EUCLID'S ALGORITHM IN CUBIC FIELDS OF NEGATIVE DISCRIMINANT.

By

H. DAVENPORT
UNIVERSITY COLLEGE, LONDON.

1. Introduction.

Let K be any algebraic number field. If, for each number λ of the field K, there is an algebraic integer ξ of K such that

$$|N(\xi-\lambda)| < 1 ,$$

where N denotes the norm, then Euclid's algorithm is said to be valid in K. For complex quadratic fields, the question is almost trivial. For real quadratic fields, it has been known for some years that there are only a finite number of cases in which Euclid's algorithm is valid. I have recently given[1] a proof of this result based on new principles, and this proof has led to the complete enumeration[2] of all such cases.

Now let K be a cubic field of negative discriminant, that is, a field generated by a real cubic irrationality whose conjugates are complex. The main result of the present paper is that *Euclid's algorithm is valid only in a finite number of such fields.*

As in the quadratic case, the result is closely connected with one which relates to a more general situation. Let

$$(1) \qquad \begin{cases} \xi \ = \alpha u+\beta v+\gamma w , \\ \xi' = \alpha' u+\beta' v+\gamma' w , \\ \xi''= \alpha'' u+\beta'' v+\gamma'' w \end{cases}$$

[1] "Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields", *Proc. London Math. Soc.* (in course of publication).

[2] See H. Chatland and H. Davenport, "Euclid's algorithm in real quadratic fields", *Canadian J. of Math.* (in course of publication).

be any three linear forms in which α, β, γ are real numbers, α', β', γ' are complex numbers, and $\alpha'', \beta'', \gamma''$ are the complex conjugates of α', β', γ'. Let the determinant of the forms be $i\Delta \neq 0$, so that without loss of generality we can suppose $\Delta > 0$. Write

$$f(u, v, w) = \xi \xi' \xi'' . \tag{2}$$

Our basic result is:

Theorem 1. *Suppose none of the adjoint linear forms Ξ, Ξ', Ξ'', defined by* (7), *represents zero for integral values, not all zero, of the variables. Then there exist real numbers u^*, v^*, w^* such that*

$$|f(u+u^*, v+v^*, w+w^*)| \geqq c\Delta \tag{3}$$

for all integers[1] *u, v, w, where c is a certain positive absolute constant.*

This result, though of interest in connection with some problems of Diophantine approximation, has in itself no application to the question of Euclid's algorithm. For that we need the following vital addition.

Theorem 2. *Suppose that the ternary cubic form $f(u, v, w)$ has integral coefficients and that $f(u, v, w) \neq 0$ for all integers u, v, w except* 0, 0, 0. *Then the numbers u^*, v^*, w^*, whose existence is asserted in Theorem 1, can be so chosen as to be rational.*

Now let K be a cubic field of discriminant $-d < 0$, and let α, β, γ be a basis for the algebraic integers of K. Let α', β', γ' and $\alpha'', \beta'', \gamma''$ be the algebraic conjugates of α, β, γ in some fixed order. Then ξ, the linear form in (1), with integral variables u, v, w, represents the general algebraic integer of K, and ξ', ξ'' are its algebraic conjugates. The determinant of these three linear forms is $\pm i\sqrt{d}$, and we can suppose without loss of generality that the determinant is $i\sqrt{d}$. The ternary cubic form $f(u, v, w)$ is the norm of a general algebraic integer of K, and so it has integral coefficients and is not zero unless u, v, w are all zero. The hypotheses of Theorem 2 are satisfied. If we write

$$\lambda = \alpha u^* + \beta v^* + \gamma w^* , \tag{4}$$

then λ is a number of K, since u^*, v^*, w^* are rational. We have, then, a number λ of K such that

$$|N(\xi+\lambda)| \geqq c\sqrt{d} \tag{5}$$

for all algebraic integers ξ of K. Thus Theorem 2 implies the following:

[1] The word *integer*, without the qualification *algebraic*, will always be used to mean rational integer.

Theorem 3. *Euclid's algorithm cannot hold in a cubic field of discriminant* $-d$ *if* $d > c^{-2}$.

Since, by a classical result[1], the number of cubic fields with bounded discriminants is finite, this justifies the assertion made earlier, that Euclid's algorithm is valid only in a finite number of cubic fields of negative discriminant.

The plan of the paper is as follows. After a number of lemmas, we prove Theorem 1, relating to general linear forms, in § 4. In § 5 and § 6 the proof is reconsidered, in the light of the additional hypothesis of Theorem 2, and that theorem is then established in § 7.

Throughout the paper, small Latin letters, other than c, f, i, x, y, z, denote integers.

2. Preliminary Lemmas.

Definitions. Let the cofactors of the elements of the matrix

$$\begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix},$$

after dividing each of them by $i\Delta$, be denoted by the corresponding capital letter, so that $i\Delta A = \beta'\gamma''-\beta''\gamma'$, etc. It is plain that A, B, Γ are real, and that A'', B'', Γ'' are the complex conjugates of A', B', Γ'. Also

$$(6) \qquad \begin{vmatrix} A & B & \Gamma \\ A' & B' & \Gamma' \\ A'' & B'' & \Gamma'' \end{vmatrix} = (i\Delta)^{-1}.$$

Let Ξ, Ξ', Ξ'' be the linear forms

$$(7) \qquad \begin{cases} \Xi = AU+BV+\Gamma W, \\ \Xi' = A'U+B'V+\Gamma'W, \\ \Xi''= A''U+B''V+\Gamma''W, \end{cases}$$

of determinant $(i\Delta)^{-1}$. We have the obvious identity

$$(8) \qquad \xi\Xi+\xi'\Xi'+\xi''\Xi'' = uU+vV+wW.$$

We write

$$(9) \qquad X = \Xi, \quad Y+iZ = \Xi'\sqrt{2}, \quad Y-iZ = \Xi''\sqrt{2}.$$

[1] See, for example, Minkowski, *Diophantische Approximationen*, Kap. 4, § 5.

Then X, Y, Z are real linear forms in U, V, W, and their determinant is Δ^{-1}. By the hypothesis of Theorem 1, we know that $X(Y^2+Z^2) \neq 0$ for any integers U, V, W other than 0, 0, 0.

Lemma 1. *Let $Q(U, V, W)$ be a positive definite ternary quadratic form of determinant D. Then Q can be transformed, by an integral linear substitution of determinant ± 1, into a form $\mathfrak{A}U^2+\mathfrak{B}V^2+\mathfrak{C}W^2+\cdots$, whose minimum is $\mathfrak{A}$ and for which*

$$\mathfrak{A} \leqq \mathfrak{B} \leqq \mathfrak{C}, \quad \mathfrak{A}\mathfrak{B}\mathfrak{C} \leqq 2D\,. \tag{10}$$

This was first proved by Gauss in 1831; for his proof, and also a proof by Dirichlet, see Bachmann, *Die Arithmetik der quadratischen Formen* II, Kap. 6, § 9.

