quad P\to\infty$$

provided $m \geqslant 17$.

Proof. We fix the major arcs from now on by choosing $\theta = 1/(2n+6)$. Also put $\sigma = (\theta/n)-\epsilon$. For this choice of σ, we will show that $\mathscr{R}(\sigma) \subseteq \mathscr{C}\mathfrak{m}$. To see this, let $\alpha\in\mathscr{R}(\sigma)$. By (13), there is a non-zero μ in $\mathfrak{O}_K$ and a ν in δ^{-1} such that $\mu\in P^{2\sigma+\epsilon}B^{(0)}$ and

$$\mu\alpha - \nu = \sum_{1\leqslant i\leqslant n} \beta_i\rho_i,$$

with $|\beta_i| < P^{-3+2\sigma}$. Dividing by μ and putting $\gamma = \nu/\mu$, the last equation becomes

$$\begin{aligned}\alpha - \gamma &= \sum_{1\leqslant i\leqslant n} \beta_i(\rho_i/\mu) \\ &= \sum_{1\leqslant i\leqslant n} \beta_i \sum_{1\leqslant j\leqslant n} \alpha_{ij}\rho_j \\ &= \sum_{1\leqslant j\leqslant n}\Big(\sum_{1\leqslant i\leqslant n} \alpha_{ij}\beta_i\Big)\rho_j \\ &= \sum_{1\leqslant j\leqslant n} \beta'_j\rho_j,\end{aligned}$$

where (a_{ij}) is the regular representation matrix of μ^{-1} with respect to the basis $\rho_1, \ldots, \rho_n$ of K over Q, in which case (a_{ij}) is the inverse of the regular representation matrix of μ with respect to the same basis. Therefore, for any i, j $(1 \leqslant i, j \leqslant n)$, we have

$$\begin{aligned}|a_{ij}| &\ll P^{(n-1)(2\sigma+\epsilon)}/N(\mu) \\ &\ll P^{(n-1)(2\sigma+\epsilon)}/N(a(\gamma)),\end{aligned}$$

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

since $$\mu \in a(\gamma) \quad \text{implies} \quad N(a(\gamma)) \leqslant N(\mu).$$

Hence, for any j $(1 \leqslant j \leqslant n)$,

$$|\beta_j'| \ll P^{-3+2\sigma+(n-1)(2\sigma+\epsilon)}/N(\alpha(\gamma))$$
$$\leqslant P^{-3+2\theta}/N(a(\gamma))$$

by the choice of σ. Therefore, α is congruent $(\text{mod}\, \delta^{-1})$ to an element of $\mathfrak{M}$. So $\alpha \in \mathscr{C}\mathfrak{m}$ by definition. Since α in $\mathscr{R}(\sigma)$ was arbitrary, we have $\mathscr{R}(\sigma) \subseteq \mathscr{C}\mathfrak{m}$.

By Lemma 5·2, for any small, but fixed, $\epsilon > 0$, we have $\mathscr{R} \subseteq \mathscr{R}(\sigma_h)$, where $\sigma_h = \frac{3}{4} + \epsilon$. Therefore, $\mathscr{R}(\sigma_h) - \mathscr{R}(\sigma) \supseteq \mathscr{R} - \mathscr{C}\mathfrak{m} = \mathfrak{m}$. Choose a sequence of positive numbers $\sigma = \sigma_0 < \sigma_1 < \ldots < \sigma_h$ so that

$$4(\sigma_j - \sigma_{j-1}) - \sigma_{j-1}/4 + \epsilon < 0 \quad \text{for} \quad 1 \leqslant j \leqslant h.$$

Such a choice of σ_j, $0 \leqslant j \leqslant h$, can clearly be made, where the number h is independent of P.

