EUCLID'S ALGORITHM IN CERTAIN QUARTIC FIELDS

BY
H. DAVENPORT

1. **Introduction.** In a recent paper(1), I have proved that Euclid's algorithm is valid only in a finite number of cubic fields of negative discriminant. In the present paper, the same methods will be used to prove the analogous result for complex quartic fields whose conjugate fields are also complex. This exhausts the types of algebraic field which have exactly one fundamental unit, and so far I have not been able to extend my work to other types.

As in the quadratic and cubic cases, the result is proved in connection with another theorem, which relates to a more general situation. Let

$$x = au + bv + cw + dt, \qquad x' = a'u + b'v + c'w + d't \tag{1}$$

be two linear forms with complex coefficients, and let $\bar{x}$, $\bar{x}'$ be the complex conjugate forms. We suppose that the determinant Δ of the four forms x, $\bar{x}$, x', $\bar{x}'$ is not zero; since Δ is real, we may suppose without loss of generality that $\Delta>0$. Write

$$f(u, v, w, t) = x\bar{x}x'\bar{x}' = |\, xx' \,|^2. \tag{2}$$

The main theorem which will be proved is as follows.

THEOREM 1. *Suppose neither of the adjoint linear forms X, X', defined by* (11), *represents zero for integral values, not all zero, of the variables. Then there exist real numbers u^*, v^*, w^*, t^* such that*

$$f(u + u^*, v + v^*, w + w^*, t + t^*) > \kappa\Delta \tag{3}$$

for all integers u, v, w, t, where κ is a certain positive absolute constant.

By modifying and supplementing the proof of Theorem 1 in the light of the additional hypothesis, we then prove the following further result.

THEOREM 2. *Suppose the quaternary quartic form $f(u, v, w, t)$ has integral coefficients and does not represent zero for integral values, not all zero, of the variables. Then the numbers u^*, v^*, w^*, t^* of Theorem* 1 *can be so chosen as to be rational.*

This has an immediate application to the problem of the validity of Euclid's algorithm in quartic fields of the type already mentioned. Let K be

Presented to the Society, December 29, 1949; received by the editors August 16, 1949.

(1) *Euclid's algorithm in cubic fields of negative discriminant*, Acta Math (in course of publication). This paper will be referred to as I.

such a field, and a, b, c, d a basis for the algebraic integers(2) of the field. Then x represents the general algebraic integer of the field, and $\bar{x}$, x', $\bar{x}'$ are the algebraic conjugates of x. We have

$$f(u, v, w, t) = N(x), \tag{4}$$

where N denotes the norm. The hypotheses of Theorem 2 are satisfied. Let u^*, v^*, w^*, t^* be the rational numbers whose existence is asserted in Theorem 2, and write

$$-\lambda = u^*a + v^*b + w^*c + t^*d. \tag{5}$$

Then λ is a number of the field K, and (3) asserts that

$$N(x - \lambda) > \kappa\Delta \tag{6}$$

for all algebraic integers x of K. Now Δ^2, in the present case, is the discriminant of K. Thus Theorem 2 implies the following:

THEOREM 3. *Euclid's algorithm cannot hold in a complex quartic field, whose conjugate fields are also complex, if the discriminant of the field is greater than a certain absolute constant.*

Since, by a classical result(3), the number of quartic fields with bounded discriminants is finite, this shows that Euclid's algorithm is valid only in a finite number of quartic fields of the type under consideration.

The ideas of the paper are essentially the same as those of **I**, except for one new complication. This is the process which I have called "the first process of selection" (§5). The necessity for it arises from the fact that without this process of selection, the upper bound for $|2\Re(A_k b_k)|$ in Lemma 10 would be simply 1. This is not sufficiently precise for the later argument, and the new process of selection serves to improve the upper bound to $1-10^{-8}$.

As the notation is inevitably different from that of **I**, I have made the present paper independent of **I**. The only exception is Lemma 6, which is quoted from **I**. This, however, is a self-contained result of a non-arithmetical nature.

2. **Definitions and notation.** Let the cofactors of the elements $a, \cdots, \bar{d}'$ of the coefficient-matrix of the linear forms $x, \bar{x}, x', \bar{x}'$, after dividing each cofactor by Δ, be denoted by the corresponding capital letters $A, \cdots, \overline{D}'$. This is legitimate, since it is easily verified that (for example) A and $\overline{A}$ are in fact complex conjugates. We have the identities

$$Aa + \overline{A}\bar{a} + A'a' + \overline{A}'\bar{a}' = 1, \tag{7}$$

$$Ab + \overline{A}\bar{b} + A'b' + \overline{A}'\bar{b}' = 0, \tag{8}$$

$$Ac + \overline{A}\bar{c} + A'c' + \overline{A}'\bar{c}' = 0, \tag{9}$$

(2) The word *integer*, without the qualification *algebraic*, will always mean *rational integer*.

(3) See, for example, Minkowski, *Diophantische Approximationen*, Kap. 4, §5.

$$Ad + \overline{A}\bar{d} + A'd' + \overline{A}'\bar{d}' = 0. \tag{10}$$

Let X, X' be the linear forms, with complex coefficients, given by

$$X = AU + BV + CW + DT, \quad X' = A'U + B'V + C'W + D'T. \tag{11}$$

We have

$$\det(X, \overline{X}, X', \overline{X}') = \{\det(x, \bar{x}, x', \bar{x}')\}^{-1} = \Delta^{-1}. \tag{12}$$

The hypothesis of Theorem 1 asserts that $X \neq 0$ and $X' \neq 0$ for any integers U, V, W, T other than 0, 0, 0, 0.

We write also

$$X = Y + iZ, \qquad X' = Y' + iZ', \tag{13}$$

where Y, Z, Y', Z' are linear forms with real coefficients. Then

$$\det(Y, Z, Y', Z') = -\{\det(X, \overline{X}, X', \overline{X}')\}/4 = -(4\Delta)^{-1}. \tag{14}$$

3. **The quadratic forms** $Q(R; U, V, W, T)$. We consider the quadratic forms

$$\begin{aligned} Q(R; U, V, W, T) &= R^2 |X|^2 + R^{-2} |X'|^2 \\ &= R^2(Y^2 + Z^2) + R^{-2}(Y'^2 + Z'^2), \end{aligned} \tag{15}$$

where R takes all positive values. This form, for any R, is a positive definite quaternary quadratic form. Its determinant is independent of R, and is given by

$$\det Q = \{\det(Y, Z, Y', Z')\}^2 = (4\Delta)^{-2}, \tag{16}$$

by (14). The form $Q(R; U, V, W, T)$ has, for any R, a certain minimum, attained for integers U, V, W, T not all zero; we denote this minimum value by $\mathcal{A}(R)$. By a classical result of Korkine and Zolotareff(4), we have

$$\mathcal{A}(R) \leqq (4 \det Q)^{1/4} = (2\Delta)^{-1/2}. \tag{17}$$

The following two lemmas are due essentially to Hermite(5).

LEMMA 1. *There exist positive numbers*

$$\cdots < R_{-2} < R_{-1} < R_0 < R_1 < R_2 < \cdots$$

with the following properties. For every integer n there are integers U_n, V_n, W_n, T_n, not all zero, such that

$$Q(R; U_n, V_n, W_n, T_n) = \mathcal{A}(R) \qquad \text{for } R_n \leqq R \leqq R_{n+1}, \tag{18}$$

$$Q(R; U_n, V_n, W_n, T_n) > \mathcal{A}(R) \qquad \text{for } R < R_n \text{ and } R > R_{n+1}. \tag{19}$$

(4) See, for example, Bachmann, *Die Arithmetik der quadratischen Formen*, II, pp. 267–270.

(5) For a brief account of Hermite's theory, see Bachmann, loc. cit. Kap. 12.

Proof. For any positive number R_1 there are integers, say U_1, V_1, W_1, T_1, and corresponding values X_1, X_1' of the linear forms X, X', which provide the minimum of $Q(R_1)$, so that

$$R_1^2 \left| X_1 \right|^2 + R_1^{-2} \left| X_1' \right|^2 = \mathcal{A}(R_1).$$

Suppose that the same values also provide the minimum of $Q(R_2)$, where R_2 is some number greater than R_1, so that

$$R_2 \left|^2 X_1 \right|^2 + R_2^{-2} \left| X_1' \right|^2 = \mathcal{A}(R_2).$$

We prove that these same values then also provide the minimum of $Q(R)$ for all R satisfying $R_1 \leqq R \leqq R_2$. To establish this, we observe that

$$R_1^2 \left| X \right|^2 + R_1^{-2} \left| X' \right|^2 \geqq R_1^2 \left| X_1 \right|^2 + R_1^{-2} \left| X_1' \right|^2$$

and

$$R_2^2 \left| X \right|^2 + R_2^{-2} \left| X' \right|^2 \geqq R_2^2 \left| X_1 \right|^2 + R_2^{-2} \left| X_1' \right|^2$$

for all values of X and X' which arise from integral values, not all zero, of U, V, W, T. If $R_1 < R < R_2$, we can determine positive numbers μ_1 and μ_2 such that

$$R^2 = \mu_1 R_1^2 + \mu_2 R_2^2, \qquad R^{-2} = \mu_1 R_1^{-2} + \mu_2 R_2^{-2}.$$

Then it is plain that the above inequalities imply that

$$R^2 \left| X \right|^2 + R^{-2} \left| X' \right|^2 \geqq R^2 \left| X_1 \right|^2 + R^{-2} \left| X_1' \right|^2.$$

It follows that the number on the right is the minimum of $Q(R)$.

