Nach (46) bekommt man also für $0 < q \leqslant b-a$

(340) $$a^{-1/2}S(a,b) \ll (a/q)^{1/2} + (tq)^{1/7} + (tq)^{13/56}a^{-1/4} + (a^3/tq)^{1/4} + (tq/a)^{1/5}.$$

Hierzu bemerken wir, daß wegen (49) und (50) die Ungleichung

(341) $$(a^3/tq)^{1/4} \leqslant (a/q)^{1/2} \quad \text{für} \quad 0 < q \leqslant b-a$$

gilt.

Nun sei speziell

$$q = a^{7/9}t^{-2/9}.$$

Dann stimmen die beiden ersten Terme auf der rechten Seite von (340) überein. Wenn also außerdem $q \leqslant b-a$ ist, so folgt in Verbindung mit (341)

(342) $$a^{-1/2}S(a,b) \ll (at)^{1/9} + (at)^{13/72}a^{-1/4} + (a^{-2/9}t^{7/9})^{1/5}.$$

Dies gilt aber auch im Falle $q > b-a$, da dann aus (49) und (50) mit der trivialen Abschätzung

$$a^{-1/2}S(a,b) \ll q+1 = a^{7/9}t^{-2/9}+1 \ll (at)^{1/9}$$

folgt.

Damit ist (342) unter den Voraussetzungen (49) und (50) bewiesen. Nun folgt aber aus (339)

$$(at)^{1/9} \ll t^{6/37}.$$

Im Falle $a > t^{10/37}$ ist

$$(at)^{13/72}a^{-1/4} = t^{13/72}a^{-5/72} \ll t^{6/37},$$

und wegen $a \geqslant 1$ ist jedenfalls

$$(a^{-2/9}t^{7/9})^{1/5} \ll t^{7/45} \ll t^{6/37}.$$

Die Abschätzung (336) folgt also im Falle $a > t^{10/37}$ aus (342). Im Falle $a \leqslant t^{10/37}$ ist (336) trivial.

Wegen (48) ist damit unser Hauptsatz bewiesen.

Literaturverzeichnis

[1] H. Behnke und F. Sommer, *Theorie der analytischen Funktionen einer komplexen Veränderlichen*, Berlin 1955.

[2] R. Fricke, *Lehrbuch der Algebra*, Bd. 1, Braunschweig 1924.

[3] S. H. Min, *On the order of $\zeta(\frac{1}{2}+it)$*, Trans. Amer. Math. Soc. 65 (1949), S. 448-472.

[4] E. Pascal, *Repertorium der höheren Mathematik*, Bd. 1, Leipzig und Berlin 1910.

[5] E. C. Titchmarsh, *On Epstein's Zeta-Function*, Proc. London Math. Soc. (2) 36 (1934), S. 485-500.

[6] — *On the order of $\zeta(\frac{1}{2}+it)$*, Quart. J. Math. Oxford Ser. 13 (1942), S. 11-17.

[7] — *The theory of the Riemann Zeta-Function*, Oxford 1951.

[8] B. L. van der Waerden, *Algebra I*, Berlin 1955.

Reçu par la Rédaction le 27. 2. 1963

ACTA ARITHMETICA
VIII (1963)

On the genera of quadratic and hermitian forms over an algebraic number field

by

V. C. Nanda (Bombay)

§ 1. Introduction. Pursuing the study of the theory of genera of quadratic forms initiated by Gauss, Minkowski [6] defined a genus of rational integral quadratic forms, in any number of variables, to consist of all forms which are equivalent in the real number field and modulo all positive integers. He then showed that all forms in a genus have the same signature, determinant s and class mod $8s^3$, and that these finitely many invariants determine a genus completely. C. L. Siegel [7] gave an alternative proof of this result, and also obtained a finite set of genus invariants for forms with coefficients in an algebraic number field [8].

The converse problem of proving the existence of a genus of rational integral quadratic forms with prescribed invariants was also solved by Minkowski. H. Braun [1] later gave another set of invariants and a solution of the corresponding converse problem. She [2] also extended the results of Minkowski to hermitian forms over an imaginary quadratic extension of the rational number field.

In this paper we consider quadratic and hermitian forms over an arbitrary algebraic number field. We prove that a genus of hermitian forms can be defined by means of a finite set of invariants. We also prove the existence of genera of quadratic and hermitian forms with prescribed invariants. We use the methods of H. Braun in the proof of our results.

The main difficulty in this discussion is caused by the fact that, unlike in the case of the rational number field, the ring of integers in an algebraic number field is not, in general, a principal ideal domain, so that it is also necessary to take into account singular matrices. For this purpose, the reciprocity formula for Gauss sums (an important tool in the proof), is generalized to cover the case of singular matrices (Lemma 5). This formula appears to be of interest, independently of the application that we make of it.

Our results can be applied to simplify, and to generalize to arbitrary quadratic or hermitian forms over any algebraic number field, a formula originating in the work of Gauss, and proved for totally definite forms over totally real fields by Siegel ([8], Lemmas 92, 93). This formula constitutes an important step in the proof of Siegel's main theorem. We hope to give this generalization elsewhere. The author wishes to express his sincere thanks to Professor K. G. Ramanathan for constant encouragement and guidance throughout the preparation of this paper.

§ 2. Notation and definitions. Let K be an algebraic number field with an automorphism τ satisfying $\tau^2 = 1 =$ the identity automorphism. Let k be the fixed field of τ. If $\tau = 1$, then $k = K$. If $\tau \neq 1$, K is the field of rational functions of the square root of a number $d \in k$, and then $(a+b\sqrt{d})^\tau = a-b\sqrt{d}$, where $a, b \in k$. Let $\mathfrak{o}$ and $\mathfrak{O}$ denote respectively, the rings of integers in k and K. We choose $d \in \mathfrak{o}$, not divisible by the square of an integer, other than a unit. In case $\tau = 1$, we always assume that $d = 1$.

Let $\mathfrak{a}$ denote the extension to K of an ideal in k briefly denoted as a *k-ideal*. For an integral k-ideal $\mathfrak{a}$, denote by $R(\mathfrak{a})$, the residue class ring $\mathfrak{O}/\mathfrak{a}$. It is easy to see that τ gives rise in a natural way to an automorphism of $R(\mathfrak{a})$. We denote this automorphism also by τ.

Let R denote any of the rings $K, \mathfrak{O}, R(\mathfrak{a})$. Let $S = (s_{ij})$ be a matrix with $s_{ij} \in R$ (we use the notation $S \in R$ to express this fact, the number of rows and columns being, in general, understood from the context). If $S^\tau = (s_{ij}^\tau) = S'$, then S is defined to be a *hermitian matrix* (h-matrix), and the expression $S[X] = X^{\tau'}SX$ a *hermitian form* (h-form); here $X' = (x_1, \ldots, x_{m_1})$ is a row varying over R (in particular, therefore, S has m_1 rows and columns). In the particular case when $\tau = 1$, S is *symmetric* (s-matrix) and $S[X]$ is a *quadratic form* (q-form). In the following, the statements about h-forms will, in general, include statements about q-forms.

Let $T[Y]$, where $Y' = (y_1, \ldots, y_{m_2})$ be another h-form in R. We say that *S represents T in R* or that $S[X]$ represents $T[Y]$ in R (all statements made about h-matrices are also assumed made about h-forms), if there exists a matrix $C \in R$ such that $S[C] = T$. C is called a *representation of T by S in R*. If T also represents S in R, then we say that S and T are *equivalent in R* ($S \sim T$ in R). This is an equivalence relation and a *class in R* is defined to be a complete set of equivalent matrices.

In R, all equivalent matrices have the same rank, called the *rank of the class*. It may be shown as in [2], Lemma 5, that if further, every ideal in R is a finite R-module, generated by r elements, then in every class of rank m, there is a matrix of rm rows. If R is a field of characteristic either zero, or coprime with $2d$, then there is a diagonal matrix of m rows in a class of rank m.

For a matrix $A \in R$, a matrix $E_A \in \mathfrak{O}$ is called a *right unit* (r-unit) if rank $r(E_A)$ of $E_A = r(A)$ and $AE_A = A$. For a *left unit* (l-unit), similarly defined, we use the notation E_A^*. Siegel ([8], Lemma 9) has proved the existence of these units. For an r-unit E_A and an l-unit E_A^* of $A \in K$, the unique solution X, in K ([8], Lemma 12) of $AX = E_A^*$, $E_AX = X$ is called the *$E_AE_A^*$ inverse* of A. We denote this matrix X by A^{-1} if there no danger of confusion. For $A \in K$ of rank m, $\delta(A) =$ *discriminant* of A is defined to be the ideal generated by all the m-rowed subdeterminants of A. For an h-matrix S, $\delta(S)$ is a k-ideal.

Let $S, T \in R$ be two h-matrices. A representation B of T by S in R is called an *E_SE_T reduced representation* if $E_SBE_T = B$. From any representation B_1, one can construct a reduced representation $B = E_SB_1E_T$.

A matrix $U \in \mathfrak{O}$ is called (a) *unimodular* if $|U| \neq 0$, and $U^{-1} \in \mathfrak{O}$, (b) *primitive* if $\delta(U) = \mathfrak{O}$ and (c) *primitive modulo an integral k-ideal* $\mathfrak{a}$ if $(\delta(U), \mathfrak{a}) = \mathfrak{O}$.

We adopt the notation $k^{(1)}, \ldots, k^{(r_1)}$ for the r_1 real and $k^{(r_1+1)}, k^{(r_1+r_2+1)}, \ldots, \ldots, k^{(r_1+r_2)}, k^{(r_1+2r_2)}$ for the r_2 conjugate-complex pairs of conjugates of k. For $a \in k$, $a^{(l)}$ denotes the conjugate of a belonging to $k^{(l)}$. In case $\tau \neq 1$, we assume further, the notation so chosen that $d^{(l)} < 0$ for $0 \leqslant l \leqslant r_\tau \leqslant r_1$. Define

$$r = \begin{cases} r_\tau & \text{if} \quad \tau \neq 1, \\ r_1 & \text{if} \quad \tau = 1. \end{cases}$$

For a matrix $A = (a_{ij}) \in k$, $A^{(l)}$ is defined to be $(a_{ij}^{(l)})$.

Let $S \in K$ be an h-matrix. Let $r(S) = m$, so that $S \sim T$ in K, where $T = [t_1 \ldots t_m] =$ the *diagonal matrix* with $t_1 \ldots t_m$ on the diagonal, $|T| \neq 0$ and $t_i \in k$. If $r > 0$, then for $l \leqslant r$, let u_l, v_l denote respectively the number of positive and negative elements of $T^{(l)}$. We define $\mathrm{sig}(S) =$ *the system of signatures of the h-matrix S* by

$$\mathrm{sig}(S) = \{(u_l, v_l)\}_{l=1,\ldots,r}, \qquad \text{or briefly} \qquad \{(u_l, v_l)\}.$$

For a number $a \in k$, $\mathrm{sgn}(a)$ is defined by

$$\mathrm{sgn}(a) = \left\{\frac{a^{(l)}}{|a^{(l)}|}\right\}_{l=1,\ldots,r}, \qquad \text{or briefly} \qquad \left\{\frac{a^{(l)}}{|a^{(l)}|}\right\}.$$

Let $S \in K$ be an h-matrix of rank m. Let T be a non-singular matrix such that $S = \begin{pmatrix} T & 0 \\ 0 & 0 \end{pmatrix}[A]$, $A \in K$. Let B denote the matrix of the first m rows of A. Then $S = T[B]$. It can be shown as in [8], Lemma 31, that the class of the ideal $\delta(B)$ is uniquely fixed by S. We call it the *ideal class of S*. Also fixed uniquely, therefore, is the set $\{|T| \cdot aa^\tau|, a \in K\}$ or briefly $\langle|T|\rangle$, called the *kernel* of S, denoted by $K(S)$.

h-matrices $S, T \in K$ are said to *belong to the same genus* if and only if $S \sim T$ modulo all integral k-ideals and $\mathrm{sig}(S) = \mathrm{sig}(T)$.

