ON IDEALS IN A QUATERNION ALGEBRA AND THE REPRESENTATION OF INTEGERS BY HERMITIAN FORMS*

BY

CLAIBORNE G. LATIMER

1. **Introduction.** In another paper,† it was shown that there is a one-to-one correspondence between certain classes of ideals, called regular classes, in a quaternion ring $\mathfrak{G}$, and certain classes of binary Hermitian forms. A binary Hermitian form is in one of these classes if and only if (a) its coefficients are in the set G of all integral numbers in a certain quadratic field of discriminant Δ, (b) the variables range over G, (c) its determinant is a certain integer α, (d) it represents positive integers.

Let f be such a form and let m be a positive integer. We shall show that f represents m if and only if there is an ideal of norm m in a certain class $\mathcal{C}$ of ideals in $\mathfrak{G}$. $\mathcal{C}$ is uniquely determined by f. If f is a definite form with exactly k automorphs, we shall show that the number of representations of m by f is exactly kN, where N is the number of ideals in $\mathcal{C}$ of norm m. We then show that if m is prime to $2\alpha\Delta$, the number of ideals in $\mathfrak{G}$ of norm m is exactly $\sigma(m)$, the sum of the positive divisors of m.

Let $f_1, f_2, \cdots, f_H$ be representatives of those classes of forms mentioned above and assume that they are definite forms. If m is positive and prime to $2\alpha\Delta$, if k_i is the number of automorphs of f_i $(i=1, 2, \cdots, H)$ and if every representation of m by f_i be counted as $1/k_i$, then, by the above mentioned results, the total number of representations of m by all the f's is exactly $\sigma(m)$.

We also prove a theorem, which includes one due to Humbert, on certain "generalized" or symbolic representations of an integer by the above f's. It will be seen that such representations may be interpreted explicitly in terms of the corresponding ideals in $\mathfrak{G}$.

There are many results in the literature on the representation of integers by special quaternary quadratic forms which may be written as binary Hermitian forms.‡ A large number of these may be readily obtained from the results of Tr. and of this paper. Several examples are given in the last paragraph.

---

* Presented to the Society, April 10, 1936; received by the editors March 25, 1936.

† *On ideals in generalized quaternion algebras and Hermitian forms*, these Transactions, vol. 38 (1935), pp. 436–446. This paper will be referred to hereafter as Tr.

‡ Cf. Dickson, *History of the Theory of Numbers*, vol. 3, Chapter 10.

2. **The representation of an integer by an Hermitian form.** We shall use the same definitions and notations as used in Tr. unless the contrary is explicitly stated. It will be assumed, as in Tr., that all ideals referred to are left ideals. We shall also assume throughout the paper that all ideals considered are regular ideals.

Let

$$f(x, y) \equiv axx' + bx'y + b'xy' + cyy'$$

be an Hermitian form over G, which represents positive integers, of determinant $bb' - ac = \alpha$, a and c being rational integers and b a number in G. Let m be a positive integer. If $f(r, s) = m$, where r and s are in G, f will be said to represent m. We shall consider the representations of m by f.

Let $f'(x, y) \equiv f(x', y')$. By Theorem 3 of Tr., there is a uniquely determined class $\mathcal{C}$ of ideals in $\mathfrak{G}$ corresponding to the class of forms containing f'. By §5 of Tr., we have

LEMMA 1. *An ideal of $\mathfrak{G}$ is in $\mathcal{C}$ if and only if it has a proper basis Z_1, Z_2 such that*

$$\begin{aligned} EZ_1 &= -b'Z_1 + aZ_2, \\ EZ_2 &= -cZ_1 + bZ_2. \end{aligned} \tag{1}$$

If Z_1, Z_2 form a proper basis of an ideal $\mathfrak{L}$, then the Z's satisfy (1) *if and only if* $N(xZ_1 + yZ_2) = N(\mathfrak{L})f'(x, y)$.*

We shall next prove

LEMMA 2. *If r, s are numbers in G such that $f(r, s) = m > 0$, then*

$$\begin{aligned} \omega_1 &\equiv ar + bs - Es = ar + bs - s'E, \\ \omega_2 &\equiv b'r + cs + Er = b'r + cs + r'E, \end{aligned} \tag{2}$$

form a proper basis of an ideal $\mathfrak{L}$ in $\mathcal{C}$ and $N(\mathfrak{L}) = m$. If $\mathfrak{L}$ is in $\mathcal{C}$ and $N(\mathfrak{L}) = m$, then $\mathfrak{L}$ has a proper basis ω_1, ω_2 as above, where r and s are in G and $f(r, s) = m$.