Lemma 2. *There exists a chain*[1] *of values x_n, y_n, z_n of the linear forms X, Y, Z, each set arising from integral values of U, V, W, not all zero, with the following properties. First, for every integer n there is a positive number R such that*

$$R^2x_n^2+2R^{-1}(y_n^2+z_n^2) \leqq R^2X^2+2R^{-1}(Y^2+Z^2) \tag{11}$$

for all integral U, V, W, not all zero. Secondly, for every integer n,

$$x_n > 0, \quad x_{n+1} < x_n, \quad y_{n+1}^2+z_{n+1}^2 > y_n^2+z_n^2\,, \tag{12}$$

$$x_n(y_{n+1}^2+z_{n+1}^2) \leqq \sqrt{2}\Delta^{-1}\,, \tag{13}$$

$$x_n \to 0 \quad \textit{and} \quad y_n^2+z_n^2 \to \infty \quad \textit{as} \quad n \to +\infty\,, \tag{14}$$

$$x_n \to \infty \quad \textit{and} \quad y_n^2+z_n^2 \to 0 \quad \textit{as} \quad n \to -\infty\,. \tag{15}$$

Proof.[2] For every $R > 0$ we consider the quadratic form

$$Q_R(U, V, W) = R^2X^2+2R^{-1}(Y^2+Z^2)\,.$$

This is a positive definite ternary quadratic form, whose determinant is $D=4\Delta^{-2}$, since the determinant of the real linear forms X, Y, Z is Δ^{-1}.

For every R, the minimum of $Q_R(U, V, W)$ is attained for certain integral values of U, V, W, not all zero, and to these there correspond certain values x, y, z of the linear forms X, Y, Z. We can restrict ourselves, without loss of generality, to positive values of x, since $X \neq 0$ by hypothesis.

[1] The word *chain* is used to denote a set of objects which is in one-to-one correspondence with the set of all integers (positive, negative and zero).

[2] The argument is essentially that of Hermite; for an exposition of the general theory, see Bachmann, *loc.cit.*, Kap. 12.

If x, y, z correspond to the minimum of the form both when $R=R_1$ and $R=R_2$, they do so also for all values of R satisfying $R_1 \leqq R \leqq R_2$. For we can determine positive numbers μ_1, μ_2 such that

$$R^2 = \mu_1 R_1^2 + \mu_2 R_2^2, \quad R^{-1} = \mu_1 R_1^{-1} + \mu_2 R_2^{-1} ,$$

and then it is clear that the inequalities

$$R_1^2 x^2 + 2R_1^{-1}(y^2+z^2) \leqq R_1^2 X^2 + 2R_1^{-1}(Y^2+Z^2) ,$$

$$R_2^2 x^2 + 2R_2^{-1}(y^2+z^2) \leqq R_2^2 X^2 + 2R_2^{-1}(Y^2+Z^2)$$

imply

$$R^2 x^2 + 2R^{-1}(y^2+z^2) \leqq R^2 X^2 + 2R^{-1}(Y^2+Z^2) .$$

It is now plain that all positive numbers R fall into an enumerable set of closed intervals, in each of which the minimum of $Q_R(U, V, W)$ occurs for the same U, V, W, and so for the same values x, y, z of X, Y, Z. These intervals have no point of accumulation (other than at 0 and ∞). For, by Lemma 1, the minimum of $Q_R(U, V, W)$ satisfies

$$(16) \qquad R^2 x^2 + 2R^{-1}(y^2+z^2) \leqq (2D)^{\frac{1}{3}} = 2\Delta^{-\frac{2}{3}};$$

and so, if R and R^{-1} are bounded below, then x, y, z are bounded above, and there are only a finite number of possible choices of integers U, V, W among which must occur all the minima for the range of R in question.

It follows that the above intervals for R, and the corresponding values of x, y, z can be enumerated according to increasing values of R. We ignore any interval for R which consists of a single point, and enumerate the x, y, z as x_n, y_n, z_n. Here n takes all integral values, since it is impossible for the same x, y, z to provide the minimum of $Q_R(U, V, W)$ for arbitrarily large R, or for arbitrarily small R. This follows from (16); if this inequality were true for arbitrarily large R we would have $x = 0$, and if it were true for arbitrarily small R we would have $y = z = 0$, either of which is contrary to the hypothesis that $X(Y^2+Z^2) \neq 0$ for integral U, V, W not all zero.

Now consider any two consecutive sets, x_n, y_n, z_n and $x_{n+1}, y_{n+1}, z_{n+1}$ in the above enumeration. By definition, there exist numbers R_n and R_{n+1} such that $R_n < R_{n+1}$ and

$$R_n^2 x_n^2 + 2R_n^{-1}(y_n^2+z_n^2) \leqq R_n^2 x_{n+1}^2 + 2R_n^{-1}(y_{n+1}^2+z_{n+1}^2) ,$$

$$R_{n+1}^2 x_{n+1}^2 + 2R_{n+1}^{-1}(y_{n+1}^2+z_{n+1}^2) \leqq R_{n+1}^2 x_n^2 + 2R_{n+1}^{-1}(y_n^2+z_n^2) .$$

It follows that

$$R_n^3(x_n^2 - x_{n+1}^2) \leqq 2(y_{n+1}^2 + z_{n+1}^2 - y_n^2 - z_n^2) \leqq R_{n+1}^3(x_n^2 - x_{n+1}^2) .$$

Hence $x_{n+1} \leqq x_n$. Since the linear form X does not represent zero, we have $x_{n+1} < x_n$, and it now follows that $y_{n+1}^2+z_{n+1}^2 > y_n^2+z_n^2$. This proves (12).

It is plain that our definition ensures the truth of the first assertion in the enunciation; indeed, it is further true that for every R there is an n with the minimal property (11).

It follows from (16) that $y_n^2+z_n^2 \to 0$ as $R \to 0$, that is, as $n \to -\infty$. Also $y_n^2+z_n^2 \to \infty$ as $R \to \infty$, that is, as $n \to +\infty$; for if $y_n^2+z_n^2$ were bounded under this operation, then, as x_n is necessarily bounded we would get some one set x_n, y_n, z_n providing the minimum for arbitrarily large R, which we have seen to be impossible. Similarly for the other assertions in (14) and (15).

