ON GENERALIZED QUATERNIONS

BY
GORDON PALL

1. **Introduction.** In this article we shall present a basic investigation of the arithmetics of generalized quaternions, as they arise naturally out of the study of integral ternary quadratic forms. It was, indeed, out of the theory of quadratic forms, that (perhaps unnoticed) generalized quaternions first originated, in a form suitable for use in arithmetic. Thus, in 1854, Hermite [6](1) obtained a general expression for the automorphs of a ternary quadratic form. He found it simpler to express the automorphs, not of $f=\sum a_{\alpha\beta}x_\alpha x_\beta$ ($a_{\alpha\beta}=a_{\beta\alpha}$; $\alpha,\beta=1,2,3$), but of its adjoint adj $f=\sum A_{\alpha\beta}x_\alpha x_\beta$, where the $A_{\alpha\beta}$ are the cofactors of the $a_{\alpha\beta}$. (As the automorphs of f are the transpose of those of adj f, this involves no loss.) Hermite expressed the automorphs of adj f (cf. §2) by means of four parameters, say t_0, t_1, t_2, t_3, subject to the condition $t_0^2+\sum A_{\alpha\beta}t_\alpha t_\beta=1$. Now a product of two automorphs is, from their very nature, again an automorph. Hermite found that the product of the two automorphs corresponding to the parameters u_i and t_i is given by v_i, where

$$
\begin{aligned}
v_0 &= u_0t_0 - \sum A_{\alpha\beta}u_\alpha t_\beta,\\
v_\alpha &= u_0t_\alpha + u_\alpha t_0 + (u_2t_3 - u_3t_2)a_{1\alpha} + (u_3t_1 - u_1t_3)a_{2\alpha} + (u_1t_2 - u_2t_1)a_{3\alpha}.
\end{aligned}
\tag{1}
$$

Further, under (1), there holds the "composition identity"

$$
(u_0^2 + \sum A_{\alpha\beta}u_\alpha u_\beta)(t_0^2 + \sum A_{\alpha\beta}t_\alpha t_\beta) = (v_0^2 + \sum A_{\alpha\beta}v_\alpha v_\beta). \tag{2}
$$

This formula for *multiplying* the quaternion (u_0, u_1, u_2, u_3) by (t_0, t_1, t_2, t_3) to obtain the product quaternion (v_0, v_1, v_2, v_3) is the essence of a quite general, linear, associative, quaternion algebra. U. V. Linnik [11] proposed to call the elements of this algebra *hermitions*. The author developed some factorization properties of these algebras in 1938 [12], in the special case where the matrix $(a_{\alpha\beta})$ is integral. These results are perfected in the present article, and extended to the case where the form $f=\sum a_{\alpha\beta}x_\alpha x_\beta$ is integral, that is, the $a_{\alpha\alpha}$ and $2a_{\alpha\beta}$ are integers.

With each form f, where the $a_{\alpha\beta}$ are rational numbers and $|a_{\alpha\beta}|\neq 0$, is associated the quaternion algebra defined by (1). The elements of this algebra can be written as $u=u_0+i_1u_1+i_2u_2+i_3u_3$, where the u_i are rational numbers and the i_α satisfy the multiplication table of §2(1). If we apply the rational transformation $U=(u_{\alpha\beta})$ to $(a_{\alpha\beta})$, then by Theorem 1, the basal elements i_α are replaced by $k_\alpha=U_{1\alpha}i_1+U_{2\alpha}i_2+U_{3\alpha}i_3$, where the $U_{\alpha\beta}$ are the cofactors of

Presented to the Society, November 24, 1945; received by the editors July 26, 1945.

(1) Numbers in brackets refer to the Bibliography at the end of the paper.

the $u_{\alpha\beta}$. Thus the algebras associated with $(a_{\alpha\beta})$ and $U'(a_{\alpha\beta})U$ are rationally equivalent. Indeed, the correspondence between elements $u_0+\sum u_\alpha i_\alpha$ and $v_0+\sum v_\alpha k_\alpha$ becomes actual equality under the transformation $v_0=u_0$, $u_\alpha=U_{\alpha 1}v_1+U_{\alpha 2}v_2+U_{\alpha 3}v_3$.

The system of Hamiltonian quaternions (for which $i_\alpha^2=-1$, $i_2i_3=i_1=-i_3i_2$, and so on) is associated with $f_1=x_1^2+x_2^2+x_3^2$, or with the identity matrix.

With every integral form f is associated a system $\sum(f)$ of integral quaternions, consisting of the quantities $t=t_0'+\sum i_\alpha t_\alpha$, where $t_0'=t_0+2^{-1}\sum\epsilon_\alpha t_\alpha$, and t_0, t_1, t_2, t_3 are rational integers (§3). Here the ϵ_α have the values 0 or 1 in accordance with §3(1). The sum, difference, and product of two elements of $\sum(f)$ are in $\sum(f)$. The trace $2t_0'$ and the norm $(t_0+2^{-1}\sum\epsilon_\alpha t_\alpha)^2+\sum A_{\alpha\beta}t_\alpha t_\beta$ are rational integers. The quantities 1 and $j_\alpha=i_\alpha+\epsilon_\alpha/2$ $(\alpha=1, 2, 3)$ form a basis of $\sum(f)$. If we apply a unimodular transformation U to f to obtain g, the systems $\sum(f)$ and $\sum(g)$ are isomorphic, and the trace and norm of each element are invariant. If U is integral, but $|U|>1$, $\sum(g)$ is a subset of $\sum(f)$. The system $\sum(f)$ is maximal in the sense of Dickson, if and only if the form adj f cannot be derived by an integral transformation from any form adj g, where g is also integral (cf. §3).

If $f=f_1$, then $\sum(f)$ consists of the Lipschitz integral quaternions

$$t_0+i_1t_1+i_2t_2+i_3t_3, \tag{3}$$

the t_i rational integers, the i_α the Hamiltonian units. This system is not maximal. For, if $g_1=x_1^2+x_2^2+x_3^2+x_2x_3+x_3x_1+x_1x_2$, then adj $g_1=(3x_1^2+3x_2^2+3x_3^2-2x_2x_3-2x_3x_1-2x_1x_2)/4$, and adj $f_1=y_1^2+y_2^2+y_3^2$ is obtained from adj g_1 by the transformation $x_1=y_2+y_3$, $x_2=y_1+y_3$, $x_3=y_1+y_2$ of determinant 2.

Any system $\sum(f)$ can be put (cf. §11) into other forms by applying rational transformations, and expressing the conditions on the coefficients of elements in the resulting algebras which correspond to the integrality of the elements of $\sum(f)$. For example, since the diagonal multiplication table for f_1 is simpler than that for g_1 (in the preceding paragraph), we may seek a set of elements in the quaternion algebra for f_1 arithmetically equivalent to the set $\sum(g_1)$. With an eye on the identity

$$\text{adj } g_1=(x_2+x_3-x_1)^2/4+(x_3+x_1-x_2)^2/4+(x_1+x_2-x_3)^2/4 \tag{4}$$

and noting that $\epsilon_1=\epsilon_2=\epsilon_3=1$ for g_1, we set

$$\begin{aligned} y_0&=2x_0+x_1+x_2+x_3, & y_1&=x_2+x_3-x_1,\\ y_2&=x_3+x_1-x_2, & y_3&=x_1+x_2-x_3, \end{aligned} \tag{5}$$

whence the norm-form $(x_0+2^{-1}\sum\epsilon_\alpha x_\alpha)^2+\sum A_{\alpha\beta}x_\alpha x_\beta$ becomes $(y_0^2+y_1^2+y_2^2+y_3^2)/4$. On solving (5) for the x_i we obtain $2x_1=y_2+y_3$, $2x_2=y_3+y_1$, $2x_3=y_1+y_2$, $2x_0=y_0-y_1-y_2-y_3$, whence the integrality condition that $x_0+\sum j_\alpha x_\alpha$

have integral coordinates is equivalent to the condition that y_0, y_1, y_2, y_3 are integers satisfying

$$y_0 \equiv y_1 \equiv y_2 \equiv y_3 \pmod 2; \tag{6}$$

while the corresponding integral quaternions are given by

$$(y_0 + i_1y_1 + i_2y_2 + i_3y_3)/2, \tag{7}$$

the i_α being the Hamiltonian units. Thus this system of integral quaternions, given by A. Hurwitz, is isomorphic with $\sum(g_1)$. The form g_1, we should observe, is the reduced, positive-definite, integral ternary of least determinant $(=1/2)$.

The much debated question of whether one should use the Hurwitz system rather than that of Lipschitz is thus seen from the point of view of quadratic form theory to amount to this, whether one should confine attention to fundamental forms (not derivable from integral forms of a smaller determinant) or not. The form $f_1=x_1^2+x_2^2+x_3^2$ is, to the worker with quadratic forms, just as important as the form g_1, even though the form adj f_1 may not be fundamental. Similarly, from the standpoint of quadratic forms, nonmaximal systems of integral quaternions are just as important as maximal systems, even though they may not be as simple (for, if adj g is carried into adj f by an integral transformation of determinant k, the primes dividing k will play an exceptional role in $\sum(f)$).

In this article we shall not confine attention to maximal systems. We shall make no restriction on f, for arithmetical applications, except that it be integral. However, we shall sometimes be compelled to restrict the norms of certain quaternions, and it will usually be seen that these restrictions are vacuous when the system is maximal.

Out of personal experience with Hurwitz or Lipschitz quaternions, the author may say that it makes no essential difference which one uses. Using Lipschitz quaternions one must sometimes restrict the norm to be odd, but this is counterbalanced by the simplifying fact that there are fewer units.

Interesting points to which we may call attention here are: the easily remembered multiplication table (§2(1)), and its simple law of transformation (Theorem 1); the definition of a system of integral quaternions (§3); the theorem on the uniqueness of factorization of primitive quaternions in every system $\sum(f)$ (§5); the algorithm for finding factors of a given norm in §6; the exact formula (when F is fundamental) for the integral automorphs of adj f and the norm-form F, which points to the essential rightness of our definition of integral quaternion (§7); the determination of *all* systems with positive-definite norm-forms in which factorization is always possible (Theorems 10 and 11). We may point also to Theorem 12, which states that there do not exist genera of more than one class of positive-definite norm-forms, which do not also contain classes of minimum greater than 1; there should surely be an easier way of proving this.

Principal notations. f denotes a ternary form of matrix $(a_{\alpha\beta})$; the matrix of adj f is $A=(A_{\alpha\beta})$; the multiplication table of its algebra is given in §2, (1) or (2); the basal elements of the algebra are usually designated $1, i_1, i_2, i_3$; elements of the algebra, *quaternions*, are usually denoted by the letters $t, u, \cdots, z$, and their coordinates indicated by subscripts. If f is an integral form, a basis of the integral elements $\sum(f)$ is $1, j_1, j_2, j_3$ (§3); $d=4\left|a_{\alpha\beta}\right|$; F always denotes the *norm-form* $(x_0+\epsilon_1x_1/2+\epsilon_2x_2/2+\epsilon_3x_3/2)^2+\sum A_{\alpha\beta}x_\alpha x_\beta$, where the ϵ_α ($=0$ or 1) are chosen to make F an integral form. Subscripts α and β always range over 1, 2, 3; subscripts i and j over 0, 1, 2, 3, unless otherwise indicated. F, G denote quaternary forms; other italic capitals denote square matrices and their linear transformations; $T'=$ transpose of matrix T; $\bar{t}=$ the conjugate of the quaternion t (§2).

We shall employ freely (without indications of proof) certain facts about the form-residues modulo k to which a quadratic form can be reduced by integral transformations of determinant prime to k; certain standard properties of genera of quadratic forms; and the invariants c_p of quadratic forms under rational, linear transformations. The latter invariants are due to Hasse [4], and in the ternary case to Hensel [5, p. 337]. An exposition of all these tools will be given shortly in a book by the author.

2. **The Hermite quaternion algebra.** The quaternion algebra pertaining to the form f, or symmetric matrix $(a_{\alpha\beta})$, will now be defined. This algebra has four basal elements $1, i_1, i_2, i_3$ satisfying the multiplication table

$$(1)\qquad \begin{aligned} i_\alpha^2 &= -A_{\alpha\alpha} \qquad (\alpha=1,2,3),\\ i_2i_3 &= -A_{23}+\sum a_{1\alpha}i_\alpha, \qquad i_3i_2 = -A_{32}-\sum a_{1\alpha}i_\alpha, \end{aligned}$$

with i_3i_1, and so on, obtained by permuting subscripts cyclically. In matrix notations, the multiplication table can be written

$$(2)\quad \mathfrak{i}\mathfrak{i}' = -A+K, \text{ where } K=\begin{bmatrix} 0 & \sum a_{3\alpha}i_\alpha & -\sum a_{2\alpha}i_\alpha \\ -\sum a_{3\alpha}i_\alpha & 0 & \sum a_{1\alpha}i_\alpha \\ \sum a_{2\alpha}i_\alpha & -\sum a_{1\alpha}i_\alpha & 0 \end{bmatrix},$$

where $\mathfrak{i}'$ denotes the row vector (i_1, i_2, i_3) and the prime indicates "transpose." The elements of the algebra have the form

$$(3)\qquad x=x_0+\sum i_\alpha x_\alpha = x_0+\mathfrak{i}'\xi,$$

where $\xi'=(x_1, x_2, x_3)$; and the x_i may range over some field containing the coefficients $a_{\alpha\beta}$.

It is sometimes more convenient to speak of the i_α as pertaining to the matrix $(A_{\alpha\beta})$. Note that $(A_{\alpha\beta})$ is the adjoint also of $(-a_{\alpha\beta})$, and that the corresponding multiplication table is obtained by changing the i_α for $(a_{\alpha\beta})$ to their negatives.

We can easily verify that if $u=u_0+\sum i_\alpha u_\alpha$ and $t=t_0+\sum i_\alpha t_\alpha$, then $ut=v$ is given by Hermite's formulae (1) of §1.

If T is any nonsingular matrix of order 3,

$$x_0 + \mathfrak{i}'\xi = x_0 + \mathfrak{k}'\eta, \quad \text{where} \quad \xi = T\eta, \quad \mathfrak{k}' = \mathfrak{i}'T. \tag{4}$$

By (2), $\mathfrak{k}\mathfrak{k}' = T'\mathfrak{i}\mathfrak{i}'T = -T'AT+T'KT$. This suggests the following theorem.

THEOREM 1. *Let U denote a matrix of order 3 and nonzero determinant λ. If $(a_{\alpha\beta})$ is replaced by $(b_{\alpha\beta}) = U'(a_{\alpha\beta})U$, whence A is replaced by $B=T'AT$ (where $T'U=UT'=\lambda I$), then the basal elements k_α pertaining to B are related to the i_α of A by the linear transformation*

$$\mathfrak{k} = T'\mathfrak{i}. \tag{5}$$

We shall base our proof on the interesting identity:

$$C'[\mathfrak{p}^*]C = [\mathfrak{q}^*], \quad \text{where} \quad \mathfrak{q} = D\mathfrak{p}. \tag{6}$$

Here $\mathfrak{p}$ denotes any column vector, $\mathfrak{p}' = (p_1, p_2, p_3)$, and $[\mathfrak{p}^*]$ denotes the skew-symmetric matrix formed from $\mathfrak{p}$ as follows:

$$[\mathfrak{p}^*] = \begin{bmatrix} 0 & p_3 & -p_2 \\ -p_3 & 0 & p_1 \\ p_2 & -p_1 & 0 \end{bmatrix}; \tag{7}$$

C is any matrix of order 3, and D' is the matrix of its cofactors, that is, $CD=DC=\gamma I$, where $\gamma = |C|$. Obviously, the left side of (6) is skew-symmetric. We leave the verification of (6) to the reader.

To complete the proof of Theorem 1 we must show that $T'KT=[\mathfrak{q}^*]$, where $\mathfrak{q}=(b_{\alpha\beta})\mathfrak{k}$. We have immediately,

$$\begin{aligned} T'KT &= T'[\mathfrak{p}^*]T, \quad \text{where} \quad \mathfrak{p} = (a_{\alpha\beta})\mathfrak{i}, \\ &= [\mathfrak{q}^*], \qquad \text{where} \quad \mathfrak{q} = \lambda U'(a_{\alpha\beta})\mathfrak{i} = U'(a_{\alpha\beta})UT'\mathfrak{i} = (b_{\alpha\beta})\mathfrak{k}. \end{aligned}$$

The form $\sum A_{\alpha\beta}x_\alpha x_\beta$ is derivable from $x_1^2+x_2^2+x_3^2$ by means of a complex linear transformation $\xi=T\eta$, hence $A=T'T$. It follows from Theorem 1 that the basal elements i_α pertaining to A are related to the Hamiltonian units, say h_α (these being usually denoted by i, j, k), by the transformation $\mathfrak{i}=T'\mathfrak{h}$.

We define the conjugate $\bar{x}$ of x to be $\bar{x}=x_0-i_1x_1-i_2x_2-i_3x_3$. In the case of Hamiltonian quaternions, $\bar{x}x=\sum x_i^2$. Hence, by the preceding paragraph, there holds in our generalized quaternion algebra,

$$\bar{x}x = x\bar{x} = x_0^2 + \xi'A\xi = x_0^2 + \sum A_{\alpha\beta}x_\alpha x_\beta. \tag{8}$$

We call this the norm of x and denote it by Nx. It will be seen from (1) and the distributivity of multiplication that the conjugate of $(u_0+\sum i_\alpha u_\alpha)(t_0+\sum i_\alpha t_\alpha)$ is $(t_0-\sum i_\alpha t_\alpha)(u_0-\sum i_\alpha u_\alpha)$, that is

$$\overline{ut} = \bar{t}\cdot\bar{u}. \tag{9}$$

Hence if $v=ut$, then $\bar{v}=\bar{t}\bar{u}$, $v\bar{v}=ut\bar{t}\bar{u}=u\bar{u}\cdot t\bar{t}$, or $Nv=Nu\cdot Nt$. This is of course Hermite's identity (2) of §1.

The correspondence in (4) replaces each quaternion x by an equal quaternion, expressed in terms of a new basis. This correspondence is preserved under addition and, by Theorem 1, under multiplication. The "real part" x_0 of x, and the norm, are invariant.

We call x *pure* if $\bar{x}=-x$, whence $2x_0=0$. If x is pure and t is any quaternion, then $y=\bar{t}xt$ is also pure, and $Ny=Nx(Nt)^2$. Here Nx is given by the ternary form $\sum A_{\alpha\beta}x_\alpha x_\beta$. Thus if $Nt=1$, the linear transformation expressing the y_α in terms of the x_β, obtained on expanding $y=\bar{t}xt$, is an automorph of the form $\sum A_{\alpha\beta}x_\alpha x_\beta$. It is of determinant $+1$, and will be found to coincide with the general expression of Hermite, mentioned in the Introduction.

Indeed, we easily prove that $y=\bar{t}xt$ where $Nt=1$ gives the most general automorph of determinant $+1$ of any form $A=(A_{\alpha\beta})$, provided it is true for one particular form, say for the identity matrix I, or the matrix of $x_1x_3-x_2^2$ (a relatively easy case [1, pp. 22–23]). For, if E denotes the general automorph of determinant $+1$ of (say) I, and T is a particular transformation of I into A, then an obvious argument shows that $T^{-1}ET$ is the general automorph of determinant $+1$ of A. Let t denote the I-quaternion for which $y=\bar{t}xt$ expands into $\eta=E\xi$. Consider the corresponding equation in A-quaternions $y=\bar{t}xt$. Then the I-coordinates of y are those of the vector $T\eta$, and those of x are those of $T\xi$; cf. (4). Hence the A-equation $y=\bar{t}xt$ is equivalent to the linear transformation $T\eta=E(T\xi)$, or $\eta=(T^{-1}ET)\xi$. It therefore yields every automorph of determinant $+1$ of A.

LEMMA 1. *Let $(a_{\alpha\beta})$ be a rational, symmetric matrix of order 3, $|a_{\alpha\beta}|\neq 0$. Let $1, k_1, k_2, k_3$ be linearly independent quaternions in the algebra of $(a_{\alpha\beta})$ satisfying the same multiplication table as the basal elements $1, i_1, i_2, i_3$. Then there exists a quaternion q in the algebra and a sign $\sigma=\pm 1$ such that*

$$\sigma k_1 = qi_1q^{-1}, \qquad \sigma k_2 = qi_2q^{-1}, \qquad \sigma k_3 = qi_3q^{-1}. \tag{10}$$

For since k_α^2 is real and $1, k_1, k_2, k_3$ are linearly independent, k_α is pure and we can find a nonsingular rational matrix T such that $\mathfrak{k}=T'\mathfrak{i}$ (cf. (5)). Hence the multiplication table of the k_α is that connected with the form $T'AT$. By hypothesis, $T'AT=A$, or T is a rational automorph of A. Choose the sign of T and adjust σ so that $|T|=+1$. Then there exists a rational quaternion t such that the equation $y=txt^{-1}$ is equivalent to the matrix equation $\eta=T\xi$. If $x=i_1$, then $\xi'=(1, 0, 0)$, and $\eta'=\xi'T'$, whence η' is the first row of T'; thus the coordinates of η' are the i-coordinates of k_1, that is $k_1=ti_1t^{-1}$. Similarly, $k_2=ti_2t^{-1}$, $k_3=ti_3t^{-1}$.

3. **Quaternion arithmetics.** Let $(a_{\alpha\beta})$ be any nonsingular symmetric matrix of order 3, which is *semi-integral*. That is, a_{11}, a_{22}, a_{33}, and $2a_{23}$, $2a_{31}$, $2a_{12}$ are rational integers; and the ternary form $f=\sum a_{\alpha\beta}x_\alpha x_\beta$ is an integral form. The adjoint matrix $A=(A_{\alpha\beta})$ may have some of its coefficients with denomi-

nator 4. It will be convenient to introduce three numbers ϵ_1, ϵ_2, ϵ_3 each equal to 0 or 1 according as (respectively) $2a_{23}$, $2a_{31}$, $2a_{12}$ is even or odd. It is easily seen that

$$4A \equiv \begin{bmatrix} \epsilon_1^2 & \epsilon_1\epsilon_2 & \epsilon_1\epsilon_3 \\ \epsilon_2\epsilon_1 & \epsilon_2^2 & \epsilon_2\epsilon_3 \\ \epsilon_3\epsilon_1 & \epsilon_3\epsilon_2 & \epsilon_3^2 \end{bmatrix} \equiv \epsilon\epsilon' \pmod 2, \tag{1}$$

where ϵ' denotes the vector $(\epsilon_1, \epsilon_2, \epsilon_3)$.

The Hermite "norm-form" $x_0^2+\sum A_{\alpha\beta}x_\alpha x_\beta$ is not always integral for integral forms f. However, it is found (cf. (1)) that the form

$$\begin{aligned} F &= (x_0 + \epsilon_1x_1/2 + \epsilon_2x_2/2 + \epsilon_3x_3/2)^2 + \sum_{\alpha,\beta=1}^{3} A_{\alpha\beta}x_\alpha x_\beta \\ &= x_0^2 + \sum \epsilon_\alpha x_0x_\alpha + \sum (A_{\alpha\alpha} + \epsilon_\alpha^2/4)x_\alpha^2 + (2A_{23} + \epsilon_2\epsilon_3/2)x_2x_3 \\ &\quad + (2A_{31} + \epsilon_3\epsilon_1/2)x_3x_1 + (2A_{12} + \epsilon_1\epsilon_2/2)x_1x_2 \end{aligned} \tag{2}$$

always has integral coefficients. By replacing x_0 by $x_0+\sum h_\alpha x_\alpha$, where the h_α are integers, we can evidently replace the ϵ_α by arbitrary integers of the same respective parities. The form (2) then becomes identical with a form shown by Brandt to be the most general satisfying a certain type of composition identity. We shall refer to (2) as the *Brandt norm-form* or simply *norm-form*.

We now introduce new basal elements j_α by the equations

$$i_\alpha = j_\alpha - \epsilon_\alpha/2 \qquad (\alpha = 1, 2, 3), \tag{3}$$

with the ϵ_α as defined above. The elements of the algebra can be written as

$$t = t_0 + j_1t_1 + j_2t_2 + j_3t_3, \tag{4}$$

where the t_i are (say) rational. We define t to be an *integral quaternion* if the j-coordinates t_0, t_1, t_2, t_3 are rational integers. Clearly,

$$t = t_0 + 2^{-1}\sum \epsilon_\alpha t_\alpha + \sum i_\alpha t_\alpha = t_0' + \sum i_\alpha t_\alpha, \tag{5}$$

say, and the real part t_0' of an integral quaternion t is in general only half an integer, while the other coordinates (always integers) are the same for both the i_α and j_α.

The sum of two integral quaternions is evidently integral. Also,

$$\begin{aligned} j_\alpha^2 &= \epsilon_\alpha j_\alpha - A_{\alpha\alpha} - \epsilon_\alpha^2/4, \\ j_2j_3 &= (i_2 + \epsilon_2/2)(i_3 + \epsilon_3/2) = -A_{23} - 2^{-1}\sum a_{1\alpha}\epsilon_\alpha - \epsilon_2\epsilon_3/4 \\ &\quad + a_{11}j_1 + (a_{12} + \epsilon_3/2)j_2 + (a_{13} + \epsilon_2/2)j_3. \end{aligned} \tag{6}$$

Here $A_{23}+2^{-1}\sum a_{1\alpha}\epsilon_\alpha+\epsilon_2\epsilon_3/4=(a_{12}+\epsilon_3/2)(a_{31}+\epsilon_2/2)-a_{11}(a_{32}+\epsilon_1/2)+a_{11}\epsilon_1$, and is always integral. Hence a product of integral quaternions is always integral.