Since the sets of integers U, V, W, T are enumerable, the result just proved implies that all positive numbers R fall into an enumerable number of closed intervals, such that the minimum of $Q(R)$ throughout each interval is attained for the same integers U, V, W, T, and so for the same values of the linear forms X, X', and such that two sets of values which correspond to different intervals are themselves different.

These intervals have no point of accumulation, other than at 0 and ∞. For, by (17), the values of X and X' which provide the minimum of $Q(R)$ satisfy

$$R^2 \left| X \right|^2 + R^{-2} \left| X' \right|^2 \leqq (2\Delta)^{-1/2}. \tag{20}$$

If R and R^{-1} are both bounded above, then $\left|X\right|$ and $\left|X'\right|$ are both bounded, and so there are only a finite number of possible choices for the integers U, V, W, T, whence only a finite number of intervals in any such range of values of R.

It follows now that the intervals for R can be enumerated in increasing

order. We enumerate them as (R_n, R_{n+1}), ignoring any interval which consists of a single point. Here the suffix n must take all integral values, positive, negative, and zero. For it is impossible that the same U, V, W, T should provide the minimum of $Q(R)$ for arbitrarily large R, or for arbitrarily small R. This follows from (20); for if (20) were true for arbitrarily large R, we would have $X=0$, and if it were true for arbitrarily small R we would have $X'=0$, either of which contradicts the hypothesis that $X\neq 0$ and $X'\neq 0$ for any integers U, V, W, T not all zero .

If we denote the values of U, V, W, T which provide the minimum of $Q(R)$ for $R_n \leqq R \leqq R_{n+1}$ by U_n, V_n, W_n, T_n, the conclusions of the lemma follow.

LEMMA 2. *If X_n and X_n' denote the values of the linear forms X and X' which correspond to U_n, V_n, W_n, T_n, then for each integer n we have*

$$|X_{n+1}| < |X_n|, \tag{21}$$

$$|X'_{n+1}| > |X'_n|, \tag{22}$$

$$|X_n| \to 0 \quad \text{and} \quad |X'_n| \to \infty \qquad \text{as } n \to +\infty, \tag{23}$$

$$|X'_n| \to 0 \quad \text{and} \quad |X_n| \to \infty \qquad \text{as } n \to -\infty, \tag{24}$$

$$R^2|X_n|^2 + R^{-2}|X'_n|^2 = \mathcal{A}(R) \qquad \text{for } R_n \leqq R \leqq R_{n+1}, \tag{25}$$

$$R^2|X_n|^2 + R^{-2}|X'_n|^2 > \mathcal{A}(R) \qquad \text{for } R < R_n \text{ and for } R > R_{n+1}. \tag{26}$$

Proof. (25) and (26) are simply restatements of (18) and (19). We proceed to prove (23) and (24). By (25) with $R=R_n$, and by (17), we have

$$|X_n|^2 \leqq (2\Delta)^{-1/2} R_n^{-2}, \qquad |X'_n|^2 \leqq (2\Delta)^{-1/2} R_n^2.$$

As $n\to+\infty$, we have $R_n\to\infty$, whence $X_n\to 0$. Also $|X'_n|$ must tend to infinity as $n\to+\infty$, for the sets X_n, X'_n which correspond to different values of n are different, and there are only a finite number of sets for which both $|X_n|$ and $|X'_n|$ are bounded. This proves (23), and similarly for (24).

By (25) with $R=R_n$, we have

$$R_n^2|X_n|^2 + R_n^{-2}|X'_n|^2 = \mathcal{A}(R_n).$$

By (26), with $n+1$ in place of n, and $R=R_n$, we have

$$R_n^2|X_{n+1}|^2 + R_n^{-2}|X'_{n+1}|^2 > \mathcal{A}(R_n).$$

Hence

$$R_n^2(|X_n|^2 - |X_{n+1}|^2) < R_n^{-2}(|X'_{n+1}|^2 - |X'_n|^2).$$

But by (25) with n and $n+1$, and $R=R_{n+1}$, we have

$$R_{n+1}^2 |X_n|^2 + R_{n+1}^{-2} |X_n'|^2 = \mathcal{A}(R_{n+1}) = R_{n+1}^2 |X_{n+1}|^2 + R_{n+1}^{-2} |X_{n+1}'|^2.$$

Hence

$$R_n^4(|X_n|^2 - |X_{n+1}|^2) < |X_{n+1}'|^2 - |X_n'|^2 = R_{n+1}^4(|X_n|^2 - |X_{n+1}|^2).$$

Since $R_{n+1} > R_n$, this proves (21) and (22). All the results are now established.

4. **A property of the numbers R_n.**

LEMMA 3. *Let l be an integer greater than 2. The inequality*

$$(R_{n+1}/R_n)^{32l^4} < l/2 \tag{27}$$

cannot hold for $(2l)^4$ consecutive values of n.

Proof. Write $k = (2l)^4$. Suppose that (27) holds for k consecutive values of n; without loss of generality we can take these values to be $0, 1, \cdots, k-1$. We have then, in particular, by (27),

$$R_0 \leqq R_n < (l/2)^{1/2} R_0 \qquad \text{for } n = 0, 1, \cdots, k. \tag{28}$$

By two cases of (25), we have

$$\mathcal{A}(R_n) = R_n^2 |X_n|^2 + R_n^{-2} |X_n'|^2,$$
$$\mathcal{A}(R_{n+1}) = R_{n+1}^2 |X_n|^2 + R_{n+1}^{-2} |X_n'|^2.$$

Since $R_{n+1} > R_n$, we obtain by division

$$\mathcal{A}(R_{n+1})/\mathcal{A}(R_n) < (R_{n+1}/R_n)^2 < (l/2)^{1/k},$$

for $n = 0, 1, \cdots, k-1$. Hence

$$\mathcal{A}(R_n) < (l/2)\mathcal{A}(R_0) \qquad \text{for } n = 0, 1, \cdots, k. \tag{29}$$

We now write, as in (13), $X_n = Y_n + iZ_n$, $X_n' = Y_n' + iZ_n'$, and obtain upper bounds for $|Y_n|$, $|Z_n|$, $|Y_n'|$, $|Z_n'|$, valid for $n = 0, 1, \cdots, k$. By (25) with $R = R_n$, we have

$$|X_n| \leqq R_n^{-1} \mathcal{A}^{1/2}(R_n) < (l/2)^{1/2} R_0^{-1} \mathcal{A}^{1/2}(R_0),$$
$$|X_n'| \leqq R_n \mathcal{A}^{1/2}(R_n) < (l/2) R_0 \mathcal{A}^{1/2}(R_0).$$

Hence

$$|Y_n|, |Z_n| < (l/2) R_0^{-1} \mathcal{A}^{1/2}(R_0), \quad |Y_n'|, |Z_n'| < (l/2) R_0 \mathcal{A}^{1/2}(R_0). \tag{30}$$

These inequalities are valid for $n = 0, 1, \cdots, k$. We apply the familiar principle of Dirichlet ($k+1$ objects in k compartments). The four-dimensional region represented by the inequalities (30) can be divided into $k = (2l)^4$ compartments, the compartments being obtained by dividing each of the ranges

for Y_n, Z_n, Y_n', Z_n' in (30) into $2l$ equal parts. There must be two different suffixes, say n and m, in the set $0, 1, \cdots, k$ for which the points (Y_n, Z_n, Y_n', Z_n'), (Y_m, Z_m, Y_m', Z_m') lie in the same compartment. This implies that

$$\begin{aligned} &|Y_n - Y_m|, |Z_n - Z_m| < R_0^{-1}\mathcal{A}^{1/2}(R_0)/2, \\ &|Y_n' - Y_m'|, |Z_n' - Z_m'| < R_0\mathcal{A}^{1/2}(R_0)/2. \end{aligned} \tag{31}$$

The numbers $Y_n - Y_m$, $Z_n - Z_m$, $Y_n' - Y_m'$, $Z_n' - Z_m'$ are values of the linear forms Y, Z, Y', Z' which arise from integral values, not all zero, of the variables U, V, W, T. By (31), they satisfy

$$R_0^2(Y^2 + Z^2) + R_0^{-2}(Y'^2 + Z'^2) < \mathcal{A}(R_0),$$

which contradicts the definition of $\mathcal{A}(R_0)$ as the minimum of the quadratic form on the left. This contradiction proves the lemma.