To prove (13) we observe that for any n there is a value of R such that the form $Q_R(U, V, W)$ assumes its minimum twice, namely with x_n, y_n, z_n and with $x_{n+1}, y_{n+1}, z_{n+1}$; this value of R being the point where two adjacent intervals abut. From the two corresponding cases of (16), we obtain

$$R^2x_n^2 \leqq 2\Delta^{-\frac{2}{3}}, \quad 2R^{-1}(y_{n+1}^2+z_{n+1}^2) \leqq 2\Delta^{-\frac{2}{3}} .$$

This gives (13), and the proof is complete.

Lemma 3. *Let $T(n)$ be defined for every integer n, and have the properties*

$$(17) \qquad T(n+1) > T(n) ,$$

$$(18) \qquad T(n) \to 0 \quad as \quad n \to -\infty ,$$

$$(19) \qquad T(n) \to \infty \quad as \quad n \to +\infty .$$

Let $C > 1$ be given. Then there exist integers n_k, defined for every integer k, such that

$$(20) \qquad n_{k+1} > n_k ,$$

$$(21) \qquad CT(n_k) \leqq T(n_{k+1}) < C^2T(n_k+1) .$$

Proof. Case 1. Suppose that

$$(22) \qquad T(n+1) < CT(n)$$

for every integer n. Define n_0 arbitrarily, and define $n_1, n_2, \ldots$ by recurrence, through the condition

$$(23) \qquad T(n_{k+1}-1) < CT(n_k) \leqq T(n_{k+1}) \quad (k \geqq 0) .$$

This is possible, in a unique manner, by (17) and (19). Then (20) is satisfied for $k \geqq 0$, as also is the left hand half of (21). To prove the right hand half of (21) for $k \geqq 0$, we observe that, by (22), (23) and (17),

$$T(n_{k+1}) < CT(n_{k+1}-1) < C^2T(n_k) < C^2T(n_k+1) .$$

Next, define $n_{-1}, n_{-2}, \ldots$ by recurrence, through the condition

$$T(n_k) \leqq C^{-1}T(n_{k+1}) < T(n_k+1) \quad (k \leqq -1) . \tag{24}$$

This is possible, in a unique manner, by (17) and (18). Now (20) is satisfied for $k \leqq -1$, as also is (21), with C in place of C^2 on the right.

Case 2. Suppose that there are numbers n which violate (22), and that such numbers are bounded above. Take n_0 to be larger than the largest of them, so that (22) is valid for $n \geqq n_0$. The preceding proof applies, since (22) was used only with $n = n_{k+1}-1 \geqq n_k$, where $k \geqq 0$.

Case 3. If the hypotheses of Case 1 and Case 2 are not satisfied, then there exists an increasing sequence $g_1, g_2, \ldots$ of integers such that

$$T(g_r+1) \geqq CT(g_r) . \tag{25}$$

We define integers $n_0^{(r)}, n_{-1}^{(r)}, n_{-2}^{(r)}, \ldots$ by taking $n_0^{(r)} = g_r$, and defining $n_k^{(r)}$ for every $k \leqq -1$ by (24), with the superscript r. We denote by $\mathfrak{N}^{(r)}$ the set of numbers $n_0^{(r)}, n_{-1}^{(r)}, \ldots$. Then (21) is valid for any two consecutive numbers of $\mathfrak{N}^{(r)}$.

We now observe that the set $\mathfrak{N}^{(r+1)}$ contains the set $\mathfrak{N}^{(r)}$. To prove this, define k by

$$n_k^{(r+1)} \leqq g_r < n_{k+1}^{(r+1)}. \tag{26}$$

Then $k \leqq -1$, since $n_0^{(r+1)} = g_{r+1} > g_r$. Thus, by (24),

$$C^{-1}T(n_{k+1}^{(r+1)}) < T(n_k^{(r+1)}+1) .$$

But

$$T(n_{k+1}^{(r+1)}) \geqq T(g_r+1) \geqq CT(g_r) ,$$

by (26) and (25). Hence

$$T(g_r) < T(n_k^{(r+1)}+1) ,$$

whence $g_r \leqq n_k^{(r+1)}$, and so $g_r = n_k^{(r+1)}$, by (26). This proves that the set $\mathfrak{N}^{(r+1)}$ contains g_r, and by the uniqueness of the construction the numbers in the set less than g_r are the same as those in $\mathfrak{N}^{(r)}$.

Take the integers n_k to consist of the numbers in *all* sets $\mathfrak{N}^{(r)}$. Then any two consecutive terms n_k, n_{k+1} are also consecutive terms in $\mathfrak{N}^{(r)}$, for all sufficiently large r, and we have already proved that (21) is valid for them.

Lemma 4. *There exists a chain of values $\mathscr{X}_j$, $\mathscr{Y}_j$, $\mathscr{Z}_j$ of the linear forms X, Y, Z, each set arising from integral values of U, V, W, not all zero, with the following properties. First, for every integer j there is a positive number R such that*

$$R^2\mathscr{X}_j^2+2R^{-1}(\mathscr{Y}_j^2+\mathscr{Z}_j^2) \leqq R^2X^2+2R^{-1}(Y^2+Z^2) \tag{27}$$

for all integral U, V, W, not all zero. Secondly, for all j we have

$$\mathscr{X}_j > 0\,, \quad \mathscr{X}_{j+1} < \mathscr{X}_j\,, \tag{28}$$

$$\mathscr{Y}_{j+1}^2+\mathscr{Z}_{j+1}^2 \geqq C^2(\mathscr{Y}_j^2+\mathscr{Z}_j^2)\,, \tag{29}$$

$$\mathscr{X}_j(\mathscr{Y}_{j+1}^2+\mathscr{Z}_{j+1}^2) < \sqrt{2}\Delta^{-1}C^4\,, \tag{30}$$

$$\mathscr{X}_j \to 0 \quad as \quad j \to +\infty, \qquad \mathscr{X}_j \to \infty \quad as \quad j \to -\infty\,. \tag{31}$$

Proof. With the notation of Lemma 2, define

$$T(n) = y_n^2+z_n^2\,.$$

The hypotheses of Lemma 3 are satisfied; hence, by that lemma with C^2 in place of C, there exists an increasing chain of integers n_j such that

$$C^2T(n_j) \leqq T(n_{j+1}) < C^4T(n_j+1) \tag{32}$$

for all j. We define

$$\mathscr{X}_j = x_{n_j}, \quad \mathscr{Y}_j = y_{n_j}, \quad \mathscr{Z}_j = z_{n_j}\,.$$

The first result stated is immediate, and so are (28), (29) and (31). Also (30) follows from (13) and the second inequality in (32).