Capital Roman letters will, in general, be reserved for matrices, small Roman for numbers, capital Gothic for ideals in K, and small Gothic for k-ideals. For a square matrix X, $|X|$ denotes its determinant. For a number $a \in K$, (a) denotes the principal ideal generated by a, and $|a|$ the absolute value of a. $N\mathfrak{a}$ denotes the norm of the ideal $\mathfrak{a} \subset k$ over the rational number field Γ. $\sigma(a)$ denotes the trace of a number $a \in k$ over Γ. The letter $\mathfrak{d}$ is reserved for the different of the field k. E will denote the identity matrix and 0 the zero matrix of order clear from the context.

§ 3. Some preliminary results. In this section we prove several lemmas, which we use later in the proof of the main theorem in § 4.

LEMMA 1. *Let S, $T \in \mathfrak{O}$ be h-matrices of rank m. Let $\delta(S) = \delta(T) = \mathfrak{s}_0$. Let $\mathfrak{q}$ be a k-ideal such that $4\mathfrak{d}\mathfrak{s}_0 \mid \mathfrak{q}$. Let $\mathfrak{p}$ be the extension to K of a prime ideal in k* (briefly called a k-*prime ideal*), *and let $\mathfrak{p}^a \| \mathfrak{q}$ (i.e. $\mathfrak{p}^a \mid \mathfrak{q}$ and $\mathfrak{p}^{a+1} \nmid \mathfrak{q}$ with rational integral $a \geqslant 0$). Then $S \sim T \bmod \mathfrak{p}^l \Rightarrow S \sim T \bmod \mathfrak{p}^{l+l_1}$ for $l_1 \geqslant 0$ provided $l \geqslant a+1$.*

Proof. Let us suppose C_l is an integral matrix satisfying

$$(3.1) \qquad S[C_l] \equiv T \bmod \mathfrak{p}^l, \qquad E_S C_l E_T = C_l .$$

Let S^{-1} denote the $E_S E_S^{\tau\prime}$ inverse of S, C_l^{-1} the $E_T E_S$ inverse of C_l and $S_1 = S[C_l] - T$. From (3.1), $S_1 \in \mathfrak{p}^l$ and $E_T^{\tau\prime} S_1 E_T = S_1$. Define

$$C_{l+1} = C_l - \tfrac{1}{2} S^{-1} C_l^{\tau -1} S_1 .$$

Then $S[C_{l+1}] \equiv T \bmod \mathfrak{p}^{l+1}$ and C_{l+1} is $E_S E_T$ reduced. Also, since $l \geqslant a+1$, the denominators of elements of C_{l+1} are coprime with $\mathfrak{p}$. By repeating the procedure l_1 times we see that S represents $T \bmod \mathfrak{p}^{l+l_1}$.

Interchanging the roles of S and T, we get the lemma.

LEMMA 2. *Let $S, T, \mathfrak{s}_0$ be as in Lemma 1. Let $\mathfrak{p}$ be a k-prime ideal such that $\mathfrak{p} \nmid 2\mathfrak{d}\mathfrak{s}_0$. In case $\tau = 1$, let us assume further that $K(S) = K(T)$. Then $S \sim T \bmod \mathfrak{p}$.*

Proof. Case I: $\tau = 1$. The result follows trivially from [8], Lemma 56.

Case II: $\tau \neq 1$. We may, without loss of generality, assume S, T to be diagonal matrices. So that let $S = [s_1 \dots s_m]$, $T = [t_1 \dots t_m]$ where $s_i, t_i \in \mathfrak{o}$. Further $(\mathfrak{p}, \mathfrak{s}_0) = \mathfrak{O}$. Thus to prove Lemma 2, it suffices to show that *for a prime ideal $\mathfrak{p} \nmid (2\mathfrak{d})$, every element of $\mathfrak{o}$, which is coprime with $\mathfrak{p}$ is congruent* mod $\mathfrak{p}$ *to the relative norm of an element in $\mathfrak{O}$*. This is shown exactly as in [3], § 47.

This completes the proof of Lemma 2.

LEMMA 3. *Let $S, T \in \mathfrak{O}$ be h-matrices. Then S, T are in the same genus, if and only if $\mathrm{sig}(S) = \mathrm{sig}(T)$, $\delta(S) = \delta(T) = \mathfrak{s}_0$, $S \sim T \bmod \mathfrak{q}$, where $4\mathfrak{d}\mathfrak{s}_0\mathfrak{P} \mid \mathfrak{q}$, with*

$$(3.2) \qquad \mathfrak{P} = p(\mathfrak{s}_0) = \prod_{\substack{\mathfrak{p} \mid 2\mathfrak{d}\mathfrak{s}_0 \\ \mathfrak{p} = k\text{-prime ideal}}} \mathfrak{p} ,$$

and, in addition, in case $\tau = 1$, $K(S) = K(T)$.

Proof. Let S, T be in the same genus. Then $\mathrm{sig}(S) = \mathrm{sig}(T)$. Next, from $S[A] \equiv T \bmod \mathfrak{s}\mathfrak{t}$ where $\mathfrak{s} = \delta(S)$ and $\mathfrak{t} = \delta(T)$, $A \in \mathfrak{O}$, it follows that $\mathfrak{s} \mid \mathfrak{t}$. Similarly $\mathfrak{t} \mid \mathfrak{s}$. And therefore, $\mathfrak{s} = \mathfrak{t} = \mathfrak{s}_0$ (say). Trivially $S \sim T \bmod \mathfrak{q}$ and it is proved in [8], Lemma 63, that they have the same kernel in case $\tau = 1$.

Conversely $S \sim T \bmod \mathfrak{p}$ for $\mathfrak{p} \nmid \mathfrak{q}$ in view of Lemma 2, and we are given that $S \sim T \bmod \mathfrak{q}$. In view of Lemma 1, therefore, $S \sim T \bmod \mathfrak{p}^l$ for every k-prime ideal $\mathfrak{p}$ and positive integer l. Our result would be proved, if we show that $S \sim T \bmod \mathfrak{a}_1$ and $S \sim T \bmod \mathfrak{a}_2$ together imply $S \sim T \bmod \mathfrak{a}_1\mathfrak{a}_2$ provided that $(\mathfrak{a}_1, \mathfrak{a}_2) = \mathfrak{O}$. And this follows easily form the Chinese remainder theorem.

Lemma 3 is thus proved.

We next generalize a result of Siegel ([8], Lemma 33), to h-forms.

LEMMA 4. *Let $S \in \mathfrak{O}$ be an h-matrix, and let $\mathfrak{b}$ be an integral ideal in the ideal class of S. Then there exists a matrix $B \in \mathfrak{O}$ with $\delta(B) = \mathfrak{b}$, and a non-singular h-matrix $T = (t_{ij})$ such that $S = T[B]$ and $t_{ij}\mathfrak{b}\mathfrak{b}^\tau \subset \mathfrak{O}$ for all i, j.*

Proof. Let S be m_1-rowed, and let $r(S) = m$. For $m = m_1$, the assertion is trivial. Let us assume therefore that $m < m_1$.

We already know that $S = T_1[B_1]$, where T_1 is non-singular and $\delta(B_1) = \mathfrak{b}_1$ belongs to the ideal class of S. By [8], Lemma 8, there exists a non-singular matrix F, and a unimodular matrix U, such that

$$FB_1U = \begin{pmatrix} E & 0 \\ 0 & B_2 \end{pmatrix}$$

where E is the $(m-1)$-rowed identity matrix, and $B_2 = (b_1 \dots b_{m_1-m+1})$. Clearly the g.c.d. $(b_1, \dots, b_{m_1-m+1}) = \delta(FB_1) = |F| \cdot \mathfrak{b}_1 = \mu\mathfrak{b}$ where $0 \neq \mu \in K$. We can actually assume $\mu = 1$ (for, by multiplying the last row of F by μ^{-1}, we can achieve the same). Define

$$T = T_1[F^{-1}], \qquad B = FB_1 .$$

Then we have $S = T[B]$, B integral, $\delta(B) = \mathfrak{b}$ and T non-singular. We still have to show that all $t_{ij}\mathfrak{b}\mathfrak{b}^\tau$ are integral. For this purpose, we consider all the m-rowed submatrices $A_1, \dots, A_t$ of B. Let $a_1, \dots, a_t$ be their respective determinants. Then $(a_1, \dots, a_t) = \mathfrak{b}$. Since $S = T[B]$, the matrices $T[A_k]$ are all integral, and therefore $a_k^\tau a_l T$ are all integral. The result follows from the fact that $\mathfrak{b}\mathfrak{b}^\tau = (\dots, a_k^\tau a_l, \dots)$.

This finishes the proof of Lemma 4.

In the remainder of this section, we restrict ourselves to the case $\tau = 1$. We prove here a reciprocity formula for generalized Gauss sums, defined below; deriving it from a general 'θ-transformation formula'.

Let $S = (s_{ij}) \in k$ be an s-matrix. Let $\mathfrak{a}$ be an integral ideal satisfying 1) $s_{ii}\mathfrak{a}$ and $2s_{ij}\mathfrak{a}$ are integral for all i, j and 2) if for an integral ideal $\mathfrak{b}$, $s_{ii}\mathfrak{b}$ and $2s_{ij}\mathfrak{b}$ are all integral then $\mathfrak{a} \mid \mathfrak{b}$. The ideal $\mathfrak{a}$ is then called *the denominator of the s-matrix* S $|\mathrm{den}(s)|$.

Let $\varrho \in k$ be such that $\varrho\mathfrak{d} = \mathfrak{a}\mathfrak{b}^{-1}$, $\mathfrak{a}, \mathfrak{b}$ coprime integral ideals and $\mathfrak{d}$ the different of k/Γ. For an s-matrix S such that $\mathrm{den}(S) \mid \mathfrak{a}$, we define the *Gauss sum* (see [8]) $G(\varrho, S)$ by

$$G(\varrho, S) = \sum_{\substack{X \bmod \mathfrak{b} \\ E_S X = X}} \exp\big(2\pi i \sigma(\varrho S[X])\big)$$

where the sum is over a complete set of incongruent $\bmod \mathfrak{b}$ columns X, satisfying $E_S X = X$, E_S being an r-unit of S. This is a generalization of the Gauss sum for non-singular S. It is independent of the choice of the representative X of the residue class $\bmod \mathfrak{b}$ and the r-unit E_S. It has the following properties, which are simple to prove.