The norm of t evidently coincides with the Brandt norm-form in the j-coordinates of t as variables, and with the Hermite norm-form in the i-coordinates. If t is integral, Nt is an integer. The same is true of $t+\bar{t}$, or $2t_0'$. Hence t satisfies the algebraic equation $t^2-2t_0't+Nt=0$ in which the coefficients are rational integers.

A quaternion is called *primitive* if it is integral, and the g.c.d. of its j-coordinates t_0, t_1, t_2, t_3 is 1; primitive mod κ if this g.c.d. is prime to κ; *purely-integral* if it is pure and t_1, t_2, and t_3 are integers (*pure* meaning, even if j-coordinates are used, that $t_0+2^{-1}\sum\epsilon_\alpha t_\alpha=0$); *purely-primitive* if it is purely-integral and the g.c.d. of t_1, t_2, t_3 is 1. A purely-integral quaternion is therefore not integral unless $\sum\epsilon_\alpha t_\alpha$ is even.

Our set of integral elements has all the properties prescribed by L. E. Dickson [3(a), p. 141; (b), p. 154] for the integral elements of an algebra, except that in some cases our set is not maximal, and can be imbedded in a larger set of integral elements.

It can easily be shown directly, or by using some results of Brandt, or of C. G. Latimer [10], that the set $\sum(f)$ is maximal if and only if adj f is fundamental, in the sense that adj f cannot be obtained by an integral linear transformation of determinant greater than 1 from the adjoint of an integral form. For, if $d=4\left|a_{\alpha\beta}\right|$, it is easy to prove that adj f *is fundamental if and only if*

(7) d is squarefree, and $c_p=-1$ for each prime p in d.

(In view of Theorem 7, the same result holds with F in place of adj f.) An examination of Latimer's work will show that every maximal set of integral elements in a rational generalized quaternion algebra is associated with a ternary form satisfying (7). It should be noted that he appears in his work to omit the condition that c_2 is -1 when d is even (an essential condition if f is indefinite); and that, after transforming his problem so that in effect $\epsilon_1=1$ and $\epsilon_2=\epsilon_3=0$, he uses as his key form the norm of $2x_1i_1+x_2i_2+x_3i_3$ (integrality requiring that the coefficient of i_1 in a pure quaternion is even), whence his matrix Γ is obtained from our A by multiplying the first row and column by 2.

Several writers have investigated canonical bases of (maximal) integral sets. Since our multiplication table is so easy to remember, handle, and transform, we prefer not to canonicize it any further, but rather, when we have the need, to use all the resources of quadratic form theory to obtain the most expedient form for a particular problem.

4. **Integrality is preserved if T is unimodular.** We prove somewhat more. Suppose T is an integral matrix such that $B=T'AT$ is the adjoint of a semi-integral matrix. (This is always true if $\left|T\right|=1$.) To see that integral quaternions associated with B are still integral when referred back to A, we need only show that

(1) $$\sum\epsilon_\alpha x_\alpha\equiv\sum\epsilon_\alpha^* y_\alpha \pmod 2,$$

where the ϵ_α^* are the parameters 0 or 1 related to B; and where $\xi = T\eta$, $x_0 + 2^{-1}\sum \epsilon_\alpha x_\alpha = y_0 + 2^{-1}\sum \epsilon_\alpha^* y_\alpha$.

Now $4A \equiv \epsilon\epsilon' \bmod 2$ by §3(1). Hence $4B \equiv \epsilon^*\epsilon^{*\prime} \equiv T'4AT \equiv T'\epsilon\epsilon' T \bmod 2$. Hence $\epsilon^{*\prime} \equiv \epsilon' T$, and $\sum \epsilon_\alpha x_\alpha = \epsilon'\xi = \epsilon' T\eta \equiv \epsilon^{*\prime}\eta \equiv \sum \epsilon_\alpha^* y_\alpha \bmod 2$.

Note that the transformation replacing the norm-form $(x_0 + 2^{-1}\sum \epsilon_\alpha x_\alpha)^2 + \xi' A\xi$ by the norm-form $(y_0 + 2^{-1}\sum \epsilon_\alpha^* y_\alpha)^2 + \eta' B\eta$ is the integral transformation $\xi = T\eta$, $x_0 = y_0 + (\epsilon^{*\prime} - \epsilon' T)\eta/2$ (see §8).

5. The factors of a given norm of a primitive quaternion are essentially unique. If $v = ut$ in integral quaternions, t is a *right-divisor*, u is a *left-divisor*, of v. Necessarily, $Nt \mid Nv$. We designate *units*, that is integral quaternions of norm 1, by the letter θ. The quaternions θt are called *left-associates* of t; all, or none, are right-divisors of v. By definition of integral quaternion, v is divisible by a rational integer m if and only if each of the j-coordinates of v is divisible by m. We now prove:

THEOREM 2. *Let x be primitive. If $Nt = m$, and t is a right-divisor of x, the only right-divisors of x with norm m are the left-associates θt, provided*

$$\text{(1)} \qquad \begin{cases} m \text{ is not divisible by any prime } p \text{ such that } p^2 \mid d \\ (\text{where } d = 4\lvert a_{\alpha\beta}\rvert) \text{ or such that } p \| d \text{ and } c_p = +1. \end{cases}$$

It will be noted that the restriction (1) on m is vacuous if the integral system is maximal (as we remarked in §1). The proof depends on three lemmas, from which the theorem will follow, since $x + zm$ and t have the same right-divisors of norm m, $t = ut_1$ with $Nt = Nt_1 = m$, $Nu = 1$, $u = \theta$.

LEMMA 2a. *If $x \equiv y \pmod m$, x and y have the same right-divisors of norm m.*

Proof. If $y = x + zm$ and $x = ut$ where $Nt = m$, then $y = (u + z\bar{t})t$.

LEMMA 2b. *If Nw is prime to m, x and wx have the same right-divisors of norm m.*

Proof. Choose q so that $qNw \equiv 1 \pmod m$. If $wx = ut$, $q\bar{w}wx = q\bar{w}ut \equiv x \pmod m$.

LEMMA 3. *If m satisfies (1), x is primitive, $x = ut$, and $Nt = m$, then we can choose an integral quaternion z such that $N(x + zm)/m$ is prime to m.*

Proof. Set $q = (Nx)/m$. Then

$$\text{(2)} \qquad N(x + zm)/m = q + x\bar{z} + z\bar{x} + z\bar{z}m,$$

and we set

$$\text{(3)} \qquad r = x\bar{z} + z\bar{x} = 2(x_0'z_0' - \sum A_{\alpha\beta}x_\alpha z_\beta).$$

We can apply to f any unimodular transformation to obtain a more convenient residue, since divisibility will be invariant under such transformation. We

interpolate here a lemma on form-residues embodying facts needed here and later.

LEMMA 4. *Let* $d=4|a_{\alpha\beta}|$. *If* p *is an odd prime not dividing* d *or dividing* d *at most once, we can assume*

$$f \equiv a_1x_1^2 + a_2x_2^2 + p^{\alpha_3}a_3x_3^2 \pmod{p^r}, \tag{4}$$

r *arbitrary, where* a_1, a_2, a_3 *are prime to* p, *and* α_3 *is* 0 *or* 1; *if* $\alpha_3=1$, $c_p=(-a_1a_2|p)$. *If* d *is odd,* f *is equivalent* mod 2^r *to the form*

$$f \equiv x_1x_2 + a_3x_3^2, \tag{5}$$

a_3 *odd; and if* $d\equiv 2 \pmod 4$ *and* $c_2=-1$, f *is equivalent* mod 2^r *to the form*

$$f \equiv x_1^2 + x_1x_2 + x_2^2 + 2a_3x_3^2, \tag{6}$$

a_3 *odd. Form-residues for coprime moduli can be achieved simultaneously.*

To continue with the proof of Lemma 3, if $p|m$ and $p\nmid q$, we make $q+r$ prime to m by taking $z\equiv 0 \pmod{p^2}$. If $p|m$, $p|q$, and $p\nmid d$, then by (4) with $\alpha_3=0$ and (5),

$$r \equiv 2(x_0'z_0' - a_2a_3x_1z_1 - a_3a_1x_2z_2 - a_1a_2x_3z_3) \pmod{p^2}, \text{ if } p > 2,$$

$$r \equiv 2[(x_0 + x_3/2)(z_0 + z_3/2) + a_3x_1z_2/2 + a_3x_2z_1/2 + x_3z_3/4]$$

$$\equiv (2x_0 + x_3)z_0 + a_3x_2z_1 + a_3x_1z_2 + (x_0 + x_3)z_3 \pmod 4, \text{ if } p = 2.$$

Clearly, x being primitive, $q+r$ is prime to p by choice of z mod p. Finally, the case $p|m$, $p|q$, $p\|d$, $c_p=-1$, cannot hold with x primitive:

LEMMA 5. *If* x *is primitive and* $m|Nx$, *then if* p *is a prime dividing* d *precisely once and satisfying* $c_p=-1$, m *cannot be divisible by* p^2.

For by (4) with $\alpha_3=1$ and (6),

$$Nx \equiv x_0'^2 + pa_3(a_2x_1^2 + a_1x_2^2) + a_1a_2x_3^2 \equiv 0 \pmod{p^2},$$

$$Nx \equiv x_0^2 + x_0x_3 + x_3^2 + 2a_3(x_1^2 - x_1x_2 + x_2^2) \equiv 0 \pmod 4,$$

whence x_0 and x_3, then x_1 and x_2, are seen to be divisible by p.

In view of Lemma 5, m has the following form:

(7) $m=2^\mu m_1m_2$, where μ is unrestricted ($\geqq 0$) if d is odd, μ is 1 or 0 if $d\equiv 2 \pmod 4$ and $c_2=-1$, $\mu=0$ otherwise; m_1 is squarefree, and consists only of odd primes p dividing d once and such that $c_p=-1$; m_2 contains no primes dividing $2d$.

6. Conditions for the existence of a right-divisor of norm m. A method of obtaining the right-divisors if any, of a given norm will now be given.

THEOREM 3. *Let* m *be a nonzero integer represented by some form in the genus*

of F, and assume §5(1), *x primitive, $m \mid Nx$. Then, by an algorithm explained below, every factorization*

$$x = ut, \tag{1}$$

in which $Nt = m$, is associated with a representation of the number 1 *by a certain quaternary form in the genus of F. Hence, unless the genus of F contains a class of forms which do not represent* 1, *there exists a right-divisor t of x, of norm m and necessarily (by Theorem* 2*) unique up to a left unit factor.*

By (1), $x\bar{t} \equiv 0 \bmod m$; conversely, if $x\bar{t} \equiv 0$ and $Nt = m$, then $x\bar{t} = um$ with u integral, $x\bar{t}t = utm$, $x = ut$. We seek the general solution t of the system of four congruences $x\bar{t} \equiv 0 \bmod m$, with the intention of substituting this general solution in the condition $Nt = m$.

If m is even we can use the residue

$$f \equiv jx_1^2 + x_1x_2 + jx_2^2 + \lambda x_3^2 \pmod{2^{3\mu}} \tag{2}$$

where $j = 0$ and λ is odd, except that $j = 1$ and $\lambda \equiv 2 \bmod 4$ if $d \equiv 2 \bmod 4$ and $c_2 = -1$. Simultaneously we can assume that

$$f \equiv a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \pmod{m_1m_2}, \tag{3}$$

where a_1, a_2, and a_3/m_1 are integers prime to m_1m_2, and $c_p = (-a_1a_2 \mid p) = -1$ for each prime p in m_1.

The four coordinates of $x\bar{t}$ in terms of the j_α must be divisible by m. In particular, on expanding $(x_0 + x_3/2 + \sum i_\alpha x_\alpha)(t_0 + t_3/2 - \sum i_\alpha t_\alpha)$ with $(a_{\alpha\beta})$ as in (2), and $(A_{\alpha\beta})$ as given by

$$\operatorname{adj} f \equiv \lambda(jx_1^2 - x_1x_2 + jx_2^2) + (j - 1/4)x_3^2,$$

and then using $i_1 = j_1$, $i_2 = j_2$, $i_3 = j_3 - 1/2$, we get

$$\begin{aligned}
&x_0t_0 + \lambda(jx_1 - x_2)t_1 + \lambda(jx_2)t_2 + (x_0 + jx_3)t_3 \equiv 0,\\
&x_1t_0 + (-x_0 - x_3)t_1 + jx_3t_2 + (x_1 - jx_2)t_3 \equiv 0,\\
&x_2t_0 + (-jx_3)t_1 + (-x_0)t_2 + (jx_1)t_3 \equiv 0,\\
&x_3t_0 + \lambda x_2t_1 + (-\lambda x_1)t_2 + (-x_0)t_3 \equiv 0, \bmod 2^\mu.
\end{aligned} \tag{4}$$

For the odd modulus m_1m_2 we can use the i-coordinates, since x_0' and t_0' are integral mod m_1m_2, and have

$$\begin{aligned}
&x_0't_0' + a_2a_3x_1t_1 + a_3a_1x_2t_2 + a_1a_2x_3t_3 \equiv 0,\\
&x_1t_0' - x_0't_1 + a_1x_3t_2 - a_1x_2t_3 \equiv 0,\\
&x_2t_0' - a_2x_3t_1 - x_0't_2 + a_2x_1t_3 \equiv 0,\\
&x_3t_0' + a_3x_2t_1 - a_3x_1t_2 - x_0't_3 \equiv 0, \bmod p^r,
\end{aligned} \tag{5}$$

where p^r ranges over each of the prime-powers in m_1m_2.

For success the following process requires that the number of independent congruences in (4) or (5) be two.

First, let $p \mid m_1$, whence $p \mid a_3$. Since $Nx \equiv x_0'^2 + a_2a_3x_1^2 + a_3a_1x_2^2 + a_1a_2x_3^2 \equiv 0$, $x_0' \equiv x_3 \equiv 0 \pmod{p}$. Hence the matrix of (5) has the first and fourth rows zero mod p, and the second and third $(x_1\ 0\ 0\ -a_1x_2)$ and $(x_2\ 0\ 0\ a_2x_1)$. Clearly, (5) can be solved for t_0' and t_3 (hence for t_0 and t_3) in terms of t_1 and t_2 (mod p).

Second, let $p=2$, $d \equiv 2 \pmod 4$, whence $j=\mu=1$. Then $Nx \equiv x_0^2 + x_0x_3 + x_3^2 \equiv 0 \pmod 2$, $x_0 \equiv x_3 \equiv 0 \pmod 2$, and the matrix of (4) reduces mod 2 like the preceding case; we can solve for t_0 and t_3 in terms of t_1 and t_2 mod 2.

If $p \nmid d$, it may be remarked that (4) or (5) will usually involve three independent congruences (if $p^r \mid Nx$ and $p \nmid x$). However, if $p^r \mid x_0'$ or $2^\mu \mid 2x_0 + x_3$, we shall prove that the number of independent congruences is two. For example, if $p \nmid x_3$, multiplying (5_2), (5_3), and (5_4) by $a_2a_3x_1$, $a_1a_3x_2$, and $a_1a_2x_3$, and adding, we get 0 mod p^r, whence (5_4) is a consequence of (5_2) and (5_3); using x_3, $-a_3x_2$, and a_3x_1 on (5_1), (5_2), and (5_3) shows the same for (5_1). As $p \nmid x_3$ and $p \mid a_2a_3x_1^2 + a_3a_1x_2^2 + a_1a_2x_3^2$ the determinant of the coefficients of t_0' and t_3 in (5_2) and (5_3) is prime to p, and we can solve for t_0' and t_3 in terms of t_1 and t_2 mod p^r. Similarly in (4) if $x_3 \equiv -2x_0 \pmod{2^\mu}$, then as $j=0$ and $2^\mu \mid -x_0^2 - \lambda x_1x_2$, (4_1) and (4_2) are proportional, and $(\lambda x_2)(4_2) + (\lambda x_1)(4_3) - x_0(4_4) \equiv 0$.

To secure $p^r \mid x_0'$ and $2^\mu \mid 2x_0 + x_3$, we use Lemma 2b, and the following lemma.

LEMMA 6. *If $p \nmid d$, and x is primitive, we can find an integral quaternion residue w mod p^s (s given not less than 0), such that Nw is prime to p, and the real part $2(wx)_0$ of $2wx$ is divisible by p^s.*

We use (2) with $j=0$ and modulus 2^s; (3) with a_3 prime to p and modulus p^s. Hence if $p=2$, $Nw \equiv w_0^2 + w_0w_3 - w_1w_2 \pmod 2$, and

$$(6) \qquad 2(wx)_0 \equiv w_0(2x_0 + x_3) + w_1(\lambda x_2) + w_2(\lambda x_1) + w_3(x_0 + x_1), \bmod 2^s,$$

and if $p>2$, $Nw \equiv w_0'^2 + a_2a_3w_1^2 + a_3a_1w_2^2 + a_1a_2w_3^2 \pmod p$, and

$$(7) \qquad (wx)_0 \equiv w_0'x_0' - a_2a_3w_1x_1 - a_3a_1w_2x_2 - a_1a_2w_3x_3 \pmod{p^s}.$$

Since x is primitive, (6) can be solved for one of the w_i, say $w_1 \equiv b_0w_0 + b_2w_2 + b_3w_3 \pmod{2^s}$. This implies mod 2 that $w_1 = 2v_1 + b_0v_0 + b_2v_2 + b_3v_3$, $w_0 = v_0$, $w_2 = v_2$, $w_3 = v_3$. Substituting this in the expression for Nw gives a quaternary form of determinant $(d/4)^2 \cdot 2^2$, whence not every term in v_0, v_2, v_3 has an even coefficient. Hence Nw can be made odd by specifying v_0, v_2, and v_3 mod 2, and then $2(wx)_0 \equiv 0$ mod 2^s by choice of w_1. A similar argument applies to (7).

To sum up, for each prime-power p^r in m, the condition $x\bar{l} \equiv 0$ mod p^r reduces to a pair of congruences such as $t_0 \equiv \alpha t_2 + \beta t_3$, $t_1 \equiv \gamma t_2 + \delta t_3 \pmod{p^r}$, where $\alpha, \beta, \gamma, \delta$ are integers; or what is the same thing, to

$$(8) \qquad t_0 = p^r s_0 + \alpha s_2 + \beta s_3, \qquad t_1 = p^r s_1 + \gamma s_2 + \delta s_3, \qquad t_2 = s_2, \qquad t_3 = s_3,$$

in which the s_i are arbitrary integers, a substitution of determinant p^{2r}. If these last expressions are substituted for the t_i in the system of congruences corresponding to $x\bar{l}\equiv 0 \pmod{p_2^{r_2}}$, where $p_2^{r_2}$ is another prime-power in m, we obtain four congruences in $s_0, \cdots, s_3$ equivalent, since p and p_2 are coprime, to $x\bar{l}\equiv 0 \pmod{p_2^{r_2}}$, and hence having a solution of determinant $p_2^{2r_2}$ expressing the s_i in terms of four new integer parameters. Continuing in this way, and finally compounding the linear substitutions, we see that the general solution of $x\bar{l}\equiv 0 \pmod{m}$ is given by a system of the type

$$t_i = \sum_{j=0}^{3} p_{ij}z_j, \qquad i = 0, \cdots, 3, \ p_{ij} \text{ integers}, \ |p_{ij}| = m^2. \tag{9}$$

Furthermore, for arbitrary integers $z_0, \cdots, z_3$ the t_i determined by (9) must satisfy

$$(t_0 + 2^{-1}\sum \epsilon_\alpha t_\alpha)^2 + \sum A_{\alpha\beta}t_\alpha t_\beta \equiv 0 \pmod{m}.$$

For they satisfy $x\bar{l}\equiv 0$, $x\bar{l}t\equiv 0$, $x(Nt)\equiv 0$, where x is primitive and Nt is a rational integer.

On substituting the expressions (9) for t_i in the equation

$$(t_0 + 2^{-1}\sum \epsilon_\alpha t_\alpha)^2 + \sum A_{\alpha\beta}t_\alpha t_\beta = m, \tag{10}$$

we obtain an equation of the form

$$\sum r_{ij}z_iz_j = m, \tag{11}$$

where the form on the left has integral coefficients. Also, by the preceding paragraph this form has a value divisible by m for all integers z_i and z_j. It follows that m divides every r_{ij}. Setting $r_{ij}=ms_{ij}$ we get

$$\sum s_{ij}z_iz_j = 1. \tag{12}$$

Conversely, for any solution $z_0, \cdots, z_3$ of (12), the integers t_i determined by (9) satisfy (10) along with $x\bar{l}\equiv 0 \pmod{m}$, hence (1).

Finally, to prove that F and $G=\sum s_{ij}x_ix_j$ are in the same genus, we need only show that they have the same index, the same determinant $d^2/16$, and the same form-residues modulo d^2. Let F and G stand for their own matrices. Since G was obtained from F by applying the transformation (9) of matrix $P=(p_{ij})$, and cancelling m, we have

$$P'FP = mG. \tag{13}$$

By (13), since $|P| = m^2$, the determinants of F and G are equal. Also, the indices are equal, since P is real, m is positive if F is definite, and the indices of F and $-F$ are the same if F is indefinite.

We assumed that m is representable by the genus of F. Hence $m = F(v_0, v_1, v_2, v_3)$, where the v_i are rational numbers of denominator prime to $2d$. Thus $m=Nv$, and $mF=N(vt)$ determines a linear transformation of

determinant m^2 of F into mF, with rational coefficients of denominators prime to $2d$. By (13), $P'mFP=m^2G$; hence F can be carried into G by a rational transformation with denominators divisible by m but by no other prime factors of $2d$. Hence, first, F and G have the same values for all their rational invariants c_p, and, second, it remains only to prove that F and G are equivalent mod p^r, where p divides both m and $2d$. That the last holds true follows from the easily proved lemma:

LEMMA 7. *Let $p\nmid d$; or $p\|d$ and $c_p=-1$. Then every integral quaternary form of determinant $d^2/16$ is equivalent to a form with the following residue* mod p^r:

$$x_0x_1+d^2x_2x_3, \quad \text{if } p=2 \text{ and } d \text{ is odd}; \tag{14}$$

$$x_0^2+x_0x_1+x_1^2+(d^2/18)(x_2^2+x_2x_3+x_3^2), \quad \text{if } p=2\|d \text{ and } c_2=-1; \tag{15}$$

$$x_0^2+nx_1^2+p(x_2^2+nx_3^2), \quad \text{if } p>2,\ p\|d \text{ and } c_p=-1. \tag{16}$$

In (16), $-n$ *denotes a certain quadratic non-residue* mod p.

This completes the proof of Theorem 3. The reader's attention should be drawn at this point to Theorems 11, 12, and 13.

When f is indefinite, then at least when adj f is fundamental, it follows from a well known theorem of A. Meyer [3(c), p. 54] and adj f is in a genus of one class. But it does not necessarily follow that this is true of F. However, Latimer's theorem that, in the indefinite and fundamental case, every one-sided ideal in an integral set is principal implies that if F is indefinite and fundamental, F is in a genus of one class. For, according to Brandt [2, p. 29], the ideal-classes correspond to the classes in the genus of F.

We shall in §15 prove a result showing that Theorem 3 is in some measure best possible.

A word should be added here about the restriction on m in Theorem 3. The genus of F represents all integers m (having the necessary sign if F is definite) for which $F(x_0, x_1, x_2, x_3)\equiv m \pmod{k}$ is solvable for every modulus k. It is easily seen that if F is fundamental, and in certain other cases, this congruence is solvable for every k. Hence in this case there is no restriction on m, except for sign when F is definite.

7. **The automorphs of adj f and F.** The integral automorphs of any integral ternary quadratic form can be expressed most conveniently by means of our systems of integral quaternions. If adj f is fundamental the result will be surprisingly precise.

We first make some remarks by way of orientation. The automorphs of g and κg are the same for any form g and constant κ. The automorphs of f are the transposes of those of adj f. For if $A=\text{adj } a$, and $\Delta=|a|$, $S'AS=A$ implies $S'ASa=\Delta I$, $S'A$ and SA are permutable, hence $SaS'=a$. If there is one automorph of determinant -1, all such are obtained by multiplying it on one side by each positive automorph, where *positive* signifies determinant $+1$.

The automorph $-I$ can be so used if the number of variables is odd. The form F has the automorph

$$\begin{bmatrix} 1 & \epsilon' \\ 0 & -I \end{bmatrix}, \tag{1}$$

I of order 3, of determinant -1. Hence the number of integral automorphs of F is double the number of its integral positive automorphs.

Our main result in this section is the following:

THEOREM 4. *Let f be integral and* adj f *be fundamental. Then every positive integral automorph $y_\alpha=\sum e_{\alpha\beta}x_\beta$ of* adj f *is obtained by equating i-coordinates in*

$$y = (\bar{t}xt)/Nt \qquad (x = \sum i_\alpha x_\alpha,\ y = \sum i_\alpha y_\alpha), \tag{2}$$

as t ranges over the primitive quaternions such that $Nt \mid d$. Every positive integral automorph $y_i=\sum h_{ij}x_j$ of $F=(x_0+2^{-1}\sum\epsilon_\alpha x_\alpha)^2+\sum A_{\alpha\beta}x_\alpha x_\beta$ is obtained by equating j-coordinates in

$$y = (txu)/Nt \qquad (x = x_0 + \sum j_\alpha x_\alpha,\ y = y_0 + \sum j_\alpha y_\alpha), \tag{3}$$

as t and u range over the primitive quaternions such that $Nt=Nu$ and $Nt \mid d$. All automorphs so obtained are integral, and each appears exactly twice, once for t and once for $-t$ in (2), *once for (t, u) and once for $(-t, -u)$ in* (3).