Suppose $f(r, s) = m > 0$. It may be verified that ω_1, ω_2 in (2) satisfy (1). Hence they form a basis of an ideal $\mathfrak{L}$ in $\mathfrak{G}$. Since the determinant

$$\begin{vmatrix} ar + bs & -s' \\ b'r + cs & r' \end{vmatrix} = f(r, s) = m,$$

it follows that the ω's form a proper basis and $N(\mathfrak{L}) = m$. By Lemma 1, $\mathfrak{L}$ is in $\mathcal{C}$. We shall say that the representation $f(r, s) = m$ belongs to $\mathfrak{L}$.

* The statement "there is a one-to-one correspondence · · · " in lines 8, 9, p. 442, Tr. is false. There is a correspondence but it is not one-to-one. For if the transformation (8) of Tr. is an automorph of f, then f corresponds to the bases ω_1, ω_2 and ζ_1, ζ_2. This error does not affect the validity of any subsequent proof or theorem.

Suppose $\mathfrak{L}$ is an ideal in $\mathcal{C}$ of norm m. By Lemma 1, $\mathfrak{L}$ has a proper basis $\omega_i = g_{i1} + g_{i2}E$ $(i = 1, 2)$, where the ω's satisfy (1) and $N(x\omega_1 + y\omega_2) = mf'(x, y)$. We have $m = N(\mathfrak{L}) = |g_{ij}| = g_{22}\omega_1 - g_{12}\omega_2$. Hence $f'(g_{22}, -g_{12}) = f(g_{22}', -g_{12}') = m$. Replace each Z_i in (1) by $g_{i1} + g_{i2}E$ and equate the coefficients of E. We obtain the first pair of equations below.

$$g_{11} = ag_{22}' - bg_{12}', \qquad \omega_1 = ag_{22}' - bg_{12}' + g_{12}E,$$
$$g_{21} = b'g_{22}' - cg_{12}', \qquad \omega_2 = b'g_{22}' - cg_{12}' + g_{22}E.$$

Noting that $f(g_{22}', -g_{12}') = m$ and comparing the last pair of equations with (2), the lemma follows.

Let $\mathfrak{L}$ be an ideal in $\mathcal{C}$ of norm m and let $f(r, s) = m$ be an arbitrarily chosen but fixed representation belonging to $\mathfrak{L}$. We shall consider the set of all representations of m by f which belong to $\mathfrak{L}$.

Let T be an automorph of f, i.e., a transformation

$$x = t_{11}x_1 + t_{21}y_1, \qquad (3)$$
$$y = t_{12}x_1 + t_{22}y_1$$

which transforms f into itself, the t's being in G and the determinant $|t_{ij}| = 1$. Let $\bar{r}, \bar{s}$ be defined by the equations obtained by replacing x, y, x_1, y_1 in (3) by $r, s, \bar{r}, \bar{s}$ respectively. Then $f(\bar{r}, \bar{s}) = m$. This representation will be said to correspond to T.

We shall show that a representation of m by f belongs to $\mathfrak{L}$ if and only if it corresponds to an automorph of f; also that the representations corresponding to distinct automorphs are distinct. We shall thus have a one-to-one correspondence between those representations of m by f which belong to $\mathfrak{L}$ and the automorphs of f.