COROLLARY. *The inequality*

$$(R_{n+1}/R_n)^{2592} < 3/2 \tag{32}$$

cannot hold for 1296 *consecutive values of* n.

This is the case $l = 3$ of Lemma 3.

LEMMA 4. *Let* n *be any integer for which*

$$(R_{n+1}/R_n)^{2592} \geqq 3/2. \tag{33}$$

Then there is a number R *satisfying* $R_n \leqq R \leqq R_{n+1}$ *for which*

$$2|X_nX_n'| < (1 - 10^{-8})\mathcal{A}(R). \tag{34}$$

Proof. Suppose $R_n \leqq R \leqq R_{n+1}$. By (25),

$$\mathcal{A}(R)/|X_nX_n'| = R^2|X_n/X_n'| + R^{-2}|X_n'/X_n| = H + H^{-1},$$

say. As R varies in the interval $R_n \leqq R \leqq R_{n+1}$, the number H varies in some interval $H_0 \leqq H \leqq H_1$, where $0 < H_0 < H_1$ and

$$H_1/H_0 \geqq (3/2)^{2/2592},$$

by (33). In any such interval there is a number H for which

$$H + H^{-1} \geqq (3/2)^{1/2592} + (2/3)^{1/2592} > 2 + 2.2 \times 10^{-8}.$$

For the corresponding value of R, we have

$$2|X_n X_n'| < (1 + 1.1 \times 10^{-8})^{-1}\mathcal{A}(R) < (1 - 10^{-8})\mathcal{A}(R).$$

5. **The first process of selection.** We select all integers n for which (33) holds, and enumerate them as

$$\cdots < n_{-1} < n_0 < n_1 < \cdots .$$

This series of numbers does not terminate in either direction, by the corollary to Lemma 3. We denote X_{n_m} by $X_{(m)}$, and X'_{n_m} by $X'_{(m)}$. We denote the number R satisfying $R_{n_m} \leqq R \leqq R_{n_m+1}$, whose existence for every m is asserted in Lemma 4, by $R_{(m)}$. Then, by (34),

$$2\,|\,X_{(m)}X'_{(m)}\,| < (1 - 10^{-8})\mathcal{A}(R_{(m)}) \tag{35}$$

for every integer m.

LEMMA 5. *We have, for every integer m,*

$$|\,X_{(m+1)}\,| < |\,X_{(m)}\,|, \tag{36}$$

$$|\,X'_{(m+1)}\,| > |\,X'_{(m)}\,|, \tag{37}$$

$$R^2_{(m)}\,|\,X_{(m)}\,|^2 + R^{-2}_{(m)}\,|\,X'_{(m)}\,|^2 = \mathcal{A}(R_{(m)}), \tag{38}$$

$$|\,X_{(m)}X'_{(m+1)}\,| < \Delta^{-1/2}. \tag{39}$$

Also

$$|\,X_{(m)}\,| \to 0 \quad \textit{and} \quad |\,X'_{(m)}\,| \to \infty \qquad \textit{as } m \to +\infty, \tag{40}$$

$$|\,X'_{(m)}\,| \to 0 \quad \textit{and} \quad |\,X_{(m)}\,| \to \infty \qquad \textit{as } m \to -\infty. \tag{41}$$

Proof. As the new values of X and X' are a selection from the old values, (36) and (37) follow at once from (21) and (22), and (40) and (41) from (23) and (24). Also (38) is a particular case of (25). The only result which still requires proof is (39).

There are two cases to be considered. Suppose first that the two selected intervals which correspond to m and $m+1$ were consecutive intervals of the original system, so that $n_{m+1} = n_m + 1$. Write, for brevity, $n_m = \nu$. Then $X_{(m)} = X_\nu$ and $X_{(m+1)} = X_{\nu+1}$, and similarly with accents. By two cases of (25), we have

$$R^2_{\nu+1}\,|\,X_\nu\,|^2 + R^{-2}_{\nu+1}\,|\,X'_\nu\,|^2 = R^2_{\nu+1}\,|\,X_{\nu+1}\,|^2 + R^{-2}_{\nu+1}\,|\,X'_{\nu+1}\,|^2 = \mathcal{A}(R_{\nu+1}).$$

Hence

$$|\,X_\nu\,|^2 \leqq R^{-2}_{\nu+1}\mathcal{A}(R_{\nu+1}), \qquad |\,X'_{\nu+1}\,|^2 \leqq R^2_{\nu+1}\mathcal{A}(R_{\nu+1}),$$

whence

$$|\,X_\nu X'_{\nu+1}\,| \leqq \mathcal{A}(R_{\nu+1}) \leqq (2\Delta)^{-1/2}$$

by (17). This proves (39) in the present case.

Now suppose there is a gap between the two selected intervals, so that $n_{m+1} > n_m + 1$. By the method of selection, (32) holds for every n satisfying $n_m + 1 \leqq n < n_{m+1}$. Also, by the Corollary to Lemma 3, we have $n_{m+1} - n_m$

$\leqq 1296$. We write, for brevity, $\nu = n_m$ and $\mu = n_{m+1}$. Then, by multiplying together the inequalities (32) for the values of n just specified, we obtain

$$R_\mu / R_{\nu+1} < (3/2)^{1296/2592} = (3/2)^{1/2}. \tag{42}$$

From two cases of (25), we have

$$|X_\nu|^2 \leqq R_{\nu+1}^{-2}\mathcal{A}(R_{\nu+1}), \qquad |X'_\mu|^2 \leqq R_\mu^2 \mathcal{A}(R_\mu).$$

Using (42) and (17), it follows that

$$|X_\nu X'_\mu|^2 \leqq (R_\mu/R_{\nu+1})^2 \mathcal{A}(R_{\nu+1})\mathcal{A}(R_\mu) < (3/2)(2\Delta)^{-1} < \Delta^{-1}.$$

Since $X_{(m)} = X_\nu$ and $X'_{(m+1)} = X'_\mu$, this proves (39).

6. **The second and third processes of selection.**

LEMMA 6. *Let $T(m)$ be any function of m, defined for every integer m, which has the following properties:*

$$T(m+1) > T(m) \qquad \text{for every } m, \tag{43}$$

$$T(m) \to 0 \qquad \text{as } m \to -\infty, \tag{44}$$

$$T(m) \to \infty \qquad \text{as } m \to +\infty. \tag{45}$$

Let G be a given number, greater than 1. Then there exist integers

$$\cdots < m_{-1} < m_0 < m_1 < \cdots,$$

the sequence continuing to infinity in both directions, such that

$$GT(m_k) \leqq T(m_{k+1}) < G^2 T(m_k + 1) \tag{46}$$

for every integer k.

Proof. This is Lemma 3 of I.

LEMMA 7. *There exist sets of values Ξ_j, Ξ'_j of the complex linear forms X, X', each set arising from integral values, not all zero, of the variables U, V, W, T, with the following properties. First, a set exists for every integer j, positive, negative or zero. Secondly, for every integer j there is a positive number P_j such that*

$$\mathrm{P}_j^2 |\Xi_j|^2 + \mathrm{P}_j^{-2} |\Xi'_j|^2 = \mathcal{A}(\mathrm{P}_j), \tag{47}$$

and

$$2|\Xi_j \Xi'_j| < (1 - 10^{-8})\mathcal{A}(\mathrm{P}_j). \tag{48}$$

Also, for every j,

$$|\Xi_{j+1}| < |\Xi_j|, \tag{49}$$

$$|\Xi'_{j+1}| \geqq G|\Xi'_j|, \tag{50}$$

$$|\Xi_j \Xi'_{j+1}| < G^2 \Delta^{-1/2}. \tag{51}$$

Finally

$$|\Xi_j| \to 0 \text{ as } j \to +\infty \text{ and } \to \infty \text{ as } j \to -\infty. \tag{52}$$

Proof. With the notation introduced at the beginning of the preceding section, we define $T(m)$ by

$$T(m) = |X'_{(m)}|. \tag{53}$$

The hypotheses of Lemma 6 are satisfied, by (37), (40), (41). By that lemma, there exist integers $\cdots < m_{-1} < m_0 < m_1 < \cdots$ such that

$$GT(m_j) \leqq T(m_{j+1}) < G^2 T(m_j + 1) \tag{54}$$

for all j. We define Ξ_j, Ξ'_j by

$$\Xi_j = X_{(m_j)}, \qquad \Xi'_j = X'_{(m_j)}. \tag{55}$$

These are values of the linear forms X, X' which arise from integral values, not all zero, of U, V, W, T. Taking $\mathbf{P}_j$ to be $R_{(m_j)}$, the conclusions (47) and (48) follow from (38) and (35). The conclusions (49), (52) are obvious from (36), (40), (41). Also (50) follows from (53), (55), and the first half of (54). Finally, (51) follows from (39) with $m = m_j$, on using (53), (55), and the second half of (54).