(i) Let the matrix U be either primitive $\bmod \mathfrak{b}$ satisfying $E_S U = U$, or unimodular. Then $G(\varrho, S[U]) = G(\varrho, S)$.

(ii) Let $\mathfrak{b}$ be an *odd integral ideal* (i.e. $(\mathfrak{b}, 2) = \mathfrak{o}$). Then $G(\varrho, aS) = \left[\frac{a}{\mathfrak{b}}\right] \cdot G(\varrho, S)$ provided that $\mathrm{den}(S) \mid \mathfrak{a}$; $\left[\frac{a}{\mathfrak{b}}\right]$ being the generalized Jacobi symbol (see [3]).

(iii) Let $\mathfrak{b} \mid \mathfrak{b}_1$. Then $G(\varrho, S) = N(\mathfrak{b}_1\mathfrak{b}^{-1})^m \sum_{\substack{X \bmod \mathfrak{b}_1 \\ E_S X = X}} \exp\big(2\pi i \sigma(\varrho S[X])\big)$.

(iv) Let $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$ with $(\mathfrak{b}_1, \mathfrak{b}_2) = \mathfrak{o}$ and $s \in \mathfrak{o}$. Let $\mathfrak{c}_1, \mathfrak{c}_2$ be integral ideals such that $\mathfrak{b}_i\mathfrak{c}_i = (a_i)$, $a_i \in k$ and $(\mathfrak{c}_1\mathfrak{c}_2, \mathfrak{b}) = \mathfrak{o}$. Define $\beta = \varrho a_1 a_2$. Then $G(\varrho, s) = G(\beta a_1^{-1} a_2^{-1}, s) = G(a_1^{-1} a_2 \beta, s) \cdot G(a_2^{-1} a_1 \beta, s)$. For the proof see [3].

We now derive the reciprocity formula for the Gauss sums from the general θ-transformation formula. *The denominator of an ideal* $\mathfrak{c}$ $(\mathrm{den}(\mathfrak{c}))$ is defined to be an ideal $\mathfrak{c}_1$ such that $\mathfrak{c}\mathfrak{c}_1$ is integral and prime to $\mathfrak{c}_1$. *The system of indices of an s-matrix* S $|\mathrm{ind}(S)|$, is defined to be the set $\{f_l\}$ where $f_l = u_l - v_l$ if $\mathrm{sig}(S) = \{(u_l, v_l)\}$. We notice here that if $r(S) = m$, $f_l + m$ is always an even number.

LEMMA 5. *Let $S \in \mathfrak{o}$ be an s-matrix of rank m. Let S^{-1} denote its $E_S E_S'$ inverse (and therefore symmetric). Then*

$$N\mathfrak{b}^{-m/2} G(\varrho, S) = \exp\left(\frac{\pi i}{4} \sum f_l e_l\right) N(2\mathfrak{a}\mathfrak{a}_1^{-2})^{m/2} N\mathfrak{s}^{\frac{1}{2}} \sum_{\substack{X \bmod \mathfrak{a}_1 \\ E_S' X = X}} \exp\left(2\pi i \sigma\left(\frac{-\omega^2}{4\varrho} S^{-1}[X]\right)\right)$$

where $\mathrm{sgn}(\varrho) = \{e_l\}$, $\mathrm{ind}(S) = \{f_l\}$, $\delta(S) = \mathfrak{s}$, $\mathfrak{a}_1 = \mathrm{den}\left(\frac{\mathfrak{b}}{4\mathfrak{a}\mathfrak{s}}\right)$ *and $\omega \in k$ is such that $\omega\mathfrak{b}$ is integral and prime to $\mathfrak{a}_1$.*

Proof. Corresponding to $S^{(l)}$, $l = 1, \dots, r_1 + r_2$, we define $P^{(l)}$ as follows. Let

$$S = T[A], \quad A \in \mathfrak{o}, \quad AE_S = A, \quad |T| \neq 0. \tag{3.3}$$

For $l \leqslant r_1$, define $Q^{(l)}$ to be a real positive symmetric solution of $Q^{(l)} T^{(l)-1} Q^{(l)} = T^{(l)}$, and for $r_1 < l \leqslant r_1 + r_2$, define $Q^{(l)}$ to be a positive hermitian solution of $\bar{Q}^{(l)} T^{(l)-1} Q^{(l)} = \bar{T}^{(l)}$. These solutions are known to exist. Now define $P^{(l)} = A^{(l)\prime} Q^{(l)} \bar{A}^{(l)} = Q^{(l)}(A^{(l)})$ for $l = 1, \dots, r_1 + r_2$. Clearly $\bar{P}^{(l)} S^{(l)-1} P^{(l)} = \bar{S}^{(l)}$ and $P^{(l)} \bar{E}_{S^{(l)}} = P^{(l)} = E'_{S^{(l)}} P^{(l)}$. For $t > 0$; $\mathfrak{g}$ an integral ideal; $Y \in k$ a column satisfying $E_S Y = Y$; $\xi = \sum_{i=1}^{n} \xi_i \alpha_i$ where $\alpha_1, \dots, \alpha_n$ is a basis of $\mathfrak{o}/\Gamma$ and $\xi_1, \dots, \xi_n$ are arbitrary real numbers; define

$$\theta = \theta(S, P, \mathfrak{g}, \xi, Y) = \sum_{\substack{X \in \mathfrak{g} \\ E_S X = X}} \exp\Big(-\pi t^{-1} \sigma\big(P(X+Y)\big) + 2\pi i \sigma\big(\xi S[X+Y]\big)\Big) \tag{3.4}$$

where σ now denotes the trace in the obvious general sense. Define

$$X_1 = AX, \quad Y_1 = AY \tag{3.5}$$

where A is defined in (3.3). Let $N\big(\delta(A)\big) = (a)$. Then the set of all X_1, contains all m-rowed columns in $a\mathfrak{g}$, and is contained in the set of integral m-rowed columns Z. This proves i) the set of all X_1 form a lattice L of dimension mn over Γ and ii) the sum (3.4) converges absolutely, since $\sum_{Z \text{ integral}} \exp\big(-\pi\sigma\big(Q(Z)\big)\big)$ converges for $Q > 0$ (see [3]). Thus

$$\theta = \sum_{X_1 \in L} \exp\Big(-\pi t^{-1} \sigma\big(Q(X_1 + Y_1)\big) + 2\pi i \sigma\big(\xi T[X_1 + Y_1]\big)\Big). \tag{3.6}$$

Applying the well known θ-transformation formula for non-singular matrices, we get

$$\theta = \Phi(t, \xi) |N|T||^{-\frac{1}{2}} \big(\delta(L)\big)^{-m} \times \times \sum_{Z_1 \in \tilde{L}} \exp\left(-\pi\sigma\left(\frac{t^{-1}\bar{Q}^{-1}(Z_1) + 2i\bar{\xi}T^{-1}[Z_1]}{t^{-2} + 4|\xi|^2} - 2iZ_1'Y_1\right)\right) \tag{3.7}$$

where

$$\Phi(t,\xi)=\prod_{l=1}^{r_1}(t^{-1}-2i\xi^{(l)})^{-u_l/2}(t^{-1}+2i\xi^{(l)})^{-v_l/2}\prod_{l=r_1+1}^{r_1+r_2}(t^{-2}+4|\xi^{(l)}|^2)^{-m/2}$$

where the signs of the square roots are chosen so as to be positive when the quantities are real and positive, $\delta(L)=$ the discriminant of the lattice $L=\mathfrak{a}^{-m}N(\mathfrak{g}^2\mathfrak{d})^{\frac{1}{2}}$, and $\widetilde{L}$ is the lattice complementary to L. Now if $P^{-1}=\bar{A}^{-1}Q^{-1}A'^{-1}$ where A^{-1} is the E_SE_T inverse of A, using (3.5) we have the general θ-transformation formula

$$\theta(S,P,\mathfrak{g},\xi,Y)=N(\mathfrak{s}^{-1}\mathfrak{g}^{-2m}\mathfrak{d}^{-m})^{\frac{1}{2}}\Phi(t,\xi)\times \tag{3.8}$$
$$\times\sum_{\substack{Z\in\mathfrak{g}^{-1}\mathfrak{d}^{-1}\\ E_S'Z=Z}}\exp\left(-\pi\sigma\left(\frac{t^{-1}\bar{P}^{-1}(Z)+2i\bar{\xi}S^{-1}[Z]}{t^{-2}+4|\xi|^2}-2iZ'Y\right)\right).$$

Now consider $t^{-mn/2}\theta(S,P,\mathfrak{o},\varrho,0)$. Taking the limit as $t\to\infty$ and using (3.8), we get in the usual way (see [1]), the result of Lemma 5.

By an argument similar to that in [1], formula 8, p. 37 we get

COROLLARY 1. *Let $S[C]=T$, $C\in\mathfrak{o}$, $E_SCE_T=C$, $\delta(C)=\mathfrak{c}$. Let ϱ be as in Lemma 5. If $(\operatorname{den}(4^{-1}\varrho^{-1}T^{-1}),\mathfrak{c})=\mathfrak{o}$, then*

$$G(\varrho,T)=N(\mathfrak{c})\cdot G(\varrho,S).$$

§ 4. The Genus theorem. In this section, we prove our main result, concerning the existence of a genus of h-forms with given invariants.

THEOREM. *Suppose that we are given the following:*

i) *a natural number m,*

ii) *a set of pairs of non-negative rational integers $\{(u_l,v_l)\}_{l=1,\dots,r}$ or equivalently $\{f_l\}_{l=1,\dots,r}$ where $f_l=u_l-v_l$ and $u_l+v_l=m$,*

iii) *integral k-ideals $\mathfrak{s}_0$ and $\mathfrak{q}$ satisfying $4d\mathfrak{s}_0\mathfrak{P}\mid\mathfrak{q}$, where $\mathfrak{P}$ is defined in* (3.2),

iv) *a set* $\langle\langle s_0\rangle\rangle=\left\{s\in k\ \middle|\ \begin{matrix}s\equiv s_0x\bar{x}\ \mathrm{mod}\ \mathfrak{q},\ (x,\mathfrak{q})=\mathfrak{O}\ \text{if}\ \tau\neq1\\ s=s_0x^2\ \text{if}\ \tau=1\end{matrix}\right\}$ *where the representative s_0 satisfies $\operatorname{sgn}(s_0)=\{(-1)^{v_l}\}$, $s_0\mathfrak{s}_0^{-1}=\mathfrak{C}\bar{\mathfrak{C}}$ with $(\mathfrak{C},\mathfrak{q})=\mathfrak{O}$, and*

v) *a class $S(\mathfrak{q})$ of h-matrices modulo $\mathfrak{q}$ of rank m, where the representative S is chosen m-rowed, integral.*

Then there exists an integral h-matrix $S_0\in S(\mathfrak{q})$, such that

$$r(S_0)=m,\quad \delta(S_0)=\mathfrak{s}_0,\quad \operatorname{sig}(S_0)=\{(u_l,v_l)\},\quad K(S_0)=\langle s_0\rangle$$

if and only if

$$|S|\equiv s_0x\bar{x}\ \mathrm{mod}\ \mathfrak{q},\quad x\in K,\quad (x,\mathfrak{q})=\mathfrak{O} \tag{4.1}$$

and, in addition, if $\tau=1$,

$$G(\varrho,S)=\exp\left(\frac{\pi i}{4}\sum f_le_l\right)N(2^m\mathfrak{s}_0\mathfrak{q}^m\mathfrak{g}^{-m})^{\frac{1}{2}}\left[\frac{s_0}{\mathfrak{g}}\right]\left(G\left(\frac{-\omega^2}{4\varrho};1\right)\right)^m, \tag{4.2}$$

where

$$\varrho\in k,\quad \varrho\mathfrak{d}=\mathfrak{g}\mathfrak{q}^{-1},\quad (\mathfrak{g},\mathfrak{C}\mathfrak{q})=\mathfrak{o},\quad \operatorname{sgn}(\varrho)=\{e_l\}, \tag{4.3}$$

$\omega\in k$ is such that $\omega\mathfrak{d}$ is integral and prime to $\mathfrak{g}$, and $\left[\frac{s_0}{\mathfrak{g}}\right]$ is the generalized Jacobi symbol.