Lemma 5. *There exists a chain of values X_k, Y_k, Z_k of the linear forms X, Y, Z, each set arising from integral values of U, V, W, not all zero, with the following properties. First, for every integer k there is a positive number R such that*

$$R^2X_k^2+2R^{-1}(Y_k^2+Z_k^2) \leqq R^2X^2+2R^{-1}(Y^2+Z^2) \tag{33}$$

for all integral U, V, W, not all zero. Secondly, for all k we have

$$X_k > 0\,, \quad X_k \geqq CX_{k+1}\,, \tag{34}$$

$$Y_{k+1}^2+Z_{k+1}^2 \geqq C^2(Y_k^2+Z_k^2)\,, \tag{35}$$

$$X_k(Y_{k+1}^2+Z_{k+1}^2) < \sqrt{2}\Delta^{-1}C^6\,. \tag{36}$$

Proof. With the notation of Lemma 4, define

$$T(n) = \mathscr{X}_{-n} = \mathscr{X}(-n)\,,$$

say, to avoid complicated suffixes later. The hypotheses of Lemma 3 are satisfied, hence there exists an increasing chain of integers n_k such that (21) holds. We write $n_{-k} = -m_k$; then m_k is an increasing chain of integers. Let

$$X_k = \mathcal{X}(m_k)\,, \quad Y_k = \mathcal{Y}(m_k)\,, \quad Z_k = \mathcal{Z}(m_k)\,.$$

We have

$$X_k = \mathcal{X}(m_k) = T(n_{-k}) \leqq C^{-1}T(n_{-k+1}) = C^{-1}\mathcal{X}(m_{k-1}) = C^{-1}X_{k-1}\,,$$

which proves (34). Also

$$X_k = T(n_{-k}) < C^2T(n_{-k-1}+1) = C^2\mathcal{X}(m_{k+1}-1)\,.$$

Hence

$$X_k(Y_{k+1}^2+Z_{k+1}^2) < C^2\mathcal{X}(m_{k+1}-1)\{\mathcal{Y}^2(m_{k+1})+\mathcal{Z}^2(m_{k+1})\} < \sqrt{2}\Delta^{-1}C^6,$$

by (30). The remaining assertions are obvious.

3. Further Lemmas.

Definitions. By Lemma 5 there exists, for every integer k, a number $R = R_k$ such that the form

$$Q_R(U, V, W) = R^2X^2+2R^{-1}(Y^2+Z^2)$$

has for its minimum value

$$R^2X_k^2+2R^{-1}(Y_k^2+Z_k^2)\,.$$

By Lemma 1 there exists an integral unimodular substitution (depending on k) from the variables U, V, W to new variables U_k, V_k, W_k which transforms the form $Q_R(U, V, W)$ into one whose leading coefficients, say $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$, satisfy

$$\mathcal{A}_k = R^2X_k^2+2R^{-1}(Y_k^2+Z_k^2)\,, \tag{37}$$

$$\mathcal{A}_k \leqq \mathcal{B}_k \leqq \mathcal{C}_k\,, \tag{38}$$

$$\mathcal{A}_k\mathcal{B}_k\mathcal{C}_k \leqq 2D = 8\Delta^{-2}\,. \tag{39}$$

Let the forms Ξ, Ξ', Ξ'', when expressed in terms of the new variables, become

$$\begin{cases} \Xi \;= A_kU_k+B_kV_k+\Gamma_kW_k\,, \\ \Xi' = A_k'U_k+B_k'V_k+\Gamma_k'W_k\,, \\ \Xi''= A_k''U_k+B_k''V_k+\Gamma_k''W_k\,. \end{cases} \tag{40}$$

By (9), we have

$$A_k = X_k\,, \quad \sqrt{2}A_k' = Y_k+iZ_k\,, \quad \sqrt{2}A_k'' = Y_k-iZ_k\,, \tag{41}$$

$$Q_R(U, V, W) = R^2\Xi^2+4R^{-1}|\Xi'|^2\,; \tag{42}$$

hence

$$\mathcal{A}_k = R^2 A_k^2 + 4R^{-1}|A_k'|^2, \tag{43}$$

$$\mathcal{B}_k = R^2 B_k^2 + 4R^{-1}|B_k'|^2, \tag{44}$$

$$\mathcal{C}_k = R^2 \Gamma_k^2 + 4R^{-1}|\Gamma_k'|^2, \tag{45}$$

where $R = R_k$ throughout.

We next define $\alpha_k, \ldots$ so that they have the same relation to $A_k, \ldots$ as was originally true for the symbols without suffixes. To be precise, we define α_k as the cofactor of A_k in the determinant of the coefficients on the right of (40), multiplied by $i\Delta$, and so on for all the elements. The linear forms ξ, ξ', ξ'' are then transformable into $\alpha_k u_k + \beta_k v_k + \gamma_k w_k$, etc. by an integral unimodular substitution (namely, that which is contragredient to the substitution from U, V, W to U_k, V_k, W_k).

Note that none of $A_k, \ldots, \Gamma_k''$ can be zero, by the hypothesis of Theorem 1.

Lemma 6. *We have, for all k,*

$$A_k > 0\,, \quad A_k \geqq C A_{k+1}\,, \tag{46}$$

$$|A_{k+1}'| \geqq C|A_k'|\,, \tag{47}$$

$$|A_k A_{k+1}' A_{k+1}''| < \frac{1}{\sqrt{2}} \Delta^{-1} C^6\,. \tag{48}$$

Proof. This is simply a restatement of (34), (35), (36), which is immediate by (41).

Lemma 7. *We have, for all k,*

$$|A_k \beta_k| \leqq \frac{1}{\sqrt{2}}\,, \qquad |A_k \gamma_k| \leqq \frac{1}{\sqrt{2}}\,, \tag{49}$$

$$|A_k' \beta_k'| \leqq \frac{3}{2\sqrt{2}}\,, \qquad |A_k' \gamma_k'| \leqq \frac{3}{2\sqrt{2}}\,. \tag{50}$$

Proof. By definition,

$$\beta_k = i\Delta(\Gamma_k' A_k'' - \Gamma_k'' A_k')\,,$$

hence

$$|A_k \beta_k| \leqq 2\Delta|A_k \Gamma_k' A_k'|\,.$$

By (43) and the inequality of the arithmetic and geometric means,

$$2R^{\frac{1}{2}}|A_k A_k'| \leqq \tfrac{1}{2}\mathcal{A}_k\,.$$

Also, by (45),

$$2R^{-\frac{1}{2}}|\Gamma_k'| \leqq (\mathcal{C}_k)^{\frac{1}{2}}\,.$$

Hence

$$|A_k\beta_k| \leqq \tfrac{1}{4}\Delta(\mathcal{H}_k^2\mathcal{C}_k)^{\frac{1}{2}} \leqq \tfrac{1}{4}\Delta(8\Delta^{-2})^{\frac{1}{2}} = \frac{1}{\sqrt{2}}\,,$$

by (38) and (39). The same method proves the second inequality of (49); in the final step $\mathcal{H}_k^2\mathcal{C}_k$ is replaced by $\mathcal{H}_k^2\mathcal{B}_k$.