THEOREM 5. *If f is integral and* adj f *is not fundamental, then all the positive integral automorphs of* adj f, *or F, are included among the automorphs obtained as in Theorem* 4; *but among those so obtained there may be some which are not integral.*

We consider first the uniqueness property. If we apply to adj f a non-singular transformation T, as in Theorem 1, all quaternion equations will be transformed uniquely, and the automorphs will correspond as E to $T^{-1}ET$. Hence we can suppose if we wish that

$$f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2, \qquad a_1a_2a_3 \neq 0. \tag{4}$$

The expression (2) is homogeneous: it is unchanged if t is replaced by λt, λ scalar. Conversely, we prove the following lemma.

LEMMA 8. *If the coefficient field has characteristic not* 2, *then $\bar{t}xt/Nt=\bar{u}xu/Nu$ identically in x implies that t and u differ only by a scalar factor, which may however lie in a larger field.*

We can choose λ to make $Nt=\lambda^2 Nu$, and so can assume $Nt=Nu$. We shall verify that if the values of the nine elements of $\bar{t}xt$ are fixed, as well as the value of Nt, then t_it_j are uniquely determined $(i, j=0, 1, 2, 3)$, whence $\pm t$ is determined. The explicit expansion of (2) is D/Nt, where D is

$$\begin{bmatrix} t_0^2 + a_2a_3t_1^2 - a_3a_1t_2^2 - a_1a_2t_3^2 & 2a_1(t_0t_3 + a_3t_1t_2) & 2a_1(-t_0t_2 + a_2t_3t_1) \\ 2a_2(-t_0t_3 + a_3t_1t_2) & t_0^2 - a_2a_3t_1^2 + a_3a_1t_2^2 - a_1a_2t_3^2 & 2a_2(t_0t_1 + a_1t_2t_3) \\ 2a_3(t_0t_2 + a_2t_1t_3) & 2a_3(-t_0t_1 + a_1t_2t_3) & t_0^2 - a_2a_3t_1^2 - a_3a_1t_2^2 + a_1a_2t_3^2 \end{bmatrix}. \tag{5}$$

Clearly the value of $t_0^2+a_2a_3t_1^2+a_3a_1t_2^2+a_1a_2t_3^2$ $(=Nt)$ and the values of the three diagonal elements fix the values $4t_i^2$, and the nondiagonal elements determine $4t_it_j$.

Abbreviate $A_{\alpha\alpha}$ as A_α. Equating i-coordinates in $y=txu$ we get $y_i=\sum r_{ij}x_j$, where

$$
\begin{aligned}
&r_{00}=t_0u_0-A_1t_1u_1-A_2t_2u_2-A_3t_3u_3, && r_{01}=-A_1(t_0u_1+t_1u_0-a_1t_2u_3+a_1t_3u_2),\\
&r_{02}=-A_2(t_0u_2+t_2u_0+a_2t_1u_3-a_2t_3u_1), && r_{03}=-A_3(t_0u_3+t_3u_0-a_3t_1u_2+a_3t_2u_1),\\
&r_{10}=t_0u_1+t_1u_0+a_1t_2u_3-a_1t_3u_2, && r_{11}=t_0u_0-A_1t_1u_1+A_2t_2u_2+A_3t_3u_3,\\
&r_{12}=a_1(t_0u_3-t_3u_0-a_3t_1u_2-a_3t_2u_1), && r_{13}=-a_1(t_0u_2-t_2u_0+a_2t_1u_3+a_2t_3u_1),\\
&r_{20}=t_0u_2+t_2u_0-a_2t_1u_3+a_2t_3u_1, && r_{21}=-a_2(t_0u_3-t_3u_0+a_3t_1u_2+a_3t_2u_1),\\
&r_{22}=t_0u_0+A_1t_1u_1-A_2t_2u_2+A_3t_3u_3, && r_{23}=a_2(t_0u_1-t_1u_0-a_1t_2u_3-a_1t_3u_2),\\
&r_{30}=t_0u_3+t_3u_0+a_3t_1u_2-a_3t_2u_1, && r_{31}=a_3(t_0u_2-t_2u_0-a_2t_1u_3-a_2t_3u_1),\\
&r_{32}=-a_3(t_0u_1-t_1u_0+a_1t_2u_3+a_1t_3u_2), && r_{33}=t_0u_0+A_1t_1u_1+A_2t_2u_2-A_3t_3u_3.
\end{aligned}
\tag{6}
$$

The terms occur in sets of four; for example, the r_{ii} involve t_0u_0 and $A_\alpha t_\alpha u_\alpha$. The signs in different r_{ij} of a set differ in only two terms, so that if the algebraic sum is taken to make a particular term add four times, the other three terms will cancel. Thus if the values r_{ij} are fixed, the values $4a_1a_2a_3t_iu_j$ are fixed for every i and j. If Nt and Nu also have fixed nonzero values, either (t, u) or $(-t, -u)$ are thus uniquely determined.

It will be noted that (6) reduces to (5) when $\bar{u}=t$, the first row and column becoming Nt, 0, 0, 0.

We saw in §2 that the positive rational automorphs of adj f are given by (2), but did not determine the field restrictions on the t_i. They can indeed be restricted to be rational. For, f can be carried by a rational transformation into a form of type (4) with rational nonzero a_α. We can choose λ so that Nt is rational. The discussion following (5) shows that t_it_j are rational $(i, j=0, 1, 2, 3)$. Hence $t_i=u_is^{1/2}$, where the u_i are rational, and we can replace t by u.

Before going further we prove a similar result for the rational automorphs of F.

LEMMA 9. *Let $(a_{\alpha\beta})$ be rational. Then as t and u range over the rational quaternions associated with $(a_{\alpha\beta})$, such that $Nu=1/Nt$, then $y=txu$ ranges over all the positive rational automorphs of $F_0=x_0^2+\sum A_{\alpha\beta}x_\alpha x_\beta$.*

Our proof is similar to that of Hurwitz [7, p. 63] for Hamiltonian quaternions. First notice that if the lemma holds for $A=(A_{\alpha\beta})$, it holds for $B=T'AT$, where T is rational and of positive determinant. For then

$$
S=\begin{bmatrix}1 & 0\\ 0 & T\end{bmatrix}, \quad \text{where} \quad S^{-1}=\begin{bmatrix}1 & 0\\ 0 & T^{-1}\end{bmatrix},
\tag{7}
$$

gives a rational transformation of F_0 into the new norm-form $G_0=y_0^2+\sum B_{\alpha\beta}y_\alpha y_\beta$, and all rational automorphs of G_0 are given by $S^{-1}HS$, where H ranges over all rational automorphs of F_0. Let $y=txu$ be the equation which, on equating A-coordinates, expands into the matrix equation $y=Hx$, where $y'=(y_0, y_1, y_2, y_3)$, and so on. Applying the change of basis T, consider the corresponding equation $y=txu$ in B-quaternions. The A-coordinates of y and x are respectively y_0 and $T\eta$, x_0 and $T\xi$, that is, Sy and Sx. Hence the result of equating B-coordinates in $y=txu$ must be the system of linear equations $Sy=HSx$, or $y=S^{-1}HSx$, which is any desired automorph of G_0.

If $y_i=\sum h_{ij}x_j$ is a rational automorph of F_0, then multiplying by $1, i_1, i_2, i_3$ and adding, we get $y=h_0x_0+h_1x_1+h_2x_2+h_3x_3$, where $h_j=h_{0j}+h_{1j}i_1+h_{2j}i_2+h_{3j}i_3$ are rational, linearly independent quaternions; and we see that the result of substituting for y in $y\bar{y}$ or $y_0^2+\sum A_{\alpha\beta}y_\alpha y_\beta$ must be $x_0^2+\sum A_{\alpha\beta}x_\alpha x_\beta$. The problem of finding rational automorphs reduces to that of finding rational quaternions h_j satisfying

$$(8)\quad (h_0x_0+h_1x_1+h_2x_2+h_3x_3)(\bar{h}_0x_0+\bar{h}_1x_1+\bar{h}_2x_2+\bar{h}_3x_3)=x_0^2+\sum A_{\alpha\beta}x_\alpha x_\beta,$$

identically in x_0, x_1, x_2, x_3. Comparing coefficients of x_0^2 we have $h_0\bar{h}_0=1$, and we can define rational quaternions k_α by the equations

$$(9)\qquad h_1=k_1h_0,\qquad h_2=k_2h_0,\qquad h_3=k_3h_0.$$

Hence (8) reduces to

$$(10)\quad (x_0+k_1x_1+k_2x_2+k_3x_3)(x_0+\bar{k}_1x_1+\bar{k}_2x_2+\bar{k}_3x_3)=x_0^2+\sum A_{\alpha\beta}x_\alpha x_\beta.$$

On equating coefficients we see that

$$(11)\quad k_\alpha+\bar{k}_\alpha=0,\qquad k_\alpha\bar{k}_\alpha=A_{\alpha\alpha},\qquad k_\alpha\bar{k}_\beta+k_\beta\bar{k}_\alpha=2A_{\alpha\beta}\quad(\alpha,\beta=1,2,3).$$

We now assume $A_{\alpha\beta}=0$ if $\alpha\neq\beta$, although this may not be strictly necessary. Then on eliminating the $\bar{k}_\alpha$, we get

$$(12)\quad k_\alpha^2=-A_{\alpha\alpha},\qquad k_2k_3=-k_3k_2,\qquad k_3k_1=-k_1k_3,\qquad k_1k_2=-k_2k_1.$$

Hence

$$\overline{k_1k_2k_3}=\bar{k}_3\bar{k}_2\bar{k}_1=-k_3k_2k_1=k_2k_3k_1=-k_2k_1k_3=k_1k_2k_3.$$

Hence the quaternion $k_1k_2k_3$ is equal to its conjugate, and must be real. Since $N(k_1k_2k_3)=A_{11}A_{22}A_{33}=(a_{11}a_{22}a_{33})^2$, we can set

$$(13)\qquad k_1k_2k_3=\sigma a_{11}a_{22}a_{33},\qquad \sigma=\pm 1.$$

From (13) follows $k_2k_3=-\sigma a_{11}k_1$, $k_3k_1=-\sigma a_{22}k_2$, $k_1k_2=-\sigma a_{33}k_3$. Hence the three quaternions $\sigma k_1, \sigma k_2, \sigma k_3$ satisfy the same multiplication table as the i_α. Hence we can choose q and σ to satisfy (10) of §2. Accordingly, in (8),

$$(14)\qquad y=qxq^{-1}h_0,\quad\text{or}\quad y=q\bar{x}q^{-1}h_0,$$

that is, $y=txu$ or $y=t\bar{x}u$, where t and u are rational quaternions such that $Nt\cdot Nu=1$. Continuity considerations show that the determinant is $+1$ for the first, -1 for the second of these transformations. Lemma 9 follows.

If t has rational coordinates we can choose a proportionality factor λ to make t integral and primitive. Hence every positive rational automorph of adj f is given by $y=\bar{t}xt/Nt$ with t primitive. We must see whether the various prime-powers in Nt can be cancelled to make the coefficients $\bar{t}i_1t/Nt$, $\bar{t}i_2t/Nt$, $\bar{t}i_3t/Nt$ of the x_α have integer coordinates. Similarly, every positive rational automorph of F is obtained by equating j-coordinates in

$$y = txu/m, \tag{15}$$

where t and u are primitive quaternions, m a nonzero integer, $Nt\cdot Nu=m^2$.

LEMMA 10. *Let t, u denote primitive quaternions, $N(tu)=m^2$. If txu/m is integral for every integral quaternion x, then*: (a) $Nt=Nu=\pm m$; (b) $u=\bar{t}\theta$, *where θ is a unit*; (c) $tx\bar{t}/m$ *is integral for every integral x.*

For, in particular, $tu\equiv 0 \pmod m$. If p^s is a prime-power in m, then $Nt\cdot Nu$ is divisible precisely by p^{2s}. We prove that Nt and Nu are each divisible by p^s. For if not, let Nt be divisible only by p^n, $n<s$. Then $\bar{t}tu\equiv 0 \pmod{p^s}$, $u\equiv 0 \pmod{p^{s-n}}$, contradicting the primitivity of u. Hence $Nt=Nu=\pm m$. Again, $tu=\pm m\theta$, θ integral. Since $N(tu)=m^2N\theta$, θ is a unit. Thus $u=\bar{t}\theta$. The integrality of $tx\bar{t}\theta/m$ implies that of $tx\bar{t}\theta\bar{\theta}/m$, that is, of $tx\bar{t}/m$, for every integral x.

LEMMA 11. *Let t, u be primitive, $Nt=Nu=\pm m$, $m\,|\,d$, adj f be fundamental. Then txu/m is integral for every integral quaternion x. Also, $tx\bar{t}/m$ is purely-integral for every purely-integral x.*

Let $p>2$. We can assume that (4) holds as a congruence mod p^r, r large, and can use (5) and (6) to see whether the power of p in Nt cancels. Since adj f is fundamental, p divides d precisely once and $c_p=-1$; we can suppose $p\,\|\,a_3$ and $(-a_1a_2\,|\,p)=-1$. Then if $p\,|\,Nt$ (necessarily only once) clearly $u_0\equiv u_3\equiv t_0\equiv t_3\equiv 0 \pmod p$, and every element of (5) and (6) is obviously divisible by p.

Note in advance for Lemma 13, that if p^s exceeds the power of p in d $(\equiv 4a_1a_2a_3)$, then by arguments like those following (5) and (6), p^s cannot divide every element of (5), or (6), without rendering t, or t or u, imprimitive. This applies equally to the prime 2 in case (4) holds, mod 2^r.

To facilitate the discussion of the prime 2 we need explicit expansions of (2) and (3), especially in the case $f=jx_1^2+x_1x_2+jx_2^2+\lambda x_3^2$, $j=0$ or 1. These can be used with the elements determined mod 2^r, when the expression for f is only a residue mod 2^r. To derive these expansions we take $a_1=4j-1$, $a_2=1$, $a_3=\lambda$, and so derive the adjoint form

$$\lambda(jx_1^2 - x_1x_2 + jx_2^2) + (j - 1/4)x_3^2 \tag{16}$$

from $a_2a_3x_1^2+a_3a_1x_2^2+a_1a_2x_3^2$ by the substitution

$$T=\frac{1}{2}\begin{bmatrix}1+j & -1 & 0\\ 1-j & 1 & 0\\ 0 & 0 & 1\end{bmatrix},\qquad T^{-1}=\begin{bmatrix}1 & 1 & 0\\ j-1 & 1+j & 0\\ 0 & 0 & 2\end{bmatrix},$$

of determinant $1/4$. Then we form $T^{-1}ET$, using E as in (5), and apply T to t, that is, put $t_0=u_0$, $t_1=(1+j)u_1/2-u_2/2$, $t_2=(1-j)u_1/2+u_2/2$, $t_3=u_3/2$. Finally, we replace u_0 by $u_0+u_3/2$, so that the u_i will be j-coordinates and integrality most easily discussed. If $j=0$, the result for the positive automorphs of adj f is

$$\frac{1}{Nu}\begin{bmatrix}u_0^2 & -\lambda u_1^2 & u_0u_1\\ -\lambda u_2^2 & (u_0+u_3)^2 & -u_2(u_0+u_3)\\ 2\lambda u_0u_2 & -2\lambda u_1(u_0+u_3) & u_0^2+u_0u_3+\lambda u_1u_2\end{bmatrix}, \tag{17}$$

where $Nu=u_0^2+u_0u_3-\lambda u_1u_2$ (the Brandt-norm); and if $j=1$ the result is the quotient by Nu $(=u_0^2+u_0u_3+u_3^2+\lambda(u_1^2-u_1u_2+u_2^2))$ of

$$\begin{bmatrix}u_0^2-u_3^2+\lambda(u_1^2-u_2^2) & 2u_0u_3+u_3^2+\lambda(2u_1u_2-u_1^2) & u_0u_1+2u_1u_3-2u_0u_2-u_2u_3\\ -2u_0u_3-u_3^2+\lambda(2u_1u_2-u_2^2) & 2u_0u_3+u_0^2-\lambda(u_1^2-u_2^2) & 2u_0u_1+u_1u_3-u_0u_2+u_2u_3\\ 2\lambda(u_0u_2+u_1u_3) & -2\lambda(u_0u_1+u_1u_3-u_2u_3) & u_0^2+u_0u_3+u_3^2-\lambda(u_1^2-u_1u_2+u_2^2)\end{bmatrix}. \tag{18}$$

Now (6) is obtained from $y=txu$, for the f in (4), by equating i-coordinates. To get the result of equating j-coordinates in $y_0+\sum j_\alpha y_\alpha=(t_0+\sum j_\alpha t_\alpha)\cdot(x_0+\sum j_\alpha x_\alpha)(u_0+\sum j_\alpha u_\alpha)$, we write it as $y_0+y_3/2+\sum i_\alpha y_\alpha=(t_0+t_3/2+\sum i_\alpha t_\alpha)\cdot(x_0+x_3/2+\sum i_\alpha x_\alpha)(u_0+u_3/2+\sum i_\alpha u_\alpha)$, and apply the transformation T as above, using (6).

Using the abbreviations

$$p_1=t_2u_3+t_3u_2,\quad q_1=t_2u_3-t_3u_2,\quad r_1=t_0u_1+t_1u_0,\quad s_1=t_0u_1-t_1u_0 \tag{19}$$

where subscripts 1, 2, 3 are to be permuted cyclically, and also $\rho=t_1u_1+t_2u_2$. and $\sigma=t_1u_1-t_2u_2$, we thus find for the automorphs of $F=x_0^2+x_0x_3+jx_3^2+\lambda(jx_1^2-x_1x_2+jx_2^2)=Nx$ the expression (h_{ij}/Nt), where

$$\begin{aligned}
&h_{00}=t_0u_0+\lambda t_2u_1-j(t_3u_3+\lambda\rho), && h_{01}=\lambda(t_2u_0-jr_1+jq_1),\\
&h_{02}=\lambda(t_0u_1-jr_2+jq_2), && h_{03}=\lambda t_2u_1-j(r_3+t_3u_3+\lambda\rho-\lambda q_3);\\
&h_{10}=r_1+t_3u_1+jq_1, && h_{11}=t_0u_0+t_3u_0+j(t_3u_3-\lambda\sigma),\\
&h_{12}=\lambda t_1u_1+j(s_3-\lambda p_3), && h_{13}=t_0u_1+t_3u_1-j(s_2+p_2-q_1);\\
&h_{20}=r_2+t_2u_3+jq_2, && h_{21}=\lambda t_2u_2-j(s_3+\lambda p_3),\\
&h_{22}=t_0u_0+t_0u_3+j(t_3u_3+\lambda\sigma), && h_{23}=t_2u_0+t_2u_3+j(s_1+q_2-p_1);\\
&h_{30}=r_3+t_3u_3+\lambda q_3, && h_{31}=\lambda(s_2+t_3u_2-jp_2),\\
&h_{32}=-\lambda(s_1-t_1u_3+jp_1), &&\\
&h_{33}=t_0u_0+r_3+t_3u_3-\lambda t_2u_1+j(\lambda\rho-t_3u_3). &&
\end{aligned} \tag{20}$$

These have been checked carefully. As a final check note that (20) can be reduced to (17) and (18) by setting $t=\bar{u}$, that is $t_0+t_3/2=u_0+u_3/2$, $t_1=-u_1$, $t_2=-u_2$, $t_3=-u_3$, hence $t_0=u_0+u_3$; the first element in the last three rows of (h_{ij}) then becomes zero, and the other elements become those of (17), (18); also, adding half the last row to the first gives $y_0+y_3/2=Nu(x_0+x_3/2)$.

In (18), and in (20) with $j=1$, $2 \mid Nu$ implies that u_0 and u_3 are even, and since λ is even when $j=1$, it is seen that all elements of (18) and (20) are even, so that $txi/2$ is purely integral, and $txu/2$ is integral. This completes the proof of Lemma 11.

In anticipation of Lemma 13, note that if 2^s exceeds the power of 2 in d $(=(4j-1)\lambda)$, then in (17), 2^s cannot divide the four leading elements without rendering every u_i divisible by 2; and in (18), 2^s cannot divide both Nu and the last element, without 2 dividing both $u_0^2+u_0u_3+u_3^2$ and $u_1^2-u_1u_2+u_2^2$, whence $2 \mid u$.

Again, consider (20) with j equal to zero. For any integer λ, it is easily verified that if 2^s exceeds the power of 2 in λ, and 2^s divides all 16 elements of (20), then every t_iu_j is even, so that t or u is imprimitive. A good scheme is to construct a 4-by-4 square, and check off each product t_iu_j as even, as it appears.

The proof of Theorems 4 and 5 is now complete, at least in the fundamental case, when we observe (Lemma 5) that if $j=1$, 4 cannot divide Nt if t is primitive.

We now need more complete information on the possible form-residues:

LEMMA 12. *Any integral ternary form f can be carried by a unimodular transformation into a form with the following residue* mod 2^r, *r large: either* (i) *as in* (4) *with integers a_α, or* (ii) *as $2^\delta(jx_1^2+x_1x_2+jx_2^2+\lambda x_3^2)$, or* (iii) *as $2^{\beta+2}(jx_1^2+x_1x_2+jx_2^2)+a_3x_3^2$. Here $j=0$ or 1; β and δ denote non-negative integers, λ and a_3 integers. In* (ii) *if $j=1$, λ is even. In* (iii), *the power of 2 in a_3 does not exceed 2^β.*

Forming determinants we see that the connection with d is as follows: (i) $d\equiv 4a_1a_2a_3 \pmod{2^r}$; (ii) $d\equiv(4j-1)2^{2\delta}\lambda$; (iii) $d\equiv(4j-1)2^{2\beta+4}a_3 \pmod{2^r}$.

In view of Lemma 10, we can complete the proof of Theorem 5, by proving the following lemma, thus avoiding further complicated fourth order matrices:

LEMMA 13. *Let t be a primitive quaternion of norm m. If either* (a) *$\bar{i}xt/m$ is purely-integral for every purely-integral x, or if* (b) *$\bar{i}xt/m$ is integral for every integral pure x, then $m \mid d$.*

The significance of (a) and (b) may be seen as follows. Set $y=\bar{i}xt$, where x and y are pure. Equating coordinates, we have, say,

$$y_\alpha = t_{\alpha 1}x_1 + t_{\alpha 2}x_2 + t_{\alpha 3}x_3 \qquad (\alpha = 1, 2, 3),$$

where $t_{\alpha 1}$, $t_{\alpha 2}$, $t_{\alpha 3}$ are the elements of the αth row of the matrices in, for ex-

ample, (5), (17), or (18). The column $t_{1\beta}$, $t_{2\beta}$, $t_{3\beta}$ gives the coordinates of $\bar{\imath}i_\beta t$. Now, (a) means that the y_α are integers divisible by m for all choices of integers x_α; that is, $m \mid t_{\alpha\beta}$ ($\alpha, \beta = 1, 2, 3$). But, in case adj f is given by (16), whence $\epsilon_1 = \epsilon_2 = 0$, $\epsilon_3 = 1$, then (b) means that for any integers x_1, x_2, and even integer x_3, y_1/m, y_2/m are integers and y_3/m an even integer; that is, $m \mid t_{11}$, t_{12}, t_{21}, t_{22}, $2t_{13}$, $2t_{23}$, $t_{31}/2$, $t_{32}/2$, and t_{33}.

Only the power of 2 in m, in the nonfundamental cases, remains to be considered. Consider first (ii) with $j=0$ and δ positive. The form adj $f = 2^{2\delta}(-\lambda x_1 x_2 - x_3^2/4)$ is derived from $-\lambda x_1 x_2 - x_3^2/4$ by the substitution $x_\alpha = 2^\delta y_\alpha$; note that in $T^{-1}ET$, T is $2^\delta I$, T^{-1} is $2^{-\delta}I$, and $T^{-1}ET = E$. Referring to (17), and replacing u_0 by $u_0 - u_3/2$ (cf. last step in getting (17)) before replacing u_α by $2^\delta u_\alpha$, we see that the automorph is now E_1/Nu, where the first four elements of E_1 are $(u_0 - 2^{\delta-1}u_3)^2$, $-\lambda 2^{2\delta}u_1^2$, $-\lambda 2^{2\delta}u_2^2$, $(u_0 + 2^{\delta-1}u_3)^2$; and Nu is $u_0^2 - 2^{2\delta-2}u_3^2 - 2^{2\delta}\lambda u_1 u_2$. Clearly, if 2^s divides these five numbers, but not d, every u_i is even.

Similarly in (ii) with j equal to 1, if $\delta > 0$, 2^s cannot divide $Nu = u_0^2 + 3\cdot 2^{2\delta-2}u_3^2 + 2^{2\delta}\lambda(u_1^2 - u_1u_2 + u_2^2)$ and the last diagonal element $u_0^2 + 3\cdot 2^{2\delta-2}u_3^2 - 2^{2\delta}\lambda(u_1^2 - u_1u_2 + u_2^2)$, without rendering u imprimitive.