LEMMA 8. *There exist sets of values A_k, A'_k of the complex linear forms X, X', each set arising from integral values, not all zero, of the variables U, V, W, T, with the following properties. First, a set exists for every integer k, positive, negative, or zero. Secondly, for every integer k there is a positive number S_k such that*

$$S_k^2 |A_k|^2 + S_k^{-2} |A'_k|^2 = \mathcal{A}(S_k), \tag{56}$$

$$2|A_k A'_k| < (1 - 10^{-8})\mathcal{A}(S_k). \tag{57}$$

Also, for every integer k,

$$|A_{k+1}| \leqq G^{-1} |A_k|, \tag{58}$$

$$|A'_{k+1}| \geqq G |A'_k|, \tag{59}$$

$$|A_k A'_{k+1}| < G^4 \Delta^{-1/2}. \tag{60}$$

Proof. Using the notation of Lemma 7, we define a new function $T(m)$ by

$$T(-j) = |\Xi_j|. \tag{61}$$

The hypotheses of Lemma 6 are satisfied for this function, by (49) and (52). Hence there exist integers $\cdots < j_{-1} < j_0 < j_1 < \cdots$ such that

$$GT(j_k) \leqq T(j_{k+1}) < G^2 T(j_k + 1)$$

for all k. We write $-j_k = J_{-k}$; the last assertion, with k changed into $-k$, tells

us that

$$GT(-J_k) \leqq T(-J_{k-1}) < G^2T(-J_k+1) \tag{62}$$

for all k. We define A_k, A_k' by

$$A_k = \Xi_{J_k}, \qquad A_k' = \Xi'_{J_k}. \tag{63}$$

These are values of the linear forms X, X' which arise from integral values, not all zero, of U, V, W, T. Taking S_k to be $\mathbf{P}_{J_k}$, the conclusions (56) and (57) are immediate from (47) and (48). Also (59) follows from (50), since the new values are a subset of the old. Further, the first half of (62), using (61) and (63), implies (58) with $k-1$ in place of k. Finally, (60) follows from (51) with $j=J_{k+1}-1$, on using the second half of (62) with k replaced by $k+1$, and (61) and (63).

7. **A lemma on quadratic forms.**

LEMMA 9. *Let $Q(U, V, W, T)$ be a positive definite quadratic form in four variables. Let $\mathcal{A}$ be the minimum of Q and let U_0, V_0, W_0, T_0 be any set of integers for which the minimum is attained. Then there exists a linear substitution, with integral coefficients and determinant* 1, *which transforms U_0, V_0, W_0, T_0 into* 1, 0, 0, 0, *and which transforms Q into a form*

$$\mathcal{A}U^2 + \mathcal{B}V^2 + \mathcal{C}W^2 + \mathcal{D}T^2 + \cdots \tag{64}$$

for which

$$\mathcal{A} \leqq \mathcal{B} \leqq \mathcal{C} \leqq \mathcal{D}, \tag{65}$$

$$\mathcal{A}\mathcal{B}\mathcal{C}\mathcal{D} \leqq 4 \det Q. \tag{66}$$

Proof. See K. Mahler, Nieuw. Archief voor Wiskunde (1946) pp. 207–212. Mahler establishes the inequality (66) for any form which is *reduced* in the sense of Minkowski. It is immediate from Minkowski's definition of reduction that the substitution by which the reduction is achieved can be so chosen that any set of integral values for which the minimum is attained shall be transformed into the values 1, 0, 0, 0 of the new variables.

It should, perhaps, be pointed out that in Minkowski's definition, substitutions of determinant ± 1 are admitted. But as we are concerned here only with the leading coefficients $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, we can restrict ourselves to substitutions of determinant 1.

It is an interesting fact that Mahler's proof of (66), which is based on an idea of Minkowski, deduces it from the inequality (17), which is itself a particular consequence of (65) and (66).

8. **The unimodular substitutions.** The quadratic form

$$Q(S_k; U, V, W, T) = S_k^2 |X|^2 + S_k^{-2} |X'|^2 \tag{67}$$

has minimum $\mathcal{A}(S_k)$, and by Lemma 8 this minimum is attained when X, X'

have the values A_k, A_k'. By Lemma 9, there is a linear substitution $\mathfrak{T}_k$, with integral coefficients and determinant 1, which transforms the above form into one whose leading coefficients, say $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, $\mathcal{D}_k$, satisfy

$$\mathcal{A}_k = \mathcal{A}(S_k), \qquad \mathcal{A}_k \leqq \mathcal{B}_k \leqq \mathcal{C}_k \leqq \mathcal{D}_k, \tag{68}$$

$$\mathcal{A}_k\mathcal{B}_k\mathcal{C}_k\mathcal{D}_k \leqq 4 \det Q = (2\Delta)^{-2}. \tag{69}$$

Moreover, we can suppose the substitution so chosen that when the new variables are 1, 0, 0, 0 the values of X, X' are A_k, A_k'.

Let the linear forms X, X', after transformation by $\mathfrak{T}_k$, become

$$X = A_kU + B_kV + C_kW + D_kT, \quad X' = A_k'U + B_k'V + C_k'W + D_k'T. \tag{70}$$

Comparing coefficients in the transformed quadratic form, we have

$$S_k^2 \left| A_k \right|^2 + S_k^{-2} \left| A_k' \right|^2 = \mathcal{A}_k, \tag{71}$$

and similarly with A, $\mathcal{A}$ replaced by B, $\mathcal{B}$ or C, $\mathcal{C}$ or D, $\mathcal{D}$. We note that none of $A_k, \cdots, D_k'$ can be zero, since they are values of the linear forms X, X'.

The next step is to define $a_k, \cdots, \bar{d}_k'$ for all k, in such a way that they bear the same relation to $A_k, \cdots, \overline{D}_k'$ as was true for the original symbols without suffixes. This is attained by defining them as the cofactors of the corresponding elements of the coefficient-matrix of the four linear forms X, $\overline{X}$, X', $\overline{X}'$, as given in (70), each cofactor multiplied by Δ. We observe that the determinant of that coefficient-matrix is Δ^{-1}, since the substitution $\mathfrak{T}_k$ has determinant 1. The identities (7), (8), (9), (10) remain valid if the suffix k is added throughout.

It is important to note that there exists, for every k, a linear substitution, with integral coefficients and determinant 1 which transforms the linear forms x, x' into $a_ku + b_kv + c_kw + d_kt$, $a_k'u + b_k'v + c_k'w + d_k't$. This is the contragredient substitution to $\mathfrak{T}_k$.

9. **Inequalities for A_kb_k, and so on.**

LEMMA 10. *For every integer k, we have*

$$\left| 2\Re(A_kb_k) \right| < 1 - 10^{-8}, \tag{72}$$

and the same inequality holds if b_k is replaced by c_k or d_k.

Proof. For brevity of writing, we omit the suffix k for the time being, and then have

$$b = -\Delta \begin{vmatrix} \overline{A}, & \overline{C}, & \overline{D} \\ A', & C', & D' \\ \overline{A}', & \overline{C}', & \overline{D}' \end{vmatrix}.$$

We write, temporarily,

$$(73)\qquad \begin{aligned} A &= \Upsilon + iZ, & C &= \Upsilon_c + iZ_c, & D &= \Upsilon_d + iZ_d, \\ A' &= \Upsilon' + iZ', & C' &= \Upsilon_c' + iZ_c', & D' &= \Upsilon_d' + iZ_d'. \end{aligned}$$

From the above determinant, we have

$$\begin{aligned} -\Delta^{-1}b &= \begin{vmatrix} \Upsilon - iZ, & \Upsilon_c - iZ_c, & \Upsilon_d - iZ_d \\ \Upsilon' + iZ', & \Upsilon_c' + iZ_c', & \Upsilon_d' + iZ_d' \\ \Upsilon' - iZ', & \Upsilon_c' - iZ_c', & \Upsilon_d' - iZ_d' \end{vmatrix} \\ &= 2i\{(\Upsilon - iZ)(\Upsilon_d'Z_c' - \Upsilon_c'Z_d') + (\Upsilon_c - iZ_c)(\Upsilon'Z_d' - \Upsilon_d'Z') \\ &\qquad + (\Upsilon_d - iZ_d)(\Upsilon_c'Z' - \Upsilon'Z_c')\}. \end{aligned}$$

Multiplying by $A = \Upsilon + iZ$, and taking the real part, we obtain

$$\begin{aligned} \Delta^{-1}\Re(Ab) &= 2(\Upsilon Z_c - \Upsilon_c Z)(\Upsilon_d'Z' - \Upsilon'Z_d') \\ &\quad + 2(\Upsilon Z_d - \Upsilon_d Z)(\Upsilon'Z_c - \Upsilon_c'Z'). \end{aligned}$$

Now

$$(\Upsilon Z_c - \Upsilon_c Z)^2 \leqq (\Upsilon^2 + Z^2)(\Upsilon_c^2 + Z_c^2) = |AC|^2,$$

by (73). A similar result holds for the other expressions. Hence

$$\Delta^{-1}|\Re(Ab)| \leqq 2|ACA'D'| + 2|ADA'C'|.$$

We can now restore the suffix k without risk of confusion. The inequality (57) tells us that

$$2|A_kA_k'| < (1 - 10^{-8})\mathcal{A}_k.$$

Also we have

$$\begin{aligned} (|C_kD_k'| + |C_k'D_k|)^2 &\leqq (S_k^2|C_k|^2 + S_k^{-2}|C_k'|^2)(S_k^2|D_k|^2 + S_k^{-2}|D_k'|^2) \\ &= \mathcal{C}_k\mathcal{D}_k, \end{aligned}$$

by the analogues of (71). Hence

$$\Delta^{-1}|\Re(A_kb_k)| \leqq (1 - 10^{-8})\mathcal{A}_k(\mathcal{C}_k\mathcal{D}_k)^{1/2} \leqq (1 - 10^{-8})(2\Delta)^{-1},$$

by (68) and (69). This proves (72), and the results with c_k, d_k are proved in exactly the same way.