Again, by definition,

$$\beta_k' = i\Delta(\Gamma_k''A_k - \Gamma_k A_k'')\,,$$

hence

$$|A_k'\beta_k'| \leqq \Delta|A_kA_k'\Gamma_k'| + \Delta|A_k'|^2|\Gamma_k|\,.$$

The first term on the right has already been estimated above as not exceeding $\dfrac{1}{2\sqrt{2}}$. For the second term, we have

$$4R^{-1}|A_k'|^2 \leqq \mathcal{H}_k\,, \quad R|\Gamma_k| \leqq (\mathcal{C}_k)^{\frac{1}{2}}\,,$$

by (43) and (45), whence

$$\Delta|A_k'|^2|\Gamma_k| \leqq \tfrac{1}{4}\Delta(\mathcal{H}_k^2\mathcal{C}_k)^{\frac{1}{2}} \leqq \frac{1}{\sqrt{2}}\,.$$

It follows that

$$|A_k'\beta_k'| \leqq \frac{3}{2\sqrt{2}}\,,$$

and the same method proves the second inequality of (50).

Definition. We observe that, by the definitions of $\alpha_k, \ldots, \gamma_k''$ we have

$$A_k\beta_k + A_k'\beta_k' + A_k''\beta_k'' = 0\,, \tag{51}$$

$$A_k\gamma_k + A_k'\gamma_k' + A_k''\gamma_k'' = 0\,. \tag{52}$$

Hence we can write

$$\begin{cases} A_k'\beta_k' = -\tfrac{1}{2}A_k\beta_k + i\sigma_k\,, \\ A_k'\gamma_k' = -\tfrac{1}{2}A_k\gamma_k + i\tau_k\,, \end{cases} \tag{53}$$

where σ_k and τ_k are real. Note that

$$\sigma_k\gamma_k - \tau_k\beta_k = -iA_k'(\beta_k'\gamma_k - \beta_k\gamma_k') = -\Delta A_k'A_k'' \neq 0\,. \tag{54}$$

Lemma 8. *There exist, for every integer k, integers p_k, q_k, such that*

$$\frac{1}{2\sqrt{2}} < A_k(p_k\beta_k + q_k\gamma_k) \leqq \frac{1}{\sqrt{2}}\,, \tag{55}$$

$$|A_k'(p_k\beta_k' + q_k\gamma_k')| \leqq \frac{9}{2\sqrt{2}}\,. \tag{56}$$

Proof. For brevity of writing, we omit the suffix k in the proof. First we observe that, by (49), we can satisfy (55) with $q = 0$ and $p = \pm 1$ or ± 2 or ± 3 unless $A|\beta| \leqq \frac{1}{6\sqrt{2}}$. If we can do this, then (56) is satisfied, since

$$3|A'\beta'| \leqq \frac{9}{2\sqrt{2}},$$

by (50). Similarly if $A|\gamma| > \frac{1}{6\sqrt{2}}$. Hence we may suppose that

$$A|\beta| \leqq \frac{1}{6\sqrt{2}}, \quad A|\gamma| \leqq \frac{1}{6\sqrt{2}}. \tag{57}$$

Suppose, without loss of generality, that $|\sigma| \geqq |\tau|$. Note that $\sigma \neq 0$, by (54). For any integer q we can determine an integer p so that

$$|p+\frac{\tau}{\sigma}q| \leqq \frac{1}{2}.$$

If we can choose q so that

$$\frac{1}{2\sqrt{2}}+\frac{1}{2}A|\beta| < A\left(-\frac{\tau}{\sigma}\beta q+\gamma q\right) \leqq \frac{1}{\sqrt{2}}-\frac{1}{2}A|\beta|, \tag{58}$$

then (55) will be satisfied. Also (56) will be satisfied, since

$$\begin{aligned}|A'\beta'p+A'\gamma'q| &\leqq \frac{1}{2}A|\beta p+\gamma q|+|\sigma p+\tau q| \\ &\leqq \frac{1}{2\sqrt{2}}+\frac{1}{2}|\sigma| \\ &\leqq \frac{1}{2\sqrt{2}}+\frac{1}{4}A|\beta|+\frac{1}{2}|A'\beta'|, \\ &\leqq \frac{1}{2\sqrt{2}}+\frac{1}{4\sqrt{2}}+\frac{3}{4\sqrt{2}},\end{aligned}$$

by (53), (55).

It remains to choose q to satisfy (58). This is possible if

$$\frac{1}{\sqrt{2}}-\frac{1}{2\sqrt{2}}-A|\beta| \geqq A\left|\frac{\tau\beta-\gamma\sigma}{\sigma}\right|. \tag{59}$$

Now, in fact, since $|\tau| \leqq |\sigma|$,

$$A\left|\frac{\tau\beta-\gamma\sigma}{\sigma}\right| \leqq A|\beta|+A|\gamma| ,$$

and

$$A|\beta|+A|\gamma| \leqq \frac{1}{\sqrt{2}}-\frac{1}{2\sqrt{2}}-A|\beta|$$

by (57). Hence (59) is true, and this proves the result.

4. Proof of Theorem 1.

Theorem 1 asserts, in effect, that there exist a real number λ and a complex number λ' such that

$$|(\xi+\lambda)(\xi'+\lambda')(\xi''+\lambda'')| \geqq c\Delta$$

for all integers u, v, w, where ξ, ξ', ξ'' are the linear forms (1), of determinant $i\Delta$, and λ'' is the complex conjugate of λ'. By an integral unimodular substitution on the variables, we can transform ξ, ξ', ξ'' into $\alpha_0u+\beta_0v+\gamma_0w$, etc. Hence it suffices to determine $\lambda_0, \lambda_0', \lambda_0''$ so that

(60) $$|(\alpha_0u+\beta_0v+\gamma_0w+\lambda_0)(\alpha_0'u+\beta_0'v+\gamma_0'w+\lambda_0')(\alpha_0''u+\beta_0''v+\gamma_0''w+\lambda_0'')| \geqq c\Delta$$

for all integers u, v, w.