Remark. As a result of this theorem, the invariants uniquely determine a genus, namely the genus containing S_0. The uniqueness follows from the fact that if $S_0^*\in S(\mathfrak{q})$ has rank m system of signatures $\{(u_l,v_l)\}$, discriminant $\mathfrak{s}_0$, and kernel $\langle s_0\rangle$, then S_0 and S_0^* are in the same genus, in view of Lemma 3.

For the proof of the theorem, we need

LEMMA 6. *Let S, $\langle\langle s_0\rangle\rangle$, $\mathfrak{q}$ have the same meaning as in the theorem. Let $m\geqslant2$, let $a\in\mathfrak{o}$ be representable primitively by S mod $\mathfrak{q}$ and let $|S|\equiv s_0x\bar{x}$ mod $\mathfrak{q}$ with $(x,\mathfrak{q})=\mathfrak{O}$. Let $(a)=\mathfrak{a}_1\mathfrak{a}_2$ where $\mathfrak{a}_1,\mathfrak{a}_2$ are k-ideals satisfying $(\mathfrak{a}_1,\mathfrak{q})=\mathfrak{O}$ and $\mathfrak{a}_2$ is divisible only by such prime ideals as already divide $\mathfrak{q}$. In case $m=2$, $\tau=1$, we further assume that $\mathfrak{a}_1$ is a k-prime ideal and $-s_0=y^2$ mod $\mathfrak{a}_1$.*

Then there exists $S_1\equiv S$ mod $\mathfrak{q}$, such that S_1 represents a primitively mod $\mathfrak{q}\mathfrak{a}_1^b$ *for any natural number b and*

$$|S_1|\equiv s_0x_1\bar{x}_1\ \mathrm{mod}\ \mathfrak{q}\mathfrak{a}_1^b,\quad (x_1,\mathfrak{q})=\mathfrak{O}.$$

Proof of Lemma 6. As in [1], define $D=\begin{pmatrix}s_0&0\\0&E\end{pmatrix}$, where E is the $(m-1)$-rowed identity matrix. Let $\lambda,\mu\in\mathfrak{o}$ satisfy

$$\lambda\equiv\begin{cases}0\ \mathrm{mod}\ \mathfrak{a}_1^b,\\ 1\ \mathrm{mod}\ \mathfrak{q},\end{cases}\qquad \mu\equiv\begin{cases}0\ \mathrm{mod}\ \mathfrak{q},\\ 1\ \mathrm{mod}\ \mathfrak{a}_1^b.\end{cases} \tag{4.4}$$

Define

$$S_1=\lambda S+\mu D. \tag{4.5}$$

We will show that this is the required S_1.

In view of the definition of λ, μ, we have, trivially, $S_1\equiv S$ mod $\mathfrak{q}$ and

$$|S_1|\equiv\begin{cases}s_0x\bar{x}\ \mathrm{mod}\ \mathfrak{q},\ (x,\mathfrak{q})=\mathfrak{O},\\ s_0\ \mathrm{mod}\ \mathfrak{a}_1^b.\end{cases} \tag{4.6}$$

Let $x_1=\lambda x+\mu$. From (4.6) we have $|S_1|\equiv s_0x_1\bar{x}_1$ mod $\mathfrak{q}\mathfrak{a}_1^b$, also $(x_1,\mathfrak{q}\mathfrak{a}_1)=\mathfrak{O}$. To complete the proof of the lemma, we have only *to show that S_1 represents a primitively* mod $\mathfrak{q}\mathfrak{a}_1^b$.

Let us assume for a moment that $D[Y] \equiv a \bmod \mathfrak{a}_1^b$, with Y primitive mod $\mathfrak{a}_1$. Further, by hypothesis, $S[X] \equiv a \bmod \mathfrak{q}$, with X primitive mod $\mathfrak{q}$. It is easy to see that with λ, μ as defined in (4.4), $S_1[\lambda X + \mu Y] \equiv a \bmod \mathfrak{q}\mathfrak{a}_1^b$ and $\lambda X + \mu Y$ is primitive mod $\mathfrak{q}\mathfrak{a}_1^b$. Thus to prove that S_1 represents a primitively mod $\mathfrak{q}\mathfrak{a}_1^b$, we have only *to show that D represents a primitively* mod $\mathfrak{a}_1^b$.

Next let us assume that

$$s_0 y_1 y_1^\tau + y_2 y_2^\tau \equiv a \bmod \mathfrak{a}_1^b, \qquad (y_1, y_2, \mathfrak{a}_1) = \mathfrak{O}. \tag{4.7}$$

Then $D[Y] \equiv a \bmod \mathfrak{a}_1^b$ has a primitive solution $Y = \begin{pmatrix} y_1 \\ y_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

Thus in order to prove Lemma 6, we have only *to prove that* (4.7) *has a solution.* We prove this by induction on b.

Let $b = 1$. We have to show, since $a \equiv 0 \bmod \mathfrak{a}_1$, that

$$s_0 y_1 y_1^\tau + y_2 y_2^\tau \equiv 0 \bmod \mathfrak{a}_1, \qquad (y_1, y_2, \mathfrak{a}_1) = \mathfrak{O}. \tag{4.8}$$

Now s_0 in $\langle\langle s_0 \rangle\rangle$ may be chosen coprime with $\mathfrak{a}_1$, and then (4.8) will have a solution if $-s_0 \equiv z z^\tau \bmod \mathfrak{a}_1$ has a solution. In case $\tau = 1$, this is a part of our hypothesis; whereas, in case $\tau \neq 1$, it may be proved exactly as in [3], § 47.

Now let $b > 1$ and let

$$s_0 z_1 z_1^\tau + z_2 z_2^\tau \equiv a \bmod \mathfrak{a}_1^{b-1}, \qquad (z_1, z_2, \mathfrak{a}_1) = \mathfrak{O}. \tag{4.9}$$

Let $\alpha \in \mathfrak{a}_1$ be an integer satisfying $(\alpha, \alpha\mathfrak{a}_1^{-1}) = \mathfrak{O} = (\alpha\mathfrak{a}_1^{-1}, \mathfrak{a}_1)$. Substituting $z_i + \alpha^{b-1} t_i$ (where $t_i \in \mathfrak{O}$), for z_i in (4.9), we have

$$\begin{aligned} & s_0(z_1 + \alpha^{b-1}t_1)(z_1 + \alpha^{b-1}t_1)^\tau + (z_2 + \alpha^{b-1}t_2)(z_2 + \alpha^{b-1}t_2)^\tau \\ & \qquad \equiv s_0 z_1 z_1^\tau + z_2 z_2^\tau + \alpha^{b-1}(s_0 z_1 t_1^\tau + z_2 t_2^\tau) + \alpha^{b-1}(s_0 z_1^\tau t_1 + z_2^\tau t_2) \bmod \mathfrak{a}_1^b \end{aligned}$$

so that *our result would be proved if we can choose* t_1, t_2 *to satisfy*

$$(s_0 z_1 t_1^\tau + z_2 t_2^\tau) + (s_0 z_1^\tau t_1 + z_2^\tau t_2) \equiv \frac{s_0 z_1 z_1^\tau + z_2 z_2^\tau - a}{\alpha^{b-1}} \bmod \mathfrak{a}_1. \tag{4.10}$$

Since $(2, \mathfrak{a}_1) = \mathfrak{O}$, there exists $\delta \in \mathfrak{o}$, such that $(s_0 z_1 z_1^\tau + z_2 z_2^\tau - a)\alpha^{1-b} \equiv 2\delta \bmod \mathfrak{a}_1$. Consider now the congruence

$$s_0 z_1 t_1^\tau + z_2 t_2^\tau \equiv \delta \bmod \mathfrak{a}_1.$$

This is a linear congruence in t_1^τ, t_2^τ, with $(s_0 z_1, z_2, \mathfrak{a}_1) = \mathfrak{O}$, and therefore has a solution in $\mathfrak{O}$. Passing to the conjugates, the same t_1^τ, t_2^τ give a solution of $s_0 z_1^\tau t_1 + z_2^\tau t_2 \equiv \delta \bmod \mathfrak{a}_1$. Together, then the congruences give us (4.10).

This completes the proof of Lemma 6.

Proof of the theorem.

Remark. For the proof of the theorem, we may, whenever necessary, choose S suitably in its equivalence class mod $\mathfrak{q}$ or its residue class mod $\mathfrak{q}$.

To prove that the conditions (4.1) and (4.2) are *necessary*, let $S_0 \in \mathfrak{O}$ satisfy $r(S_0) = m$, $\delta(S_0) = \mathfrak{s}_0$, $\operatorname{sig}(S_0) = \{(u_l, v_l)\}$, $K(S_0) = \langle s_0 \rangle$ and

$$S_0[F] \equiv S \bmod \mathfrak{q}, \qquad (\delta(F), \mathfrak{q}) = \mathfrak{O}, \qquad E_{S_0} F = F. \tag{4.11}$$

By Lemma 4, there exists a matrix $C_1 \in \mathfrak{O}$ such that

$$S_0 = S_1[C_1], \qquad |S_1| \neq 0, \qquad (\delta(C_1), \mathfrak{q}) = \mathfrak{O}, \qquad C_1 E_{S_0} = C_1. \tag{4.12}$$

From (4.11) and (4.12),

$$S \equiv S_1[C_1 F] \bmod \mathfrak{q}. \tag{4.13}$$

Now $C_1 F$ is non-singular and $(|C_1 F|) = \delta(C_1)\,\delta(F)$ is coprime with $\mathfrak{q}$. Further, in view of Lemma 4, $|S_1| \cdot \delta(C_1) \cdot \delta(C_1^\tau)$ is integral. Let $c \in \delta(C_1)$ satisfy $\big(c(\delta(C_1))^{-1}, \mathfrak{q}\big) = \mathfrak{O}$. Putting $s_0 = |S_1| \cdot c c^\tau$, $x = |C_1 F| \cdot c^{-1}$ in (4.13), we get

$$|S| \equiv s_0 x x^\tau \bmod \mathfrak{q}, \qquad (x, \mathfrak{q}) = \mathfrak{O}.$$

Also from (4.12) it follows that $s_0 \mathfrak{s}_0^{-1} = |S_1| c c^\tau \cdot \delta(C_1^\tau)^{-1} \cdot \delta(C_1)^{-1} \cdot |S_1|^{-1} = c\delta(C_1)^{-1} \cdot \big(c\delta(C_1)^{-1}\big)^\tau$ and $\big(c\delta(C_1)^{-1}, \mathfrak{q}\big) = \mathfrak{O}$. Finally $\operatorname{sgn}(s_0) = \operatorname{sgn}(|S_1|) = \{(-1)^{v_l}\}$. This proves the necessity of condition (4.1).