LEMMA 11. *For every integer k, we have*

$$(74)\qquad |A_kb_k| \leqq 3, \qquad |A_k'b_k'| \leqq 3,$$

and the same inequalities hold if b is replaced by c or d.

Proof. These inequalities, in which the precise constant is not important, can be proved with less attention to detail than was needed in the previous

lemma. We have, by the determinantal definition of b_k,

$$|b_k| \leqq \Delta\{|A_kC_k'D_k'| + |C_kD_k'A_k'| + |D_kA_k'C_k'| + |A_kD_k'C_k'| + |C_kA_k'D_k'| + |D_kC_k'A_k'|\}.$$

By (71),

$$|A_k| \leqq S_k^{-1}\mathcal{A}_k^{1/2}, \qquad |A_k'| \leqq S_k\mathcal{A}_k^{1/2},$$

and similarly for C_k, D_k, C_k', D_k'. Hence

$$|A_kb_k| \leqq 6\Delta\mathcal{A}_k(\mathcal{C}_k\mathcal{D}_k)^{1/2} \leqq 6\Delta(2\Delta)^{-1} = 3.$$

A similar proof holds for $|A_k'b_k'|$, and also when b is replaced by c or d.

10. **The integers p_k, q_k, r_k.**

LEMMA 12. *Let β, γ, δ, $\beta^{(1)}$, $\gamma^{(1)}$, $\delta^{(1)}$, $\beta^{(2)}$, $\gamma^{(2)}$, $\delta^{(2)}$ be real numbers satisfying*

$$\det(\beta, \gamma, \delta) \neq 0, \tag{75}$$

$$|\beta|, |\gamma|, |\delta| < 1 - 10^{-8}, \tag{76}$$

$$|\beta^{(i)}|, |\gamma^{(i)}|, |\delta^{(i)}| \leqq 3 \qquad \text{for } i = 1, 2. \tag{77}$$

Then there exist integers p, q, r such that

$$10^{-1} < p\beta + q\gamma + r\delta < 1 - 10^{-8}, \tag{78}$$

$$|p\beta^{(i)} + q\gamma^{(i)} + r\delta^{(i)}| \leqq 3 \qquad \text{for } i = 1, 2. \tag{79}$$

Proof. Suppose first that one at least of β, γ, δ is numerically greater than 10^{-1}, say $|\beta| > 10^{-1}$. Then we take $q=0$, $r=0$, and $p = \pm 1$, so that $p\beta = |\beta|$. We then have

$$10^{-1} < p\beta < 1 - 10^{-8},$$

and consequently (78) is satisfied. Also (79) is obviously satisfied.

There remains the case in which

$$|\beta|, |\gamma|, |\delta| \leqq 10^{-1}. \tag{80}$$

Write

$$L = \gamma^{(1)}\delta^{(2)} - \gamma^{(2)}\delta^{(1)}, \qquad M = \delta^{(1)}\beta^{(2)} - \delta^{(2)}\beta^{(1)}, \qquad N = \beta^{(1)}\gamma^{(2)} - \beta^{(2)}\gamma^{(1)}.$$

Let P denote the determinant in (75), so that

$$\beta L + \gamma M + \delta N = P, \qquad \beta^{(i)}L + \gamma^{(i)}M + \delta^{(i)}N = 0 \qquad (i = 1, 2). \tag{81}$$

We may suppose, without loss of generality, that

$$|L| \geqq |M|, \qquad |L| \geqq |N|. \tag{82}$$

Then $|L| > 0$, since $P \neq 0$ by (75).

For any integer p, we can determine integers q and r such that

$$q = ML^{-1}p + \theta, \qquad r = NL^{-1}p + \phi,$$

where $|\theta| \leqq 1/2$, $|\phi| \leqq 1/2$. We then have, for any choice of p,

$$\begin{aligned} p\beta^{(i)} + q\gamma^{(i)} + r\delta^{(i)} &= p(\beta^{(i)} + ML^{-1}\gamma^{(i)} + NL^{-1}\delta^{(i)}) + \gamma^{(i)}\theta + \delta^{(i)}\phi \\ &= \gamma^{(i)}\theta + \delta^{(i)}\phi, \end{aligned}$$

by (81), where i is 1 or 2. Hence (79) is satisfied. It remains to choose p so that (78) holds.

We have

$$p\beta + q\gamma + r\delta = p(\beta + ML^{-1}\gamma + NL^{-1}\delta) + \gamma\theta + \delta\phi = PL^{-1}p + 10^{-1}\theta'$$

by (80) and (81), where $|\theta'| < 1$. Hence (78) will certainly hold if

$$10^{-1} + 10^{-1} < PL^{-1}p < 1 - 10^{-8} - 10^{-1}.$$

Subtracting the two sides, we see that an integer p satisfying this requirement will certainly exist if

$$0 < |PL^{-1}| < 0.7 - 10^{-8}.$$

Now $P \neq 0$ by (75) and, by (80), (81), (82),

$$|PL^{-1}| = |\beta + ML^{-1}\gamma + NL^{-1}\delta| \leqq |\beta| + |\gamma| + |\delta| \leqq 0.3.$$

LEMMA 13. *There exist, for every integer k, integers p_k, q_k, r_k such that*

$$\begin{aligned} 10^{-1} < p_k(A_k b_k + \overline{A}_k \bar{b}_k) + q_k(A_k c_k + \overline{A}_k \bar{c}_k) + r_k(A_k d_k + \overline{A}_k \bar{d}_k) \\ < 1 - 10^{-8}, \end{aligned} \tag{83}$$

$$|A_k(p_k b_k + q_k c_k + r_k d_k)| < 4, \tag{84}$$

$$|A_k'(p_k b_k' + q_k c_k' + r_k d_k')| < 4. \tag{85}$$

Proof. Since

$$A_k b_k + \overline{A}_k \bar{b}_k + A_k' b_k' + \overline{A}_k' \bar{b}_k' = 0, \tag{86}$$

we can write

$$2A_k b_k = \beta_k + 2i\beta_k^{(1)}, \qquad 2A_k' b_k' = -\beta_k + 2i\beta_k^{(2)}, \tag{87}$$

where β_k, $\beta_k^{(1)}$, $\beta_k^{(2)}$ are real. We use a similar notation with c_k and γ_k, and with d_k and δ_k. By Lemma 10,

$$|\beta_k|, |\gamma_k|, |\delta_k| < 1 - 10^{-8}.$$

Also, by Lemma 11,

$$|\beta_k^{(1)}| \leqq |A_k b_k| \leqq 3,$$

and similarly for $\gamma_k^{(1)}, \cdots, \delta_k^{(2)}$. Hence the hypotheses (76) and (77) of Lemma 12 are satisfied by these numbers.

As regards the hypothesis (75), we have

$$\begin{vmatrix} \beta_k, & \gamma_k, & \delta_k \\ \beta_k^{(1)}, & \gamma_k^{(1)}, & \delta_k^{(1)} \\ \beta_k^{(2)}, & \gamma_k^{(2)}, & \delta_k^{(2)} \end{vmatrix} = \begin{vmatrix} A_k b_k + \overline{A}_k \bar{b}_k, & \cdots \\ (A_k b_k - \overline{A}_k \bar{b}_k)/(2i), & \cdots \\ (A_k' b_k' - \overline{A}_k' \bar{b}_k')/(2i), & \cdots \end{vmatrix}$$

$$= - \begin{vmatrix} \overline{A}_k \bar{b}_k, & \overline{A}_k \bar{c}_k, & \overline{A}_k \bar{d}_k \\ A_k' b_k', & A_k' c_k', & A_k' d_k' \\ \overline{A}_k' \bar{b}_k', & \overline{A}_k' \bar{c}_k', & \overline{A}_k' \bar{d}_k' \end{vmatrix},$$

on using (86). The last expression is

$$- (\overline{A}_k A_k' \overline{A}_k')(\Delta A_k) = - \Delta \mid A_k A_k' \mid^2 \neq 0.$$

It follows from Lemma 12 that there exist integers p, q, r which satisfy (78), (79), with the suffix k throughout. Now (83) is simply a restatement of (78), and (84) follows from

$$\begin{aligned} 2 \mid A_k(p_k b_k + q_k c_k + r_k d_k) \mid &\leqq \mid p_k \beta_k + q_k \gamma_k + r_k \delta_k \mid \\ &\quad + 2 \mid p_k \beta_k^{(1)} + q_k \gamma_k^{(1)} + r_k \delta_k^{(1)} \mid \\ &< (1 - 10^{-8}) + 6 < 8, \end{aligned}$$

using (87), (78), (79). A similar proof holds for (85).