LEMMA 3. *A representation of m by f belongs to $\mathfrak{L}$ if and only if it corresponds to an automorph.*

Consider the representation $f(\bar{r}, \bar{s}) = m$ which corresponds to T. Then, employing (2), we have

$$\bar{\omega}_1 \equiv t_{11}'\omega_1 + t_{12}'\omega_2 = g_{11} - E\bar{s}, \qquad (4)$$
$$\bar{\omega}_2 \equiv t_{21}'\omega_1 + t_{22}'\omega_2 = g_{21} + E\bar{r},$$

where g_{11}, g_{21} are certain numbers in G. Since $|t_{ij}'| = 1$, the $\bar{\omega}$'s form a proper basis of $\mathfrak{L}$ by §4 of Tr. We have $x_1\bar{\omega}_1 + y_1\bar{\omega}_2 = x\omega_1 + y\omega_2$, where

$$x = t_{11}'x_1 + t_{21}'y_1, \qquad (5)$$
$$y = t_{12}'x_1 + t_{22}'y_1.$$

Since (3) is an automorph of f, (5) is an automorph of f'. Hence $N(x_1\bar{\omega}_1+y_1\bar{\omega}_2) = mf'(x_1, y_1)$. By Lemma 1, the $\bar{\omega}$'s satisfy (1). Therefore, as in the second part of the proof of Lemma 2, we may express g_{11}, g_{21} in terms of $\bar{r}$, $\bar{s}$ and find

$$\begin{aligned} \bar{\omega}_1 &= a\bar{r} + b\bar{s} - E\bar{s}, \\ \bar{\omega}_2 &= b'\bar{r} + c\bar{s} + E\bar{r}. \end{aligned} \tag{6}$$

Comparing these equations with (2), we see that the representation $f(\bar{r}, \bar{s}) = m$ belongs to $\mathfrak{L}$.

Conversely, suppose $f(\bar{r}, \bar{s}) = m$ is a representation which belongs to $\mathfrak{L}$. The $\bar{\omega}$'s of (6) satisfy (1) and form a proper basis of $\mathfrak{L}$. Then they may be expressed in terms of the ω's as in (4), the t_{ij}' being in G and $|t_{ij}'| = 1$. It may be shown that (5) is an automorph of f' and hence (3) is an automorph of f. If in the first pair of equations (4) we replace each ω_i, $\bar{\omega}_j$ by the expressions (2) and (6) and equate the coefficients of E, we see that $f(\bar{r}, \bar{s}) = m$ is the representation which corresponds to the automorph (3). This completes the proof of the lemma.

Suppose (k_{ji}) is the matrix of an automorph of f. Let $\bar{\omega}_i \equiv k_{i1}'\omega_1 + k_{i2}'\omega_2$ $(i = 1, 2)$, where the ω's are given by (2). Then, as in the preceding proof, the $\bar{\omega}$'s satisfy (1) and we have

$$\begin{aligned} E\bar{\omega}_1 &= -b'\bar{\omega}_1 + a\bar{\omega}_2, & E\omega_1 &= -b'\omega_1 + a\omega_2, \\ E\bar{\omega}_2 &= -c\bar{\omega}_1 + b\bar{\omega}_2, & E\omega_2 &= -c\omega_1 + b\omega_2. \end{aligned}$$

In the first pair of equations, set each $\bar{\omega}_i = k_{i1}'\omega_1 + k_{i2}'\omega_2$, replace each $Ek_{ij}'\omega_j$ by $k_{ij}E\omega_j$, and eliminate the $E\omega_j$ by use of the second pair of equations. Employing the left linear independence of the ω's with respect to G (§4, Tr.), we obtain a system of equations equivalent to the following:*

$$\begin{aligned} bk_{11}' + ck_{12}' &= bk_{11} - ak_{21}, & bk_{21}' + ck_{22}' &= ck_{11} - b'k_{21}, \\ ak_{11}' + b'k_{12}' &= -bk_{12} + ak_{22}, & ak_{21}' + b'k_{22}' &= -ck_{12} + b'k_{22}. \end{aligned} \tag{7}$$

We shall now prove

LEMMA 4. *Let $f(\bar{r}, \bar{s}) = m$, $f(R, S) = m$ be the representations belonging to $\mathfrak{L}$ which correspond to the distinct automorphs T, T_1 respectively. Then $(\bar{r}, \bar{s}) \neq (R, S)$.*

We have

$$\begin{aligned} \bar{r} &= k_{11}R + k_{21}S, \\ \bar{s} &= k_{12}R + k_{22}S, \end{aligned} \tag{8}$$

where (k_{ji}) is the matrix of the automorph $T^{-1}T_1$. Suppose $(\bar{r}, \bar{s}) = (R, S)$.