Finally, in (iii), adj $f = 2^{2\beta+4}(j - 1/4)x_3^2 + 2^{\beta+2}a_3(jx_1^2 - x_1x_2 + jx_2^2)$, and is derived from (16) by taking $\lambda = 2^{\beta+2}a_3$ and replacing x_3 by $2^{\beta+2}x_3$. The third row of (17) or (18) is therefore to be multiplied by $2^{-\beta-2}$, and then the third column by $2^{\beta+2}$, $u_0 - u_3/2$ is to be substituted for u_0, and then u_3 is to be replaced by $2^{\beta+2}u_3$. The new Nu is $u_0^2 + (4j-1)2^{2\beta+2}u_3^2 + 2^{\beta+2}a_3(ju_1^2 - u_1u_2 + ju_2^2)$. Now 2^s exceeds the power of 2 in $2^{2\beta+4}a_3$. Hence if $j=0$, 2^s cannot divide the first four elements $(u_0 - 2^{\beta+1}u_3)^2$, $-2^{\beta+2}a_3u_1^2$, $-2^{\beta+2}a_3u_1^2$, and $(u_0 + 2^{\beta+1}u_3)^2$, without 2 dividing u. Finally, if $j=1$, and 2^s divides Nu and the last diagonal element $u_0^2 + 3\cdot 2^{2\beta+2}u_3^2 - 2^{\beta+2}a_3(u_1^2 - u_1u_2 + u_2^2)$, then we see that $2^{\beta+2} \mid u_1^2 - u_1u_2 + u_2^2$ and that $u_0 = 2^{\beta+1}v_0$, $2^{s-3-2\beta} \mid v_0^2 + 3u_3^2$. If a_3 is even, $s \geqq 2\beta+6$; and if a_3 and β are odd, $2^{2\beta+5} \mid 2^{\beta+2}a_3(u_1^2 - u_1u_2 + u_2^2)$; in these cases $8 \mid v_0^2 + 3u_3^2$, whence u_3 is even. But if a_3 is odd and β is even, and $s = 2\beta+5$, then putting $u_1 = 2^{\beta/2+1}v_1$, $u_2 = 2^{\beta/2+1}v_2$, $u_0 = 2^{\beta+1}v_0$, we find for the first two diagonal elements the expressions $2^{2\beta+2}[(v_0 \mp u_3)^2 - 4u_3^2 \pm 4a_3(v_1^2 - v_2^2)]$. The bracketed expression in both cases must be divisible by 8. If u_3 could be odd, then $v_0 - u_3$ and $v_0 + u_3$ would both be congruent to 2, or both to 0, mod 4. Neither case is possible, and u_3 must be even. This completes the proof of Theorem 5.

THEOREM 6. *Let* adj f *be fundamental, that is, let* d *be squarefree and* c_p *be* -1 *for each prime* p *in* d. *Then*: (i) *if* $m \mid d$, *all solutions* t *of* $Nt = m$ *are obtained from any one solution by multiplying it on one side (whichever we please) by all the units*; (ii) *if* $Nt = m_1$ *and* $Nu = m_2$, *where* $m_1 \mid d$ *and* $m_2 \mid d$, *then* tu *is divisible by the* g.c.d. m_3 *of* m_1 *and* m_2, *and* $N(tu/m_3) = m_1m_2/m_3^2$; (iii) *the number of divisors* m *of* d, *for which there exist quaternions of norm* m, *is a power of* 2.

say 2^h; (iv) *if the number* w *of units is finite, then* adj f *has* $2^{h-1}w$ *positive, integral automorphs, and* F *has* $2^{h-1}w^2$ *positive, integral automorphs.*

Proof. (i) By Lemma 10, $u=\bar{\imath}\theta$, where u and t are any two quaternions of norm m. (ii) We can suppose $f\equiv a_1x_1^2+a_2x_2^2+pa_3x_3^2 \bmod p^2$, for any odd p in d, where $(-a_1a_2|p)=-1$ and $p\nmid a_3$; and that if $d\equiv 2 \bmod 4$, $f\equiv x_1^2+x_1x_2+x_2^2+2\mu x_3^2 \bmod 8$, μ odd. Hence if $Nt\equiv 0 \bmod p$, $t_0\equiv t_3\equiv 0 \bmod p$. Suppose $Nt\equiv Nu\equiv 0 \pmod p$. If $p>0$, then $tu\equiv(i_1t_1+i_2t_2)(i_1u_1+i_2u_2)\equiv 0 \pmod p$, since $i_1^2\equiv i_2^2\equiv i_1i_2\equiv i_2i_1\equiv 0 \bmod p$. If $p=2$, the same result is easily verified; for example, by (1) of §1,

$$\begin{aligned}(tu)_0+(tu)_3/2 &= t_0'u_0' - 2\mu t_1u_1 - \mu(t_1u_2+t_2u_1) - 2\mu t_2u_2 - 3t_3u_3/4\\ &\quad + (t_0'u_3+t_3'u_0+2\mu(t_1u_2-t_2u_1))/2\\ &= t_0u_0+t_0u_3+t_3u_0-2\mu(t_1u_1+t_2u_2)\equiv 0 \pmod 2,\\ (tu)_1 &= t_0'u_1+t_1'u_0+1(t_2u_3-t_3u_2)+(t_3u_1-t_1u_3)/2\\ &= t_0u_1+t_1u_0+t_3u_1+t_2u_3-t_3u_2\equiv 0 \pmod 2,\end{aligned}$$

and so on. It follows that if $Nt=m_1$, and $Nu=m_2$, then tu has m_3 as divisor. Since d is squarefree, tu/m_3 can have no further rational integer divisor, and (ii) follows. (iii) is an easy consequence of (ii), and (iv) now follows from Theorem 4.

At this point we draw attention to Theorem 8, which can also be verified (though less simply) by the preceding methods. Indeed, one finds, whether adj f is fundamental or not, that txu/m is integral for all integral x if and only if $tx\bar{\imath}/m$ is purely-integral for all purely-integral x.

8. **The connection between** f **and** F. We now proceed more easily:

THEOREM 7. *If* $F=(x_0+2^{-1}\sum\epsilon_\alpha x_\alpha)^2+$ adj f *is carried into* $G=(x_0+2^{-1}\sum\eta_\alpha x_\alpha)^2+$adj g *by an integral transformation, then* adj f *is carried into* adj g *by an integral transformation. In particular, if* $F\sim G$, *then* adj $f\sim$adj g, *whence* $f\sim\pm g$.

For, if A and B denote the matrices of adj f and adj g, then A_1 and B_1 are integral matrices, where $A_1=A+\epsilon\epsilon'/4$, $B_1=B+\eta\eta'/4$. Any integral transformation of F into G is expressible in the form

$$(1)\qquad \begin{bmatrix} t_0 & \tau' \\ \sigma & T' \end{bmatrix}\begin{bmatrix} 1 & \epsilon'/2 \\ \epsilon/2 & A_1 \end{bmatrix}\begin{bmatrix} t_0 & \sigma' \\ \tau & T \end{bmatrix}=\begin{bmatrix} 1 & \eta'/2 \\ \eta/2 & B_1 \end{bmatrix},$$

where $\sigma'=(s_1, s_2, s_3)$, $\tau'=(t_1, t_2, t_3)$, and T are integral matrices. The expansion of (1) gives the following three equations:

$$(2)\qquad (t_0+\tau'\epsilon/2)^2+\tau'A\tau=1,$$

$$(3)\qquad (t_0+\tau'\epsilon/2)(\sigma'+\epsilon'T/2)+\tau'AT=\eta'/2,$$

$$(4)\qquad (\sigma+T'\epsilon/2)(\sigma'+\epsilon'T/2)+T'AT=B+\eta\eta'/4,$$

the transpose of (3) being $(\sigma+T'\epsilon/2)(t_0+\epsilon'\tau/2)+T'A\tau=\eta/2$.

Hence if $t=t_0+\sum j_\alpha t_\alpha$, $Nt=1$ (in the set of quaternions related to F) and the coordinates of t form the first column of the transformation replacing F by G. Now $y=tx$ (where $y=y_0+\sum j_\alpha y_\alpha$, $x=x_0+\sum j_\alpha x_\alpha$) is evidently an automorphic transformation of F, since $Nt=1$ and $Ny=Nx$; and the first column, giving the coefficients of x_0, also consists of the coordinates of t. The inverse of this transformation multiplied by the transformation applied to F in (1) produces another transformation replacing F by G, which has $t_0=1$, and $t_1=t_2=t_3=0$. Supposing this to be the transformation employed at the start, we find that (3) and (4) imply $\sigma'+\epsilon'T/2=\eta'/2$, $\sigma+T'\epsilon/2=\eta/2$,

$$T'AT = B. \tag{5}$$

Thus T is a transformation replacing adj f by adj g, and the theorem follows.

Suppose now that $F=G$, so that (1) defines an automorph of F. The preceding process associates with every integral automorph of F a uniquely determined integral automorph of adj f, satisfying, that is,

$$T'AT = A, \tag{6}$$

and a uniquely determined quaternion t of norm 1. Conversely, if T is any integral solution of (6), the matrix

$$\begin{bmatrix} 1 & \epsilon'(I-T)/2 \\ 0 & T \end{bmatrix} \tag{7}$$

is an integral automorph of F. For if we put $t_0=1$, $\tau=0$, we see that equations (2)–(4) are satisfied with $\sigma=(I-T')\epsilon/2$. Also, σ is integral, since by (1) of §3, $4A\equiv\epsilon\epsilon'$ mod 2, $T'(4A)T=4A$, $T'\epsilon\epsilon'T\equiv\epsilon\epsilon'$; hence if $T'\epsilon=\zeta$, $\zeta_\alpha^2\equiv\epsilon_\alpha^2$ ($\alpha=1, 2, 3$), or $\epsilon\equiv T'\epsilon$ mod 2. Finally, if t is any unit quaternion, the automorph $y=tx$ multiplied by that in (7) produces any desired integral automorph of F. We have thus proved the following theorem.

THEOREM 8. *The number of integral automorphs of F is equal to the number of integral automorphs of f multiplied by the number of units.*

In particular, if the only units are ±1, every integral automorph of F is given by (7) or its negative, where T ranges over the integral automorphs of adj f. This case occurs when f is definite and the minimum of adj f exceeds 1.

The definite forms f for which adj f has minimum 3/4 or 1 will be determined in the next section. At the same time, for later use, we shall isolate also the forms for which adj f has minimum 7/4 or 2.

THEOREM 9. *Every form G of minimum 1 in the genus of a norm-form F is equivalent to a norm-form belonging to a ternary g in the genus of $\pm f$.*

For G is equivalent to a form $(x_0+2^{-1}\sum\eta_\alpha x_\alpha)^2+\sum B_{\alpha\beta}x_\alpha x_\beta$, where the η_α

are 0 or 1, and $B+\eta\eta'/4$ is an integral matrix. Comparison of determinants gives $|B| = |A|$. Since F and G are in the same genus, (1) holds with t_0, σ, τ, and T having rational elements with denominators prime to $2d$. Now $y=tx$ determines a rational transformation of denominators prime to $2d$, with t in the first column. Proceeding as before, we get (5) with T rational and of denominator prime to $2d$. Hence $4A$ and $4B$ are in the same genus, and the theorem follows.

9. **The positive, integral forms f such that adj f has minimum not greater than 2.**

(i) First suppose that $\xi'A\xi$ represents 3/4. By a unimodular transformation we can take $A_{33}=3/4$. Hence $a_{11}x_1^2+2a_{12}x_1x_2+a_{22}x_2^2$ becomes an integral positive binary form of determinant 3/4. All such forms are equivalent to $x_1^2+x_1x_2+x_2^2$, and we can therefore assume $a_{11}=2a_{12}=a_{22}=1$. Next by a translation on x_3 in adj f, we can obtain $|2A_{13}| \leqq 3/4$, $|2A_{23}| \leqq 3/4$. Hence $A_{13}=\alpha_1/4$, $A_{23}=\alpha_2/4$, where $\alpha_1=0$ or ± 1, $\alpha_2=0$ or ± 1. The matrices of f and adj f now have the following appearance:

$$(1) \qquad \begin{bmatrix} 1 & 1/2 & \cdot \\ 1/2 & 1 & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}, \qquad \frac{1}{4}\begin{bmatrix} 4A_{11} & 4A_{12} & \alpha_1 \\ 4A_{21} & 4A_{22} & \alpha_2 \\ \alpha_1 & \alpha_2 & 3 \end{bmatrix}.$$

Let $d=4|a_{\alpha\beta}|$. Then adj adj $f=df/4$, and in particular,

$$(2) \qquad 4d = 12A_{11} - \alpha_1^2, \quad 2d = \alpha_1\alpha_2 - 12A_{12}, \quad 4d = 12A_{22} - \alpha_2^2.$$

Hence $\alpha_1^2 \equiv \alpha_2^2 \equiv -2\alpha_1\alpha_2 \bmod 3$, and we can suppose either $\alpha_1=\alpha_2=0$, or $\alpha_1=\alpha_2=-1$ (the signs of both α_1 and α_2 can evidently be changed without affecting (1_1)). In these two cases, $d=3k-1$ or $3k$, where k is a positive integer, and adj f has the respective matrices

$$(3) \qquad \frac{1}{4}\begin{bmatrix} 4k-1 & 1-2k & -1 \\ 1-2k & 4k-1 & -1 \\ -1 & -1 & 3 \end{bmatrix}, \qquad \frac{1}{4}\begin{bmatrix} 4k & -2k & 0 \\ -2k & 4k & 0 \\ 0 & 0 & 3 \end{bmatrix};$$

the corresponding forms f are as follows:

$$(4) \qquad x_1^2 + x_2^2 + kx_3^2 + x_1x_2 + x_1x_3 + x_2x_3, \qquad x_1^2 + x_1x_2 + x_2^2 + kx_3^2.$$

(ii) Suppose that adj f has minimum 1. We can take $A_{33}=1$. Hence $a_{11}x_1^2+2a_{12}x_1x_2+a_{22}x_2^2$ can be taken to be $x_1^2+x_2^2$. By a translation we get $|2A_{13}| \leqq 1$, $|2A_{23}| \leqq 1$. Hence $A_{13}=\alpha_1/4$, $A_{23}=\alpha_2/4$, where α_1, $\alpha_2=0$, ± 1, or ± 2. Since the coefficient of x_1x_2 in f is 0, the negative α_i can be dropped. We have (1) with 0 in place of each 1/2 in the upper left, and 4 in place of the 3 on the lower right. Hence

$$4d = 16A_{11} - \alpha_1^2, \quad 4d = 16A_{22} - \alpha_2^2, \quad 0 = \alpha_1\alpha_2 - 16A_{12};$$

$\alpha_1^2 \equiv \alpha_2^2 \equiv \alpha_1\alpha_2 \equiv 0 \pmod 4$. We can set $\alpha_i = 2\beta_i$, where $\beta_i = 0$ or 1. Then $A_{11} = (d+\beta_1^2)/4$, $A_{22} = (d+\beta_2^2)/4$, $A_{12} = \beta_1\beta_2/4$, and

$$F = (x_0 + 2^{-1}\sum \epsilon_\alpha x_\alpha)^2 + (d+\beta_1^2)x_1^2/4 + (d+\beta_2^2)x_2^2/4 + x_3^2 + \beta_1 x_1 x_3 + \beta_2 x_2 x_3 + \beta_1\beta_2 x_1 x_2/2. \tag{5}$$

Since F must have integral coefficients, $\epsilon_3 = 0$, $\epsilon_1\epsilon_2 + \beta_1\beta_2$ is even and $\epsilon_1^2 + \beta_1^2 \equiv \epsilon_2^2 + \beta_2^2 \bmod 4$. This implies that $\epsilon_1 = \beta_2$, $\epsilon_2 = \beta_1$, and $d \equiv -\epsilon_1^2 - \epsilon_2^2 \bmod 4$. The forms f obtained from $(\epsilon_1, \epsilon_2) = (0, 1)$ and $(1, 0)$ are equivalent. There remain three forms f:

$$x_1^2 + x_2^2 + kx_3^2 - x_2x_3 - x_3x_1,\ x_1^2 + x_2^2 - x_1x_3 + kx_3^2,\ x_1^2 + x_2^2 + kx_3^2, \tag{6}$$

and d is respectively $4k-2$, $4k-1$, and $4k$. We can suppose $k \geqq 1$ in connection with (6_3), $k \geqq 2$ in (6_1) and (6_2). For, if $k = 1$ in (6_1) or (6_2), adj f represents $3/4$, and it is seen that f is equivalent respectively to the case $k = 1$ of (4_1) and (4_2).

(iii) Let adj f have minimum $7/4$. As before we readily obtain:

$$\begin{bmatrix} 1 & 1/2 & \cdot \\ 1/2 & 2 & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}, \qquad \frac{1}{4}\begin{bmatrix} 4A_{11} & 4A_{12} & \alpha_1 \\ 4A_{21} & 4A_{22} & \alpha_2 \\ \alpha_1 & \alpha_2 & 7 \end{bmatrix};$$

where α_1, $\alpha_2 = 0, \pm 1, \pm 2, \pm 3$; $4A_{11} = (\alpha_1^2 + 8d)/7$, $4A_{22} = (\alpha_2^2 + 4d)/7$, $4A_{12} = (\alpha_1\alpha_2 - 2d)/7$; $-4\alpha_1\alpha_2 \equiv \alpha_1^2 \equiv 2\alpha_2^2 \pmod 7$; $(\alpha_1, \alpha_2) = (0, 0)$ and $d = 7k$, $(\alpha_1, \alpha_2) = (1, -2)$ and $d = 7k-1$, $(\alpha_1, \alpha_2) = (-2, -3)$ and $d = 7k-4$, or $(\alpha_1, \alpha_2) = (-3, -1)$ and $d = 7k-2$. Hence we have four forms, with d respectively $7k-4$, $7k-2$, $7k-1$, and $7k$, and each demanding $k \geqq 2$:

$$\begin{gathered} x_1^2 + 2x_2^2 + kx_3^2 + x_1x_2 + x_1x_3 + 2x_2x_3, \\ x_1^2 + 2x_2^2 + kx_3^2 + x_2x_3 + x_3x_1 + x_1x_2, \\ x_1^2 + 2x_2^2 + kx_3^2 + x_1x_2 + x_2x_3, \qquad x_1^2 + 2x_2^2 + kx_3^2 + x_1x_2. \end{gathered} \tag{7}$$

(iv) Let adj f have the minimum 2. Then we have

$$\begin{bmatrix} 1 & 0 & \cdot \\ 0 & 2 & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}, \qquad \frac{1}{4}\begin{bmatrix} 4A_{11} & 4A_{12} & \alpha_1 \\ 4A_{21} & 4A_{22} & \alpha_2 \\ \alpha_1 & \alpha_2 & 8 \end{bmatrix};$$

α_1, $\alpha_2 = 0$, 1, 2, 3, or 4; $4A_{11} = (\alpha_1^2 + 8d)/8$, $4A_{22} = (\alpha_2^2 + 4d)/8$, $\alpha_1\alpha_2 = 32A_{12}$; $\alpha_1 = 4\beta_1$, $\alpha_2 = 2\beta_2$, $\beta_1 = 0$ or 1, $\beta_2 = 0$, 1, or 2; $\epsilon_3 = 0$,

$$(x_0 + \epsilon_1 x_1/2 + \epsilon_2 x_2/2)^2 + (2\beta_1^2 + d)x_1^2/4 + (\beta_2^2 + d)x_2^2/8 + 2x_3^2 + \beta_1\beta_2 x_1x_2/2 + 2\beta_1 x_1x_3 + \beta_2 x_2x_3 \tag{8}$$

is integral, $d \equiv -\epsilon_1^2 - 2\beta_1^2 \bmod 4$, $d \equiv -\beta_2^2 - 2\epsilon_2^2 \bmod 8$, $\epsilon_1\epsilon_2 + \beta_1\beta_2$ is even. We

thus have six cases: (a) $d=8k-6$, $\epsilon_1=0$, $\epsilon_2=1$, $\beta_1=1$, $\beta_2=2$; (b) $d=8k-4$, $\epsilon_1=\epsilon_2=\beta_1=0$, $\beta_2=2$; (c) $d=8k-3$, $\epsilon_1=\epsilon_2=\beta_1=\beta_2=1$; (d) $d=8k-2$, $\epsilon_1=0$, $\epsilon_2=1=\beta_1$, $\beta_2=0$; (e) $d=8k-1$, $\epsilon_1=1$, $\epsilon_2=0=\beta_1$, $\beta_2=1$; (f) $d=8k$, $\epsilon_1=\epsilon_2=\beta_1=\beta_2=0$. The corresponding forms f are respectively:

$$(9)\quad \begin{array}{ll} x_1^2+2x_2^2+kx_3^2-x_1x_3-2x_2x_3\ (k\geqq 3), & x_1^2+2x_2^2+kx_3^2-2x_2x_3\ (k\geqq 2),\\ x_1^2+2x_2^2+kx_3^2-x_1x_3-x_2x_3\ (k\geqq 3), & x_1^2+2x_2^2+kx_3^2-x_1x_3\ (k\geqq 3),\\ x_1^2+2x_2^2+kx_3^2-x_2x_3\ (k\geqq 2), & x_1^2+2x_2^2+kx_3^2\ (k\geqq 2). \end{array}$$

10. Problem; to find all the fundamental definite norm-forms F for which factorization, as of Theorem 3, is always possible. The genus of a fundamental norm-form represents all positive integers. Hence F must represent 2, and so must belong to one of the forms in (4), (6), (7), and (9) of §9. We number these in order, 1° to 15°. Note also that d must be squarefree (excluding 5°, 11°, and 15°), and c_p is -1 for each p in d. Since f is definite this implies that d contains an odd number of primes.

1°. Then $F=(x_0+x_1/2+x_2/2+x_3/2)^2+\phi/4$, where

$$\phi = 3x_3^2 + (4k-1)x_2^2 + (4k-1)x_1^2 - (4k-2)x_1x_2 - 2x_1x_3 - 2x_2x_3.$$

Since ϕ is Eisenstein-reduced if $k\geqq 1$, the least number primitively represented by ϕ with $(x_1, x_2)\neq(0, 0)$ is $4k-1$. Since $F(x_0, 0, 0, x_3)=x_0^2+x_0x_3+x_3^2\neq 2$, F does not represent 2 if $k\geqq 3$.

There remain the cases $k=1$ and 2, that is, $d=2$ and 5, when F is indeed fundamental and in a genus of one class (Theorem 10).

2°. $F=x_0^2+x_0x_3+x_3^2+k(x_1^2+x_1x_2+x_2^2)$, and $F\neq 2$ if $k\geqq 3$. If $k=2$, $d=6$ and contains two primes. *There remains $k=1$, or $d=3$* (Theorem 10).

3°. $F=(x_0+x_1/2+x_2/2)^2+\phi/4$, $\phi=4x_3^2+(4k-1)x_2^2+(4k-1)x_1^2+2x_1x_2+4x_1x_3+4x_2x_3$. Hence if $k\geqq 4$, $F\neq 3$. Since $c_p=(2-4k, -1)_p$, $c_2=(-1)^k$; and if $k=3$, $c_5=1$. Hence no fundamental F remains, as $k\geqq 2$.

4°. $F=x_0^2+x_0x_2+kx_2^2+x_3^2+x_3x_1+kx_1^2$. If $k\geqq 4$, $F\neq 3$. If $k=3$, we might point to the fact that $f=(1, 1, 3, 0, -1/2, 0)$ is not alone in its genus, being accompanied by $g=(1, 1, 4, 1/2, 1/2, 1/2)$. (For further information on f, see [8, p. 173].) Hence $G=(x_0+2^{-1}\sum x_\alpha)^2+(15x_1^2+15x_2^2+3x_3^2-14x_1x_2-2x_1x_3-2x_2x_3)/4$ is in the same genus as F; and since $G\neq 2$, G and F are inequivalent. However, although this proves that F is not in a genus of one class, it does not prove (since G represents 1) that factorization, as of Theorem 3, may fail. For this reason, we point to the following third form in the genus, of minimum 2:

$$\begin{aligned} 2x_0^2+2x_1^2+2x_2^2+2x_3^2+x_0x_1-x_0x_2+2x_0x_3-2x_1x_2-x_2x_3 &= 2(x_0+x_1/4-x_2/4+x_3/2)^2\\ &\quad +(12x_3^2+15x_2^2-15x_1^2-14x_1x_2-4x_1x_3-4x_2x_3)/8, \end{aligned}$$

whence indeed factorization must sometimes fail.

There remains the case $k=2$, $d=7$ (Theorem 10).