11. **The numbers λ_k, λ_k'.**

For any integer k we define complex numbers λ_k, λ_k' by

$$\lambda_k = \sum_{\nu=-\infty}^{k} (p_\nu b_\nu + q_\nu c_\nu + r_\nu d_\nu), \tag{88}$$

$$-\lambda_k' = \sum_{\nu=k+1}^{\infty} (p_\nu b_\nu' + q_\nu c_\nu' + r_\nu d_\nu'). \tag{89}$$

These series are absolutely convergent. For

$$\mid p_\nu b_\nu + q_\nu c_\nu + r_\nu d_\nu \mid < 4 \mid A_\nu \mid^{-1}, \tag{90}$$

and similarly with accents, by (84) and (85); and

$$\mid A_{\nu-1}/A_\nu \mid \geqq G, \qquad \mid A_\nu'/A_{\nu-1}' \mid \geqq G \tag{91}$$

by (58) and (59), where $G > 1$.

LEMMA 14. *λ_k and λ_k' satisfy the recurrence relations*

$$\lambda_k = p_k b_k + q_k c_k + r_k d_k + \lambda_{k-1}, \tag{92}$$

$$\lambda_k' = p_k b_k' + q_k c_k' + r_k d_k' + \lambda_{k-1}'. \tag{93}$$

They also satisfy the inequalities

$$10^{-1} - 8(G-1)^{-1} < A_k\lambda_k + \overline{A}_k\bar{\lambda}_k < 1 - 10^{-8} + 8(G-1)^{-1}, \tag{94}$$

$$|A_k'\lambda_k' + \overline{A}_k'\bar{\lambda}_k'| < 8(G-1)^{-1}. \tag{95}$$

Proof. The recurrence relations (92) and (93) follow at once from (88) and (89). To prove (94), we observe that

$$A_k\lambda_k + \overline{A}_k\bar{\lambda}_k = p_k(A_kb_k + \overline{A}_k\bar{b}_k) + q_k(A_kc_k + \overline{A}_k\bar{c}_k) + r_k(A_kd_k + \overline{A}_k\bar{d}_k) + \sum_{\nu=-\infty}^{k-1} \{A_k(p_\nu b_\nu + q_\nu c_\nu + r_\nu d_\nu) + \overline{A}_k(p_\nu\bar{b}_\nu + q_\nu\bar{c}_\nu + r_\nu\bar{d}_\nu)\}.$$

Now, using (90) and (91), we have

$$\sum_{\nu=-\infty}^{k-1} |A_k(p_\nu b_\nu + q_\nu c_\nu + r_\nu d_\nu)| < 4\sum_{\nu=-\infty}^{k-1} |A_k/A_\nu| \leqq 4\sum_{\nu=-\infty}^{k-1} G^{\nu-k} = 4(G-1)^{-1}. \tag{96}$$

Combining this result with (83), we see that $A_k\lambda_k+\overline{A}_k\bar{\lambda}_k$ lies between $10^{-1}-8(G-1)^{-1}$ and $1-10^{-8}+8(G-1)^{-1}$. The proof of (95) is similar; in place of (96) we have

$$\sum_{\nu=k+1}^{\infty} |A_k'(p_\nu b_\nu' + q_\nu c_\nu' + r_\nu d_\nu')| < 4\sum_{\nu=k+1}^{\infty} |A_k'/A_\nu'| \leqq 4\sum_{\nu=k+1}^{\infty} G^{k-\nu} = 4(G-1)^{-1}.$$

LEMMA 15. *Let u_0, v_0, w_0, t_0 be any integers. Then there exist, for any integer k, integers u_k, v_k, w_k, t_k such that*

$$\begin{aligned} a_0u_0 + b_0v_0 + c_0w_0 + d_0t_0 + \lambda_0 &= a_ku_k + b_kv_k + c_kw_k + d_kt_k + \lambda_k, \\ a_0'u_0 + b_0'v_0 + c_0'w_0 + d_0't_0 + \lambda_0' &= a_k'u_k + b_k'v_k + c_k'w_k + d_k't_k + \lambda_k'. \end{aligned} \tag{97}$$

Proof. As we saw at the end of §8, there exists, for any k, a linear substitution with integral coefficients and determinant 1 which transforms the original linear forms x, x' into

$$a_ku + b_kv + c_kw + d_kt, \qquad a_k'u + b_k'v + c_k'w + d_k't.$$

Hence there is a substitution which transforms the last two forms into

$$a_{k+1}u + b_{k+1}v + c_{k+1}w + d_{k+1}t, \qquad a_{k+1}'u + b_{k+1}'v + c_{k+1}'w + d_{k+1}'t.$$

Now, by (92) and (93),

$$\lambda_k = -b_{k+1}p_{k+1} - c_{k+1}q_{k+1} - d_{k+1}r_{k+1} + \lambda_{k+1},$$

and similarly with accents. Hence, if we follow the substitution just men-

tioned by one which replaces v, w, t by $v+p_{k+1}$, $w+q_{k+1}$, $t+r_{k+1}$, we obtain a nonhomogeneous linear substitution with integral coefficients and determinant 1 which transforms the nonhomogeneous linear forms with suffix k into those with suffix $k+1$. The conclusion of the lemma follows, by repetition of this process and of the inverse process, starting from $k=0$.

12. **Proof of Theorem 1.** We recall that the object of Theorem 1 is to establish the existence of real numbers u^*, v^*, w^*, t^* such that (3) holds, where f is defined by (2). This is the same as establishing the existence of complex numbers λ, λ' such that

$$|(x+\lambda)(x'+\lambda')|^2 > \kappa\Delta \tag{98}$$

for all integers u, v, w, t where x, x' are the given linear forms (1). Here κ is to be some positive absolute constant. We shall prove that the numbers $\lambda=\lambda_0$, $\lambda'=\lambda_0'$ defined in (88) and (89) have the desired property, provided that G, which is still at our disposal, is suitably chosen.

Suppose there exist integers u, v, w, t which violate (98), with $\lambda=\lambda_0$, $\lambda'=\lambda_0'$. Since the linear forms x, x' can be transformed into

$$a_0u+b_0v+c_0w+d_0t, \qquad a_0'u+b_0'v+c_0'w+d_0't$$

by some linear substitution which transforms integers into integers, our supposition implies the existence of integers u_0, v_0, w_0, t_0 such that

$$|(a_0u_0+b_0v_0+c_0w_0+d_0t_0+\lambda_0)(a_0'u_0+b_0'v_0+c_0'w_0+d_0't_0+\lambda_0')|^2 \leqq \kappa\Delta. \tag{99}$$

We now choose a particular integer k. Suppose first that the first factor, say Λ, in the product on the left of (99) is not zero. We choose k, as we can do uniquely, so that

$$\kappa^{1/4}G^2|A_{k-1}|^{-1} \leqq |\Lambda| < \kappa^{1/4}G^2|A_k|^{-1}. \tag{100}$$

For the numbers $|A_k|$ decrease as k increases, and have the limits ∞, 0 as $k\to-\infty$, $+\infty$ respectively. It follows from (99) and (100) that the second factor, say Λ', satisfies

$$|\Lambda'| \leqq (\kappa\Delta)^{1/2}\kappa^{-1/4}G^{-2}|A_{k-1}| < \kappa^{1/4}G^2|A_k'|^{-1},$$

on using (60). Thus we have determined k so that the factors Λ, Λ' in (99) satisfy

$$|\Lambda| < \kappa^{1/4}G^2|A_k|^{-1}, \tag{101}$$

$$|\Lambda'| < \kappa^{1/4}G^2|A_k'|^{-1}. \tag{102}$$

This is also possible when the first factor on the left of (99) is zero. For then (101) is true for all k, and (102) is true for all sufficiently small k since $|A_k'|\to 0$ as $k\to-\infty$.