* The condition $|k_{ij}| = 1$ and (7) imply that (k_{ij}) is the matrix of an automorph of f. If $a \neq 0$, $|k_{ij}| = 1$ and the first pair of (7) imply the second pair.

By (8), $(k_{11}-1)(k_{22}-1)-k_{12}k_{21}=0$. Since $|k_{ji}|=1$, $k_{11}+k_{22}=2$. By (8_2), $k_{12}R=(k_{11}-1)S$. We have $k_{12}k_{12}'m=f(k_{12}R,\ k_{12}S)=f(k_{11}-1,\ k_{12})SS'$. But $f(k_{11}-1,\ k_{12})=f(k_{11},\ k_{12})-(k_{11}+k_{11}')a-(k_{12}b+k_{12}'b')+a$. Since $T^{-1}T_1$ is an automorph, $f(k_{11},\ k_{12})=a$. By (7_2), $k_{12}b+k_{12}'b'=(k_{22}-k_{11}')a$. Therefore $f(k_{11}-1,\ k_{12})=2a-(k_{11}+k_{22})a=0$, $k_{12}=0$ and $k_{11}=k_{22}=1$. From $k_{21}S=(k_{22}-1)R$ we find similarly $k_{21}=0$. Therefore $T^{-1}T_1$ is the identity transformation and $T=T_1$, contrary to hypothesis. The lemma follows.

By Lemmas 2, 3, and 4, we have

THEOREM 1. *Let $f(x, y)$ be an Hermitian form over G, of determinant α, which represents positive integers, let $f'(x, y)\equiv f(x', y')$, and let $\mathfrak{C}$ be the class of ideals in $\mathfrak{G}$ which corresponds to the class of forms containing f'. Every representation of a positive integer m by f belongs to a uniquely determined ideal $\mathfrak{L}$ in $\mathfrak{C}$ of norm m and for every such ideal $\mathfrak{L}$, there is a representation of m by f which belongs to $\mathfrak{L}$. Those representations of m by f which belong to the same ideal may be placed in one-to-one correspondence with the automorphs of f.*

If f is a definite form, it has only a finite number of automorphs and we have the

COROLLARY. *If f is a definite form, if k is the number of automorphs of f and if $N(\geqq 0)$ is the number of ideals in $\mathfrak{C}$ of norm m, then the number of representations of m by f is exactly kN.*

3. **The number of ideals with given components.** If $p_1,\ p_2,\ \cdots,\ p_n$ are the distinct prime factors of an integer a prime to 2Δ, let

$$\Psi(a) \equiv a\prod_{i=1}^{n}\left[1-\left(\frac{\Delta}{p_i}\right)\frac{1}{p_i}\right],$$

where (Δ/p_i) is Legendre's symbol. Let $\Psi(1)\equiv 1$. If A, B are relatively prime, $\Psi(A)\cdot\Psi(B)=\Psi(AB)$. The following is an immediate consequence of a result due to Hermite.*

LEMMA 5. *If a is an integer prime to $2\alpha\Delta$, there are exactly $\Psi(a)$ numbers X, in G, no two of which are congruent modulo a, such that*

$$N(X) - \alpha \equiv 0 \pmod{a}. \tag{9}$$

By Lemma 2 of Tr., the first and second components of an ideal in $\mathfrak{G}$ are $a\mathfrak{b}$ and $\mathfrak{b}$, where a is a positive rational integer and $\mathfrak{b}$ is an ideal in G. Let a be a positive rational integer prime to $2\alpha\Delta$, and let $\mathfrak{b}$ be an ideal in G. We shall show that there are exactly $\Psi(a)$ ideals in $\mathfrak{G}$ whose components are $a\mathfrak{b}$ and $\mathfrak{b}$.

* *Oeuvres*, vol. 1, pp. 247–250.