6°. $F=(x_0+x_2/2+x_3/2)^2+\phi/4$, $\phi=7x_3^2+(4k-1)x_2^2+(8k-4)x_1^2-(4k-4)x_1x_2-4x_1x_3-6x_2x_3$. Hence as $F(x_0, 0, 0, x_3)=x_0^2+x_0x_3+2x_3^2\neq 3$, F does not represent 3 if $(4k-1)/4>3$, or $k\geqq 4$. If $k=2$, $d=10$. Finally, if $k=3$, whence $d=17$, then besides another norm-form in the genus corresponding to $g=(1, 1, 6, 1/2, 1/2, 1/2)$, there is the following form of minimum 2 in the genus of F:

$$2(x_0+x_1/4-x_2/4+x_3/2)^2+(23x_1^2+23x_2^2+12x_3^2-4x_2x_3-4x_1x_3-22x_1x_2)/8$$
$$=2x_0^2+3x_1^2+3x_2^2+2x_3^2+x_0x_1-x_0x_2+2x_0x_3-3x_1x_2-x_2x_3.$$

7°. $F=(x_0+x_1/2+x_2/2+x_3/2)^2+\phi/4$, $\phi=(8k-1)x_1^2+(4k-1)x_2^2+7x_3^2-(2k-1)x_1x_2-3x_1x_3-x_2x_3$. If $k=2$, $d=12$. If $k\geqq 4$, $F\neq 3$. If $k=3$, the genus of F contains the following form of minimum 2:

$$2(x_0+x_1/4-x_2/2)^2+(23x_1^2+20x_2^2+16x_3^2+4x_1x_2+16x_1x_3+8x_2x_3)/8$$
$$=2x_0^2+3x_1^2+2x_2^2+2x_3^2+x_0x_1-2x_0x_2+2x_1x_3+x_2x_3.$$

8°. $F=(x_0+x_1/2+x_3/2)^2+\phi/4$, $\phi=(8k-1)x_1^2+4kx_2^2+7x_3^2+4kx_1x_2+2x_1x_3+4x_2x_3$. Hence if $k\geqq 4$, $F\neq 3$. If $k=3$, $d=20$.

If $k=2$, $d=13$, *and* F *is in a genus of one class* (Theorem 10).

9°. $F=x_0^2+x_0x_3+2x_3^2+k(2x_1^2+x_1x_2+x_2^2)$. Hence if $k\geqq 4$, $F\neq 3$. If $k=2$ or 3, $d=14$ or 21, and F is not fundamental.

10°. $F=(x_0+x_2/2)^2+\phi/4$, $\phi=(8k-4)x_1^2+(4k-1)x_2^2+8x_3^2+4x_1x_2+8x_1x_3+8x_2x_3$. Since $d=8k-6$, $c_2=1$ if k is even. If $k=3$ or 5, $d=18$ or 34. If $k\geqq 7$, $F(x_0, 0, 0, x_3)=x_0^2+2x_3^2\neq 5$, and $(4k-1)/4>5$; $F\neq 5$.

12°. $F=(x_0+x_1/2+x_2/2)^2+\phi/4$, $\phi=(8k-1)x_1^2+(4k-1)x_2^2+8x_3^2+2x_1x_2+8x_1x_3+4x_2x_3$. If $k\geqq 6$, $F\neq 5$. If $k=3$, $d=21$. But if $k=4$ or 5, $d=29$ or 37, we have again to construct forms of minimum 2 in the genus of F:

$$2(x_0+x_2/4-x_3/4)^2+(32x_1^2+31x_2^2+15x_3^2+16x_1x_2+8x_1x_3+2x_2x_3)/8$$
$$=2x_0^2+4x_1^2+4x_2^2+2x_3^2+x_0x_2-x_0x_3+2x_1x_2+x_1x_3;$$
$$2(x_0+x_1/4+x_2/4-x_3/4)^2+(39x_1^2+31x_2^2+23x_3^2-10x_1x_2-6x_1x_3-22x_2x_3)/8$$
$$=2x_0^2+5x_1^2+4x_2^2+3x_3^2+x_0x_1+x_0x_2-x_0x_3-x_1x_2-x_1x_3-3x_2x_3.$$

13°. $F=x_0^2+x_0x_2+kx_2^2+2(x_3^2+x_3x_1+kx_1^2)$. Here c_2 is 1 unless k is odd. If $k=3$ or 5, $d=22$ or 38. If $k\geqq 7$, $F\neq 5$.

14°. $F=x_0^2+x_0x_1+2kx_1^2+kx_2^2+x_2x_3+2x_3^2$. If $k=2$ or 5, $c_3=1$. If $k\geqq 6$, $F\neq 5$. But if $k=3$ or 4, $d=23$ or 31, we need the following forms of minimum 2 in the genus of F:

$$2x_0^2+x_0x_1+kx_1^2+2x_2^2+x_2x_3+kx_3^2.$$

Summing up, we can state the following theorem:

THEOREM 10. *The only fundamental definite norm-forms in whose (maximal)*

quaternion arithmetics factorization is always possible are the following:

$$
\begin{aligned}
&F_2 = x_0^2+x_1^2+x_2^2+x_3^2+x_0x_1+x_0x_2+x_0x_3, && \text{where } d=2;\\
&F_3 = x_0^2+x_0x_3+x_3^2+x_1^2+x_1x_2+x_2^2, && d=3;\\
(1)\qquad &F_5 = x_0^2+x_1^2+2x_2^2+2x_3^2+x_0x_1+x_0x_2+x_0x_3-x_1x_2, && d=5;\\
&F_7 = x_0^2+x_0x_2+2x_2^2+x_3^2+x_3x_1+2x_1^2, && d=7;\\
&F_{13} = x_0^2+4x_1^2+2x_2^2+2x_3^2+x_0x_1+x_0x_3+2x_1x_2+x_1x_3+x_2x_3, && d=13.
\end{aligned}
$$

To complete the proof we must show that each of these five forms is in a genus of one class. This can be done by means of formulae for the weight of a genus, making use of the number of automorphs. (See references to Smith in §§13 and 14.) This is possible since, the determinant being a square, the weight of the quaternary genus can be expressed in a finite form. And indeed this method was used by the author in 1941, but not published, to obtain 37 norm-forms in genera of one class, two of the forms in Theorem 11 being overlooked. This was not as good a result as we have now, since it left open the possibility of a genus containing several classes, which all have minimum 1.

A result of Korkine and Zolotareff [9] shows that $a^4 \leqq 4\delta$, where a is the minimum and δ is the determinant of a definite quaternary form G. In the present case $\delta = d^2/16$. Hence $a=1$ for the genera of F_2, F_3, F_5, and F_7; but a is 1 or 2, for the genus of F_{13}. Now the ternaries f corresponding to the five F_d are easily seen to be in genera of one class. It remains only to show that there is no form of minimum 2 in the genus of F_{13}.

If the minimum is 2 we can take $G = 2x_0^2 + x_0(a_1x_1+a_2x_2+a_3x_3) + \cdots$. If all the a_α could be even, the determinant of G would be either half or quarter of an integer; but the determinant is 169/16. Hence we can suppose that the g.c.d. of the a_α is 1, and can replace (through the inverse of a unimodular transformation) $\sum a_\alpha x_\alpha$ by x_1. We thus obtain

$$G = 2x_0^2 + x_0x_1 + \cdots = 2(x_0 + x_1/4)^2 + \phi(x_1, x_2, x_3)/8,$$

whence $\phi \equiv 7x_1^2 \pmod 8$. Indeed, ϕ is equivalent to a form congruent mod 2^r to $7y_1^2+8y_2y_3$, since $1 \equiv \det(2G) \equiv (-1)(-1) \pmod 8$. Also, the form-residue mod 13^r of F shows that $\phi \sim \nu z_1^2 + 13(z_2^2+\nu z_3^2) \pmod{13^r}$, where ν is a quadratic non-residue mod 13. Since $\det \phi = 52^2$, we have $\operatorname{adj} \phi = 52\psi$, where ψ is an improperly primitive form of determinant 52, and $\operatorname{adj} \psi = \phi$. The minimum a of ψ satisfies $a^3 \leqq 104$, $a=2$ or 4. If $a=2$, then $3a^2/4 \leqq C \leqq (416/3)^{1/2}$, $3 \leqq C \leqq 11$; since C must be represented by ϕ, C may be 7 or 8 (which agree with the form-residues of ϕ above). But if ϕ represents 7 (necessarily with x_1 odd), $G = 2(x_0+x_1/4)^2+\phi/8$ evidently represents 1; if ϕ represents 8, $4 \mid x_1$, and G again represents 1. If $a=4$, $12 \leqq C \leqq (832/3)^{1/2} < 17$. The only C consistent with the form-residues of ϕ is $C=15$. But $\phi(0, x_2, x_3) = Bx_2^2+2Rx_2x_3+Cx_3^2$,

where $BC-R^2=4\cdot 52$; and this is impossible since $(-208|3)=-1$. Hence there is no form in the genus of minimum 2. The reader will discern here the essentials of the method used to get forms of minimum 2 in §10.

11. **Diagonal forms for the arithmetics of $F_2, \cdots, F_{13}$.** We saw in §1 that the system of integral quaternions related to F_2 can be carried by the transformation (5) of §1 into the system Σ_2:

$$(1) \qquad (y_0 + i_1y_1 + i_2y_2 + i_3y_3)/2, \qquad y_0 \equiv y_1 \equiv y_2 \equiv y_3 \pmod 2,$$

the y_i integers, the i_α pertaining to (1, 1, 1).

Clearly, any system of integral quaternions can be transformed into infinitely many such diagonal systems. It is only necessary to transform the norm-form into a form $Y_0^2+a_2a_3Y_1^2+a_3a_1Y_2^2+a_1a_2Y_3^2$, where the Y_i are linear expressions with rational coefficients in the x_i, and to work out the conditions of integrality.

For example, consider F_5. Since adj f has $c_5=-1$, and c_p is $+1$ for all other p, we seek a form (a_2a_3, a_3a_1, a_1a_2) of a small determinant, with the same property, so that it shall be rationally equivalent to adj f. We easily find (5, 10, 2). Now 4 adj $f=7x_1^2+7x_2^2+3x_3^2-6x_1x_2-2x_1x_3-2x_2x_3$, and has determinant 100, and cannot be expressed as $5(\ )^2+10(\ )^2+2(\ )^2$, where the indicated linear forms are to have integer coefficients. We therefore take the next best, 16 adj f, and find the expression

$$5(-2x_2)^2 + 10(x_1 - x_3)^2 + 2(3x_1 - 2x_2 + x_3)^2.$$

We therefore obtain a norm-form $(y_0/2)^2+5(y_1/2)^2+10(y_2/4)^2+2(y_3/4)^2$, by

$$(2) \quad y_0 = 2x_0 + x_1 + x_2 + x_3,\ y_1 = -x_2,\ y_2 = x_1 - x_3,\ y_3 = 3x_1 - 2x_2 + x_3.$$

The y_i are then integers with the x_i, but the integrity of the x_i requires $y_2+y_3\equiv 2y_1 \pmod 4$, $y_0+y_1\equiv y_2 \pmod 2$. Hence the system of integral quaternions associated with F_5 becomes transformed into Σ_5:

$$(3) \qquad \begin{gathered}(2y_0 + 2y_1i_1 + y_2i_2 + y_3i_3)/4,\\ y_0 + y_1 \equiv y_2 \pmod 2, \qquad y_2 + y_3 \equiv 2y_1 \pmod 4,\end{gathered}$$

the y_i integers, the i_α pertaining to $f=(2, 1, 5)$. That is, for the last, $i_1^2=-5$, $i_2^2=-10$, $i_3^2=-2$, $i_1i_2=-i_2i_1=5i_3$, and so on.

In a similar way, using the respective transformations

$$(4) \quad y_0 = 2x_0 + x_1,\ y_1 = x_1,\ y_2 = x_2,\ y_3 = x_2 + 2x_3, \quad \text{for } F_3 \text{ and } F_7,$$

$$(5) \quad y_0 = 2x_0 + x_1 + x_3,\ y_1 = +x_1,\ y_2 = -x_3,\ y_3 = 2x_1 + 4x_2 + x_3, \quad \text{for } F_{13},$$

we find for F_3, F_7, and F_{13} the arithmetics Σ_3, Σ_7, and Σ_{13}:

$$(6) \qquad (y_0 + i_1y_1 + i_2y_2 + i_3y_3)/2, \qquad y_0 \equiv y_1, y_2 \equiv y_3 \pmod 2,$$

the y_i integers, the i_α pertaining to $f=(1, 1, 3)$ for Σ_3, to $(1, 1, 7)$ for Σ_7;

$$(7)\qquad (2y_0 + 2y_1i_1 + y_2i_2 + y_3i_3)/4,$$
$$y_0 + y_1 \equiv y_2 \pmod 2,\ y_2 + y_3 \equiv 2y_1 \pmod 4,$$

the i_α pertaining to $f=(2, 1, 13)$ for Σ_{13}.

The author wishes here to acknowledge the valuable assistance of Miss C. S. Williams, who checked most of the computations in this and the following sections.

The preceding diagonal forms will simplify the work of deriving the non-maximal systems in which, subject to (1) of §5, factorization is always possible.

12. **Integral transformations, especially of norm-forms into norm-forms.** Two integral matrices T_1, T_2 are called *right-equivalent* if there exists a unimodular matrix U such that $T_1=T_2U$. H. J. S. Smith [13, vol. I, p. 389] has shown that any integral matrix of order r and determinant n (>0) is right-equivalent to a unique matrix

$$(1)\qquad \begin{bmatrix} n_1 & n_{12} & \cdots & n_{1r} \\ 0 & n_2 & \cdots & n_{2r} \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & n_r \end{bmatrix}, \qquad n = n_1 \cdots n_r,\ 0 \leqq n_{ij} < n_i.$$

Hermite was the first to give a general enunciation of this [6(b), p. 192]. Hence, if n is a prime p, an integral matrix of order 3 is right-equivalent to one and only one of the p^2+p+1 *prime* matrices

$$(2)\qquad \begin{bmatrix} p & \alpha & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & p & \alpha \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p \end{bmatrix}, \qquad \alpha, \beta = 0, 1, \cdots, p-1.$$

We shall now prove the following lemma.

LEMMA 14. *Let T be an integral matrix of determinant n. Then for every expression $n=p_1p_2 \cdots p_s$ as a product of primes in some order, we can find prime matrices $P_1, \cdots, P_s$ such as in* (2) *and of respective determinants $p_1, \cdots, p_s$, and a unimodular matrix U, such that*

$$(3)\qquad T = P_1P_2 \cdots P_sU.$$

It is easily seen that T can be expressed in this form with the primes p_i in some particular order. For example,

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & pn & \alpha \\ 0 & 0 & m \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & n & \alpha \\ 0 & 0 & m \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

and unit factors can eventually be moved to the extreme right, by Smith's result. It remains only to show that if P and Q are of determinants p and q, where p and q are distinct primes, then $PQ=Q_1P_1U_1$. We can suppose P and Q to be of the types in (2); hence PQ is of one of the forms

$$\begin{bmatrix} pq & \alpha & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} p & \alpha & \beta \\ 0 & q & \gamma \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} p & \alpha & \beta \\ 0 & 1 & 0 \\ 0 & 0 & q \end{bmatrix}, \quad \begin{bmatrix} q & \alpha & \beta \\ 0 & p & \gamma \\ 0 & 0 & 1 \end{bmatrix},$$

and so on. In the first three cases the diagonal matrix $\{p, 1, 1\}$ can obviously be factored out to the right. In the fourth case,

$$\begin{bmatrix} q & \alpha & \beta \\ 0 & p & \gamma \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n_2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} q & 0 & \beta - n_2\gamma \\ 0 & p & \gamma \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & n_1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where n_1 and n_2 are integers such that $\alpha=n_2p+n_1q$. Clearly, $\{1, p, 1\}$ can be factored out at the right of the middle matrix.

We consider now the conditions under which a norm-form G is derivable from a norm-form F by applying an integral transformation T of determinant n to the variables x_α, that is, to adj f, and then a translation on x_0 (to make the coefficients of x_0x_α be 0 or 1. If $A=(A_{\alpha\beta})=\text{adj}(a_{\alpha\beta})$, where $(a_{\alpha\beta})$ is semi-integral, the matrix $T'AT$ will not, in general (if $n>1$), be the adjoint of a semi-integral matrix $(b_{\alpha\beta})$. If $T'AT$ is the adjoint of some semi-integral matrix, we shall call T a *suitable* transformation for A.

If T is suitable, and $T'AT=\text{adj}(b_{\alpha\beta})$, then comparing determinants we get $n^2\Delta^2=|b_{\alpha\beta}|^2$, and we can choose the sign of $(b_{\alpha\beta})$ to get $|b_{\alpha\beta}|=n\Delta$. Hence if U is the matrix of cofactors of T, whence $U'T=TU'=UT'=nI$, then

$$U'(a_{\alpha\beta})U = n(b_{\alpha\beta}). \tag{4}$$

Conversely, (4) implies $T'AT=\text{adj}(b_{\alpha\beta})$. Hence: *a necessary and sufficient condition that T be suitable for A is that $U'(a_{\alpha\beta})U$ be "divisible by n,"* the quotient to be semi-integral.

If $n=p^sm$, where p is a prime not dividing m, and if T is suitable, then T_1 must be suitable, if we factor T as T_1T_2, $|T_1|=p^s$, $|T_2|=m$, T_1 and T_2 integral. For if (in obvious notations)

$$U_2'U_1'(a_{\alpha\beta})U_1U_2 = p^sm(b_{\alpha\beta}),$$

where $(b_{\alpha\beta})$ is semi-integral, then multiplying by T_2 and T_2', we get

$$U_1'(a_{\alpha\beta})U_1 = p^s(T_2(b_{\alpha\beta})T_2'/m).$$

Since the leftside is semi-integral, the right side must be likewise, and since m is prime to p, $T_2(b_{\alpha\beta})T_2'$ must be "divisible by m."

LEMMA 15. *If* $|T| = p^s$ $(s \geqq 1)$, *and if* T *is suitable for* A, *then* T *has a left-divisor of determinant* p *which is suitable for* A, *except that* (i) *if* d *is prime to* p, *and* (ii) *if* $f \sim a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \pmod{p^r}$, *where* $p > 2$, $p \mid a_3$, *and* $(-a_1a_2 \mid p) = -1$, *or if* $f \sim x_1^2 + x_1x_2 + x_2^2 + \kappa x_3^2 \pmod{2^r}$, *where* $p = 2$ *and* κ *is even, then* T *may not have a suitable left-divisor of determinant* p, *but if so will have one of determinant* p^2.

Using Hermite's result we can suppose that

$$T = \begin{bmatrix} p^\rho & \lambda & \mu \\ 0 & p^\sigma & \nu \\ 0 & 0 & p^\tau \end{bmatrix}, \qquad \begin{matrix} 0 \leqq \lambda, \mu < p^\rho, \ 0 \leqq \nu < p^\sigma, \\ \rho + \sigma + \tau = s, \ \rho, \sigma, \tau \geqq 0. \end{matrix} \tag{5}$$

We shall actually prove a little more in case (ii), namely that if we take the $\sim$ as being $\equiv$ (as we can, by a unimodular transformation), then any matrix which has no suitable left-divisor of determinant p will be right-equivalent to a matrix (5) where $\rho > 0$, $\sigma > 0$, $\tau = 0$, $\lambda \equiv 0 \bmod p$, and then

$$P_{\mu\nu}' = \begin{bmatrix} p & 0 & \mu \\ 0 & p & \nu \\ 0 & 0 & 1 \end{bmatrix} \tag{6}$$

is a left-divisor of T, and is suitable for A.

If f has the form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \bmod p^r$, then the three diagonal elements of $U'(a_{\alpha\beta})U$, and the doubles of the three non-diagonal elements, are:

$$p^{2\rho+2\sigma}a_3, \ p^{2\rho+2\tau}a_2 + p^{2\rho}\nu^2a_3, \ p^{2\sigma+2\tau}a_1 + p^{2\tau}\lambda^2a_2 + (\lambda\nu - p^\sigma\mu)^2a_3; \tag{7}$$

$$-2p^{2\rho+\sigma}\nu a_3, \ 2p^{\rho+\sigma}(\lambda\nu - p^\sigma\mu)a_3, \ -2p^{\rho+2\tau}\lambda a_2 - 2p^{\rho}\nu(\lambda\nu - p^\sigma\mu)a_3. \tag{8}$$

The condition for T to be suitable is that p^s divide these six numbers.

If p divides every a_α, evidently every matrix of determinant p is suitable. If p divide a_2 and a_3 but not a_1, then if T is suitable, $\sigma + \tau > 0$; if now $\tau > 0$, the diagonal matrix $P_p = \{1, 1, p\}$ is a suitable left-divisor of T; and if $\tau = 0$ but $\sigma > 0$, the matrix

$$P_\nu = \begin{bmatrix} 1 & 0 & 0 \\ 0 & p & \nu \\ 0 & 0 & 1 \end{bmatrix} \tag{9}$$

is a suitable left-divisor of T. Hence assume $p \nmid a_1a_2$. Also, let $p \mid a_3$. The matrices P_p and $P_{\mu\nu}'$ are suitable. If we left-multiply T in (5) by P_p^{-1} we get an integral product if $\tau \geqq 1$. Hence let $\tau = 0$. Then the suitability of T implies by (7_2) that $\rho > 0$.

Now assume $p > 2$. Then either $\sigma > 0$ and $p \mid \lambda$ (by (8_3)), or $\sigma = 0$ and $p \mid a_1 + a_2\lambda^2$ (by (7_3)). In the last case, $\nu = 0$ and

$$P_{\lambda\mu} = \begin{bmatrix} p & \lambda & \mu \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{10}$$

is a suitable left-divisor of T. But if $\rho>0$, $\sigma>0$, and $p\,|\,\lambda$, then $P_{\mu\nu}'$ is a suitable left-divisor of T. Further, $P_{\mu\nu}'$ has no suitable left-divisor of determinant p if $(-a_1a_2\,|\,p)=-1$, and has $P_{\lambda\mu}$ as a left-divisor if $p\,|\,a_1+a_2\lambda^2$.

Similarly, let $p=2$. Then by (7_3), either $\sigma=0$ and λ is odd, or $\sigma>0$ and λ is even. In the first case, $P_{\lambda\mu}$ is a suitable left-divisor of T. In the second case $P_{\mu\nu}'$ is a suitable left-divisor of T, and has $P_{1,\mu-\nu}$ as a suitable left-divisor.

Next assume that $p\nmid a_1a_2a_3$, $p>2$. It can be verified that the matrix $P_{\lambda\mu}$ is suitable if $p\,|\,a_1+a_2\lambda^2+a_3\mu^2$, P_ν is suitable if $p\,|\,a_2+a_3\nu^2$; and that the three matrices of determinant p^2,

$$P_p' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{bmatrix}, \qquad P_\lambda' = \begin{bmatrix} p & \lambda & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p \end{bmatrix}, \qquad P_{\mu_1\nu_1}', \tag{11}$$

are suitable. In connection with (11) we make the respective assumptions

$$(-a_2a_3\,|\,p) = -1, \quad p\nmid a_1+a_2\lambda^2, \quad p\nmid a_1a_2+a_2a_3\mu_1^2+a_3a_1\nu_1^2. \tag{12}$$

For, if (12_1) does not hold, P_p' is left-divisible by P_ν; if (12_2) does not hold, P_λ' is left-divisible by $P_{\lambda 0}$. Lastly, P_ν will be a left-divisor of $P_{\mu_1\nu_1}'$ if $p\,|\,a_2+a_3\nu^2$, excluded by (12_3) if $p\,|\,\mu_1$. Again, $P_{\lambda\mu}$ will be a left-divisor of $P_{\mu_1\nu_1}'$ if and only if λ and μ satisfy

$$a_1+a_2\lambda^2+a_3\mu^2 \equiv 0, \qquad \mu_1-\lambda\nu_1-\mu \equiv 0 \pmod{p}.$$

Eliminating μ, and assuming that $p\,|\,a_1a_2+a_2a_3\mu_1^2+a_3a_1\nu_1^2$, we readily obtain $(a_1\nu_1+a_2\mu_1\lambda)^2\equiv 0 \pmod{p}$, which is solvable for λ if $p\nmid\mu_1$.

Now T has P_p' as a left-divisor if $\sigma\geqq 1$, $\tau\geqq 1$, and $p\,|\,\nu$. (i) Suppose that $\sigma=0$, whence $\nu=0$. Since $p^{\rho+\tau}\,|\,(7_1)$, (8_2), and (7_3), we have $\tau\leqq\rho$, $\mu=p^\tau\mu_1$, $p^{\rho-\tau}\,|\,a_1+a_2\lambda^2+a_3\mu_1^2$. If here $\rho=\tau$, then as $0\leqq\mu<p^\rho$, $\mu=0$ and $P_{\lambda\mu}$ is a left-divisor of T. But if $\rho>\tau$, then $P_{\lambda\mu_1}$ is a left-divisor. (ii) Suppose $\sigma\geqq 1$, $\tau=0$. If $p\,|\,a_2+a_3\nu^2$, P_ν is a left-divisor of T. Assume $p\nmid a_2+a_3\nu^2$. Then $\sigma\leqq\rho$ by (7_2), $\lambda=p^\sigma\lambda_1$ by (8_3), $p^{\rho-\sigma}\,|\,a_1+a_2\lambda_1^2+a_3(\lambda_1\nu-\mu)^2$ by (7_3). If now $\rho=\sigma$, whence $\lambda=0$, then $P_{\mu\nu}'$ is a left-divisor of T. But if $\rho>\sigma$, then $P_{\lambda_1,\mu-\lambda_1\nu}$ is a left-divisor. (iii) Finally suppose $\sigma\geqq 1$, $\tau\geqq 1$, $p\nmid\nu$. By (8_1), $\tau\leqq\rho$. If now $\sigma\leqq\tau$, then by (8_3), $p^{\sigma+\tau}\,|\,\lambda\nu-p^\sigma\mu$, $\lambda=p^\sigma\lambda_1$, λ_1 an integer, and $p\,|\,\lambda_1\nu-\mu$. And if $\sigma>\tau$, then by (8_2), $\lambda=p^\tau\lambda_2$; by (8_3), $p^\sigma\,|\,\lambda_2(a_2p^{2\tau}+a_3\nu^2)-p^{\sigma-\tau}a_3\mu\nu$, $p^{\sigma-\tau}\,|\,\lambda_2$, $\lambda=p^\sigma\lambda_1$, $p^\tau\,|\,a_3\nu(\lambda_1\nu-\mu)$, $p\,|\,\lambda_1\nu-\mu$. In either case, P_{λ_1}' is a left-divisor of T.