Now $$\mathscr{R}(\sigma_h) - \mathscr{R}(\sigma_0) = \bigcup_{1 \leqslant j \leqslant h} \{\mathscr{R}(\sigma_j) - \mathscr{R}(\sigma_{j-1})\},$$

where the union is meant in the sense of set theory. On the set $\mathscr{R}(\sigma_j) - \mathscr{R}(\sigma_{j-1})$, we have the estimate

$$|T(\alpha)| < P^{n(m-m\sigma_{j-1}/4+\epsilon)},$$

since we have assumed that Alternative (B) holds. The measure of $\mathscr{R}(\sigma_j) - \mathscr{R}(\sigma_{j-1})$ does not exceed the measure of $\mathscr{R}(\sigma_j)$, which is bounded by a constant factor times $P^{n(-3+4\sigma_j+\epsilon)}$ (cf. (6), p. 701, 1, 25). Therefore,

$$\left| \int_{\mathfrak{m}} T(\alpha)\, d\alpha \right| \ll \sum_{1 \leqslant j \leqslant h} P^{n(m-3-m\sigma_{j-1}/4+4\sigma_j+\epsilon)}$$
$$= o(P^{n(m-3)})$$

as $P \to \infty$, since $m \geqslant 17$ and since we have

$$-17\sigma_{j-1}/4 + 4\sigma_j + \epsilon < 0.$$

Q.E.D.

We now turn to the integral of $T(\alpha)$ over $\mathfrak{M}$, the major arcs. We will enlarge them from

$$\bigcup_{\substack{\gamma\,(\text{mod}\,\delta^{-1}) \\ N(a(\gamma)) \leqslant P^{2\theta}}} B(\gamma) \quad \text{to} \quad \bigcup_{\substack{\gamma\,(\text{mod}\,\delta^{-1}) \\ N(a(\gamma)) \leqslant P^{2\theta}}} \tilde{B}(\gamma),$$

where $$\tilde{B}(\gamma) = \{\alpha \in K_{\mathscr{R}} | \alpha - \gamma = \sum_{1 \leqslant i \leqslant n} \beta_i \rho_i,\ |\beta_i| < P^{-3+2\theta}\}. \tag{14}$$

This enlargement is justified since the contribution made by the increment to $\int T(\alpha) d\alpha$ is already covered by the estimate in Lemma 5·3.

In order to simplify notation, put

$$\tau = P^{\Delta}, \quad \Delta = 2\theta. \tag{15}$$

Henceforth, denote the enlarged major arcs by $\tilde{\mathfrak{M}}$. Note that the enlarged major arcs do not intersect; for if $\gamma \neq \gamma'$ and if $\tilde{\mathscr{B}}(\gamma) \cap \tilde{\mathscr{B}}(\gamma') \neq \phi$, then

$$\gamma - \gamma' = \sum_{1 \leqslant i \leqslant n} \gamma_i \rho_i, \quad |\gamma_i| < 2P^{-3+2\theta}.$$

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

Since $a(\gamma)\,a(\gamma')\,(\gamma-\gamma') \subset \delta^{-1}$, $N(a(\gamma))\,N(a(\gamma'))\,\gamma_i$ is a rational integer for each i; and since

$$\begin{aligned}|N(a(\gamma))\,N(a(\gamma'))\,\gamma_i| &\ll P^{-3+2\theta+4\theta}\\ &= P^{-3+6\theta}\\ &= P^{-3+\frac{3}{n+6}}\\ &< 1,\end{aligned}$$

$\gamma_i = 0$ for all i; and so $\gamma = \gamma'$.

LEMMA 5·4. $\sum\limits_{\substack{\gamma \,(\mathrm{mod}\,\delta^{-1})\\ a(\gamma)=a}} 1 \leqslant Na.$

Proof. $(\gamma)\,\delta = b(\gamma)/a(\gamma)$, where $(b(\gamma), a(\gamma)) = (1)$. So $(\gamma) = b(\gamma)\,\delta^{-1}/a(\gamma)$, and γ is in $(a\delta)^{-1}$. Therefore, the sum in the statement of the lemma does not exceed the number of γ in a complete residue system of $(a\delta)^{-1}$ modulo δ^{-1}, which is Na. Q.E.D.

We use $\sum\limits_{Z\,(\mathrm{mod}\,N)}$ to denote $\sum\limits_{Z_{ij}\,(\mathrm{mod}\,N)}$ for $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, where $Z = (Z_1, \ldots, Z_m)$ and $Z_i = \sum\limits_{1 \leqslant j \leqslant m} Z_{ij}\omega_j$. We also put $|\beta| < \tau$ in place of $|\beta_i| < \tau$ for $1 \leqslant i \leqslant n$, and $d\beta = d\beta_1 \ldots d\beta_n$.