We shall achieve this by the definitions

(61) $$\lambda_0 = \sum_{r=-\infty}^{0} (p_r\beta_r+q_r\gamma_r) ,$$

(62) $$-\lambda_0' = \sum_{r=1}^{\infty} (p_r\beta_r'+q_r\gamma_r') ,$$

(63) $$-\lambda_0'' = \sum_{r=1}^{\infty} (p_r\beta_r''+q_r\gamma_r'') ,$$

where p_r, q_r are the integers determined in Lemma 8, provided that C is taken to be sufficiently large. These series are absolutely convergent, since

$$0 < p_r\beta_r+q_r\gamma_r \leqq \frac{1}{\sqrt{2}A_r} ,$$

$$|p_r\beta_r'+q_r\gamma_r'| \leqq \frac{9}{2\sqrt{2}|A_r'|} ,$$

and A_r, A_r' satisfy (46) and (47). Also λ_0 is real and λ_0'' is the complex conjugate of λ_0'. We define λ_k, λ_k', λ_k'' for all integers k by similar series:

(64)
$$\lambda_k = \sum_{r=-\infty}^{k} (p_r\beta_r+q_r\gamma_r) ,$$

(65)
$$-\lambda_k' = \sum_{r=k+1}^{\infty} (p_r\beta_r'+q_r\gamma_r') ,$$

(66)
$$-\lambda_k'' = \sum_{r=k+1}^{\infty} (p_r\beta_r''+q_r\gamma_r'') .$$

By (55), (46) we have

$$\frac{1}{2\sqrt{2}} < A_k\lambda_k \leqq \frac{1}{\sqrt{2}} + \sum_{r=-\infty}^{k-1} A_k(p_r\beta_r+q_r\gamma_r)$$

$$\leqq \frac{1}{\sqrt{2}}\left\{1+\sum_{r=-\infty}^{k-1}\frac{A_k}{A_r}\right\}$$

$$\leqq \frac{1}{\sqrt{2}}\left\{1+\sum_{r=-\infty}^{k-1} C^{r-k}\right\} ,$$

i. e.

(67)
$$\frac{1}{2\sqrt{2}} < A_k\lambda_k \leqq \frac{C}{\sqrt{2}(C-1)} .$$

Also, from (56) and (47),

(68)
$$|A_k'\lambda_k'| \leqq \frac{9}{2\sqrt{2}}\sum_{r=k+1}^{\infty}\left|\frac{A_k'}{A_r'}\right| \leqq \frac{9}{2\sqrt{2}(C-1)} .$$

Suppose there exist integers u, v, w which violate (60). Write

(69)
$$\xi_0 = \alpha_0 u+\beta_0 v+\gamma_0 w , \quad \text{etc.} ,$$

so that our hypothesis is that

(70)
$$|(\xi_0+\lambda_0)(\xi_0'+\lambda_0')(\xi_0''+\lambda_0'')| < c\Delta .$$

Define ξ_k, ξ_k', ξ_k'' for all integers k by the recurrence relations

(71)
$$\xi_{k-1} = p_k\beta_k+q_k\gamma_k+\xi_k , \quad \text{etc.} .$$

Then, in virtue of (64), (65), (66) and (71), we have

(72)
$$\xi_0+\lambda_0 = \xi_k+\lambda_k , \ \xi_0'+\lambda_0' = \xi_k'+\lambda_k' , \ \xi_0''+\lambda_0'' = \xi_k''+\lambda_k''$$

for all k. It is important to observe that ξ_k, ξ_k', ξ_k'' are values of the linear forms ξ, ξ', ξ'' which arise from integral values of the variables.

We now define a particular integer k by the condition

$$\frac{C^2 c^{\frac{1}{3}}}{A_{k-1}} \leqq |\xi_0+\lambda_0| < \frac{C^2 c^{\frac{1}{3}}}{A_k}, \tag{73}$$

which is uniquely soluble for k unless $\xi_0+\lambda_0 = 0$ (a case which we return to in a moment). By (70) we have

$$\begin{aligned} |\xi_0'+\lambda_0'|^2 &< c\Delta A_{k-1} C^{-2} c^{-\frac{1}{3}} \\ &< c\Delta\left(\frac{1}{\sqrt{2}}\Delta^{-1} C^6 |A_k'|^{-2}\right) C^{-2} c^{-\frac{1}{3}} \\ &< C^4 c^{\frac{2}{3}} |A_k'|^{-2}, \end{aligned}$$

using (48). Thus

$$|\xi_0'+\lambda_0'| < \frac{C^2 c^{\frac{1}{3}}}{|A_k'|}. \tag{74}$$

In the case when $\xi_0+\lambda_0 = 0$, we simply choose k so large that (74) holds.

Since $\xi_0+\lambda_0 = \xi_k+\lambda_k$, etc., and since ξ_k, ξ_k', ξ_k'' are values of the linear forms ξ, ξ', ξ'', this gives us the existence of integers u, v, w such that

$$\begin{aligned} |\alpha_k u+\beta_k v+\gamma_k w+\lambda_k| &< \frac{C^2 c^{\frac{1}{3}}}{A_k}, \\ |\alpha_k' u+\beta_k' v+\gamma_k' w+\lambda_k'| &< \frac{C^2 c^{\frac{1}{3}}}{|A_k'|}, \\ |\alpha_k'' u+\beta_k'' v+\gamma_k'' w+\lambda_k''| &< \frac{C^2 c^{\frac{1}{3}}}{|A_k''|}. \end{aligned}$$

If we multiply the homogeneous linear expressions on the left by A_k, A_k', A_k'' and add, we obtain simply u. Hence

$$|u+A_k\lambda_k+A_k'\lambda_k'+A_k''\lambda_k''| < 3C^2 c^{\frac{1}{3}}. \tag{75}$$

But, by (67) and (68),

$$\frac{1}{2\sqrt{2}} - \frac{9}{\sqrt{2}(C-1)} < A_k\lambda_k+A_k'\lambda_k'+A_k''\lambda_k'' \leqq \frac{C}{\sqrt{2}(C-1)} + \frac{9}{\sqrt{2}(C-1)}.$$

This contradicts (75) if c is chosen to satisfy both

$$3C^2 c^{\frac{1}{3}} < \frac{1}{2\sqrt{2}} - \frac{9}{\sqrt{2}(C-1)} \tag{76}$$

and

$$3C^2 c^{\frac{1}{3}} < 1 - \frac{C}{\sqrt{2}(C-1)} - \frac{9}{\sqrt{2}(C-1)}. \tag{77}$$

It is plain that if C is suitably chosen as a large positive constant, these can be satisfied by a positive value of c. Thus the hypothesis (70) has led to a contradiction, and this proves Theorem 1.

The second of (76), (77) is always more stringent than the first. If we choose $C = 37 \cdot 5$, we find that 8×10^{13} is a legitimate value for c^{-1}.

5. Preliminary Lemmas for the Proof of Theorem 2.

The hypothesis of Theorem 2 is that the ternary cubic form

$$f(u, v, w) = (\alpha u + \beta v + \gamma w)(\alpha' u + \beta' v + \gamma' w)(\alpha'' u + \beta'' v + \gamma'' w) \tag{78}$$

has integral coefficients, and is not zero for integral values of u, v, w other than 0, 0, 0. We proceed to develop some consequences of this hypothesis. In the course of this we shall see (in Lemma 11) that the above hypothesis implies that the adjoint forms Ξ, Ξ', Ξ'' also do not represent zero; a hypothesis which was made explicitly in Theorem 1.