Now assume $p\nmid a_1a_2a_3$, $p=2$. The suitability of T implies (i) $\rho+\sigma>0$; (ii) $\rho>0$, or $\rho=0$ and $2\,|\,2^\tau+\nu$; (iii) $\tau>0$ and $2\,|\,\lambda\nu-2^\sigma\mu$, or $\tau=0$ and $2\,|\,2^\sigma+\lambda+\lambda\nu-2^\sigma\mu$. Hence, if $\rho=0$, then $\sigma>0$, $\lambda=\mu=0$, and P_ν is a suitable

left-divisor of T. If $\rho>0$, and $\sigma=\tau=0$, then $\nu=0$ and $\lambda+\mu$ is odd; hence $P_{\lambda\mu}$ is a suitable left-divisor. If $\rho>0$ and $\tau=0<\sigma$, then $2\mid\lambda(1+\nu)$; then $P_{\lambda_1\mu_1}$ is a left-divisor if λ is even, and $\mu-\lambda_1\nu-\mu_1$ even, and is suitable if $\lambda_1+\mu_1$ is odd: this can be achieved when λ is even unless ν is odd. Also, if ν is odd, P_ν is a suitable left-divisor. Lastly, if $\rho>0$ and $\tau>0$, then $2\mid\lambda\nu-2^\sigma\mu$, and P_2 succeeds.

We assume next that $f\equiv jx_1^2+x_1x_2+jx_2^2+(j+1)\gamma x_3^2$, $j=0$ or 1, γ an integer. Then 2^e must divide the six numbers

$$\begin{aligned}&(j+1)2^{2\rho+2\sigma}\gamma,\ j2^{2\rho+2\tau}+(j+1)2^{2\rho}\gamma\nu^2,\ 2^{2\sigma+2\tau}j-2^{\sigma+2\tau}\lambda+2^{2\tau}\lambda^2j\\ &\qquad+(j+1)\gamma(\lambda\nu-2^\sigma\mu)^2;\\ &(j+1)2^{2\rho+\sigma+1}\gamma\nu,\ (j+1)2^{\rho+\sigma+1}\gamma(\lambda\nu-2^\sigma\mu),\ 2^{\rho+\sigma+2\tau}-j\lambda2^{\rho+2\tau+1}\\ &\qquad-(j+1)2^{\rho+1}\gamma\nu(\lambda\nu-2^\sigma\mu).\end{aligned}\tag{13}$$

(Note also that if f is replaced by $2^\delta f$, $\delta>0$, these six numbers are multiplied by 2^δ, and every matrix of determinant 2 is suitable.)

Let γ be odd. The suitable matrices of determinant 2 or 4, omitting some of determinant 4 which have suitable left-divisors of determinant 2, are P_2 and $P_{\mu\nu_1}'$ if $j=1$, and the following if $j=0$:

$$P_2^*=\begin{bmatrix}1&0&0\\0&2&0\\0&0&1\end{bmatrix},\quad P_{\lambda_1\lambda_1}=\begin{bmatrix}2&\lambda_1&\lambda_1\\0&1&0\\0&0&1\end{bmatrix},\quad P_{1,1}'=\begin{bmatrix}2&0&1\\0&2&1\\0&0&1\end{bmatrix}.\tag{14}$$

Now let $j=0$. Evidently P_2^* is a left-divisor of T if $\sigma\geqq1$ and ν is even; $P_{\lambda_1\lambda_1}$ is a left-divisor (for λ_1 zero or one) if $\rho>0$, $\sigma=0$, $\mu\equiv2^{2\tau}\lambda \bmod 2$; or if

$$\rho>0,\ \sigma>0,\ \lambda \text{ is even, } \nu \text{ is odd, } 2^\tau\mu \text{ is even;}\tag{15}$$

likewise for $P_{1,1}'$ if

$$\rho>0,\ \sigma>0,\ \lambda \text{ is even, } \nu \text{ is odd, } 2^\tau\mu \text{ is odd.}\tag{16}$$

Further, if $\sigma=0$ (whence $\nu=0$) and T is suitable, then by (13), $2^{\rho+\tau}\mid-2^{2\tau}\lambda+\gamma\mu^2$, $\mu\equiv2^{2\tau}\lambda \bmod 2$. Hence let $\sigma>0$ and ν be odd. Then by (13_2), $\rho\geqq\sigma+\tau>0$, and by (13_3), λ is even; and either (16) or (15) holds.

Now let $j=1$. Then P_2 is a left-divisor if and only if $\tau\geqq1$; and if $\tau=0$, $P_{\mu\nu_1}'$ is a left-divisor of T (for some choice of μ_1, $\nu_1=0$ or 1) if and only if $\rho\geqq1$, λ is even, μ is even if $\tau>0$, $\sigma\geqq1$, ν is even if $\tau>0$. But if T is suitable and $\tau=0$, then (13_3) shows that $\sigma\geqq1$ and λ is even, (13_2) that $\rho\geqq\sigma$. Thus in all cases P_2 or $P_{\mu\nu_1}'$ is a divisor.

Let γ be even. If $\tau>0$, P_2 is a suitable divisor. If $\tau=0$, $\sigma>0$, and $j=0$, then P_ν is effective. If $j=1$ and $\tau=0$, then if T is suitable, $\rho>0$ by (13_2), $\sigma>0$ by (13_3), λ is even by (13_3), and $P_{\mu\nu}'$ is a left-divisor of T and has no

suitable left-divisors of determinant 2. If $j=0$, $\tau=0=\sigma$, then $\rho>0$, and λ must be even by (13_3), and $P_{\lambda\mu}$ succeeds.

Finally, let $f\equiv 2^{\alpha}a_1x_1^2+2^{\beta+2}(jx_2^2+x_2x_3+jx_3^2)$, where $j=0$ or 1, a_1 is odd, and $\alpha\leqq\beta$. If $\alpha>0$ every matrix of determinant 2 is suitable. Let $\alpha=0$. If T is suitable, $\sigma+\tau>0$. If $\tau>0$, use P_2; if $\tau=0$ and $\sigma>0$, use P_ρ.

It follows from these lemmas that if a norm-form G arises from a norm-form F by an integral transformation of determinant n, then a form equivalent to G can be arrived at by a succession of transformations of type (5). And further we can use the prime factors of n in any desired order, starting with a transformation of determinant p or p^2, in most cases continuing with transformations of determinant p, and obtaining norm-forms at each step.

Suppose that at some step a norm-form F_1 is obtained for which a particular factorization with the properties in Theorem 3 is not possible. Then the genus of F_1 must contain a form G_1 of minimum greater than 1. (Note that if an indefinite norm-form represents -1, then by composition with itself it represents $+1$.) If we now apply a further integral transformation to F_1 to obtain G, then the same transformation replaces G_1 by a form G_2 in the genus of G. Since G_1 represents all the numbers represented by G_2, the minimum of G_2 is also greater than 1. Hence we need seek no further for genera containing norm-forms only. All this will be illustrated and applied in §§13–15.

13. **Norm-forms derived from F_d by transformations of determinant 2^s.** We shall now investigate the genera which: (a) contain norm-forms G, (b) are derived from F_2 by integral transformations of determinant a power of 2, and (c) contain no classes of minimum greater than 1. We shall find that there are exactly ten such genera, including that of F_2, and that each contains only one class.

We have first a lemma, which follows easily from Lemma 12, giving a form-residue mod 2^r of any norm-form:

LEMMA 16. *If G is a norm-form corresponding to an integral ternary form g, then G is equivalent to a form with one of the following residues* mod 2^r, *r large*:

$$x_0^2 + a_2a_3x_1^2 + a_3a_1x_2^2 + a_1a_2x_3^2; \tag{1}$$

$$x_0^2 + x_0x_3 + jx_3^2 + \lambda(jx_1^2 + x_1x_2 + jx_2^2); \tag{2}$$

$$x_0^2 + (4j-1)2^{2\beta}x_3^2 + \lambda(jx_1^2 + x_1x_2 + jx_2^2). \tag{3}$$

Here $j=0$ or 1, λ and the a_α are integers, β is a non-negative integer; if $j=1$ then λ is even. Also, in (3), *the power of 2 in λ exceeds 2^β and must not equal $2^{2\beta+1}$. In* (3) *the cases $j=0$ and 1 are equivalent* mod 2^r *if the power of 2 in λ is $2^{2\beta}$ or $2^{2\beta+2}$. The values of c_2 are given by $c_2=(-a_1a_2,\ -a_1a_3)_2$ in* (1); *and in* (2) *and* (3) *by*

$$\begin{aligned} c_2 &= (-1)^i \quad \text{if } \lambda \text{ contains an odd power of } 2; \\ &= +1 \quad \text{if } \lambda \text{ contains an even power of } 2. \end{aligned} \tag{4}$$

Since G is now to be derived from F_2, we must have $c_2 = -1$. Hence in both (2) and (3), $j=1$ and λ contains an odd power of 2. Also, in (1), $(-a_1a_2, -a_1a_3)_2$ must be -1. Further we can replace g by mg, m odd, since this will not affect the form-residue of G mod 2^r; and so can suppose that the odd part of det g is congruent to 1 mod 8. Hence an examination of the *unique* form-residues attainable in (1) for g will show that if det g is 1, 2, 4, or 8, then (a_1, a_2, a_3) can be taken to be one of the triples

$$(5) \qquad \begin{gathered}(1,1,1);\ (1,1,2);\ (1,2,2),\ (1,1,4);\\ (2,2,2),\ (1,2,4),\ (1,1,8),\ (1,3,24),\ (-1,3,-24), \qquad \text{mod } 2^r.\end{gathered}$$

I. *Forms G of determinant* 1. The only residue in (1), (2), and (3) consistent with det $G=1$, and with λ limited as above, is $x_0^2+x_1^2+x_2^2+x_3^2$ mod 2^r. That is, there is only one genus of determinant 1 to be considered. Evidently this genus contains the form

$$(6) \qquad F_4 = y_0^2 + y_1^2 + y_2^2 + y_3^2,$$

and (as is well known) this is in a genus of one class. Note that F_4 is derivable from F_2 by the transformation $x_1=y_2+y_3$, $x_2=y_3+y_1$, $x_3=y_1+y_2$, $x_0=y_0-y_1-y_2-y_3$, of determinant 2.

II. *Forms G of determinant* 4. The possible genera are determined by the form-residues $x_0^2+2x_1^2+2x_2^2+x_3^2$ and $x_0^2+x_0x_3+x_3^2+8(x_1^2+x_1x_2+x_2^2)$, mod 2^r. These genera contain the forms

$$(7) \qquad F_8 = y_0^2 + 2y_1^2 + 2y_2^2 + y_3^2,$$

$$(8) \qquad F_8' = y_0^2 + y_1^2 + 3y_2^2 + 3y_3^2 + y_0y_1 + y_0y_2 + y_0y_3 - 2y_2y_3,$$

and each of these is easily seen to belong to a genus of one class (cf. determinant 64 below). Clearly F_8 is derived from F_4 by a transformation of determinant 2, and F_8' from F_2 by a transformation of determinant 4.

III. *Forms G of determinant* 16. There are three possible genera, corresponding to the form-residues

$$\begin{gathered}x_0^2 + 2x_1^2 + 2x_2^2 + 4x_3^2, \qquad x_0^2 + x_1^2 + 4x_2^2 + 4x_3^2,\\ x_0^2 + 3x_3^2 + 8(x_1^2 + x_1x_2 + x_2^2), \qquad \text{mod } 2^r.\end{gathered}$$

Each genus contains only one class (cf. next case). Representatives of these classes are

$$(9) \qquad F_{16} = y_0^2 + 2y_1^2 + 2y_2^2 + 4y_3^2, \qquad F_{16}' = y_0^2 + 4y_1^2 + 4y_2^2 + y_3^2,$$

$$(10) \qquad F_{16}'' = y_0^2 + 3y_1^2 + 3y_2^2 + 3y_3^2 - 2y_1y_2 - 2y_1y_3 - 2y_2y_3.$$

IV. *Forms G of determinant* 64. There are six possible genera, corresponding to the form-residues

$$(11') \qquad \begin{gathered}(1,4,4,4),\ (1,2,4,8),\ (1,1,8,8),\ (1,3,8,24),\\ (1,-3,-8,24),\ x_0^2 + x_0x_3 + x_3^2 + 32(x_1^2 + x_1x_2 + x_2^2),\ \text{mod } 2^r.\end{gathered}$$

The second, third, fourth, and sixth contain the following forms of minimum greater than 1:

$2y_0^2+3y_1^2+2y_1y_2+3y_2^2+4y_3^2$,

$2y_0^2+5y_1^2+5y_2^2+2y_3^2+2y_0y_1-2y_0y_2+2y_1y_3+2y_2y_3$,

$3(y_0+y_1/3+y_2/3-y_3/3)^2+(11y_1^2+11y_2^2+8y_3^2+10y_1y_2+8y_1y_3+8y_2y_3)/3$,

$3(y_0+y_1/3-y_2/3+y_3/2)^2+(44y_1^2+44y_2^2+27y_3^2-40y_1y_2-12y_1y_3-12y_2y_3)/12$.

However, the forms corresponding to $(11_1')$ and $(11_5')$,

$$(11) \qquad F_{32} = y_0^2 + 4y_1^2 + 4y_2^2 + 4y_3^2,$$

$$(12) \qquad F_{32}' = y_0^2 + 5y_1^2 + 5y_2^2 + 4y_3^2 + 2y_1y_2 + 4y_1y_3 + 4y_2y_3,$$

are in genera of one class. This may be seen, in the case of F_{32}, by the fact that the reciprocal (1, 1, 1, 4) of F_{32}, which will be found in various tables of quaternaries (the best, with determinant up to 25, is Townes [14]); or by our methods of construction which when applied exhaustively lead to representatives of every class in a given genus; or, most simply, by H. J. S. Smith's explicit formula [13, vol. II, p. 666] for the weight of a genus. Thus in the case of F_{32}', which has 16 positive automorphs, we have (in Smith's notations [13, vol. II, pp. 666–668]) $I_1=1$, $I_2=8$, $I_3=1$, $W=(1/12)\zeta(1/2)^0(1/2)^0 8^2(1/\pi^2)(\pi^2/8)$ $=(2/3)\zeta$, where $\zeta=(3/128)(3-1)(3-1)=3/32$, $W=1/16$; hence F_{32}' is in a genus of one class.

V. *Forms G of determinant* 256. Neither (11) nor (12), nor any of the residues mod 2^r in case III, are of the special forms in (i) or (ii) of Lemma 15. Hence we have only to consider the genera derived from (11) and (12) by suitable transformations of determinant 2. Every transformation (on the y_α) of determinant 2 is suitable for (11), and we get three derived genera, represented by

$$(13') \quad (1, 4, 4, 16),\ (1, 4, 8, 8),\ x_0^2 + 48x_3^2 + 8(x_1^2 + x_1x_2 + x_2^2), \text{ mod } 2^r;$$

from $(1, 24, -8, -3)$, whence $a_1=1$, $a_2=-3$, $a_3=-8$, we find by the suitable transformations P_2, $P_{1,\mu}$ the two form-residues

$$(13'') \qquad (1, 24, -8, -12), \qquad (1, -48, 16, -3), \qquad \text{mod } 2^r.$$

The genus of $(13_2')$ is derived also from $(11_2')$ and so contains a form of minimum greater than 1; we list such forms also for the genera with the residues $(13_1')$, $(13_1'')$, and $(13_2'')$:

$$4x_0^2 + 4x_0x_1 + 5x_1^2 + 4x_2^2 + 4x_3^2,$$

$$5(x_0 + 2x_1/5 + x_2/5)^2 + 4(4x_1^2 + 4x_1x_2 + 6x_2^2 + 5x_3^2)/5,$$

$$5(x_0 + x_1/5 - 2x_3/5)^2 + (29x_1^2 + 20x_2^2 + 16x_3^2 - 20x_1x_2 - 16x_1x_3)/5.$$

In the genus determined by $(13_3')$ mod 2^r we find the form

$$F_{64} = x_0^2 + 8(x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + x_2x_3). \tag{13}$$

Curiously enough, this case is missing in Smith [13, vol. II, pp. 669–670] (here $I_1=4$, $I_2=1$, $I_3=4$, and $\theta_1, \theta_2, \theta_3 \equiv 1, 0, 1$, mod 2, so that our case would have come under Smith's $E(b)$). However, if a is the minimum of a form in the genus of F_{64}, $a^4 \leqq 1024$, $a \leqq 5$. But $a=2$, 3, and 5 are not represented by forms in this genus. Further, 4 is not represented primitively. For if $F_{64} \equiv 4 \pmod{2^r}$, $x_0 \equiv 2 \pmod 4$, $x_0^2 \equiv 4 \pmod{32}$, $x_1^2+x_2^2+x_3^2+x_1x_2+x_1x_3+x_2x_3 \equiv 0 \pmod 4$, every x_α is even. Hence all forms in the genus represent 1, and by Theorem 9, all such forms are norm-forms. But the genus of the ternary form $f=3x_1^2+3x_2^2+3x_3^2-2x_1x_2-2x_1x_3-2x_2x_3$ contains only one class. The same follows for F_{64}.

VI. *Forms G of determinant* 1024. We have only to apply transformations of determinant 2 to $(13_3')$. The resulting form-residues are

$$x_0^2 + 192x_3^2 + 8(x_1^2 + x_1x_2 + x_2^2), \quad x_0^2 + 48x_3^2 + 8x_1^2 + 24x_2^2, \quad \text{mod } 2^r.$$

The latter form is derivable from (1, 3, 8, 24) in (11'), and so its genus contains a class of minimum greater than 1. To get a form of minimum a in the genus of the first form, note that $a^4 \leqq 4 \cdot 1024$, $a=1$, 4, or 8. Trying $a=4$ we consider $4x_0^2+4x_0x_3+kx_3^2+\cdots$, and try to satisfy $4k-4=192$. Hence we take $k=49$, and consider $4(x_0+x_3/2)^2+\phi(x_1, x_2, x_3)$, $\phi \equiv 48x_3^2+\cdots \sim 48x_3^2+8(x_1^2+x_1x_2+x_2^2) \bmod 2^r$. Here det ϕ must be 256, and adj $\phi = 16\psi$, where $\psi \sim 3x_3^2+24(x_1^2-x_1x_2+x_2^2) \bmod 2^r$, det $\psi = 16$, and adj $\psi = \phi$. A possible form ψ is easily found to be $3x_1^2+3x_2^2+3x_3^2-2x_1x_2-2x_1x_3-2x_2x_3$, and we construct

$$\begin{aligned} 4(x_0 + x_1/2 + x_2/2 + x_3/2)^2 + 8x_1^2 + 8x_2^2 + 8x_3^2 + 8x_1x_2 + 8x_1x_3 + 8x_2x_3 \\ = 4x_0^2 + 9x_1^2 + 9x_2^2 + 9x_3^2 + 4x_0x_1 + 4x_0x_2 + 4x_0x_3 \\ + 10x_1x_2 + 10x_1x_3 + 10x_2x_3, \end{aligned}$$

which is in the desired genus, since

$$\begin{aligned} 9(x_1+5x_2/9+2x_0/9+5x_3/9)^2+8(7x_2^2+5x_2x_3+7x_3^2+4x_0^2+2x_0x_2+2x_0x_3)/9 \\ \sim x_1^2+8(x_2^2+x_2x_3+x_3^2+\kappa x_0^2), \bmod 2^r, \end{aligned}$$

where by the determinant, κ can only be 24.

All further genera derived from these must contain a class of minimum greater than 1.

Consider now the genera containing norm-form classes only, which can be derived from $F_3=x_0^2+x_0x_3+x_3^2+x_1^2+x_1x_2+x_2^2$ by transformations of determinant 2^e. Now $c_3=-1$, $c_2=1$. Hence in (2) and (3), either $j=1$ and λ contains an even power of 2, or $j=0$. The residue $F_3 \sim x_0^2+3x_3^2+x_1^2+3x_2^2 \bmod 3^r$ is not changed by transformations of determinant prime to 3.

I. *Forms of determinant* 9/4. The preceding conditions allow only one genus, that with the form-residue $x_0^2+x_0x_3+2x_1x_2 \bmod 2^r$. This genus has only one class, represented by

$$(14)\quad F_6 = (x_0 + x_1/2 + x_2/2)^2 + (x_3 + x_1/2 + x_2/2)^2 + 3(x_1^2 + x_2^2)/2.$$

II. *Forms of determinant* 9. There are three genera, each of one class, containing the respective forms

$$(15)\quad F_{12} = x_0^2 + 3x_1^2 + 3x_2^2 + x_3^2,$$

$$(16)\quad F_{12}' = x_0^2 + x_0x_3 + x_3^2 + 4(x_1^2 + x_1x_2 + x_2^2),$$

$$(17)\quad F_{12}'' = (x_0 + x_1/2 + x_2/2 + x_3/2)^2 + (15x_1^2 + 7x_2^2 + 7x_3^2 - 6x_1x_2 - 6x_1x_3 - 2x_2x_3)/4.$$

Here F_{12}'' has the form-residue $x_0^2+x_0x_3+4x_1x_2 \bmod 2^r$, and is derived from F_6; F_{12} is derived by the transformation $x_0=y_0-y_2$, $x_1=y_1+y_2$, $x_2=-y_2+y_3$, $x_3=-y_2+y_3$, of determinant 2, from F_6. But F_{12}' is derived by a transformation of determinant 4 from F_3.

III. *Forms of determinant* 36. The form

$$(18)\quad F_{24} = x_0^2 + 3x_3^2 + 4(x_1^2 + x_1x_2 + x_2^2)$$

is in a genus of one class, and can be derived from any of F_{12}, F_{12}', F_{12}''. The genera with the form-residues $x_0^2+6x_1^2+6x_2^2+x_3^2$ and $x_0^2+x_0x_3+8x_1x_2$, mod 2^r, contain the following forms of minimum 2:

$$(18')\quad 2x_0^2 + 2x_1^2 + 3x_2^2 + 3x_3^2, \qquad 2(x_0 + x_1/4 + x_2/2 + x_3/2)^2 + (15x_1^2 + 28x_2^2 + 28x_3^2 - 12x_1x_2 - 12x_1x_3 - 8x_2x_3)/8.$$

IV. *Forms of determinant* 144. We must now apply transformations of determinant 2 to (18). We thus get the genus of one class containing

$$(19)\quad F_{48} = x_0^2 + 12x_3^2 + 4(x_1^2 + x_1x_2 + x_2^2);$$

and the genera with the form-residues

$$(19')\quad x_0^2 + 3x_1^2 + 4x_2^2 + 12x_3^2, \qquad x_0^2 - x_3^2 + 8x_1x_2, \qquad \bmod 2^r.$$

The latter is derivable from $(18_2')$; the former genus contains the form

$$(19'')\quad 5x_0^2 + 4x_1^2 + 4x_2^2 + 4x_3^2 + 2x_0x_1 - 4x_0x_2 + 4x_0x_3 + 4x_1x_3$$

of minimum 4.

V. *Forms of determinant* $144\cdot 2^{2s}$. The only genus derived from (19) by suitable transformations of determinant 2 is that containing $x_0^2+12x_1^2+12x_2^2+4x_3^2$, and being derived also from $(19_1')$, it contains a form of minimum greater than 1.

Proceeding next from F_5, whence $c_2=1$ and $c_5=-1$, we have $F_5 \sim x_1^2+3x_1^2+5x_2^2+15x_3^2 \bmod 5^r$.

I. *Forms of determinant* 25/4. The only residue mod 2^r is $x_0^2+x_0x_3+2x_1x_2$, and this gives a genus of one class, containing

$$(20)\qquad F_{10}=(x_0+x_2/2+x_3/2)^2+(12x_1^2+7x_2^2+7x_3^2-4x_1x_2-4x_1x_3-6x_2x_3)/4.$$

II. *Forms of determinant* 25. The possible genera have the form-residues

$$(21')\qquad x_0^2+x_1^2-x_2^2-x_3^2,\ x_0^2+x_0x_3+x_3^2+4(x_1^2+x_1x_2+x_2^2),\ x_0^2+x_0x_3+4x_1x_2,\ \text{mod } 2^r.$$

The first contains the form

$$(21)\qquad F_{20}=x_0^2+5x_1^2+3x_2^2+2x_2x_3+2x_3^2$$

in a genus of one class; and the other two contain the following forms of minimum greater than 1:

$$3x_0^2+3x_1^2+3x_2^2+3x_3^2+2x_0x_1+3x_0x_2+3x_0x_3-x_1x_2-x_1x_3+x_2x_3,$$

$$3x_0^2+3x_1^2+2x_2^2+2x_3^2+2x_0x_1-x_0x_2-x_0x_3-x_1x_2-x_1x_3-x_2x_3.$$

III. *Forms of determinant* 100. Suitable transformations on $x_0^2+x_1^2-x_2^2-x_3^2$ mod 2^r are $x_1\to 2x_1+x_2$; and $x_2\to 2x_2+x_3$; the resulting form-residues are $x_0^2+x_1^2-4x_2^2-4x_2x_3-2x_3^2\sim x_0^2+x_1^2-2x_2^2-2x_3^2$, and $x_0^2+4x_1^2+4x_1x_2-x_3^2\sim x_0^2+4x_1x_2-x_3^2$. The following forms in these genera have minimum greater than 1:

$$3x_0^2+2x_0x_3+2x_3^2+6x_1^2+4x_1x_2+4x_2^2,$$

$$5x_1^2+3x_0^2+3x_2^2+3x_3^2+2x_0x_2+2x_0x_3+2x_2x_3.$$

Proceeding similarly from F_7, the derived genus of determinant 49/4 with the residue $x_0^2+x_0x_3+2x_1x_2$ mod 2^r contains the form

$$2x_0^2+2x_1^2+2x_2^2+2x_3^2+x_0x_2-x_0x_3+x_1x_2+x_1x_3$$

of minimum 2. This disposes, for determinant 49, of the residue $x_0^2+2x_0x_3+2x_1x_2\sim(x_0+x_3)^2-x_3^2+2x_1x_2\sim x_0^2+x_1^2-x_2^2-x_3^2$ mod 2^r; or else note the form $3x_0^2+3x_1^2+3x_2^2+3x_3^2+2x_0x_2-2x_0x_3+2x_1x_2+2x_1x_3$ of minimum 3. The residue $(21_3')$ also is eliminated. But $(21_2')$ gives the form

$$(22)\qquad F_{28}=(x_0+x_2/2+x_3/2)^2+(32x_1^2+11x_2^2+11x_3^2-8x_1x_2-8x_1x_3-6x_2x_3)/4$$

in a genus of one class.