LEMMA 5·5. $\int_{\mathfrak{M}} T(\alpha)\,d\alpha = \mathfrak{S}(\tau)\,J(\tau)\,P^{n(m-3)} + o(P^{n(m-3)})$

as $P \to \infty$, *where*

$$J(\tau) = \int_{|\beta|<\tau} \int_{\mathscr{B}} e(S(\beta C(\xi)))\,d\xi\,d\beta,$$

$$\mathfrak{S}(\tau) = \sum_{Na \leqslant \tau} \sum_{\substack{\gamma \,(\mathrm{mod}\,\delta^{-1})\\ a(\gamma)=a}} N^{-mn} S_\gamma,$$

and

$$N = N(a(\gamma)), \quad S_\gamma = \sum_{Z\,(\mathrm{mod}\,N)} e(S(\gamma C(Z))).$$

Proof. The contribution of the enlarged major arcs to $\int T(\alpha)\,d\alpha$ is

$$\sum_{Na \leqslant \tau} \sum_{\substack{\gamma \,(\mathrm{mod}\,\delta^{-1})\\ a(\gamma)=a}} \tilde{I}(\gamma),$$

where

$$\tilde{I}(\gamma) = \int_{\tilde{B}(\gamma)} T(\alpha)\,d\alpha.\dagger$$

For α in $\tilde{B}(\gamma)$, put $\alpha = \beta + \gamma$, where $\beta = \sum\limits_{1 \leqslant i \leqslant n} \beta_i \rho_i$, $|\beta_i| < P^{-3+\Delta}$. We have

$$\begin{aligned}T(\alpha) &= \sum_{X \in P\mathscr{B}} e(S(\alpha C(X)))\\ &= \sum_{Z\,(\mathrm{mod}\,N)} \sum_{Y} e(S((\beta+\gamma)\,C(NY+Z))),\end{aligned}$$

where $N = N(a(\gamma))$. Therefore,

$$T(\alpha) = \sum_{Z\,(\mathrm{mod}\,N)} e(S(\gamma C(Z))) \sum_{Y} e(S(\beta C(NY+Z))),$$

† Note that if $\gamma_1 \equiv \gamma_2 (\mathrm{mod}\,\delta^{-1})$, then $\tilde{I}(\gamma_1) = \tilde{I}(\gamma_2)$.

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

where the summation in Y is over integral points Y such that $NY+Z$ is in $P\mathscr{B}$. We now estimate the difference between

$$\sum_{Y} e(S(\beta C(NY+Z))) \quad \text{and} \quad \int_{\eta} e(S(\beta C(N\eta+Z)))\,d\eta$$

where the limits of integration on $\eta=(\eta_1,\ldots,\eta_n)$, $\eta_i=\sum_{1\leqslant j\leqslant n}\eta_{ij}\omega_j$, are such that $N\eta+Z\in P\mathscr{B}$.

Put $$h(\eta)=e(S(\beta C(N\eta+Z)))$$

(where the h here is not to be confused with the h used before). Clearly, $h(\eta)$ is an entire function of the variables η_{ij}, $1\leqslant i\leqslant m$, $1\leqslant j\leqslant n$. So if Y is a fixed point in $N^{-1}(P\mathscr{B}-Z)$ satisfying $$|Y-\eta|=\max_{\substack{1\leqslant i\leqslant m\\1\leqslant j\leqslant n}}|Y_{ij}-\eta_{ij}|\leqslant \tfrac{1}{2},$$

then we have the estimate

$$|h(Y)-h(\eta)|\ll \max_{\eta}\max_{\substack{1\leqslant i\leqslant m\\1\leqslant j\leqslant n}}\left|\frac{\partial h(\eta)}{\partial\eta_{ij}}\right|,$$

where the maximum over η is taken over all η such that $N\eta+Z\in P\mathscr{B}$. We thus obtain

$$\left|\sum_{Y}h(Y)-\int_{\eta}h(\eta)\,d\eta\right|\ll NP^{-3+\Delta}P^2(P/N)^{mn}+(P/N)^{mn-1},$$

where the second term on the right allows for the difference between the number of integral points in the box $N^{-1}(P\mathscr{B}-Z)$ and the volume of $N^{-1}(P\mathscr{B}-Z)$. Summing over the N^{mn} values of Z, we have

$$\begin{aligned}\left|T(\alpha)-\sum_{Z(\mathrm{mod}\,N)}e(S(\gamma C(Z)))\int_{\eta}h(\eta)\,d\eta\right|&\\ \ll NP^{-3+\Delta+2+mn}+NP^{mn-1}&\\ \ll P^{mn-1+2\Delta}.&\end{aligned}$$