Lemma 9. *There exists a cubic field K of negative discriminant, and there exist algebraic integers $\alpha^*, \beta^*, \gamma^*$ in K, such that*

$$mf(u, v, w) = N(\alpha^* u + \beta^* v + \gamma^* w)$$

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

This is a classical result; for a proof see Bachmann, *loc. cit.*, Kap. 12, §§ 1, 2, 3.

Remark. If we prove Theorem 2 for the ternary cubic form $mf(u, v, w)$, its conclusion will also hold for $f(u, v, w)$, by considerations of homogeneity. To avoid the introduction of new symbols, we shall therefore assume henceforward that in (78), α, β, γ are algebraic integers of K, and $\alpha', \ldots$ are their algebraic conjugates in some fixed order. Since the determinant of the linear forms in (78) is then an integral multiple of the square root of the discriminant of K, we have

$$i\Delta = ih\sqrt{d}\,, \tag{79}$$

where h is a positive integer and $-d$ is the discriminant of K.

Lemma 10. *The numbers A, B, Γ are linearly independent numbers of K, and their algebraic conjugates are A', B', Γ' and A'', B'', Γ''.*

Proof. Let ϑ be a cubic irrationality which generates K. Then

$$\begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix} = \begin{pmatrix} 1 & \vartheta & \vartheta^2 \\ 1 & \vartheta' & \vartheta'^2 \\ 1 & \vartheta'' & \vartheta''^2 \end{pmatrix} \times \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{pmatrix},$$

where the p_{rs} are rational numbers, whose determinant is obviously not zero. Hence, by the definition of $A, \ldots, \Gamma''$ in § 3,

$$\begin{pmatrix} A & B & \Gamma \\ A' & B' & \Gamma' \\ A'' & B'' & \Gamma'' \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ \vartheta & \vartheta' & \vartheta'' \\ \vartheta^2 & \vartheta'^2 & \vartheta''^2 \end{pmatrix}^{-1} \times \begin{pmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{22} & q_{23} \\ q_{31} & q_{32} & q_{33} \end{pmatrix},$$

with rational numbers q_{rs}. The reciprocal matrix on the right has for its first row

$$\frac{\vartheta'\vartheta''}{(\vartheta-\vartheta')(\vartheta-\vartheta'')}, \quad -\frac{\vartheta'+\vartheta''}{(\vartheta-\vartheta')(\vartheta-\vartheta'')}, \quad \frac{1}{(\vartheta-\vartheta')(\vartheta-\vartheta'')},$$

and its other rows are obtained by cyclic permutation of $\vartheta, \vartheta', \vartheta''$. It is plain that these three numbers are linearly independent numbers of K, and that the cyclic permutation produces their algebraic conjugates in the same order as it produces those of α, β, γ. Hence the same is true of A, B, Γ, which are linear combinations of the above three numbers with rational coefficients whose determinant is not zero.

Lemma 11. *If Ξ, Ξ', Ξ'' are the linear forms defined by* (7), *then $\Delta^4\Xi\Xi'\Xi''$ is a ternary cubic form in U, V, W with integral coefficients, and is not zero for integral U, V, W, not all zero.*

Proof. By Lemma 10, A is an element of K and A', A'' are its conjugates in some fixed order. Similarly for B and Γ. Hence the coefficients in the product

$$\Xi\Xi'\Xi'' = (AU+BV+\Gamma W)(A'U+B'V+\Gamma'W)(A''U+B''V+\Gamma''W)$$

are rational. Also, since A, B, Γ are linearly independent, the product is not zero if U, V, W are integers, not all zero. Note also that Δ^4 is rational, by (79).

Moreover, since $i\Delta A = \beta'\gamma''-\beta''\gamma'$, etc., and α, β, γ are algebraic integers, it follows that $\Delta A, \Delta B, \Delta\Gamma$ are algebraic integers. As Δ is also an algebraic integer, by (79), it follows that the coefficients in the product $\Delta(\Delta\Xi)(\Delta\Xi')(\Delta\Xi'')$ are both rational, and algebraic integers, and so are integers.

6. Further Lemmas.

We know, by the work of § 3, that it is possible to find a set of integral unimodular substitutions, one for every integer k, which transform the linear forms

$\varXi, \varXi', \varXi''$ into those given in (40), such that the coefficients $A_k, \ldots, \Gamma_k''$ satisfy (43), (44), (45) [with (38), (39)] and (46), (47), (48). The assertion of Lemma 10 will obviously be valid for A_k, B_k, Γ_k. Our next lemma asserts that it is possible to do this in such a way that $A_k, \ldots, \Gamma_k''$ have an important additional property.

Lemma 12. *There exists a set of integral unimodular substitutions, one for every integer k, transforming the linear forms $\varXi, \varXi', \varXi''$ into those given in* (40), *with the following properties. First,* (43), (44), (45), [*with* (38), (39)] *and* (46), (47), (48) *are valid for all k. Secondly, there exists a positive integer j such that*

$$A_k = \omega A_{k+j}\,, \quad B_k = \omega B_{k+j}\,, \quad \Gamma_k = \omega \Gamma_{k+j} \tag{80}$$

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

$$\omega > 1\,, \quad \omega\omega'\omega'' = 1\,. \tag{81}$$

Proof.[1] We begin by considering the situation of § 3, and use the notation of that section. Let

$$F_k(U,\, V,\, W) = (A_k U + B_k V + \Gamma_k W)(A_k' U + B_k' V + \Gamma_k' W)(A_k'' U + B_k'' V + \Gamma_k'' W)\,. \tag{82}$$

By Lemma 11, $\varDelta^4 F_k(U, V, W)$ is a ternary cubic form with integral coefficients whose value for integral U, V, W is not zero unless U, V, W are all zero. We shall prove that all the coefficients in this ternary cubic form are bounded by a number independent of k.

Since

$$\varDelta^4 |F_k(U,\, V,\, W)| \geqq 1$$

for all integers U, V, W not all zero, we have, in particular,

$$A_k |A_k'|^2 \geqq \varDelta^{-4}\,.$$

Hence, by (43) and the inequality of the arithmetic and geometric means,

$$\mathscr{A}_k = R^2 A_k^2 + 4R^{-1} |A_k'|^2 \geqq 3(4A_k^2 |A_k'|^4)^{\frac{1}{3}} \geqq 3(4\varDelta^{-8})^{\frac{1}{3}}\,.$$

It follows now from (38) and (39) that $\mathscr{A}_k$, $\mathscr{B}_k$, $\mathscr{C}_k$ are bounded by a number independent of k. By (43), (44), (45),

$$RA_k\,, \quad RB_k\,, \quad R\Gamma_k\,, \quad R^{-1}|A_k'|^2, \quad R^{-1}|B_k'|^2, \quad R^{-1}|\Gamma_k'|^2$$

are bounded. It is now clear from (82) that all the coefficients in $F_k(U, V, W)$ are bounded.