All genera of norm-forms derived from F_{13} by transformations of determinant 2^s contain classes of minimum greater than 1. For, the residue $x_0^2+x_0x_3+2x_1x_2$ mod 2^r and determinant 169/4 belong to the form

$$2(x_0+x_4/4-x_2/2-x_3/4)^2+(31x_1^2+28x_2^2+15x_3^2-12x_1x_2-14x_1x_3-4x_2x_3)/8.$$

The residues $(21_1')$ and $(21_3')$ are eliminated as before; but $(21_2')$ yields a genus of determinant 169 containing the form of minimum 3,

$$3(x_0+x_1/6+x_2/6-x_3/3)^2+(59x_1^2+59x_2^2+32x_3^2-38x_1x_2-8x_1x_3-8x_2x_3)/12.$$

14. The norm-forms permitting factorization with m subject only to §5(1). Every norm-form G is derivable from a norm-form F in which adj f is fundamental. If F is not equivalent to one of the five forms F_d, the genus of F will contain a class of minimum greater than 1, and the same will hold for G. It is therefore sufficient to consider only forms derived from the F_d.

Let $F_d=(x_0+2^{-1}\sum\epsilon_\alpha x_\alpha)^2+\sum A_{\alpha\beta}x_\alpha x_\beta$. If G is derived from F_d by the application of an integral transformation T of determinant τ to the x_α, we have

$$(1)\qquad \begin{aligned} &G=(r_0+2^{-1}\textstyle\sum\epsilon_\alpha^* r_\alpha)^2+\sum B_{\alpha\beta}r_\alpha r_\beta, \qquad B=T'AT, \qquad \xi=T\rho \\ &\text{where } \rho'=(r_1,r_2,r_3), \qquad x_0+2^{-1}\textstyle\sum\epsilon_\alpha x_\alpha=r_0+2^{-1}\sum\epsilon_\alpha^* r_\alpha. \end{aligned}$$

If we should apply a full transformation of order 4 to F_d we would have a more difficult discussion of suitability of transformations and of genera. However, after narrowing the problem a little we shall use such full transformations.

We saw in §11 that, for certain integral matrices S of determinant σ, where $\sigma=4$ if $d=2$, 5, and 13, and $\sigma=2$ if $d=3$ and 7, the transformation

$$(2)\qquad \eta=S\xi, \qquad x_0+2^{-1}\textstyle\sum\epsilon_\alpha x_\alpha=y_0/2,$$

replaces F_d by the form H_d, where

$$(3)\qquad 4e^2H_d=e^2y_0^2+e^2d_1y_1^2+ed_1y_2^2+ey_3^2,$$

d_1=odd part of d, $e=1$ for $d=2$, 3, 7, $e=2$ for $d=5$, 13. Also, (2) replaces the system Σ_F of integral quaternions associated with F_d by the arithmetically equivalent system Σ_d ($d=2, 3, 7, 5, 13$).

As in Lemma 14, we can for the given S and T choose integral matrices S_1 and T_1 of determinants σ and τ, such that $ST=T_1S_1$. Hence $T=S^{-1}T_1S_1$ and replaces A by B. Let τ be odd. Consider, after (2), the transformations

$$(4)\qquad \eta=T_1\zeta, \qquad y_0/2=z_0/2,$$

$$(5)\qquad \zeta=S_1\rho, \qquad z_0/2=r_0+2^{-1}\textstyle\sum\epsilon_\alpha^* r_\alpha.$$

On applying (4) to Σ_d we obtain a subsystem Σ_d' by imposing the restriction on the y_α that the z_α be integers, that is, that $T_1^{-1}\eta$ be integral mod τ; or if we prefer to carry through the substitution, we obtain a system Σ_d'' arithmetically equivalent to Σ_d', with elements expressible as $z_0/2+z_1i_1''/2+\cdots$ where now the z_i are unrestricted mod τ but still satisfy relations mod 2 or 4 due to those on the y_i in Σ_d. As an algebra, the system Σ_d'' must be the same as that obtained by application of (5) from the system of integral quaternions Σ_G. Further, the conditions of integrality are the same, it being assumed that τ is odd: for, the condition that $S_1^{-1}\zeta$ $(=\rho)$ be integral mod σ is the same as the condition that $S^{-1}T_1\zeta(=\xi)$ be integral mod σ, since $S^{-1}T_1=TS_1^{-1}$ and T^{-1} is integral mod σ.

Hence if we prove by one instance that factorization is not possible in Σ_d',

the same will follow for Σ_G, whence the genus of G will contain a class of minimum greater than 1.

Since T_1S_1 $(=ST)$ replaces $\phi=e^2d_1y_1^2+ed_1y_2^2+ey_3^2$ by $4e^2\sum B_{\alpha\beta}r_\alpha r_\beta$, clearly T_1 is a suitable tranformation for ϕ.

We shall now apply to the y_α the suitable transformations T_1 of determinant p or p^2, where, to begin with, $p\nmid 2d$. The genus of the form G so obtained must represent 2. For, F_d represents 2, and since $|T|\,(=|T_1|)$ is prime to $2d$, we can solve the congruences $G\equiv 2 \pmod{2^r}$ and $\pmod{d^r}$. To prove that we can solve $G\equiv 2 \pmod{p^r}$, where p is now the only other prime in the determinant of G, we note that G is carried by (5) (of determinant prime to p) into $z_0^2/4+\psi/4e^2$, where ψ is as follows (cf. paragraph containing (11) in §12):

$$
\begin{aligned}
&e^2d_1(pz_1+\lambda z_2+\mu z_3)^2+ed_1z_1^2+ez_3^2, && \text{if } p\mid 1+e\lambda^2+ed_1\mu^2;\\
&e^2d_1z_1^2+ed_1(pz_2+\nu z_3)^2+ez_3^2, && \text{if } p\mid e+ed_1\nu^2;\\
&e^2d_1z_1^2+ed_1p^2z_2^2+ep^2z_3^2, && \text{if } (-d_1\mid p)=-1;\\
&e^2d_1(pz_1+\lambda' z_2)^2+ed_1z_2^2+ep^2z_3^2, && \text{if } p\mid 1+e\lambda'^2;\\
&e^2d_1(pz_1+\mu' z_3)^2+ed_1(pz_2+\nu' z_3)^2+ez_3^2, && \text{if } p\nmid e+e^2d_1\mu'^2+ed_1\nu'^2.
\end{aligned}
\tag{6}
$$

In each case ϕ has a coefficient mz_α^2 where $p\nmid m$, and the solvability of $G\equiv 2$ follows from that of $z_0^2+mz_\alpha^2\equiv 2 \pmod{p^r}$.

The quaternions of norm 2 in the various Σ_d are easily found by solving

$$ey_0^2+ed_1y_1^2+d_1y_2^2+y_3^2=8e, \tag{7}$$

subject to the restrictions on the y_i in (1), (3), (6), (7) of §11, and are as follows:

$$
\begin{aligned}
&d=2:\ \pm(1\pm i_1),\ \pm(1\pm i_2),\ \pm(1\pm i_3),\ \pm(i_2\pm i_3),\ \pm(i_3\pm i_1),\ \pm(i_1\pm i_2);\\
&d=3:\ \pm(1\pm i_3),\ \pm(2\pm i_2\pm i_3)/2,\ \pm(1\pm i_1\pm 2i_3)/2,\ \pm(1\pm i_1\pm i_2\pm i_3);\\
&d=7:\ \pm(1\pm i_3),\ \pm(1\pm i_1)/2,\ \pm(i_2\pm i_3)/2;\\
&d=5:\ \pm(\pm 2i_1+i_2+i_3)/4,\ \pm(\pm 2+i_2+3i_3)/4,\ \pm(1\pm i_1\pm i_3)/2,\ \pm i_3;\\
&d=13:\ \pm(\pm 2+i_2-i_3)/4,\ \pm i_3.
\end{aligned}
\tag{8}
$$

At the same time, we record the quaternions of norm 1:

$$
\begin{aligned}
&d=2:\ \pm 1,\ \pm i_1,\ \pm i_2,\ \pm i_3,\ \pm(1\pm i_1\pm i_2\pm i_3)/2;\\
&d=3:\ \pm 1,\ \pm i_3,\ \pm(1\pm i_1)/2,\ \pm(i_2\pm i_3)/2; \qquad d=7:\ \pm 1,\ \pm i_3;\\
&d=5:\ \pm(\pm 2+i_2-i_3)/4,\ \pm 1; \qquad d=13:\ \pm 1.
\end{aligned}
\tag{9}
$$

Suppose that T_1 is $P_{\lambda\mu}$ of §12. Then in Σ_d', $y_1\equiv\lambda y_2+\mu y_3 \bmod p$, and this is satisfied by quaternions of norm 2 as follows: by $1\pm i_1$, never; $1\pm i_2$ only if $\lambda\equiv 0$; $1\pm i_3$ and i_3 if $\mu\equiv 0$; $i_2\pm i_3$ and $2\pm i_2\pm i_3$ if $\lambda\equiv\pm\mu$; $i_1\pm i_3$ and $1\pm i_1\pm i_3$ if $\mu\equiv\pm 1$; $i_1\pm i_2$ if $\lambda\equiv\pm 1$; $1\pm i_1\pm 2i_3$ if $2\mu\equiv\pm 1$; $1\pm i_1\pm i_2\pm i_3$ if $\pm\lambda\pm\mu\equiv\pm 1$;

$\pm 2i_1+i_2+i_3$ if $\lambda+\mu\equiv\pm 1$; $\pm 2+i_2+3i_3$ if $\lambda\equiv -3\mu$; $\pm 2+i_2-i_3$ if $\lambda\equiv\mu$, mod p.

Now the number of solutions λ, μ mod p of $1+e\lambda^2+ed_1\mu^2\equiv 0$ is $p-(-d_1|p)$. Of these, the number with $\lambda\equiv 0$ is $1+(-ed_1|p)$; the number with $\mu\equiv 0$ is $1+(-e|p)$; the number with $\lambda\equiv\pm\mu$ is $2[1+(-2|p)]$ if $d=2$ or 7, $2[1+(-1|p)]$ if $d=3$; the number with $\lambda\equiv -3\mu$ is 0 if $d=5$ and $p=7$, but $1+(-7|p)$ if $d=5$ and $p\neq 7$; the number with $\lambda\equiv\mu$ is 0 if $d=13$ and $p=7$, $1+(-7|p)$ if $d=13$ and $p\neq 7$; the number with $\mu\equiv\pm 1$ is $2[1+(-2|p)]$ if $d=2$, $2[1+(-22|p)]$ if $d=5$; the number with $\lambda\equiv\pm 1$ is $2[1+(-2|p)]$ if $d=2$; the number with $2\mu\equiv\pm 1$ is $2[1+(-7|p)]$ if $d=3$; the number with $\pm\lambda\pm\mu\equiv 1$ is $4[1+(-7|p)]$ if $d=3$; if $d=5$, the number with $\lambda+\mu\equiv\pm 1$ is 2 if $p=3$, $2[1+(-2|p)]$ if $p>5$. Counting these as they come, not worrying about duplicates, we find *at most* n_d solutions (λ, μ) for which a quaternion of norm 2 may belong to Σ_d', where

$$(10)\quad n_d=\begin{cases} 8+2(-1|p)+6(-2|p) & \text{if } d=2,\\ 9+3(-1|p)+6(-7|p) & \text{if } d=3,\\ 3+(-1|p)+2(-2|p) & \text{if } d=7,\\ 6+3(-2|p)+(-7|p)+2(-22|p) & \text{if } d=5,\ p>7,\\ 2+(-2|p)+(-7|p) & \text{if } d=13,\ p\neq 7;\end{cases}$$

while $n_d=0$ if $d=5$ or 13 and $p=7$. Hence there exist solutions of $1+e\lambda^2+ed_1\mu^2\equiv 0$ mod p, for which Σ_d' contains no quaternions of norm 2, in the following cases:

$$(11)\quad \begin{aligned} &d=2, \text{ if } p=7,\ p=13, \text{ or } p\geqq 19;\quad d=3, \text{ if } p\geqq 13;\\ &d=7, \text{ if } p\geqq 3;\quad d=5, \text{ if } p\geqq 7;\quad d=13, \text{ if } p\geqq 3.\end{aligned}$$

If T_1 is P_ν of §12, which requires that $p|1+d_1\nu^2$ and $y_2\equiv\nu y_3$ mod p, we find a value of ν for which Σ_d' contains no quaternion of norm 2 in *the additional case* $d=5$ *and* $p=3$; that is, if we take $\nu=-1$, no quaternion of norm 2 satisfies $y_2\equiv -y_3$ mod 3.

Now only one genus of norm-forms G is obtained from F_d by all the suitable transformations of a given determinant p not dividing $2d$. For, the form-residue mod p_1^r of G is determined by that of F_d if $p_1\neq p$; and if $p_1=p$, of the two apparent possibilities $(1, n, p, np)$, where n may be a quadratic residue or non-residue, only one is possible, since $c_p=(-n|p)$, and c_p is invariant under all rational transformations. Here, c_p is $+1$, and we can take $n=-1$.

The preceding paragraph holds also if the transformations of determinant p are of order 4, the forms so obtained being necessarily in the genus of G, though not necessarily norm-forms. If T_2 is of determinant p and order 4, and S_2 denotes the integral transformation of order 4 and determinant 2σ which replaces H_d by F_d, then we can choose integral matrices S_3 and T_3, of determinants 2σ and p, such that $T_2S_3=S_2T_3$. For if we define S_2^* by $S_2^*S_2=2\sigma I$, we

have $S_2{}^*T_2 = T_3S_4$, and $2\sigma T_2 = S_2T_3S_4$. Hence $2\sigma S_4^{-1} = T_2^{-1}(S_2T_3)$. The left side is integral mod p, the right side mod 2. Hence $2\sigma S_4^{-1}$ is an integral matrix, say S_3; and $T_2S_3 = S_2T_3$. Now if T_3 replaces F_d by a form G_1 with a form-residue $(1, -1, p, -p)$ mod p^r, then G_1 is in the genus of G. Also, the transformation T_2S_3 replaces H_d by G_1.

We thus have four forms: F_d, H_d, H_d', and G_1; where H_d' is obtained from H_d by the transformation T_2; and hence G_1 from H_d' by S_3. The variables y_i in H_d are to be subjected to the conditions mod 2 or 4 of the system Σ_d; the variables z_i in H_d' are to be subjected to the conditions mod 2 or 4 such that, under S_3, the variables of G_1 are arbitrary integers. If we now prove that H_d', so conditioned, does not represent 1, the same holds for G_1. Since $|T_2|$ is odd, the conditions of integrality on the z_i mod 2 or 4 must be equivalent to the conditions on the y_i, connected with the z_i by T_2.

Let us therefore apply to H_d the transformation

$$(12) \qquad T_2: \quad y_0 = pz_0 + \lambda_1 z_1 + \lambda_2 z_2 + \lambda_3 z_3, \quad y_1 = z_1, \quad y_2 = z_2, \quad y_3 = z_3.$$

LEMMA 17. *Let $a_0a_1a_2a_3$ be prime to p, $p>2$. Then every third order minor determinant in the matrix of $\psi(z_0, z_1, z_2, z_3) = a_0(pz_0+\sum\lambda_\alpha z_\alpha)^2+\sum a_\alpha z_\alpha{}^2$ is divisible by p if and only if*

$$(13) \qquad p \mid a_1a_2a_3 + a_0a_2a_3\lambda_1{}^2 + a_0a_1a_3\lambda_2{}^2 + a_0a_1a_2\lambda_3{}^2.$$

Hence the form $4e^2H_d' = e^2(pz_0+\sum\lambda_\alpha z_\alpha)^2+e^2d_1z_1{}^2+ed_1z_2{}^2+ez_3{}^2$ has the form-residue $(1, n, p, np)$ mod p^r if and only if

$$(13') \qquad p \mid d_1 + \lambda_1{}^2 + e\lambda_2{}^2 + ed_1\lambda_3{}^2.$$

Now 1 will be represented in the form H_d' if and only if the coordinates of one of the units in (9) satisfies $y_0 \equiv \lambda_1y_1+\lambda_2y_2+\lambda_3y_3$. For $d=2$, this means that either some $\lambda_\alpha \equiv 0$ or that $\pm\lambda_1\pm\lambda_2\pm\lambda_3+1 \equiv 0$ for some choice of signs. Now if $p=17$, we have $17 \mid 3^2+4^2+5^2+1$, and $\pm3\pm4\pm5+1 \not\equiv 0 \pmod{17}$. Hence G does not represent 1.

If $d=3$, (9_2) shows that H_d' represents 1 if and only if $\lambda_3 \equiv 0$, or $\lambda_1 \equiv \pm 1$, or $\lambda_2 \equiv \pm\lambda_3$. Now $11 \mid 4^2+0^2+3\cdot1^2+3$, $7 \mid 2^2+2^2+3\cdot1^2+3$, and $5 \mid 2^2+0^2+3\cdot1^2+3$; hence if p is 5, 7, or 11, H_d' and G do not represent 1.

If $d=7$ we need $\lambda_3 \not\equiv 0$; we have $3 \mid 0^2+1^2+7\cdot1^2+7$, eliminating $p=3$.

If $d=13$, H_d' cannot represent 1 since $1 \not\equiv 0$.

The transformations (11) of §12, of determinant p^2, lead to two genera, Γ_1 and Γ_2, containing the respective form-residues

$$(14) \qquad (1, n, p^2, np^2) \bmod p^r,$$

where n may be either a quadratic residue or non-residue mod p. Other apparent possibilities, such as $(1, p, np, np^2)$, are excluded by the fact that ϕ is primitive in (6), and are indeed derived from the genera obtained previously by transformations of determinant p. The genera Γ_1 and Γ_2 are distinguish-

able by the coefficient $n=e+e^2d_1\mu'^2+ed_1\nu'^2$ of z_3^2. We seek to determine values of μ' and ν' which make $(n|p)$ either $+1$ or -1, and such that the conditions

$$y_1 \equiv \mu' y_3, \qquad y_2 \equiv \nu' y_3 \pmod{p} \tag{15}$$

eliminate all quaternions of norm 2. This is rather easy, since μ' and ν' now satisfy only the *incongruence* $e+e^2d_1\mu'^2+ed_1\nu'^2 \not\equiv 0 \pmod{p}$.

Referring again to (8) we see that (15) fails to hold, for all the quaternions of norm 2, unless: (a) $d=2$, $(\mu', \nu') \equiv (0, 0)$, $(0, \pm 1)$, or $(\pm 1, 0)$; (b) $d=3$, $(\mu', \nu') \equiv (0, 0)$, $(0, \pm 1)$, $(\pm 1/2, 0)$, or $(\pm 1, \pm 1)$; (c) $d=7$, $(\mu', \nu') \equiv (0, 0)$, or $(0, \pm 1)$; (d) $d=5$, $(\mu', \nu') \equiv (\pm 1, 1)$, $(\pm 1, 0)$, $(0, 0)$, or $(3\mu', 3\nu') \equiv (0, 1)$; (e) $d=13$, $(\mu', \nu') \equiv (0, 0)$ or $(0, -1) \bmod p$. These cases imply, if $d=2$ that $n \equiv 1$ or 2; if $d=3$ that $n \equiv 1$, 4, 7/4, 7; if $d=7$, $n \equiv 1$, 8; if $d=5$, $n \equiv 32$, 28/9, 22, or 2; if $d=13$, that $n \equiv 28$ or 2, mod p. Hence n can certainly be made either a quadratic residue or non-residue, if

$$d = 2,\ p \geqq 7;\ d = 3,\ p \geqq 7;\ d = 7,\ p \geqq 5;\ d = 5,\ p \geqq 11;\ d = 13,\ p \geqq 7.$$

There can also be eliminated the case $d=2$, $p=5$, since $-(1+1^2+1^2|5)=1 = (1+3\cdot 1^2+3\cdot 2^2|5)$; and the case $d=7$, $p=3$, $(n|p)=-1$, since $(1+7\cdot 1^2+7\cdot 0^2|3)=-1$. By using P_0' of §12, and the condition $y_1 \equiv 0$, $y_3 \equiv 0 \pmod{p}$ we eliminate the case $d=7$, $p=3$, and $(n|3)=+1$. Let $d=5$; the case $p=7$ is eliminated by $(2+20\cdot 2^2+10\cdot 1^2|7)=1=-(2+20\cdot 2^2+10\cdot 0^2|7)$; and the case $p=3$ by P_2', since no quaternions of norm 2 satisfy $y_1 \equiv 2y_2$, $y_3 \equiv 0 \pmod{3}$. Let $d=13$; the cases $p=3$ and 5 are eliminated by $(2+52\cdot 0^2+26\cdot 1^2|3) = 1 = -(2+52\cdot 1^2+26\cdot 1^2|3)$, and $(2+52\cdot 1^2+26\cdot 0^2|5)=1=-(2+52\cdot 1^2+26\cdot 2^2|5)$.

To sum up, we have now eliminated from consideration all cases in which τ contains a prime factor p not dividing $2d$, except that it $d=2$, we have to consider the genus obtained by transformations of determinant 3, 5, or 11, and the genera obtained by transformations of determinant 3^2. (These genera all contain only one class.) We have still to consider genera derived from these, from the genera of §13, and from the F_d by transformations of determinant divisible by d.

Let us consider next the case where $p=d>2$. If $\tau=p$ and the transformation P_p of §12 is used, the genus obtained has the residue $(1, p, ep, ep^2) \bmod p^r$. If $p=3$ or 5, this genus consists of one class. But if $p=7$ or 13, we can eliminate the genus as follows. The transformation (12) applied to H_d produces a form with the residue $(1, p, ep, ep^2) \bmod p^r$ if we take $\lambda_1=\lambda_2=0$ and choose λ_3 so that $(e^2\lambda_3^2+e|p)=1$. If $p=7$ this can be secured with $\lambda_3=1$; and it should be noted in (9_3) that no unit satisfies $y_0 \equiv y_3 \pmod{7}$. If $p=13$, take $\lambda_3=3$.

If we use transformation $P_{\mu\nu}'$, we get the same genus for all μ and ν, with the residue $(1, e, p^3, ep^3) \bmod p^r$. This genus represents 2. The norm-

form will not represent 2 unless one of the quaternions in (8) satisfies $y_1 \equiv \mu y_3$, $y_2 \equiv \nu y_3$, mod p. For $p=5$, 7, or 13, we need merely take $\mu=-\nu=2$. If $p=3$, this method fails; however we easily find in this genus the following form of minimum 2:

$$2(x_0 - x_1/4 + x_2/2)^2 + (31x_1^2 + 28x_2^2 + 16x_3^2 + 4x_1x_2 + 16x_1x_3 + 8x_2x_3)/8.$$

Thus if τ contains an odd prime p, either $d=2$ and $p=3$, 5, or 11; or $d=p=3$ or 5. We must form combinations of these with one another, and the cases of §13.

We shall now complete the discussion of the cases arising from $d=2$.

Since $15 \mid 1+3^2+2^2+1^2$, $33 \mid 1+9^2+4^2+1^2$, $55 \mid 1+7^2+2^2+1^2$, in accordance with (13), we can discard the cases in which τ is divisible by 15, 33, or 55, after noting the following.