Now let $\tau = 1$. In this case, we have also to prove the necessity of condition (4.2). Let ϱ be as defined in (4.3), then in view of (4.11),

$$G(\varrho, S) = G(\varrho, S_0).$$

Applying Lemma 5 to $G(\varrho, S_0)$, we have, in view of the above equation and properties of S_0,

$$\begin{aligned} & G(\varrho, S) \\ & \quad = \exp\Big(\frac{\pi i}{4} \sum f_l e_l\Big) N(2^m \mathfrak{s}_0 \mathfrak{q}^m \mathfrak{g}^{-m})^{\frac12} \sum_{\substack{X \bmod \mathfrak{g} \\ E_S' X = X}} \exp\Big(2\pi i \sigma \Big(\frac{-\omega^2}{4\varrho} S_0^{-1}[X]\Big)\Big), \end{aligned} \tag{4.14}$$

where $\omega \in k$ is such that $\omega\mathfrak{d}$ is integral and prime to $\mathfrak{g}$. Now $S_0^{-1} \sim D$ (diagonal) mod $\mathfrak{g}$, since $(2, \mathfrak{g}) = \mathfrak{o}$; so that the Gauss sum on the right of (4.14) equals $\Big[\frac{|D|}{\mathfrak{g}}\Big] \cdot G\Big(\frac{-\omega^2}{4\varrho}, E\Big)$. Next since $(\mathfrak{g}, \mathfrak{C}\mathfrak{q}) = \mathfrak{o}$, $|D| \equiv s_0 y^2 \bmod \mathfrak{g}$ with $(y, \mathfrak{g}) = \mathfrak{o}$, we see that $\Big[\frac{|D|}{\mathfrak{g}}\Big] = \Big[\frac{s_0}{\mathfrak{g}}\Big]$. Substituting in (4.14), we see that (4.2) is satisfied.

We now show that conditions (4.1) and (4.2) are *sufficient* for the existence of the matrix S_0 with given properties. The proof proceeds in several steps.

Step I. We show that it suffices to prove the theorem for the case $u_l > 0$ for $l = 1, \dots, r$.

Let $|S| = s_0 xx^\tau + q$ where $q \in \mathfrak{q} \cap k$ (in view of (4.1)). Let $S_1 = S + \begin{pmatrix} 0 & 0 \\ 0 & q_1 \end{pmatrix}$ where $q_1 \neq 0$, $q_1 \in \mathfrak{q} \cap k$. Then $|S_1| = s_0 xx^\tau + q + q_1 d_1$, where d_1 is the leading $(m-1)$-subdeterminant of S; and we may, without loss of generality, assume $d_1 \neq 0$, since S is determined only modulo $\mathfrak{q}$. Also $d_1 \in k$. Let $a \in \mathfrak{o}$ be chosen coprime with $xd_1 q_1 \mathfrak{g}\mathfrak{C}$, then there exists $b \in \mathfrak{o}$ such that $q + bq_1 d_1 \equiv 0 \bmod (a)$. Define

$$S_2 = S + \begin{pmatrix} 0 & 0 \\ 0 & bq_1 \end{pmatrix}$$

then

$$S_2 \equiv S \bmod \mathfrak{q}, \qquad |S_2| \equiv s_0 xx^\tau \bmod (a), \qquad G(\varrho, S_2) = G(\varrho, S).$$

Thus we may start with S such that

$$(4.15) \qquad |S| \equiv s_0 xx^\tau \bmod (a), \qquad (x, a) = \mathfrak{D}$$

where $a \in \mathfrak{o}$ satisfies $(a, xd_1 q_1 \mathfrak{g}\mathfrak{C}) = \mathfrak{D}$. This '$a$' may be chosen in such a way that it has any system of signatures, prescribed in advance.

We may assume that $u_l = 0$ for $l = 1, \dots, p$, $0 < p \leqslant r$ (there is nothing to prove if $p = 0$). Choose 'a' above satisfying $a^{(1)} < 0, \dots, a^{(p)} < 0$ and $a^{(p+1)} > 0, \dots, a^{(r)} > 0$. Write $\operatorname{sgn}(a) = \{g_l\}$.

Consider now the system $m^* = m$, $f_l^* = f_l g_l$ so that

$$u_l^* = \frac{m + f_l^*}{2} = \begin{cases} u_l & \text{if} \quad u_l > 0, \\ v_l & \text{if} \quad u_l = 0 \end{cases}$$

is positive, $S^* = aS$, $s_0^* = a^m s_0$, $\mathfrak{s}_0^* = a^m \mathfrak{s}_0$, $\mathfrak{q}^* = a^c \mathfrak{q}$ where $c = m+1$ or $m+2$ according as m is odd or even (so that c is always even). If $\mathfrak{P}^* = p(\mathfrak{s}_0^*)$ is the product of all k-prime ideal divisors of $2d\mathfrak{s}_0^*$, then $4d\mathfrak{s}_0^*\mathfrak{P}^* \mid \mathfrak{q}^*$, $s_0^* \mathfrak{s}_0^{*-1} = \mathfrak{C}\mathfrak{C}^\tau$ is coprime with $\mathfrak{q}^*$ and $\operatorname{sgn}(s_0) = \{(-1)^{v_l^*}\}$. (4.2) and (4.15) together imply

$$|S| \equiv s_0 x_2 x_2^\tau \bmod a\mathfrak{q}, \qquad (x_2, a\mathfrak{q}) = \mathfrak{D},$$

i.e. $a^m |S| \equiv a^m s_0 x_2 x_2^\tau \bmod a^{m+1}\mathfrak{q}$, and therefore by Lemma 1 (using the result in case of one variable)

$$|S^*| \equiv a^m |S| \equiv s_0^* x_3 x_3^\tau \bmod \mathfrak{q}^*, \qquad (x_3, \mathfrak{q}) = \mathfrak{D}$$

so that condition (4.1) is satisfied by the '$*$system'.

Let now $\tau = 1$. Define $\varrho^* = a^{-c}\varrho$ with ϱ as in (4.3), so that (since c is even), $\operatorname{sgn}(\varrho^*) = \{e_l^*\} = \{e_l\}$. Using property (iii) of Gauss sums (§ 3), we get

$$(4.16) \qquad G(\varrho^*, S^*) = |N(a)|^m \cdot G(a\varrho^*, S).$$

From (4.2) (since $\mathfrak{q} \mid a^{c-1}\mathfrak{q}$)

$$(4.17) \qquad G(a\varrho^*, S) = \exp\left(\sum \frac{\pi i}{4} e_l^* f_l^*\right) N(2^m \mathfrak{s}_0 a^{-m} \mathfrak{q}^{*m} \mathfrak{g}^{-m})^{\frac{1}{2}} \left[\frac{s_0}{\mathfrak{g}}\right] \left(G\left(\frac{-\omega^2}{4\varrho^*}, 1\right)\right)^m.$$

From (4.16), (4.17) we see that the '$*$system' satisfies condition (4.2).

Thus the '$*$system' satisfies the condition of the theorem, and *has further the property that* $u_l^* > 0$ *for* $l = 1, \dots, r$.

Suppose now that the theorem is proved for the '$*$system', i.e. there exists an integral h-matrix $S_0^* \sim S^* \bmod \mathfrak{q}^*$ satisfying $r(S_0^*) = m$, $\operatorname{ind}(S_0^*) = \{f_l^*\}$, $\delta(S_0^*) = \mathfrak{s}_0^*$ and $K(S_0^*) = \langle s_0^* \rangle$. Define

$$(4.18) \qquad S_0 = a^{-1} S_0^*$$

then $r(S_0) = m$, $\operatorname{ind}(S_0) = \{f_l\}$, $\delta(S_0) = \mathfrak{s}_0$, $K(S_0) = \langle s_0 \rangle$ and

$$(4.19) \qquad S_0 \sim S \bmod a^{-1}\mathfrak{q}^*.$$

(4.19) implies $S_0 \sim S \bmod \mathfrak{q}$, since $\mathfrak{q} \mid a^{-1}\mathfrak{q}^*$. We have only to show that S_0 is integral. In view of (4.18) and the assumption that S_0^* is integral, S_0 can have only prime ideal divisor of (a) in the denominator; on the other hand, in view of (4.19), since S is integral and $a \mid a^{-1}\mathfrak{q}^*$, S_0 cannot have any prime ideal divisors of (a) in the denominator. Thus S_0 is integral.

Thus *for* $m \geqslant 2$, *it is enough to prove the theorem for the case* $u_l > 0$, $l = 1, \dots, r$. We make this assumption in the sequel.

Step II. Let $m = 2$, $\tau = 1$. We show that it suffices to prove the theorem for the case $(s_{11}, \mathfrak{q}) = (\operatorname{cont} S, \mathfrak{q})$, where $\operatorname{cont} S$ = content of S = the ideal generated by all the elements of S.

We first show that S may be chosen in its class mod $\mathfrak{q}$ to satisfy $(s_{11}, \mathfrak{q}) = (\operatorname{cont} S, \mathfrak{q}) \cdot \mathfrak{b}$ where $\mathfrak{b} \mid (2)$.

We can take $s_{11} \neq 0$, by choosing S properly in its congruence class mod $\mathfrak{q}$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ be all the distinct prime ideals that divide $(s_{11}, \mathfrak{q})$. Let $(\operatorname{cont} S, \mathfrak{q}) = \mathfrak{a} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_t^{a_t}$, where $a_i \geqslant 0$. Let $\mathfrak{p}_i^{c_i} \| (2)$, $c_i \geqslant 0$ $(i = 1, \dots, t)$. We may assume that for $i = 1, \dots, j-1$, $\mathfrak{p}_i^{a_i + c_i + 1} \nmid (s_{11})$; so that $\mathfrak{p}_i^{a_i} \| (s_{11})$ if $(\mathfrak{p}_i, 2) = \mathfrak{o}$ for $i = 1, \dots, j-1$. Let $j = 1$ refer to the case when $\mathfrak{p}_i^{a_i + c_i + 1} \mid (s_{11})$ for $i = 1, \dots, t$. If $j - 1 = t$, there is nothing to prove. Let, therefore, $j - 1 < t$. We prove our result by induction on j. The unimodular transformation

$$(4.20) \qquad x_1 \to x_1, \quad x_2 \to bx_1 + x_2, \quad \mathfrak{p}_1 \dots \mathfrak{p}_{j-1} \mid (b), \quad (\mathfrak{p}_j, b) = \mathfrak{o}$$

changes the first coefficient to $s_{11}+b^2s_{22}+2bs_{12}$. Consider the following two cases:

First case: $\mathfrak{p}_j^{a_j+c_j+1} \nmid (s_{22})$. Choose b in (4.20) in such a way that $\mathfrak{p}_j^{a_j+c_j+1} \nmid (2s_{12}+bs_{22})$. Then $\mathfrak{p}_i^{a_i+c_i+1} \nmid (s_{11}+b^2s_{22}+2bs_{12})$ for $i=1,\dots,j$.