Suppose $\mathfrak{L}$ is an ideal in $\mathfrak{G}$ with those components. If $\mathfrak{b}_1$ is equivalent to $\mathfrak{b}$, as in the proof of Lemma 2 of Tr., $\mathfrak{L}t = \mathfrak{L}_1 t_1$, where t, t_1 are in G and $\mathfrak{L}_1$ is a uniquely determined ideal in $\mathfrak{G}$ with the components $a\mathfrak{b}_1$ and $\mathfrak{b}_1$. Conversely, if $\mathfrak{L}_1$ is such an ideal, the equation $\mathfrak{L}t = \mathfrak{L}_1 t_1$ defines uniquely an ideal $\mathfrak{L}$ with the components $a\mathfrak{b}$ and $\mathfrak{b}$. Since every class of ideals in G contains an ideal prime to an arbitrarily chosen integer, in our proof of the above-mentioned result, we may assume without loss of generality that $\mathfrak{b}$ is prime to $2a\alpha\Delta$.

Let λ_1, λ_2 be a canonical basis of $\mathfrak{b}$. λ_1 is a divisor of $N(\mathfrak{b})$ and hence is prime to $2a\alpha\Delta$. After adding a proper multiple of λ_1 to λ_2, we may assume that λ_2 is also prime to $2a\alpha\Delta$.

Let $\mathfrak{L}$ be an ideal with the components $a\mathfrak{b}$ and $\mathfrak{b}$. By Lemma 1, Tr.,

$$\mathfrak{L} = [a\lambda_1, a\lambda_2, b_1 + E\lambda_1, b_2 + E\lambda_2],$$

where the b's are in $\mathfrak{b}$. If $B_i \equiv b_i \pmod{a\mathfrak{b}}$ $(i = 1, 2)$, each b_i above may be replaced by B_i. Consider the congruences

$$\lambda_i \bar{b}_i \equiv b_i \pmod{a\mathfrak{b}} \qquad (i = 1, 2).$$

Since λ_i is prime to a and $\mathfrak{b}$ divides λ_i and b_i, these congruences have solutions which are uniquely determined modulo a. Then we may replace each b_i in the above basis of $\mathfrak{L}$ by $\lambda_i \bar{b}_i$. Dropping the bars and setting $\Omega_i \equiv (b_i + E)\lambda_i$ $(i = 1, 2)$, we have

$$\mathfrak{L} = [a\lambda_1, a\lambda_2, \Omega_1, \Omega_2]. \tag{10}$$

It will be understood hereafter that the b_i are as in the definitions of the Ω's and not as in the first basis of $\mathfrak{L}$ given above.

Since each $E\Omega_i$ is in $\mathfrak{L}$ and

$$E\Omega_i = b_i' \Omega_i + [\alpha - N(b_i)]\lambda_i \qquad (i = 1, 2), \tag{11}$$

it follows that

$$N(b_i) - \alpha \equiv 0 \pmod{a} \qquad (i = 1, 2); \tag{12}$$

i.e., each b_i is a solution of (9).

Let G have the basis $(1, \theta)$. Each $\theta\lambda_i$, $\theta'\lambda_i$ is in $\mathfrak{b}$ and therefore

$$\begin{aligned} \theta\lambda_i &= u_{i1}\lambda_1 + u_{i2}\lambda_2, \\ \theta'\lambda_i &= v_{i1}\lambda_1 + v_{i2}\lambda_2, \end{aligned} \qquad (i = 1, 2), \tag{13}$$

where the u's and v's are rational integers. It may be shown that $u_{12} = -v_{12} = \pm N(\lambda_1)/N(\mathfrak{b})$, $u_{21} = -v_{21} = \pm N(\lambda_2)/N(\mathfrak{b})$, $(u_{11} - \theta)(u_{22} - \theta) = (v_{11} - \theta)(v_{22} - \theta) = u_{12}u_{21} = v_{12}v_{21}$. Then $v_{12}v_{21}$ is prime to a. Employing the expressions (13) for $\theta'\lambda_i$ we find

$$\begin{aligned} \theta\Omega_1 &= v_{11}\Omega_1 + v_{12}\Omega_2 + [(\theta - v_{11})\lambda_1 b_1 - v_{12}\lambda_2 b_2], \\ \theta\Omega_2 &= v_{21}\Omega_1 + v_{22}\Omega_2 + [(\theta - v_{22})\lambda_2 b_2 - v_{21}\lambda_1 b_1]. \end{aligned} \tag{14}$$