The genera obtained from F_2 with $\tau=3^2$ contain the respective forms

$$(16)\quad F_{18}=(x_0+x_1/2+x_2/2)^2+(19x_1^2+19x_2^2+4x_3^2+2x_1x_2+4x_1x_3+4x_2x_3)/4,$$

$$(17)\quad F_{18}'=(x_0+x_2/2)^2+(20x_1^2+11x_2^2+8x_3^2+4x_1x_2+8x_1x_3+8x_2x_3)/4,$$

with the form-residues (1, 1, 9, 9) and (1, 2, 9, 18), mod 3^r. Here F_{18} is equivalent to $(y_0^2+9y_1^2+9y_2^2+y_3^2)/4$ with the condition $y_0 \equiv y_1 \equiv y_2 \equiv y_3$ mod 2; and F_{18}' is equivalent to $(y_0^2+9y_1^2+18y_2^2+2y_3^2)/4$ where $y_0=2x_0+x_2$, $y_1=x_2$, $y_2=x_1$, $y_3=x_1+x_2+2x_3$, so that $y_0 \equiv y_1$, $y_3 \equiv y_1+y_2$, mod 2. Hence the units are ± 1 and $\pm i_3$, and ± 1. Further transformations of determinants 5, 7, and 11 give genera containing classes of minimum not 1. For we have $5 \mid 9+1^2+1^2+9\cdot 1^2$, $7 \mid 9+2^2+0^2+9\cdot 2^2$, and $11 \mid 9+0^2+2^2+9\cdot 1^2$, where $\lambda_3 \not\equiv 0$ mod p (cf. (13)); and 5, 7, and 11 can divide $18+2\lambda_1^2+\lambda_2^2+9\lambda_3^2$, without having $\pm 1 \equiv \lambda_1\cdot 0+\lambda_2\cdot 0+\lambda_3\cdot 0$ mod p.

LEMMA 18. *Let p be an odd prime not dividing d. Then the norm-forms G derivable from F_d by transformations of determinant a power of p have the following form-residues* mod p^r. *Here n, n', n'' denote integers satisfying $(-n \mid p)=1$, $(n' \mid p)=-1$, $(-n'' \mid p)=-1$:*

$$(18)\quad \begin{gathered}(1, n, p, np);\ (1, 1, p^2, p^2),\ (1, n', p^2, n'p^2);\ (1, p, np, np^2);\\ (1, n, p^3, np^3);\ (1, p^2, p^2, p^2);\ (1, p, np^2, np^3),\ (1, n'p, np^2, n''p^3);\end{gathered}$$

and so on. But if $d=p>2$, then the residues mod p^r *are*:

$$(19)\quad \begin{aligned}&(1, p, -n'p, -n'p^2); \qquad (1, -n', p^2, -n'p^3);\\ &(1, p, -n'p^2, -n'p^3), \qquad (1, n'p, -n'p^2, -p^3).\end{aligned}$$

These are easily verified, using the properties that $c_p=1$ in (18), -1 in (19); that G represents 1 and has the residue $x_0^2+\phi(x_1, x_2, x_3)$, where ϕ is the adjoint of an integral form.

Besides the forms (16) and (17), we shall now see that F_2 gives rise by

transformations of determinant p^s to the following forms in genera of one class: if $p=3$,

$$
\begin{aligned}
F_6' &= x_0^2 + x_0x_3 + x_3^2 + 2(x_1^2 + x_1x_2 + x_2^2),\\
F_{18}'' &= x_0^2 + x_0x_3 + x_3^2 + 6(x_1^2 + x_1x_2 + x_2^2),\\
F_{54} &= x_0^2 + x_0x_3 + 7x_3^2 + 6(x_1^2 + x_1x_2 + x_2^2),\\
F_{54}' &= (x_0 + x_1/2 + x_2/2 + x_3/2)^2\\
&\quad + 9(3x_1^2 + 3x_2^2 + 3x_3^2 - 2x_1x_2 - 2x_1x_3 - 2x_2x_3)/4,
\end{aligned}
\tag{20}
$$

with the form-residues (1, 2, 3, 6), (1, 3, 6, 18), (1, 6, 18, 27), and (1, 9, 9, 9) mod 3^r; and if $p=5$,

$$
\begin{aligned}
F_{10}' &= (x_0+x_1/2+x_2/2)^2+(11x_1^2+11x_2^2+4x_3^2+2x_1x_2+4x_1x_3+4x_2x_3)/4,\\
F_{50} &= (x_0+x_1/2)^2+5(7x_1^2+4x_2^2+4x_3^2-4x_1x_2-4x_1x_3)/4,
\end{aligned}
\tag{21}
$$

with the residues (1, 1, 5, 5) and (1, 5, 5, 25), mod 5^r; and if $p=11$,

$$F_{22} = x_0^2 + x_0x_3 + 3x_3^2 + 2(x_1^2 + x_1x_2 + 3x_2^2), \tag{22}$$

with the residue (1, 2, 11, 22) mod 11^r. But all further genera so obtained contain classes of minimum not 1.

To prove that the forms above are in genera of one class, we must correct two misprints in Smith [13, vol. II, pp. 666–668]. On page 666, q_3 in (7) should be q_2; on page 668, f_2 should be θ_2. In our (16), (17), (20), we have respectively $(I_1, I_2, I_3) = (1, 18, 1)$, $(1, 18, 1)$, $(1, 6, 1)$, $(3, 2, 3)$, $(3, 6, 3)$, $(9, 2, 1)$; in all cases (working with F_2 since only modulus 2^r then matters) f_2 represents 3 mod 8, so that $I_1\theta_2$ and $I_3\theta_2$ are 3, mod 8, and $\zeta = 1/24$. Also, working with the form-residues mod 3^r, f_2 represents respectively 1, 2, 2, 3, 6, 9, and θ_2 represents 1, 2, 2, 1, 2, 1, mod 3; $\theta_1/2$ and $\theta_3/2$ both represent 1 mod 3. Hence by Smith's formula (7),

$$W = (1/12)(1/24)k,$$

where (respectively for F_{18}, F_{18}', F_6', F_{18}'', F_{54}, F_{54}')

$$
\begin{aligned}
k = 2^{-1}[1 - 2/3 + 1/9]18^2/8, &\quad 2^{-1}[1 + 2/3 + 1/9]18^2/8,\\
2^{-1}[1 + 2/3 + 1/9]6^2/8, &\quad 4^{-1}[1 + 1/3]27\cdot 4/9,\\
8^{-1}[1 - 1/9]27\cdot 6^2/9, &\quad 2^{-1}\cdot 27\cdot 4/9.
\end{aligned}
$$

Hence $W = 1/w$, where $w = 32, 8, 72, 72, 24, 48$. Since w is the number of positive automorphs of F (cf. Theorem 8) in each case, these six forms are in genera of one class. The forms in (21) and (22) proceed similarly.

The existence of the following forms shows that all further genera obtained by transformations of determinant p^s contain classes of minimum not 1:

$2(x_0+2^{-1}\sum x_\alpha)^2+(17x_1^2+11x_2^2+5x_3^2-10x_1x_2-4x_1x_3-2x_2x_3)/2,$

$3x_0^2+3x_1^2+7x_2^2+7x_3^2-3x_0x_1-3x_0x_2-3x_0x_3+3x_1x_3+7x_2x_3,$

$2x_0^2+5x_1^2+5x_2^2+41x_3^2+x_1x_3-3x_1x_2+2x_0x_1+2x_0x_3,$

$6x_0^2+7x_1^2+10x_2^2+13x_3^2+6x_0x_1+6x_0x_2+6x_0x_3+8x_1x_2+11x_1x_3+14x_2x_3,$

$7x_0^2+7x_1^2+7x_2^2+9x_3^2+3x_0x_3-5x_0x_2-5x_0x_1-3x_2x_3-3x_1x_3-4x_1x_2,$

$7x_0^2+7x_1^2+9x_2^2+9x_3^2+3x_0x_3+3x_0x_2-5x_0x_1+7x_2x_3+6x_1x_3+3x_1x_2,$

with respective residues (1, 2, 27, 54), (1, 3, 18, 54), (1, 1, 81, 81), (1, 6, 27, 162), (1, 9, 9, 81), (1, 9, 18, 162), mod 3^r;

$2(x_0+x_2/2)^2+(14x_1^2+9x_2^2+6x_3^2+2x_1x_2+6x_1x_3+4x_2x_3)/2,$

$2(x_0+2^{-1}\sum x_\alpha)^2+(17x_1^2+17x_2^2+3x_3^2-16x_1x_2-2x_1x_3-2x_2x_3)/2,$

$(x_0+x_1/2)^2+(155x_1^2+100x_2^2+20x_3^2-100x_1x_2-20x_1x_3)/4,$

$(x_0+x_2/2+x_3/2)^2+(260x_1^2+35x_2^2+35x_3^2-20x_1x_2-20x_1x_3-30x_2x_3)/4,$

with residues (1, 1, 25, 25), (1, 2, 25, 50), (1, 5, 25, 125), (1, 10, 25, 250), mod 5^r, the last two forms not representing 11 and 6 respectively;

$3(x_0+x_1/6+x_2/2+x_3/2)^2+(275x_1^2+99x_2^2+99x_3^2-66x_1x_2-66x_1x_3-66x_2x_3)/2,$

with the residue (1, 11, -11, -11^2) mod 11^r, the genera with the residues $(1, n, 11^2, n11^2)$, $n=\pm1$, having been eliminated earlier.

The last step, for forms arising from F_2, is to apply transformations of determinants 3^s, 5^s, or 11^s to the nine forms F_4, F_8, F_8', $\cdots$. We shall see that F_4 yields in this way only two forms in genera of one class:

(23) $F_{12}=x_0^2+3x_3^2+2(x_1^2+x_1x_2+x_2^2)$, $F_{36}=x_0^2+3x_3^2+6(x_1^2+x_1x_2+x_2^2)$,

with residues (1, 2, 3, 6) and (1, 3, 6, 18) mod 3^r. The units for F_4 are ±1, $\pm i_1$, $\pm i_2$, $\pm i_3$. If $\tau=p$, it suffices to have $p\,|\,1+\lambda_1^2+\lambda_2^2+\lambda_3^2$ with all λ_α prime to p; we have $5\,|\,1+1^2+2^2+2^2$, $11\,|\,1+1^2+2^2+4^2$. The case $\tau=p^2=5^2$ or 11^2 was eliminated by our earlier treatment of F_2. To show that transformations of determinant 3^s applied to F_4 yield only (23), we need to construct forms of minimum greater than 1 with the following residues mod 3^r: (1, 1, 9, 9), (1, 2, 9, 18), (1, 3, 18, 54), and (1, 6, 18, 27). For (1, 1, 9, 9) take F_{18}, replace x_3 by $2x_3+x_0+x_1$, and obtain a form not representing 1, which must be equivalent mod 2^r to F_4. For (1, 2, 9, 18) replace x_0 by $2x_0-x_1$ in F_{18}'. For (1, 6, 18, 27) take F_{54} and replace x_0 by $2x_0$. The case (1, 3, 18, 54) was excluded even for forms derived from F_2.

We shall now see that F_8 and F_8' yield no forms. (Since F_{16}, F_{16}', and F_{16}'' are all derivable from F_8 or F_8' this will end the case $d=2$.) For F_8, which has the units ±1 and $\pm i_3$ and is derived from F_4, we have only to note that $3\,|\,2+1^2+1^2+2\cdot1^2$ with λ_3 prime to 3. We can write F_8' as $(z_0^2+z_1^2+z_2^2+z_3^2)/4$ with $z_0=2y_0+y_1+y_2+y_3$, $z_1=y_1+y_2-3y_3$, $z_2=y_1+y_2+y_3$, $z_3=y_1-3y_2+y_3$. The

units are given by $\pm(z_0, z_1, z_2, z_3) = (2, 0, 0, 0), (\pm 1, 1, 1, 1)$. We easily find for $p = 3$, 5, and 11, solutions of $1+\lambda_1^2+\lambda_2^2+\lambda_3^2 \equiv 0 \bmod p$ not satisfying $\pm 1 \equiv \lambda_1+\lambda_2+\lambda_3 \bmod p$. For $\tau = 3^2$ replace x_0 and x_3 in F_{18} and F_{18}' by $2x_0$ and $2x_3$, and obtain forms equivalent mod 3^r to F_{18} and F_{18}', mod 2^r to F_8'.

The case $d = 2$ is now complete.

We prove for F_3 that transformations of determinant 3^s give rise only to

$$F_9 = x_0^2 + x_0x_3 + x_3^2 + 3(x_1^2 + x_1x_2 + x_2^2), \tag{24}$$

$$F_{27} = (x_0 + x_1/2 + x_2/2 + x_3/2)^2 + 3(5x_1^2 + 5x_2^2 + 5x_3^2 - 2x_1x_2 - 2x_1x_3 - 2x_2x_3)/4, \tag{25}$$

with the residues (1, 3, 3, 9) and (1, −3, 9, −27), mod 3^r. The proof, using Smith's formula, that these are in genera of one class is left to the reader. We construct the following forms of minimum greater than 1 in the genera derived from F_3 with the residues (1, 1, 27, 27), (1, 3, 9, 27), and (1, −3, −27, 81) mod 3^r:

$$2(x_0+x_1/4-x_2/2)^2+(31x_1^2+28x_2^2+16x_3^2+4x_1x_2+16x_1x_3+8x_2x_3)/8,$$

$$3(x_0+x_1/2+x_2/2+x_3/2)^2+(9x_1^2+13x_2^2+13x_3^2-6x_1x_2-6x_1x_3-10x_2x_3)/4,$$

$$7(x_0+3x_1/14-x_2/7+5x_3/14)^2 + (159x_1^2+108x_2^2+87x_3^2-72x_1x_2-30x_1x_3-36x_2x_3)/28.$$

Next, applying transformations of determinant 2^s we obtain from F_9 the two forms in genera of one class

$$F_{18}' = (x_0 + x_1/2)^2 + 3(5x_1^2 + 4x_2^2 + 4x_3^2 - 4x_1x_2 - 4x_2x_3)/4, \tag{26}$$

$$F_{36} = x_0^2 + 3x_1^2 + 3x_2^2 + 9x_3^2. \tag{27}$$

The genus derived from F_9 with the same residue mod 2^r as F_{12}' contains the form $3(x_0^2+x_0x_1+x_1^2)+4(x_2^2+x_2x_3+x_3^2)$ of minimum 3; and that with the residue $x_0^2+x_0x_3+4x_1x_2$ mod 2^r contains the form

$$3(x_0 + x_2/2 + x_3/2)^2 + (16x_1^2 + 13x_2^2 + 13x_3^2 - 8x_1x_2 - 8x_1x_3 - 10x_2x_3)/4.$$

Further cases are excluded like those in the paragraph containing (18) in §13.

The forms derived from F_{27} by transformations of determinant 2^s ($s \geqq 1$) are derived from that with the residue $x_0^2+x_0x_3+2x_1x_2$ mod 2^r. Such a form is the following, of minimum 4:

$$7(x_0 + 2x_1/7 + 2x_2/7 + x_3/2)^2 + (96x_1^2 + 24x_1x_2 + 96x_2^2 + 63x_3^2)/28.$$

The case $d = 3$ is complete.

From F_5 we get by transformations of determinant 5^s only

$$F_{25}=(x_0+x_1/2+x_2/2+x_3/2)^2+5(3x_1^2+3x_2^2+3x_3^2+2x_1x_2+2x_1x_3+2x_2x_3)/4 \tag{28}$$

in a genus of one class, with the residue (1, 5, 10, 50) mod 5^r. From F_{25}, the genus with the residue $x_0^2+x_0x_3+2x_1x_2$ mod 2^r contains the form

$$4(x_0+x_1/4+x_2/4-3x_3/8)^2+(60x_1^2+60x_2^2+55x_3^2-40x_1x_2-20x_1x_3-20x_2x_3)/16.$$

We have now proved the following two theorems:

THEOREM 11. *There are exactly* 39 *classes of positive, integral forms f for which the genus of the associated norm-form F contains only one class. These forms f are as follows, those for which F is derived from the same* F_d ($d=2, 3, 5, 7, 13$) *being grouped together:*

d	$f=(a, b, c, r, s, t)$ $=ax^2+by^2+cz^2+2ryz+2szx+2txy$	d	$f=(a, b, c, r, s, t)$
2	(1, 1, 1, 1/2, 1/2, 1/2)	3	(1, 1, 1, −1/2, 0, 0)
4	(1, 1, 1, 0, 0, 0)	6	(1, 1, 2, −1/2, −1/2, 0)
6	(1, 1, 2, 0, 0, −1/2)	9	(1, 1, 3, 0, 0, −1/2)
8	(1, 1, 2, 0, 0, 0)	12	(1, 1, 3, 0, 0, 0)
8	(1, 1, 3, 1/2, 1/2, 1/2)	12	(1, 1, 4, 0, 0, −1/2)
10	(1, 1, 3, −1/2, −1/2, 0)	12	(1, 2, 2, 1/2, 1/2, 1/2)
12	(1, 2, 2, −1, 0, 0)	18	(2, 2, 2, 1/2, 1, 1)
16	(1, 2, 2, 0, 0, 0)	24	(2, 2, 2, 0, 0, −1)
16	(1, 1, 4, 0, 0, 0)	27	(2, 2, 2, 1/2, 1/2, 1/2)
16	(2, 2, 2, 1, 1, 1)	36	(1, 3, 3, 0, 0, 0)
18	(1, 1, 5, −1/2, −1/2, 0)	48	(1, 4, 4, −2, 0, 0)
18	(1, 2, 3, −1, −1/2, 0)	5	(1, 1, 2, 1/2, 1/2, 1/2)
18	(1, 1, 6, 0, 0, −1/2)	10	(1, 2, 2, 1, 1/2, 1/2)
22	(1, 2, 3, 0, −1/2, 0)	20	(1, 2, 3, −1, 0, 0)
32	(2, 2, 2, 0, 0, 0)	25	(2, 2, 2, −1/2, −1/2, −1/2)
32	(2, 2, 3, −1, −1, 0)	7	(1, 1, 2, −1/2, 0, 0)
36	(2, 2, 3, 0, 0, −1)	28	(1, 3, 3, 1, 1/2, 1/2)
50	(2, 3, 3, 1/2, 1, 1)	13	(1, 2, 2, −1/2, 0, −1/2)
54	(2, 3, 3, −3/2, 0, 0)		
54	(3, 3, 3, 3/2, 3/2, 3/2)		
64	(3, 3, 3, −1, −1, −1)		

THEOREM 12. *If the genus of a positive norm-form F contains more than one class, then it contains at least one class not representing* 1.

Our proof of this very simple result is indeed complicated. There should be some easier way of proving that if F_1 and F_2 are inequivalent norm-forms in the same genus, then there exists a third form G in their genus which does not represent 1.

A description of the properties of the 39 systems, which will make them more easily accessible for applications, has been published in the Duke Mathematical Journal by Miss C. S. Williams and the author (vol. 12 (1945) pp. 527–539).

15. Theorem 3 is best possible.

THEOREM 13. *If the genus of a norm-form F contains a class not representing* 1, *then there exist infinitely many primes p such that*: (i) *p is represented by the genus of F, and* (ii) *for each p there exist primitive pure quaternions x (in the quaternion system associated with F) of norms divisible by p but having no right-divisors of norm p.*

We shall first prove the following lemma.

LEMMA 19. *If F_1 and F_2 are any two inequivalent forms in the genus of a norm-form F, there exist infinitely many squarefree numbers n, coprime in pairs, for each of which there exist integral matrices Q of determinant n^2 such that Q replaces F_1 by nF_2. We can suppose also that the prime factors of each n are representable by the genus of F.*

We start with the fact that there exists a transformation T/s, where s is a positive integer which can be taken prime to any assignable number, and T is an integral matrix of determinant s^4, which replaces F_1 by F_2. Hence T replaces F_1 by s^2F_2. Taking $m=s^2$, we have transformations P of determinant m^2 replacing F_1 by mF_2. Write $m=p^2r^2$, where p is a prime not dividing $2d$. We can factor P as QR, where $|Q|=p^2$, and $|R|=p^2r^4$ (cf. §12). We can suppose here that Q replaces F_1 by pF_3, where F_3 is an integral form (necessarily in the genus of F).

To prove the last statement, we apply an integral transformation of determinant ± 1 to secure $F_1 \equiv \lambda(t_0^2+t_1^2+t_2^2+t_3^2) \bmod m^2$. We can thus study more easily the structure of P and Q. Let p^{2s} be the highest power of p in m^2, and let S be the left factor of P of determinant p^{2s}. Then S replaces $t_0^2+t_1^2+t_2^2+t_3^2$ by a form all of whose coefficients are divisible by p^s. By Hermite's result in §12 we can suppose that S has the form

$$\begin{bmatrix} p^{e_1} & k_1 & k_2 & k_3 \\ 0 & p^{e_2} & k_4 & k_5 \\ 0 & 0 & p^{e_3} & k_6 \\ 0 & 0 & 0 & p^{e_4} \end{bmatrix},$$

where $2s=e_1+e_2+e_3+e_4$, $0 \leqq k_1 < p^{e_1}$, and so on. Hence p^s divides p^{2e_1}, $p^{e_1}k_1$, $k_1^2+p^{2e_2}$, and so on. From these facts we can easily deduce that S has a left factor of determinant p^2, of the form

$$(1) \qquad Q = \begin{bmatrix} p & h & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & h \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} p & 0 & h & k \\ 0 & p & -k & h \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

where p divides $1+h^2$ or $1+h^2+k^2$. Clearly, Q replaces F_1 by pG, where G is integral.

The same argument shows that we can factor m as $p_1p_2 \cdots p_s$, where the p_i are primes, and P as $P_1P_2 \cdots P_s$, where $|P_h| = p_h^2$, and have P_1 replacing F_1 by p_1G_2, P_2 replacing G_2 by p_2G_3, $\cdots$, P_s replacing G_s by p_sF_2. Let G_k be the last form in this sequence which is equivalent to F_1. Then P_k replaces F_1 by either p_kF_2 or p_kF_3, where F_3 is not equivalent to F_1. In the last case we proceed with a new transformation P replacing F_3 by mF_2, with m prime to p_k. We now take G_k to be the last form in the sequence which is equivalent to either F_3 or F_1, and so introduce a new class related to F_1 either by means of a single prime p, or a product of distinct primes pq. Eventually, since the number of classes is finite, we reach F_2. Note finally that each p is represented by the genus of F. For if (say) F_3 represents pF_4, then the solvability of $F_4 \equiv 1 \bmod k$ implies that of $F_3 \equiv p \bmod k$, for every modulus k.

Proceeding with the proof of Theorem 13, we may suppose that F is carried by means of a transformation $P=(p_{ij})$ of a determinant m^2 into mG, where m is squarefree and prime to $2d$, and G does not represent 1. It is now possible to find a primitive pure quaternion x of norm divisible by m, such that the congruence system $x\bar{l} \equiv 0 \bmod m$ has the general solution $t_i = \sum p_{ij}z_j$ (z_j integers). We can secure $F \equiv t_0^2+t_1^2+t_2^2+t_3^2$ by a slight transformation. For each prime p in m we can write $P=QR$, where $|Q| = p^2$, $|R|$ is prime to p, and Q is given by (1). The condition that $t_i = \sum p_{ij}z_j$ is equivalent for each p to the condition that $Q^{-1}t$ be integral mod p, t denoting here a column vector. We can assume that Q has the second form in (1), and on taking $x_0 \equiv 0$, $x_1 \equiv 1$, $x_2 \equiv -k$, $x_3 \equiv h$, mod p, see that (5) of §6 is equivalent to $t=Qu$ with u integral. Theorem 13 follows, since at least one factor p of m will have the properties stated.

It should perhaps be remarked that an x cannot always be found as above if m is not squarefree. For example if the rows of (p_{ij}) are $(p, 0, 0, 0)$, $(0, p, 0, 0)$, $(0, 0, p^2, k)$, and $(0, 0, 0, 1)$, and $F \equiv \sum t_i^2 \bmod p^4$, then $x\bar{l} \equiv 0 \bmod p^2$ requires that $p \mid x$.

References

1. P. Bachmann, *Die Arithmetik der quadratischen Formen*, I, Leipzig, 1898.
2. H. Brandt, *Idealtheorie in Quaternionalgebren*, Math. Ann. vol. 99 (1928) pp. 1–29.
3. L. E. Dickson, (a) *Algebras and their arithmetics*, Chicago, 1923; (b) *Algebren und ihre Zahlentheorie*, Zürich, 1927; (c) *Studies in the theory of numbers*, Chicago, 1930.
4. H. Hasse, *Über die Äquivalenz quadratischer Formen in Körper der rationalen Zahlen*, Journal für Mathematik vol. 152 (1923) pp. 205–224.
5. K. Hensel, *Zahlentheorie*, Berlin and Leipzig, 1913.
6. C. Hermite, (a) *Sur la théorie des formes quadratiques*, Journal für Mathematik vol. 47 (1854) pp. 307–342; (b) vol. 41 (1850) p. 192.
7. A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*, Berlin, 1919.
8. B. W. Jones and G. Pall, *Regular and semi-regular positive ternary quadratic forms*, Acta Math. vol. 70 (1939) pp. 165–191.

9. A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives quaternaires*, Math. Ann. vol. 5 (1872) pp. 581–583.

10. C. G. Latimer, *The classes of integral sets in a quaternion algebra*, Duke Math. J. vol. 3 (1937) pp. 237–247.

11. U. V. Linnik, (a) *On certain results relating to positive tenrary quadratic forms*, Rec. Math. (Mat. Sbornik) N.S. vol. 5 (1939) pp. 453–471; (b) *Über die Darstellung grosser Zahlen durch positive ternäre quadratische Formen*, Bull. Acad. Sci. URSS Sér. Math. vol. 4 (1940) pp. 363–402.

12. G. Pall, *On the factorization of generalized quaternions*, Duke Math. J. vol. 4 (1938) pp. 696–704.

13. H. J. S. Smith, *Collected mathematical papers*, Oxford, 1894.

14. S. B. Townes, *Table of reduced positive quaternary quadratic forms*, Ann. of Math. vol. 41 (1940) pp. 57–58.

McGill University,
Montreal, Quebec, Canada.