The right-hand side of the above inequality, when integrated over $|\beta|<P^{-3+\Delta}$ and summed over $\gamma\,(\mathrm{mod}\,\delta^{-1})$, $N(a(\gamma))\leqslant P^{\Delta}$, gives a final error

$$\begin{aligned}&\ll \sum_{Na\leqslant\tau}\sum_{\substack{\gamma\,(\mathrm{mod}\,\delta^{-1})\\a(\gamma)=a}}P^{n(-3+\Delta)}P^{mn-1+2\Delta}\\ &\ll P^{n(m-3-1/n+(1+5/n)\Delta)}\dagger\\ &=o(P^{n(m-3)}),\end{aligned}$$

since $$\Delta=2\theta=1/(n+6).$$

The expression inside the modulus signs on the left-hand side of the same inequality, when summed and integrated over the same region as the right-hand side gives

$$\int_{\widetilde{\mathfrak{M}}}T(\alpha)\,d\alpha-U,$$

† Since, by Lemma 5·4, $\sum_{\substack{\gamma\,(\mathrm{mod}\,\delta^{-1})\\a(\gamma)=a}}\ll N$; and since the number of integral ideals in K which have a given norm N is $\ll N^{\epsilon}$ for all $\epsilon>0$.

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

where
$$U = \sum_{N\alpha \leqslant \tau} \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=a}} \int_{|\beta|<P^{-3+\Delta}} \sum_{Z \pmod N} e(S(\gamma C(Z))) \int h(\eta)\, d\eta\, d\beta \tag{16}$$

and hence
$$U = \mathfrak{S}(\tau) \int_{|\beta|<P^{-3+\Delta}} \int_{P\mathscr{B}} e(S(\beta C(\xi')))\, d\xi'\, d\beta, \tag{17}$$

where we have made the change of variables $\xi' = N\eta + Z$ in the interior integral of (16). Now let $\beta = \beta' P^{-3}$ and $\xi' = \xi'' P$ in (17). We obtain

$$\begin{aligned} U &= \mathfrak{S}(\tau)\, P^{n(m-3)} \int_{|\beta'|<\tau} \int_{\mathscr{B}} e(S(\beta' C(\xi')))\, d\xi''\, d\beta' \\ &= \mathfrak{S}(\tau)\, J(\tau)\, P^{n(m-3)}. \end{aligned}$$

Therefore,
$$\int_{\mathfrak{M}} T(\alpha)\, d\alpha = \mathfrak{S}(\tau)\, J(\tau)\, P^{n(m-3)} + o(P^{n(m-3)})$$

as $P \to \infty$. Q.E.D.

LEMMA 5·6. *With a suitable choice of the box $\mathscr{B}$, we have* $\lim_{\tau\to\infty} J(\tau) = J > 0$ *for any cubic form with coefficients in $\mathfrak{O}_K$ in more than* 16 *variables.*

Proof. See (6), pp. 697–698.

LEMMA 5·7. *Let $C(X)$ be a non-degenerate, cubic form in $m > 16$ variables with coefficients in $\mathfrak{O}_K$ which does not represent* 0 *non-trivially. Then we have for any $\epsilon > 0$, $|S_\gamma| \ll N^{mn-m/8+\epsilon}$.*