Since the Ω's are in $\mathfrak{L}$ and each of the expressions in brackets above is in G, it follows that

$$\begin{aligned} (\theta - v_{11})\lambda_1 b_1 - v_{12}\lambda_2 b_2 &\equiv 0, \\ v_{21}\lambda_1 b_1 - (\theta - v_{22})\lambda_2 b_2 &\equiv 0, \end{aligned} \pmod{a}. \tag{15}$$

Since $(\theta - v_{11})(\theta - v_{22}) - v_{12}v_{21} = 0$ and $v_{12}v_{21}$ is prime to a, it follows that the congruences (15) are equivalent. From (15_1) and (13) respectively we have

$$\begin{aligned} N(\theta - v_{11})N(\lambda_1)N(b_1) &\equiv v_{12}^2 N(\lambda_2)N(b_2) \pmod{a} \\ N(\theta - v_{11})N(\lambda_1) &= v_{12}^2 N(\lambda_2). \end{aligned}$$

Hence (15_1) implies $N(b_1) \equiv N(b_2) \pmod{a}$. It follows that (12_1) and (15_1) imply (12_2) and (15_2).

Conversely, et b_1 be a root of (9). Since $v_{12}\lambda_2$ is prime to a, b_2 is uniquely determined, modulo a, by (15_1) and b_1, b_2 satisfy each of the four congruences (12) and (15). Let $\Omega_i \equiv (b_i + E)\lambda_i$ $(i = 1, 2)$. Since a is prime to $\mathfrak{b}$, it follows from (11) and (14) that each $E\Omega_i$, $\theta\Omega_i$ is a linear function, with rational integral coefficients, of $a\lambda_1$, $a\lambda_2$, Ω_1, Ω_2. The same is obviously true of each $Ea\lambda_i$, $\theta a\lambda_i$. Hence there is an ideal $\mathfrak{L}$ with a basis as in (10) with $a\mathfrak{b}$ and $\mathfrak{b}$ as its components. Let b_1 be another root of (9). We may obtain in a similar manner an ideal $\mathfrak{L}_1$. It may be shown that $\mathfrak{L}_1 = \mathfrak{L}$ if and only if $b \equiv b_1 \pmod{a}$. We have then by Lemma 5

THEOREM 2. *If a is a positive integer, prime to $2\alpha\Delta$, and $\mathfrak{b}$ is an ideal in G, there are exactly $\Psi(a)$ ideals in $\mathfrak{G}$ whose first and second components are $a\mathfrak{b}$ and $\mathfrak{b}$ respectively.*

4. **The number of ideals with a given norm.** We shall prove

THEOREM 3. *If m is a positive integer, prime to $2\alpha\Delta$, there are exactly $\sigma(m)$ ideals in $\mathfrak{G}$ of norm m.*

Since the theorem is obviously true for $m = 1$, it will be sufficient to show that if it is true for $m = m_1$, then it is true for $m = m_1 P^t$, where P is a prime not a divisor of m_1.

By the proof of Lemma 3 of Tr., for every ideal $\mathfrak{L}$ in $\mathfrak{G}$, there is a ρ in $\mathfrak{G}$ of positive norm such that $\mathfrak{L}\rho = \mathfrak{L}_1$, where $\mathfrak{L}_1$ is a reduced ideal and $n(\mathfrak{L})N^2(\rho) = n(\mathfrak{L}_1)$. Furthermore, by p. 440 of Tr., $N(\mathfrak{L})N(\rho) = N(\mathfrak{L}_1)$, $\mathfrak{L}_1 = [a_1, b_1 + E]$ and $N(\mathfrak{L}_1) = a_1$. Since $\mathfrak{L}_1 = [a_1, a_1\theta, b_1 + E, \theta(b_1 + E)]$, by Lemma 1 of Tr., $n(\mathfrak{L}_1) = a_1^2$. By the same reference, $n(\mathfrak{L}) = a^2 N^2(\mathfrak{b})$, where $a\mathfrak{b}$ and $\mathfrak{b}$ are the components of $\mathfrak{L}$. Therefore $N(\mathfrak{L}) = aN(\mathfrak{b})$. Hence by Theo-