Second case: $\mathfrak{p}_j^{a_j+c_j+1} \mid (s_{22})$. Then $\mathfrak{p}_j^{a_j} \| (s_{12})$ and therefore $\mathfrak{p}_i^{a_i+c_i+1} \nmid (s_{11}+b^2s_{22}+2bs_{22})$ for $i=1,\dots,j$.

Thus we have proved that S *may be chosen in its class* mod $\mathfrak{q}$ *to satisfy* $(s_{11},\mathfrak{q}) = (\operatorname{cont} S,\mathfrak{q})\cdot\mathfrak{b}$ *where* $\mathfrak{b}\mid(2)$.

Remark 1. This transformation holds for any m, though we prove it here only for $m=2$.

Remark 2. If S is chosen to satisfy the above condition, then it follows in view of (4.1) that for any prime ideal $\mathfrak{p}\mid\mathfrak{q}$ and for a natural number b, $\mathfrak{p}^b\mid(s_{11})$ implies $\mathfrak{p}^b\mid\mathfrak{q}$.

Now let $D=\begin{pmatrix}1&0\\0&2\end{pmatrix}$. Let $m^*=m=2$, $f_l^*=f_l$ $(l=1,\dots,r_1)$, $S^*=S[D]$, $\mathfrak{s}_0^*=4\mathfrak{s}_0$, $s_0^*=4s_0$, $\mathfrak{q}^*=4\mathfrak{q}$. Clearly $\mathfrak{P}^*=p(\mathfrak{s}_0^*)=\mathfrak{P}$, $4d\mathfrak{s}_0^*\mathfrak{P}^*\mid\mathfrak{q}^*$, $s_0^*\mathfrak{s}_0^{*-1}=\mathfrak{C}^2$ is coprime with $\mathfrak{q}^*$ and $\operatorname{sgn}(s_0^*)=\{(-1)^{(m-f_l^*)/2}\}$. Also from (4.1),

$$(4.21)\qquad |S^*|\equiv s_0^*x^2 \bmod \mathfrak{q}^*,\qquad (x,\mathfrak{q}^*)=\mathfrak{o}\,.$$

So that '$*$system' satisfies condition (4.1). Next let $\varrho^*=\frac14\varrho$ with ϱ as in (4.3), then since $\operatorname{den}(\frac14\varrho^{*-1}S^{*-1})\mid\operatorname{den}(\frac14\varrho^{*-1}|S^*|^{-1})$ and $|S^*|=s_0^*x^2+q^*$, $q^*\in\mathfrak{q}^*$ (from (4.21)), we have $\big(\operatorname{den}(\frac14\varrho^{*-1}S^{*-1}),2\big)=\mathfrak{o}$. Therefore, by Corollary 1 of Lemma 5, we have

$$(4.22)\qquad G(\varrho^*,S^*)=N|D|\cdot G(\varrho^*,S)\,.$$

Substituting ϱ^* for ϱ in (4.2), observing that ϱ^* satisfies the conditions (4.3), and comparing with (4.22), we see that the '$_*$ system' satisfies the Gauss sum condition. Further $(\operatorname{cont}S^*,\mathfrak{q}^*)=(s_{11},2s_{12},4s_{22},4\mathfrak{q})=\big((s_{11},\mathfrak{q}),2s_{12},4s_{22}\big)$ in view of Remark 2 above. Therefore, since $(s_{11},\mathfrak{q})=(\operatorname{cont}S,\mathfrak{q})\mathfrak{b}$ and $\mathfrak{b}\mid(2)$, we have

$$\begin{aligned}(\operatorname{cont}S^*,\mathfrak{q}^*)&=\big((\operatorname{cont}S,\mathfrak{q})\cdot\mathfrak{b},2s_{12},4s_{22}\big)\\&=\mathfrak{b}(\operatorname{cont}S,\mathfrak{q},2s_{12}\mathfrak{b}^{-1},4s_{22}\mathfrak{b}^{-1})\\&=\mathfrak{b}(\operatorname{cont}S,\mathfrak{q})=(s_{11},\mathfrak{q})\,.\end{aligned}$$

Now since $s_{11}=s_{11}^*$, we have $(\operatorname{cont}S^*,\mathfrak{q}^*)=(s_{11}^*,\mathfrak{q})$. Finally in view of Remark 2, $(\operatorname{cont}S^*,\mathfrak{q}^*)=(s_{11}^*,\mathfrak{q}^*)$.

Thus the '$*$system' satisfies the conditions of the theorem, and we have the additional property $(s_{11}^*,\mathfrak{q}^*)=(\operatorname{cont}S^*,\mathfrak{q}^*)$.

Suppose now that the theorem is proved for the '$*$system'; so that there exists an integral s-matrix $S_0^*\equiv S^*[U] \bmod \mathfrak{q}^*$, U reduced and primitive $\bmod\,\mathfrak{q}^*$ and such that $r(S_0^*)=2$, $\operatorname{ind}(S_0^*)=\{f_l^*\}$, $\delta(S_0^*)=\mathfrak{s}_0^*$, $K(S_0^*)=\langle s_0^*\rangle$. Now $\big(\delta(UD),\mathfrak{q}^*\big)=(2)$ and $(4)\mid\mathfrak{q}^*$. Therefore by [8], Lemma 26, there exists an integral matrix D_1, which is left equivalent with $DU \bmod \mathfrak{q}^*$, i.e. $DU\equiv U_1D_1 \bmod \mathfrak{q}^*$, U_1 primitive $\bmod\,\mathfrak{q}^*$, $E_{U_1}D_1E_{S_0^*}=D_1$ and such that $\delta(D_1)=(2)$. Define

$$(4.23)\qquad S_0=S_0^*[D_1^{-1}]$$

where D_1^{-1} is the $E_{S_0^*}E_{U_1}$ inverse of D_1. Then

$$(4.24)\qquad S_0\equiv S[U_1] \bmod \tfrac14\mathfrak{q}^*\,.$$

From (4.23) and (4.24), it follows as in step I that S_0 is integral. Further since $E_{S_0^*}$ is an l-unit of D_1^{-1}, $\delta(S_0)=\delta(S_0^*)\delta(D_1)^{-2}=\mathfrak{s}_0$. It is easy to see that this S_0 satisfies all other requirements.

As a result of steps I, II, we have shown that *in case* $m\geqslant 2$, *it suffices to prove the theorem for* $u_l>0$ $(l=1,\dots,r)$ *and further that in case* $\tau=1$, $m=2$, *we may assume* $(s_{11},\mathfrak{q})=(\operatorname{cont}S,\mathfrak{q})$. We make these assumptions in all further discussion.

Step III. Once again let $\tau=1$, $m=2$. We show that we may choose S in its class mod $\mathfrak{q}$ in such a way that i) $s_{11}\succ 0$ (i.e. $s_{11}^{(l)}>0$ for $l=1,\dots,r_1$), ii) $(s_{11})=\mathfrak{a}\mathfrak{p}$ where $\mathfrak{a}=(\operatorname{cont}S,\mathfrak{q})$ and $\mathfrak{p}$ is an odd prime ideal satisfying $(s_0,\mathfrak{p})=\mathfrak{o}$, iii) S is diagonal, iv) $\mathfrak{p}\|(s_{22})$ (therefore in particular $(s_{11},\mathfrak{q})=(\operatorname{cont}S,\mathfrak{q})$) and v) $\left[\dfrac{-s_0}{\mathfrak{p}}\right]=+1$.

Let $(s_{11},\mathfrak{q})=(\operatorname{cont}S,\mathfrak{q})=\mathfrak{a}$. Let $\mathfrak{b}$ be an integral ideal prime to $\mathfrak{q}$ such that $\mathfrak{b}\mathfrak{a}^{-1}=(a)$ is a principal ideal with $a\succ 0$. In view of step II and Remark 2 made there, $(as_{11},\mathfrak{q})=\mathfrak{o}$. There exists therefore, $b\in\mathfrak{o}$, $b\succ 0$, $(b,\mathfrak{q})=\mathfrak{o}$ with $as_{11}b\equiv 1 \bmod \mathfrak{q}$. Then by the Dirichlet-Hecke-Landau theorem ([4], [5]), there is a prime ideal $\mathfrak{p}$ (we choose it to satisfy $(s_0,\mathfrak{p})=\mathfrak{o}$) such that $b\mathfrak{b}\mathfrak{p}=(c)$ is a principal ideal, $c\in\mathfrak{o}$, $c\succ 0$ and $c\equiv 1 \bmod \mathfrak{q}$. Now $(ca^{-1}b^{-1})=\mathfrak{a}\mathfrak{p}$ is an integral ideal, so that $ca^{-1}b^{-1}$ is an integer; further $ca^{-1}b^{-1}\succ 0$, since a,b,c are all $\succ 0$. Finally $ca^{-1}b^{-1}\equiv(ca^{-1}b^{-1})(s_{11}ab)\equiv s_{11}c\equiv s_{11} \bmod \mathfrak{q}$ and $(ca^{-1}b^{-1},\mathfrak{q})=\mathfrak{a}$.

Thus we have proved that S may be chosen in its class mod $\mathfrak{q}$ to satisfy conditions i) and ii) of step III.

Now let $s'_{ij}=as_{ij}$ $(i,j=1,2)$. Then s'_{ij} are integers, so that the matrix $U=\begin{pmatrix}1&s'_{12}\\0&s'_{11}\end{pmatrix}$ is primitive mod $\mathfrak{q}$. And

$$S[U]\equiv\begin{pmatrix}s_{11}&0\\0&s_{11}a_{11}^2(s_{11}s_{22}-s_{12}^2)\end{pmatrix} \bmod \mathfrak{q}\,,$$

i.e. S may be chosen in the diagonal form. This proves iii).

From (4.1), we get

$$a^2s_{11}(s_{11}s_{22}-s_{12}^2)\equiv(as_{11})^2\cdot s_{11}^{-1}s_0x^2 \bmod \mathfrak{q}\,,\qquad (x,\mathfrak{q})=\mathfrak{o}\,.$$

Let $as_{11}x = d_2$, then in view of the foregoing, $s_0 s_{11}^{-1} d_2^2$ is an integer. Thus we have shown that we may assume that we started with an S satisfying

$$(4.25)\qquad S = \begin{pmatrix} s_{11} & 0 \\ 0 & s_{22}\end{pmatrix} = \begin{pmatrix} ca^{-1}b^{-1} & 0 \\ 0 & s_0(ca^{-1}b^{-1})^{-1}\big(a(ca^{-1}b^{-1})x\big)^2\end{pmatrix}.$$

Also $(d_2) = \mathfrak{p}\mathfrak{b}_1$, $(\mathfrak{b}_1, \mathfrak{p}\mathfrak{q}) = \mathfrak{o}$ (since $\mathfrak{p} \mid (x)$ implies $\mathfrak{p} \mid \mathfrak{q}$ in view of (4.1)). Finally since $(\mathfrak{p}, s_0) = \mathfrak{o}$, we see that $\mathfrak{p} \,\|\, (s_{22})$.

Thus we have shown that S may be chosen in its equivalence class mod $\mathfrak{q}$ to satisfy conditions i), ii), iii) and iv) of step III.