By Lemma 15, there exist integers u_k, v_k, w_k, t_k such that

$$|a_k u_k + b_k v_k + c_k w_k + d_k t_k + \lambda_k| < \kappa^{1/4} G^2 |A_k|^{-1},$$
$$|\bar{a}_k u_k + \bar{b}_k v_k + \bar{c}_k w_k + \bar{d}_k t_k + \bar{\lambda}_k| < \kappa^{1/4} G^2 |A_k|^{-1},$$
$$|a_k' u_k + b_k' v_k + c_k' w_k + d_k' t_k + \lambda_k'| < \kappa^{1/4} G^2 |A_k'|^{-1},$$
$$|\bar{a}_k' u_k + \bar{b}_k' v_k + \bar{c}_k' w_k + \bar{d}_k' t_k + \bar{\lambda}_k'| < \kappa^{1/4} G^2 |A_k'|^{-1}.$$

We multiply the four linear expressions on the left by A_k, $\overline{A}_k$, A_k', $\overline{A}_k'$ respectively, and add. In view of the identities (7), (8), (9), (10), with the suffix k, we obtain

$$|u_k + A_k\lambda_k + \overline{A}_k\bar{\lambda}_k + A_k'\lambda_k' + \overline{A}_k'\bar{\lambda}_k'| < 4\kappa^{1/4}G^2. \tag{103}$$

By Lemma 14, we have

$$10^{-1} - 16(G-1)^{-1} < A_k\lambda_k + \overline{A}_k\bar{\lambda}_k + A_k'\lambda_k' + \overline{A}_k'\bar{\lambda}_k' < 1 - 10^{-8} + 16(G-1)^{-1}.$$

Since u_k is an integer, this contradicts (103) if

$$4\kappa^{1/4}G^2 \leqq 10^{-8} - 16(G-1)^{-1}. \tag{104}$$

If we now choose

$$G = 1600000002, \qquad \kappa = (10^{-8}G^{-3}/4)^4,$$

the condition (104) is satisfied, and we have reached a contradiction. This proves that the numbers $\lambda = \lambda_0$, $\lambda' = \lambda_0'$ have the property that (98) holds for all integers u, v, w, t and so completes the proof of Theorem 1.

13. **The hypothesis of Theorem 2.** The hypothesis of Theorem 2 is that the quaternary quartic form

$$f(u, v, w, t) = x\bar{x}x'\bar{x}' = |xx'|^2 \tag{105}$$

has integral coefficients, and does not represent zero for integral values of u, v, w, t other than 0, 0, 0, 0. We proceed to develop some consequences of this hypothesis. In the course of doing so, we shall show, in Lemma 18, that the adjoint forms X, X' also do not represent zero, a condition which had to be postulated explicitly in Theorem 1.

LEMMA 16. *There exists a totally complex quartic field K and algebraic integers a^*, b^*, c^*, d^* in K, such that*

$$mf(u, v, w, t) = N(a^*u + b^*v + c^*w + d^*t) \tag{106}$$

identically in u, v, w, t, where N denotes the norm of a number of K, and m is a positive integer.

Proof. This is a particular case of a classical result, apparently due to Stouff; for a proof, see Bachmann, loc. cit. Kap. 12, §§1, 2, 3.

If we prove the theorem for the quaternary quartic form $mf(u, v, w, t)$, its truth will then follow for the form $f(u, v, w, t)$ by considerations of homogeneity. It therefore suffices if we take the product in (105) to be the product on the right of (106). This is equivalent to supposing that a, b, c, d are algebraic integers in the quartic field K, and that their algebraic conjugates, in a certain fixed order, are indicated by $\bar{a}, a', \bar{a}'$, and so on. The supposition that $f(u, v, w, t)$ does not represent zero implies that a, b, c, d are linearly independent algebraic integers of K.

In this new formulation, the determinant

$$\Delta = \det (x, \bar{x}, x', \bar{x}')$$

is necessarily an integral multiple of the square root of the discriminant d of K; we have therefore

$$\Delta = hd^{1/2}, \tag{107}$$

where h is a positive integer.

LEMMA 17. *The numbers A, B, C, D are linearly independent numbers of the field K, and their algebraic conjugates, in the fixed order already established, are $\overline{A}, A', \overline{A}'$, and so on.*

Proof. Let θ be a quartic irrationality which generates K. It suffices to prove the result when $a=1, b=\theta, c=\theta^2, d=\theta^3$. For the linear forms x, x' and X, X' in the general case are related to those in the special case by linear substitutions with rational coefficients.

In the above special case, evaluation of the determinants shows that the values of A, B, C, D are respectively

$$-s_3(\theta)/d(\theta), \quad s_2(\theta)/d(\theta), \quad -s_1(\theta)/d(\theta), \quad 1/d(\theta), \tag{108}$$

where

$$d(\theta) = (\theta - \bar{\theta})(\theta - \theta')(\theta - \bar{\theta}'),$$

and $s_1(\theta), s_2(\theta), s_3(\theta)$ are the elementary symmetric functions of $\bar{\theta}, \theta', \bar{\theta}'$. Also $\overline{A}, A', \overline{A}'$, and so on are obtained from these expressions by cyclic permutation of $\theta, \bar{\theta}, \theta', \bar{\theta}'$. Now it is plain that the four numbers in (108) are linearly independent numbers of K, and that the cyclic permutation gives their conjugates in the fixed order.

LEMMA 18. *The adjoint linear forms $X, \overline{X}, X', \overline{X}'$, defined by* (11), *have the property that $\Delta^4 X\overline{X}X'\overline{X}'$ is a quaternary quartic form in U, V, W, T with integral coefficients, which does not represent zero for integral values, not all zero, of those variables.*

Proof. That $X \neq 0$ for any integers U, V, W, T not all zero is simply a restatement of the first assertion of the preceding lemma. Also it is plain from that lemma that the coefficients in the product

$$X\overline{X}X'\overline{X}' = (AU + \cdots)(\overline{A}U + \cdots)(A'U + \cdots)(\overline{A}'U + \cdots)$$

are all rational numbers. Further, Δ^4 is a rational number, by (107).

Moreover, since ΔA is a determinant whose elements are algebraic integers, it follows that ΔA is an algebraic integer. Similarly for ΔB, ΔC, ΔD. Hence every coefficient in the product $\Delta^4 X\overline{X}X'\overline{X}'$ is both rational and an algebraic integer, and so is an integer.

14. **Modification of the unimodular substitutions.** We know, by the work of §8, that for every integer k there is a unimodular substitution which transforms the forms X, X' into those given in (70), and that the relations (57) to (60) and (71) hold, together with the subsequent results of Lemmas 10 and 11, on which the proof of Theorem 1 was based. The assertion of Lemma 17 is obviously valid with the suffix k.

Our next step is to show that this sequence of unimodular substitutions can, with the present hypothesis, be so modified that the numbers $A_k, \cdots, D_k'$, $a_k, \cdots, d_k'$ have certain additional properties. The argument is again essentially due to Hermite.

LEMMA 19. *The coefficients in all the products*

$$F_k(U, V, W, T) = (A_kU + \cdots)(\overline{A}_kU + \cdots)(A_k'U + \cdots)(\overline{A}_k'U + \cdots) \tag{109}$$

are all bounded in absolute value by a number independent of k.

Proof. By Lemma 18, the form $\Delta^4 F_k(U, V, W, T)$ has integral coefficients, and is not zero for any integers U, V, W, T other than 0, 0, 0, 0. Hence, for any such integers,

$$\Delta^4 F_k(U, V, W, T) \geqq 1.$$

In particular, we have

$$|A_kA_k'|^2 \geqq \Delta^{-4}.$$

By (71) and the inequality of the arithmetic and geometric means, it follows that

$$\mathcal{A}_k = S_k^2|A_k|^2 + S_k^{-2}|A_k'|^2 \geqq 2|A_kA_k'| \geqq 2\Delta^{-2}.$$

Now (68) and (69) imply that $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, $\mathcal{D}_k$ are all bounded above by a number independent of k. Hence, by (71) and its analogues, all the numbers

$$S_k|A_k|, \quad S_k|B_k|, \quad S_k|C_k|, \quad S_k|D_k|,$$
$$S_k^{-1}|A_k'|, \quad S_k^{-1}|B_k'|, \quad S_k^{-1}|C_k'|, \quad S_k^{-1}|D_k'|$$

are bounded. It now follows that all the coefficients in the product (109) are bounded.

LEMMA 20. *There exists a set of integral unimodular substitutions, one for every integer k, which transform the linear forms X, X' into those represented in* (70), *with the following properties. First,* (57) *to* (60) *and* (71) *are valid for every k. Secondly, there exists a positive integer s such that*

$$A_{k+s}/A_k = B_{k+s}/B_k = C_{k+s}/C_k = D_{k+s}/D_k = 1/\omega \tag{110}$$

for all k, where ω is a certain number of K satisfying

$$|\omega\omega'| = 1, \qquad |\omega| > 1. \tag{111}$$

Proof. By Lemma 19, the product $F_k(U, V, W, T)$ has coefficients which are bounded independently of k. For the moment, we call two such products of four linear forms equivalent if corresponding linear forms in the two products are proportional, with factors of proportionality whose product is 1. It is plain that there are only a finite number of nonequivalent products with bounded integral coefficients. Hence there exist integers j and s with $s>0$ such that F_j and F_{j+s} are equivalent, that is

$$A_jU + B_jV + C_jW + D_jT = \omega(A_{j+s}U + B_{j+s}V + C_{j+s}W + D_{j+s}T)$$

and

$$A'_jU + B'_jV + C'_jW + D'_jT = \omega'(A'_{j+s}U + B'_{j+s}V + C'_{j+s}W + D'_{j+s}T)$$

identically in U, V, W, T. Here ω and ω' are two complex numbers with $|\omega\omega'| = 1$. Plainly $\omega = A_j/A_{j+s}$ is a number of the field K, and its conjugates in the fixed order are $\bar{\omega}$, ω', $\bar{\omega}'$. Also $|\omega| \geqq G > 1$, by (58). This proves (110) for $k=j$.