rem 2, the number $\phi(m)$, of ideals in $\mathfrak{G}$ of norm m is $\sum\Psi[m/N(\mathfrak{b})]$ where the summation extends over all the ideals $\mathfrak{b}$ in G whose norms divide m.

Suppose $\phi(m_1)=\sigma(m_1)$. Let a be a positive integer and $\mathfrak{b}$ an ideal in G such that $aN(\mathfrak{b})=m_1$. Let P be a rational prime not a divisor of $2\alpha\Delta m_1$, and let t be a positive integer.

Suppose $(\Delta/P)=1$. For every integer $u\geqq 0$, there are exactly $u+1$ ideals in G of norm P^u. Let $0\leqq u\leqq t$ and let $\mathfrak{p}$ be an ideal of norm P^u. By Theorem 2, there are exactly $\Psi(aP^{t-u})=\Psi(a)\cdot\Psi(P^{t-u})$ ideals in $\mathfrak{G}$ with the components $aP^{t-u}\mathfrak{b}\mathfrak{p}$ and $\mathfrak{b}\mathfrak{p}$ and each of these ideals is of norm m_1P^t. But $\mathfrak{p}$ may be chosen in $u+1$ ways. Hence there are exactly

$$\Psi(a)\sum_{u=0}^{t}(u+1)\Psi(P^{t-u}) = \Psi(a)\sigma(P^t)$$

ideals in $\mathfrak{G}$ of norm m_1P^t whose second components are $\mathfrak{b}\mathfrak{p}$, where $\mathfrak{p}$ is an ideal whose norm is a power ($\geqq 0$) of P. By Theorem 2, there are exactly $\Psi(a)$ ideals of norm m_1 whose second components are $\mathfrak{b}$. And by hypothesis $\phi(m_1)=\sigma(m_1)$. It follows that

$$\phi(m_1P^t) = \sigma(m_1)\sigma(P^t) = \sigma(m_1P^t).$$

Suppose $(\Delta/P)=-1$. Then $\{P\}$ is a prime in G. If $0\leqq v\leqq t/2$, by Theorem 2 there are exactly $\Psi(aP^{t-2v})=\Psi(a)\cdot\Psi(P^{t-2v})$ ideals in $\mathfrak{G}$ of norm m_1P^t whose second components are $\mathfrak{b}P^v$. Since

$$\Psi(a)\sum_{v=0}^{[t/2]}\Psi(P^{t-2v}) = \Psi(a)\sigma(P^t),$$

where $[t/2]$ is the greatest integer $\leqq t/2$, it follows as above that

$$\phi(m_1P^t) = \sigma(m_1)\sigma(P^t) = \sigma(m_1P^t)$$

and the theorem is proved.

4. **The representation of an integer by a system of forms.** By Theorem 3 of Tr., there is a one-to-one correspondence between the classes of ideals in $\mathfrak{G}$ and those classes of binary Hermitian forms over G, of determinant α, which represent positive integers. Let $f_1, f_2, \cdots, f_H$ be representatives of those H classes of such forms which represent integers prime to $2\alpha\Delta$.

It may be shown that no two of the forms $f_i'(x,y)\equiv f_i(x',y')$ $(i=1,2,\cdots,H)$ are equivalent. Since each f_i' represents the same integers represented by f_i, it follows that they also form a system of representative forms of the above H classes. Let $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_H$ be the classes of ideals in $\mathfrak{G}$ corresponding to the classes containing $f_1', f_2', \cdots, f_H'$ respectively. Let m be a positive integer prime to $2\alpha\Delta$. If $\mathfrak{P}$ is an ideal of norm m in the class $\mathcal{C}$, every form in the

corresponding class represents m. Hence $\mathcal{C}$ is one of the $\mathcal{C}_i$. Assume that the f_i are definite forms, i.e., $\alpha<0, \Delta<0$. By the corollary of Theorem 1, the number of representations of m by a given f_i is k_iN_i, where k_i is the number of automorphs of f_i and N_i is the number of ideals in $\mathcal{C}_i$ of norm m. By Theorem 3, $N_1+N_2+\cdots+N_H=\sigma(m)$. Hence, if every representation of m by f_i be counted as $1/k_i$, the total number of representations of m by $f_1, f_2, \cdots, f_H$ is exactly $\sigma(m)$.