We now show that $\left[\frac{-s_0}{\mathfrak{p}}\right] = +1$. Let ϱ satisfy (4.3) and $(\mathfrak{g}, \mathfrak{p}\mathfrak{b}_1) = \mathfrak{o}$. In view of (4.25),

$$(4.26)\qquad G(\varrho, S) = G(\varrho, s_{11})\cdot G(\varrho, s_{22}).$$

Now $(s_{22}) = \mathfrak{p}\mathfrak{b}_1^2\mathfrak{C}^2\mathfrak{s}_0\mathfrak{a}^{-1}$ and $\operatorname{sgn}(s_{22}) = \operatorname{sgn}(s_0)$. Define

$$(4.27)\qquad \mathfrak{b}_2 = (\mathfrak{b}_1\mathfrak{C})^2.$$

Then by Lemma 5 (in view of (4.25)),

$$(4.28)\qquad G(\varrho, s_{22}) = \exp\left(\frac{\pi i}{4}\sum e_l(f_l-1)\right) N(2s_{22}\mathfrak{q}\mathfrak{g}^{-1}\mathfrak{p}^{-2}\mathfrak{b}_2^{-1})^{\frac{1}{2}} \times \sum_{x \bmod \mathfrak{p}\mathfrak{b}_2\mathfrak{g}} \exp\left(2\pi i\sigma\left(\frac{-\omega^2x^2}{4\varrho s_{22}}\right)\right)$$

where $\omega\mathfrak{d}$ is integral and prime to $\mathfrak{p}\mathfrak{g}\mathfrak{b}_2$. And with the same ω,

$$(4.29)\qquad G(\varrho, s_{11}) = \exp\left(\frac{\pi i}{4}\sum e_l\right) N(2s_{11}\mathfrak{q}\mathfrak{g}^{-1}\mathfrak{p}^{-2})^{\frac{1}{2}} \times \sum_{x \bmod \mathfrak{p}\mathfrak{g}} \exp\left(2\pi i\sigma\left(\frac{-\omega^2x^2}{4\varrho s_{11}}\right)\right).$$

From (4.2), (4.26), (4.28) and (4.29), noticing that ω in (4.2) may be chosen to be the same as in (4.28), we have

$$(4.30)\qquad \left[\frac{s_0}{\mathfrak{g}}\right]\left(G\left(\frac{-\omega^2}{4\varrho}, 1\right)\right)^2 = N(\mathfrak{p}^{-1}\mathfrak{b}_2^{-\frac{1}{2}})\cdot L\cdot M,$$

where L and M stand for the Gauss sums on the right of (4.29) and (4.28) respectively. Now $(\mathfrak{p}\mathfrak{b}_2, \mathfrak{g}) = \mathfrak{o}$. Let $\mathfrak{g}\mathfrak{h} = (\alpha)$, $\mathfrak{p}\mathfrak{b}_2\mathfrak{h}' = (\alpha')$, $(\mathfrak{h}\mathfrak{h}', \mathfrak{p}\mathfrak{g}\mathfrak{b}_2) = \mathfrak{o}$, $\beta_2 = \omega^2\alpha\alpha'(4\varrho s_{22})^{-1}$. Then by property (iv) of the Gauss sums (§ 3),

$$(4.31)\qquad M = \left\{\sum_{x \bmod \mathfrak{p}\mathfrak{b}_2} \exp\left(2\pi i\sigma\left(\frac{\alpha\beta_2}{\alpha'}x^2\right)\right)\right\}\left\{\sum_{x \bmod \mathfrak{g}} \exp\left(2\pi i\sigma\left(\frac{-\alpha'\beta_2}{\alpha}x^2\right)\right)\right\}$$

similarly with $\beta_1 = 4^{-1}\varrho^{-1}\omega^2\alpha$,

$$(4.32)\qquad L = \left\{\sum_{x \bmod \mathfrak{p}} \exp\left(2\pi i\sigma\left(\frac{\alpha\beta_1}{s_{11}}x^2\right)\right)\right\}\left\{\sum_{x \bmod \mathfrak{g}} \exp\left(2\pi i\sigma\left(\frac{-s_{11}\beta_1}{\alpha}x^2\right)\right)\right\}.$$

Now

$$(4.33)\qquad \begin{aligned} \sum_{x \bmod \mathfrak{g}} \exp\left(2\pi i\sigma\left(\frac{-s_{11}\beta_1}{\alpha}x^2\right)\right) &= \left[\frac{s_{11}}{\mathfrak{g}}\right] G\left(\frac{-\omega^2}{4\varrho}, 1\right), \\ \sum_{x \bmod \mathfrak{g}} \exp\left(2\pi i\sigma\left(\frac{-\alpha'\beta_2}{\alpha}x^2\right)\right) &= \left[\frac{s_{22}}{\mathfrak{g}}\right] G\left(\frac{-\omega^2}{4\varrho}, 1\right) \end{aligned}$$

so that since (in view of (4.25)), $s_{11}s_{22} = s_0 d_2^2$, (4.30)–(4.33) give,

$$(4.34)\qquad \left\{\sum_{x \bmod \mathfrak{p}\mathfrak{b}_2} \exp\left(2\pi i\sigma\left(\frac{\alpha\beta_2}{\alpha'}x^2\right)\right)\right\}\left\{\sum_{x \bmod \mathfrak{p}} \exp\left(2\pi i\sigma\left(\frac{\alpha\beta_1}{s_{11}}x^2\right)\right)\right\} = N\mathfrak{p}\,\mathfrak{b}_2^{\frac{1}{2}}.$$

Now $(\mathfrak{p}, \mathfrak{b}_2) = \mathfrak{o}$. Let $\mathfrak{b}_2\mathfrak{h}_1 = (\alpha_1)$, $(\mathfrak{h}_1, \mathfrak{p}\mathfrak{b}_2) = \mathfrak{o}$, $\beta_3 = \alpha\beta_2 s_{11}\alpha_1\alpha'^{-1} = 4^{-1}\varrho^{-1}s_{22}^{-1}\omega^2\alpha^2 s_{11}\alpha_1$. Then by property (iv) of Gauss sums (§ 3),

$$(4.35)\qquad \sum_{x \bmod \mathfrak{p}\mathfrak{b}_2} \exp\left(2\pi i\sigma\left(\frac{\alpha\beta_2}{\alpha'}x^2\right)\right) = \left\{\sum_{x \bmod \mathfrak{p}} \exp\left(2\pi i\sigma\left(\frac{\omega^2\alpha^2\alpha_1^2}{4\varrho s_{22}}x^2\right)\right)\right\}\left\{\sum_{x \bmod \mathfrak{b}_2} \exp\left(2\pi i\sigma\left(\frac{\omega^2\alpha^2 s_{11}^2}{4\varrho s_{22}}x^2\right)\right)\right\}.$$

Now $\mathfrak{b}_2 = \mathfrak{b}_1^2\mathfrak{C}^2$ is the square of an odd ideal, so that

$$(4.36)\qquad \sum_{x \bmod \mathfrak{b}_2} \exp\left(2\pi i\sigma\left(\frac{\omega^2\alpha^2 s_{11}^2}{4\varrho s_{22}}x^2\right)\right) = (N\mathfrak{b}_2)^{\frac{1}{2}},$$

$$\frac{\omega^2\alpha^2\alpha_1^2}{4\varrho s_{22}} = \frac{\omega^2\alpha^2\alpha_1^2 s_0^{-1}s_{11}^2 d_2^2}{4\varrho s_{11}} = -s_0^{-1}(s_{11}\alpha_1 d_2^{-1})^2\,\frac{-\omega^2\alpha^2}{4\varrho s_{11}} = -s_0^{-1}(s_{11}\alpha_1 d_2^{-1})^2(-s_{11}^{-1}\alpha\beta_1)$$

and $s_{11}\alpha_1 d_2^{-1}$ is integral. From (4.34), (4.35) and (4.36), therefore,

$$(4.37)\qquad \left\{\sum_{x \bmod \mathfrak{p}} \exp\left(2\pi i\sigma\left(\frac{\alpha\beta_1}{s_{11}}x^2\right)\right)\right\}\left\{\sum_{x \bmod \mathfrak{p}} \exp\left(2\pi i\sigma\left(\frac{\omega^2\alpha^2\alpha_1^2}{4\varrho s_{22}}x^2\right)\right)\right\} = N\mathfrak{p}$$

and from property (ii) of Gauss sums (§ 3), and $s_{11}s_{22} = s_0 d_2^2$, it follows therefore that the left side of (4.37) is $\left[\frac{-s_0}{\mathfrak{p}}\right]\cdot N\mathfrak{p}$. This implies that $\left[\frac{-s_0}{\mathfrak{p}}\right] = +1$.

Thus we have shown as a result of steps I, II and III that *in case $m \geqslant 2$, it is enough to prove the theorem for $u_l > 0$ $(l = 1, \ldots, r)$ and further* *in case* $\tau = 1$, $m = 2$ *that we may take* $s_{11} \succ 0$, $(s_{11}) = \mathfrak{a}\mathfrak{p}$ *where* $\mathfrak{a} = (\operatorname{cont} S, \mathfrak{q})$, $\mathfrak{p}$ *is a prime ideal satisfying* $(\mathfrak{p}, 2\mathfrak{s}_0) = \mathfrak{o}$,

$$S = \begin{pmatrix} s_{11} & 0 \\ 0 & s_{22} \end{pmatrix}, \quad \mathfrak{p} \,\|\, (s_{22}) \quad \textit{and} \quad \left[\frac{-s_0}{\mathfrak{p}}\right] = +1 .$$

Step IV. Let $m \geqslant 2$. We show that it suffices to prove the theorem for the case $u_l > 0$ $(l = 1, \ldots, r)$ and $s_{11} = 1$.

In case either $m > 2$ or $m = 2$ and $\tau \neq 1$, we may choose s_{11} in its congruence class mod $\mathfrak{q}$ to satisfy

$$(4.38) \qquad s_{11} \succ 0 \quad \text{and} \quad (s_{11}, \mathfrak{C}) = \mathfrak{O} .$$

This can be achieved by adding to s_{11}, a suitable positive rational integer $\epsilon\, \mathfrak{q}$, noticing the fact that $(\mathfrak{C}, \mathfrak{q}) = \mathfrak{O}$. In case $\tau = 1$ and $m = 2$, (4.38) may be assumed satisfied as a result of step III. Define $D = \begin{pmatrix} s_{11} & 0 \\ 0 & E \end{pmatrix}$ and S^* by

$$(4.39) \qquad S^*[D] = s_{11} S ,$$

and consider $m^* = m$, $u_l^* = u_l$ and $v_l^* = v_l$ for $l = 1, \ldots, r$, $\mathfrak{q}^* = s_{11}^{m+1}\mathfrak{q}$, $\mathfrak{s}_0^* = s_{11}^{m-2}\mathfrak{s}_0$, $s_0^* = s_{11}^{m-2} s_0$.

Then $u_l^* + v_l^* = m$; $4d\mathfrak{s}_0^*\mathfrak{P}^* \mid \mathfrak{q}^*$, where $\mathfrak{P}^* = p(\mathfrak{s}_0^*)$; $\operatorname{sgn}(s_0^*) = \operatorname{sgn}(s_0) = \{(-1)^{v_l^*}\}$, since $s_{11} \succ 0$ and $v_l^* = v_l$; $s_0^* \bar{s}_0^{*-1} = s_{11}^m s_0 \bar{s}_{11}^{-m} \bar{s}_0^{-1} = \mathfrak{C}\mathfrak{C}^\tau$ and $(\mathfrak{C}, \mathfrak{q}^*) = \mathfrak{O}$, in view of (4.38) and assumption iv) of the theorem. We show that (4.1) is satisfied.