We adopt the existing unimodular substitutions $\mathfrak{T}_k$ and the resulting values of A_k, B_k, C_k, D_k for all values of k satisfying $j \leqq k \leqq j+s$ but we proceed to give new definitions when k is outside this range. We define the new substitution, say $\mathfrak{T}^*_k$, to be the same as $\mathfrak{T}_k$ for $j \leqq k < j+s$. We also lay down that the substitution $\mathfrak{T}^*_{k+s}$ shall be obtained from the substitution $\mathfrak{T}^*_k$ by following $\mathfrak{T}_{j+s}$ with the substitution which transforms the forms (70) with suffix j into those with suffix k. Symbolically,

$$\mathfrak{T}^*_{k+s} = (\mathfrak{T}_{j+s}\mathfrak{T}_j^{-1})\mathfrak{T}^*_k.$$

This is a recursive definition of the $\mathfrak{T}^*_k$ which defines them for all k.

We retain the same symbols for the coefficients $A_k, \cdots, D'_k$ of the linear forms into which X and X' are transformed by $\mathfrak{T}^*_k$, though their meaning has been altered for $k<j$ and for $k>j+s$.

Write, temporarily, $\mathfrak{A}_k$ for the matrix

$$[A_k, B_k, C_k, D_k],$$

and $\mathfrak{A}$ for the corresponding matrix without suffixes. Then $\mathfrak{A}_k = \mathfrak{A}\mathfrak{T}^*_k$ for every k. The above definition ensures that

$$\mathfrak{A}_{k+s} = \mathfrak{A}\mathfrak{T}_{j+s}\mathfrak{T}_j^{-1}\mathfrak{T}_k^*$$

for every k. But

$$\mathfrak{A}\mathfrak{T}_{j+s} = \mathfrak{A}_{j+s} = \omega^{-1}\mathfrak{A}_j,$$

whence $\mathfrak{A}_{k+s} = \omega^{-1}\mathfrak{A}_k$ for every k. In other words, the identities (110) are valid for all k.

The formulae (58) to (60) are already valid for $j \leqq k < j+s$, and now follow for all k by (110). The formulae (57) and (71) involve S_k, $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, $\mathcal{D}_k$, which as yet are only defined for $j \leqq k \leqq j+s$. We abandon the existing definitions when $k = s+j$ and define these numbers generally in terms of their values when $j \leqq k < j+s$ by means of the recursive definitions

$$S_{k+s} = |\omega| S_k, \quad \mathcal{A}_{k+s} = \mathcal{A}_k, \quad \mathcal{B}_{k+s} = \mathcal{B}_k, \quad \mathcal{C}_{k+s} = \mathcal{C}_k, \quad \mathcal{D}_{k+s} = \mathcal{D}_k.$$

Then (57) and (71), being valid already for $j \leqq k < j+s$, follow for all k on using (110).

LEMMA 21. *Let $a_k, \cdots, d_k'$ be defined in terms of $A_k, \cdots, D_k'$ as at the end of* §8. *Then a_k is a number of the field K, and its conjugates, in the fixed order, are $\bar{a}_k$, a_k', $\bar{a}_k'$. Similar results hold for b_k, c_k, d_k. We have*

$$a_{k+s} = \omega a_k, \qquad b_{k+s} = \omega b_k, \qquad c_{k+s} = \omega c_k, \qquad d_{k+s} = \omega d_k, \tag{112}$$

and similarly for their conjugates, for all k. Also Lemmas 10 *and* 11 *are valid.*

Proof. As we saw at the end of §8, there exists, for every k, a unimodular substitution which transforms the linear forms x and x' into similar forms with the suffix k. Hence, by the remarks made after Lemma 16, a_k, b_k, c_k, d_k are in fact algebraic integers in K, and their conjugates are as stated.

To prove (112), we have, for example,

$$\begin{aligned}
\Delta^{-1}a_k &= \begin{vmatrix} \overline{B}_k, & \overline{C}_k, & \overline{D}_k \\ B_k', & C_k', & D_k' \\ \overline{B}_k', & \overline{C}_k', & \overline{D}_k' \end{vmatrix} \\
&= \begin{vmatrix} \bar{\omega}\,\overline{B}_{k+s}, & \bar{\omega}\,\overline{C}_{k+s}, & \bar{\omega}\,\overline{D}_{k+s} \\ \omega' B_{k+s}', & \omega' C_{k+s}', & \omega' D_{k+s}' \\ \bar{\omega}'\overline{B}_{k+s}', & \bar{\omega}'\overline{C}_{k+s}', & \bar{\omega}'\overline{D}_{k+s}' \end{vmatrix} \\
&= \bar{\omega}\omega'\bar{\omega}'\Delta^{-1}a_{k+s} = \omega^{-1}\Delta^{-1}a_{k+s},
\end{aligned}$$

by (110) and (111). Similar results hold for the general case.

As regards Lemmas 10 and 11, their proofs are still valid, since they use only (57) to (60) and (71). Or we can observe that $A_k b_k$, and so on, are all periodic functions of k with period s, so that the validity for general k follows from that already known for $j \leqq k < j+s$.

LEMMA 22. *Integers p_k, q_k, r_k exist, for every k, to satisfy* (83), (84), (85), *and also to satisfy*

$$p_{k+s} = p_k, \qquad q_{k+s} = q_k, \qquad r_{k+s} = r_k. \tag{113}$$

Also, if λ_k and λ_k' are defined as in §11, *Lemmas* 14 *and* 15 *are valid.*

Proof. Since A_kb_k, and so on, are periodic functions of k with period s, the inequalities (83), (84), (85) are the same for $k+s$ as for k, and the conclusion is immediate. Lemma 14 depends only on the definitions of λ_k, λ_k' and on Lemma 13. Lemma 15 depends only on the definitions of λ_k, λ_k' and on the existence of the substitutions mentioned at the beginning of the proof of Lemma 21.

15. **Proof of Theorem 2.** It suffices to prove that the number λ_0, defined by (88), belongs to the field K, and that its second algebraic conjugate is λ_0'. For then the real numbers u^*, v^*, w^*, t^* defined by

$$au^* + bv^* + cw^* + dt^* = \lambda_0, \qquad a'u^* + b'v^* + c'w^* + d't^* = \lambda_0'$$

will be rational. These are the numbers which occur in the enunciation of Theorem 2.

By Lemmas 21 and 22,

$$\begin{aligned}
\lambda_0 &= \sum_{\nu=-\infty}^{0} (p_\nu b_\nu + q_\nu c_\nu + r_\nu d_\nu) \\
&= \sum_{n=1}^{s} \sum_{m=1}^{\infty} (p_{n-ms}b_{n-ms} + q_{n-ms}c_{n-ms} + r_{n-ms}d_{n-ms}) \\
&= \sum_{n=1}^{s} \sum_{m=1}^{\infty} (p_nb_n + q_nc_n + r_nd_n)\omega^{-m} \\
&= (\omega - 1)^{-1} \sum_{n=1}^{s} (p_nb_n + q_nc_n + r_nd_n).
\end{aligned}$$

In the same way,

$$\begin{aligned}
-\lambda_0' &= \sum_{\nu=1}^{\infty} (p_\nu b_\nu' + q_\nu c_\nu' + r_\nu d_\nu') \\
&= \sum_{n=1}^{s} \sum_{m=0}^{\infty} (p_{n+ms}b_{n+ms}' + q_{n+ms}c_{n+ms}' + r_{n+ms}d_{n+ms}') \\
&= \sum_{n=1}^{s} \sum_{m=0}^{\infty} (p_nb_n' + q_nc_n' + r_nd_n')(\omega')^m \\
&= (1 - \omega')^{-1} \sum_{n=1}^{s} (p_nb_n' + q_nc_n' + r_nd_n').
\end{aligned}$$

From the first of the above formulae, and from the fact that b_n, c_n, d_n are numbers of K and ω is a number of K, it follows that λ_0 is a number of K. The second formula, on changing signs throughout, then shows that λ_0' is the second algebraic conjugate of λ_0. This establishes the desired result, and so completes the proof of Theorem 2.

UNIVERSITY COLLEGE,
LONDON, ENGLAND.