Proof. We apply Lemma 3·1 with $\alpha = \gamma$ and $\theta = 1/2n - \epsilon$. Since Alternative (A) has been excluded, the assumption that

$$\begin{aligned} |S_\gamma| &\geqslant N^{n(m-m\theta/4+\epsilon)} \\ &= N^{mn-m/8+\epsilon} \end{aligned}$$

implies that there is a non-zero μ in $N^{1/n-\epsilon}B_0$ and a ν in δ^{-1} such that

$$\mu\gamma - \nu = \sum_{1\leqslant i\leqslant n} \beta_i \rho_i,$$

and $|\beta_i| < N^{-3+1/n-\epsilon}$. Since $a(\gamma)\,(\mu\gamma - \nu)$ is in δ^{-1}, it follows that $\beta_i N(a(\gamma))$ is a rational integer for each i, $1 \leqslant i \leqslant n$. But

$$|\beta_i N| < N^{-2+1/n-\epsilon} < 1,$$

which implies that $\beta_i = 0$, $1 \leqslant i \leqslant n$. Therefore, μ is in $a(\gamma)$; and so $N(a(\gamma))$ divides $N(\mu)$. But $N(\mu) \ll N^{1-\epsilon}$, which implies for N sufficiently large that $N(\mu) = 0$, a contradiction. Therefore, we must have

$$|S_\gamma| \ll N^{mn-m/8+\epsilon} \quad \text{for all} \quad \epsilon > 0.\dagger$$ Q.E.D.

LEMMA 5·8. *If $C(X)$ satisfies the conditions of Lemma* 5·7, *then* $\lim_{\tau\to\infty} \mathfrak{S}(\tau)$ *exists and is positive.*

† Note that in Lemma 5·7 and Lemma 5·8 the same symbol ϵ has different values.

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press

Proof. By the definition of $\mathfrak{S}(\tau)$ in the statement of Lemma 5·5, we have

$$\mathfrak{S} = \lim_{\tau\to\infty} \mathfrak{S}(\tau) = \sum_{Na=1}^{\infty} \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=a}} N^{-mn} S_\gamma.$$

By Lemma 5·7,

$$\Big| \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ N(a(\gamma))=N}} N^{-mn}(a(\gamma))\, S_\gamma \Big| \ll N^{-mn} N^{mn-m/8+\epsilon} \sum_{\substack{\gamma \pmod{\delta^{-1}} \\ N(a(\gamma))=N}} 1 \tag{18}$$

$$\ll N^{-mn} N^{mn-m/8+\epsilon} N N^{\epsilon},$$

since $\sum_{\substack{\gamma \pmod{\delta^{-1}} \\ a(\gamma)=a}} \ll N$; and since the number of integral ideals in K which have a given norm N is $\ll N^{\epsilon}$ for all $\epsilon > 0$. Since $m > 16$, the right-hand side of (18) is equal to

$$N^{1+\epsilon-m/8} \leqslant N^{-1-u} \quad (u > 0).$$

Therefore, the sum defining $\mathfrak{S}$ is absolutely convergent. We can now conclude that $\mathfrak{S} > 0$ by (6), Lemma 3·5, p. 699. Q.E.D. Hence, if $m \geqslant 17$ and $C(X)$ does not represent 0 non-trivially, then by Lemmas 5·3, 5·5, 5·6, and 5·8, we have

$$\int_{\mathfrak{R}} T(\alpha)\, d\alpha = \mathfrak{S} J P^{n(m-3)} + o(P^{n(m-3)}),$$

as $P \to \infty$. Therefore, we conclude that $C(X)$ does represent 0 non-trivially. This proves the theorem.

REFERENCES

(1) Cassells, J. W. S. *An introduction to diophantine approximation* (Cambridge University Press, 1957).

(2) Davenport, H. Cubic forms in 32 variables. *Philos. Trans. Roy. Soc. London, Ser. A* **251** (1958), 193–232.

(3) Davenport, H. *Analytic methods for diphantine equations and inequalities* (Ann Arbor: Ann Arbor Publishers, 1962).

(4) Davenport, H. Cubic forms in 16 variables. *Proc. Roy. Soc. Ser. A* **272** (1963), 285–303.

(5) Lewis, D. J. Cubic forms over algebraic number fields. *Mathematika* **4** (1957), 97–101.

(6) Ramanujam, C. P. Cubic forms over algebraic number fields. *Proc. Cambridge Philos. Soc.* **59** (1963), 683–705.

(7) Tartakowski, W. Über Asymtotische Gesetze der 'Allgemeinen' Diophantischen Analyse mit vielen Unbekannten. *Bulletin of the Academy of Sciences, U.S.S.R.* (1935), 483–524.

https://doi.org/10.1017/S0305004100045011 Published online by Cambridge University Press