[1] The argument here is again essentially due to Hermite.

As there are only a finite number of possibilities for the form $F_k(U, V, W)$, there must exist integers g, j, with $j > 0$, such that

$$F_g(U, V, W) = F_{g+j}(U, V, W)$$

identically in U, V, W. This implies that the linear factors in $F_g(U, V, W)$ are proportional to those in $F_{g+j}(U, V, W)$, in some order, with constants of proportionality whose product is 1. Now A_g, B_g, Γ_g are linearly independent elements of K, and so are A_{g+j}, B_{g+j}, Γ_{g+j}. It is impossible that the ratios $A_g{:}B_g{:}\Gamma_g$ should be the same as the ratios $A'_{g+j} : B'_{g+j} : \Gamma'_{g+j}$; for this would imply that A_g/B_g would be in both K and K', and so would be rational, contrary to the fact that A_g and B_g are linearly independent elements of K. The only possibility is that

$$\begin{aligned} A_g U + B_g V + \Gamma_g W &= \omega\ (A'_{g+j}U + B'_{g+j}V + \Gamma'_{g+j}W)\,, \\ A'_g U + B'_g V + \Gamma'_g W &= \omega'\,(A'_{g+j}U + B'_{g+j}V + \Gamma'_{g+j}W)\,, \\ A''_g U + B''_g V + \Gamma''_g W &= \omega''(A''_{g+j}U + B''_{g+j}V + \Gamma''_{g+j}W)\,, \end{aligned}$$

identically in U, V, W, where $\omega, \omega', \omega''$ are numbers with $\omega\omega'\omega'' = 1$. Plainly $\omega = A_g/A_{g+j}$ is a number of K, and ω', ω'' are its algebraic conjugates. Also $\omega > 1$, by (46).

We adopt the existing definition of A_k, B_k, Γ_k for $g \leqq k \leqq g+j$, but proceed to modify it for $k < g$ and $k > g+j$, which we do by adopting (80) as *defining* A_k, B_k, Γ_k for such values of k. Then (46), (47), (48) are valid for $g \leqq k < g+j$ by the original definition, and follow by recurrence, using (80), for $k < g$ and $k \geqq g+j$.

We modify the definition of R_k by defining R_k for $k < g$ and $k \geqq g+j$ by the recurrence relation

$$R_{k+j} = \omega R_k\,.$$

This definition still preserves the minimal property (33) when $k = g+j$. Also we define $\mathcal{A}_k$, $\mathcal{B}_k$, $\mathcal{C}_k$ for $k < g$ and $k \geqq g+j$ by the recurrence relations

$$\mathcal{A}_{k+j} = \mathcal{A}_k\,, \quad \mathcal{B}_{k+j} = \mathcal{B}_k\,, \quad \mathcal{C}_{k+j} = \mathcal{C}_k\,.$$

Again, this is legitimate for $k = g+j$, and (43), (44), (45) [with (38), (39)] are now valid for all k. This completes the proof of Lemma 12.

Lemma 13. *If α_k, β_k, γ_k are defined in terms of the A_k, B_k, Γ_k of Lemma* 12 *by the same method as in* § 3, *then*

$$\alpha_{k+j} = \omega\alpha_k\,, \quad \beta_{k+j} = \omega\beta_k\,, \quad \gamma_{k+j} = \omega\gamma_k\,, \tag{83}$$

and similarly for their conjugates, for all k. Also (49) *and* (50) *are valid for all k.*

Proof. As (49) and (50) depend only on (43), (44), (45) [with (38), (39)] and (46), (47), (48), their validity is assured, by Lemma 12. As regards (83), we have, for example,

$$\begin{aligned} \alpha_k &= i\Delta\,(B'_k\Gamma''_k - B''_k\Gamma'_k) \\ &= i\Delta\,(B'_{k+j}\Gamma''_{k+j} - B''_{k+j}\Gamma'_{k+j})\omega'\omega'' \\ &= \frac{1}{\omega}\,\alpha_{k+j}\,, \end{aligned}$$

by (80) and (81).

Lemma 14. *Integers* p_k, q_k *can be chosen for all* k *to satisfy* (55) *and* (56), *and also*

(84) $$p_k = p_{k+j}\,, \quad q_k = q_{k+j}\,.$$

Proof. By (80) and (83),

$$A_{k+j}\beta_{k+j} = A_k\beta_k\,, \quad A_{k+j}\gamma_{k+j} = A_k\gamma_k\,,$$

and similarly for the conjugates. Thus the inequalities (55), (56) are unaltered in meaning if k is replaced by $k+j$, and the result is trivial.

7. Proof of Theorem 2.

It suffices to prove that the numbers λ_0, λ'_0, λ''_0, defined by (61), (62), (63), using the definitions of A_k, ..., α_k, ..., p_k, q_k given in § 6, are such that λ_0 is a number of K and λ'_0, λ''_0 are its algebraic conjugates. By Lemmas 13 and 14, and (61), we have

$$\begin{aligned} \lambda_0 &= \sum_{r=-\infty}^{0} (p_r\beta_r + q_r\gamma_r) \\ &= \sum_{r=1}^{j}\sum_{s=1}^{\infty} (p_r\beta_{r-sj} + q_r\gamma_{r-sj}) \\ &= \sum_{r=1}^{j}\sum_{s=1}^{\infty} (p_r\beta_r + q_r\gamma_r)\,\omega^{-s} \\ &= \left\{\sum_{r=1}^{j} (p_r\beta_r + q_r\gamma_r)\right\}(\omega-1)^{-1}\,. \end{aligned}$$

Again, by Lemmas 13 and 14, and (62),

$$\begin{aligned}-\lambda_0' &= \sum_{r=1}^{\infty} (p_r\beta_r'+q_r\gamma_r') \\ &= \sum_{r=1}^{j}\sum_{s=0}^{\infty} (p_r\beta_r'+q_r\gamma_r')(\omega')^s \\ &= \left\{\sum_{r=1}^{j} (p_r\beta_r'+q_r\gamma_r')\right\}(1-\omega')^{-1}\,.\end{aligned}$$

Similarly for λ_0''. From these expressions it is clear that λ_0 is a number of K and that λ_0', λ_0'' are its algebraic conjugates.