Let $(s_{11}) = \mathfrak{a}_1\mathfrak{b}$ where $\mathfrak{a}_1$ and $\mathfrak{b}$ are k-ideals satisfying $(\mathfrak{b}, \mathfrak{q}) = \mathfrak{O}$ and $\mathfrak{a}_1$ is divisible only by such k-prime ideals as already divide $\mathfrak{q}$. In case $m = 2$ and $\tau = 1$, we further have $\mathfrak{a}_1 = \mathfrak{a} = (\operatorname{cont} S, \mathfrak{q})$ and $\mathfrak{b} = k$-prime ideal $\mathfrak{p}$ satisfying $\left[\frac{-s_0}{\mathfrak{p}}\right] = +1$. Thus by Lemma 6, in view of (4.1) and the fact that S represents s_{11} primitively mod $\mathfrak{q}$, there corresponds, to a natural number b, an h-matrix $S_1 \equiv S \bmod \mathfrak{q}$ such that S_1 represents s_{11} *primitively* mod $\mathfrak{q}\mathfrak{b}^b$, so that S_1 is equivalent mod $\mathfrak{q}\mathfrak{b}^b$ to a matrix with s_{11} as the first element, and

$$(4.40) \qquad |S_1| \equiv s_0 x x^\tau \bmod \mathfrak{q}\mathfrak{b}^b, \qquad (x, \mathfrak{q}\mathfrak{b}) = \mathfrak{O} .$$

Thus we may already assume S to satisfy (4.40). Then by Lemma 1 (using the result in case of one variable),

$$(4.41) \qquad |S^*| \equiv s_0^* x x^\tau \bmod \mathfrak{q}^*, \qquad (x, \mathfrak{q}^*) = \mathfrak{O} .$$

Thus the '$*$system' satisfies the congruence condition (4.1).

Now let $\tau = 1$. Define $\varrho^* = s_{11}^{-m-1}\varrho$, where ϱ satisfies (4.3) and $(s_{11}, \mathfrak{g}) = \mathfrak{o}$. By Corollary 1 of Lemma 5 and (4.39),

$$(4.42) \qquad G(\varrho^*, s_{11}S) = G(\varrho^*, S^*[D]) = N(s_{11})\, G(\varrho^*, S^*) .$$

The condition in the corollary viz. $\left(\operatorname{den}(4^{-1}\varrho^{*-1}s_{11}^{-1}S^{-1}), s_{11}\right) = \mathfrak{o}$ is satisfied in view of (4.41), exactly as in step II. On the other hand

$$(4.43) \qquad G(\varrho^*, s_{11}S) = N(s_{11}^m) \cdot G(s_{11}\varrho^*, S) .$$

From (4.2), (4.42) and (4.43), it follows that the Gauss sum condition is satisfied by the '$*$system'.

Thus the '$*$system' satisfies the conditions of the theorem and we have the additional properties that $u_l^* > 0$ for $l = 1, \ldots, r$ and $s_{11}^* = 1$.

Suppose now that the theorem is proved for the '$*$ system', i.e. there exists an integral h-matrix S_0^* satisfying

$$(4.44) \qquad S_0^*[U] \equiv S^* \bmod \mathfrak{q}^*, \quad E_{S_0^*} U = U, \quad U \text{ primitive mod } \mathfrak{q}^*,$$
$$r(S_0^*) = m^*, \ \operatorname{sig}(S_0^*) = \{(u_l^*, v_l^*)\}, \ \delta(S_0^*) = \mathfrak{s}_0^*, \ K(S_0^*) = \langle s_0^* \rangle .$$

Then (4.44) and (4.39) give

$$(4.45) \qquad S_0^*[UD] \equiv s_{11} S \bmod \mathfrak{q}^* .$$

Now $\left(\delta(UD), \mathfrak{q}^*\right) = (s_{11})$ and $s_{11}^2 \mid \mathfrak{q}^*$. Thus in view of [8], Lemma 26, there exists an integral matrix D_1 satisfying

$$(4.46) \qquad E_{S_0^*} D_1 = D_1, \quad \delta(D_1) = (s_{11})$$

and

$$(4.47) \qquad UD = D_1 U_1, \quad U_1 \text{ primitive mod } q^* \quad \text{and} \quad E_{D_1} U_1 = U_1 .$$

Define

$$(4.48) \qquad S_0 = s_{11}^{-1} S_0^*[D_1] .$$

S_0 is integral in view of (4.45), (4.47) and (4.48) exactly as in step I. It is easy to see that S_1 satisfies all other requirements.

We have thus proved that *for* $m \geqslant 2$, *it is enough to prove the theorem for the case* $u_l > 0$ $(l = 1, \ldots, r)$ *and* $s_{11} = 1$.

Step V. Completion of the proof by induction.

Let $m = 1$. If s_0 and $\mathfrak{C}$ are as defined as in the theorem and if $\mathfrak{C}^{-1} = (a, b)$, then

$$S_0 = \begin{pmatrix} s_0 a a^\tau & s_0 a^\tau b \\ s_0 a b^\tau & s_0 b b^\tau \end{pmatrix}$$

can easily be seen to satisfy $r(S_0) = 1$, $\delta(S_0) = \mathfrak{s}_0$, $K(S_0) = \langle s_0 \rangle$, $\operatorname{sgn}(s_0) = \{(-1)^{v_l}\}$; also S_0 is integral. Finally $S_0 \sim s_0 \bmod \mathfrak{q}$ and (4.1) together imply $S_0 \sim S \bmod \mathfrak{q}$.

Now let $m \geqslant 2$, and let us assume the theorem proved for $m-1$. We will show that it holds for m, with $s_{11} = 1$ and $u_l > 0$ for $l = 1, \ldots, r$. Define

$$F = \begin{pmatrix} 1 & s_{12} \ldots s_{1m} \\ 0 & E \end{pmatrix} .$$

Then F is unimodular and

$$S = \begin{pmatrix} 1 & 0 \\ 0 & S^* \end{pmatrix}[F]. \tag{4.49}$$

Consider $m^* = m-1$, $u_l^* = u_l - 1$ and $v_l^* = v_l$ for $l = 1, \ldots, r$, $s_0^* = s_0$, $\mathfrak{s}_0^* = \mathfrak{s}_0$, and $\mathfrak{q}^* = \mathfrak{q}$. Then $u_l^* + v_l^* = m^*$, $s_0^* \mathfrak{s}_0^{*-1} = \mathfrak{C}\mathfrak{C}^\tau$ and $(\mathfrak{C}, \mathfrak{q}^*) = \mathfrak{O}$, $4ds_0^*\mathfrak{P} \mid \mathfrak{q}^*$ since $\mathfrak{P}^* = \mathfrak{P}$, and $\operatorname{sgn}(s_0^*) = \{(-1)^{v_l^*}\}$ since $v_l^* = v_l$. (4.1) is satisfied by the '$*$system' in view of the fact that $|S| = |S^*|$ (see (4.49)).

Now let $\tau = 1$. By property (i) of the Gauss sums and (4.49), we have

$$G(\varrho^*, S) \cdot \big(G(\varrho^*, 1)\big)^{-1} = G(\varrho^*, S^*) \tag{4.50}$$

where $\varrho^* = \varrho$ satisfies (4.3). Substituting, for $G(\varrho^*, S)$ from (4.2) and for $G(\varrho^*, 1)$ from Lemma 5, in (4.50), we see that the '$*$system' satisfies the Gauss sum condition.

Thus the '$*$system' satisfies all the conditions of the theorem and $m^* = m-1$. Therefore by the induction assumption there exists an integral h-matrix $S_0^* \sim S^* \bmod \mathfrak{q}^*$ such that $r(S_0^*) = m-1$, $\operatorname{sig}(S_0^*) = \{(u_l - 1, v_l)\}$, $\delta(S_0^*) = \mathfrak{s}_0$, $K(S_0^*) = \langle s_0 \rangle$. Then

$$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & S_0^* \end{pmatrix}$$

can easily be seen to have all the required properties.

This completes the proof of the theorem.

References

[1] H. Braun, *Geschlechter quadratischer Formen*, J. Reine. Angew. Math. 182 (1940), pp. 32-49.

[2] — *Zur Theorie der hermitischen Formen*, Abh. Math. Sem. Hans. Univ. 14 (1941), pp. 61-150.

[3] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, New York 1948.

[4] — *Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper*, Math. Werke, Göttingen (1959), pp. 178-197.

[5] E. Landau, *Über Ideale und Primideale in Idealklassen*, Math. Zeit. 2 (1918), pp. 52-154.

[6] H. Minkowski, *Gesammelte Werke*, Bd. I.

[7] C. L. Siegel, *Über die analytische Theorie der quadratischer Formen I*, Ann. Math. 36 (1935), pp. 527-606.

[8] — *Über die analytische Theorie der quadratischer Formen III*, Ann. Math. 38 (1937), pp. 212-291.

TATA INSTITUTE OF FUNDAMENTAL RESEARCH, BOMBAY

Reçu par la Rédaction le 27. 2. 1963

ACTA ARITHMETICA
VIII (1963)

On the diophantine equation $y^2 - k = x^3$

by

W. Ljunggren (Oslo)

1. Let k denote any rational integer. The problem of solving the equation

$$y^2 - k = x^3, \quad k \neq 0 \tag{1}$$

in rational integers x, y has been the subject of many papers and has attracted great interest for more than three centuries. However, no general method is known for determining all solutions of a given equation of the form (1). A summary of earlier results is given in a paper by T. Nagell [8] and in two papers by O. Hemer [3], [4]. Cf. L. J. Mordell [6] for the history of this and allied problems.

It is well-known that the solution of (1) can be brought back to the solution in rational integers u, v of a finite number of equations of the type $f(u, v) = 1$, where $f(u, v)$ is a binary cubic form with integral coefficients. By virtue of a famous theorem due to A. Thue [15] the equation (1) has only a finite number of solutions for a given k.

These cubic forms have negative or positive discriminants according as $k > 0$ or $k < 0$. In case $k > 0$ one has solved all equations with $k \leqslant 100$. An essential tool in obtaining this result is the use of the theorems due to T. Nagell and B. Delaunay [8] concerning cubic forms with negative discriminant. In case $k < 0$ is the problem much more difficult since there are not yet general theorems as to the representations of 1 by binary cubic forms with positive discriminant. Cf. Ljunggren [5].

It was shown by Mordell [7] that the diophantine equation

$$v^2 = 4u^3 - g_2 u - g_3, \tag{2}$$

where g_2 and g_3 are given rational integers, has at most a finite number of rational integral solutions (u, v), when its right-hand side has no squared factor in u. He proved that to every integral solution (u, v) of (2) there corresponded a binary *quartic* with invariants g_2 and g_3 which represented unity, and conversely.

In (1) we have $g_2 = 0$, $g_3 = -4k$, and the problem is now to find all representations of 1 by certain binary, biquadratic forms having