Consider those representations $f_i(r, s)=m$ by a given f_i in which r, s are relatively prime. Such a representation is said to be proper. By Lemma 2 and (2), every such representation belongs to an ideal $\mathfrak{L}$ of norm m in $\mathcal{C}_i$ whose second component is the unit ideal. Then the first component of $\mathfrak{L}$ is $\{m\}$. Conversely, by the same reference, for every such ideal $\mathfrak{L}$ in $\mathcal{C}_i$ there is a proper representation of m by f_i which belongs to $\mathfrak{L}$. By Theorem 2, there are exactly $\Psi(m)$ such ideals $\mathfrak{L}$ in $\mathfrak{G}$. We have then

THEOREM 4. *Let $f_1, f_2, \cdots, f_H$ be representatives of the H classes of binary Hermitian forms over G which represent positive integers prime to $2\alpha\Delta$, and assume that $\alpha<0, \Delta<0$. Let k_i be the number of automorphs of f_i $(i=1, 2, \cdots, H)$ and let m be a positive integer prime to $2\alpha\Delta$. The total number of [proper] representations of m by $f_1, f_2, \cdots, f_H$ is exactly $\sigma(m)$ $[\Psi(m)]$ if a representation by f_i be counted as $1/k_i$.**

5. **An extension of a theorem of Humbert's.** Let f be one of the f_i in Theorem 4 and let $\mathfrak{p}$ be an ideal in G. If r and s, not both zero, are in $\mathfrak{p}$ then $f(r, s)=mN(\mathfrak{p})$ where m is a positive integer. Humbert wrote symbolically $m=f(r/\mathfrak{p}, s/\mathfrak{p})$ and called this a generalized representation of m belonging to $\mathfrak{p}$. If $\mathfrak{p}$ is the g.c.d. of r, s, this representation is said to be proper. He gave the following

THEOREM. (Humbert) *If Δ is even, if m is positive and prime to $2\alpha\Delta$, and if $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_h$ are representatives of the h classes of ideals in G, then the total number of generalized representations of m belonging to $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_h$ by $f_1, f_2, \cdots, f_H$ is exactly $h\sigma(m)$, where a representation by f_i is counted as $1/k_i$.*†

We shall obtain a stronger theorem. Let $\mathfrak{p}$ be an ideal in G and let m be a positive integer prime to $2\alpha\Delta$. Suppose $a\mathfrak{b}$ and $\mathfrak{b}$ are the components of an ideal in $\mathfrak{G}$ of norm m. By Theorem 2, there are exactly $\Psi(a)$ such ideals in $\mathfrak{G}$. But by the same reference, there are exactly $\Psi(a)$ ideals in $\mathfrak{G}$ whose com-

* For the case where Δ is even, Humbert obtained the above result on the proper representations of m. See Comptes Rendus, Paris, vol. 169 (1919), pp. 309–315.

† Comptes Rendus, Paris, vol. 169 (1919), p. 365. We state the theorem in our notation. Our Δ, α, $\mathfrak{p}_i$ are Humbert's $-4P$, Δ, and I_i respectively. Humbert does not state explicitly that Δ is even but this is implied by the former condition that $P\equiv 1$ or 2 (mod 4).

ponents are $a\mathfrak{b}\mathfrak{p}$ and $\mathfrak{b}\mathfrak{p}$, and the norm of every such ideal is $mN(\mathfrak{p})$. It follows from Theorem 3 that there are exactly $\sigma(m)$ ideals in $\mathfrak{G}$ of norm $mN(\mathfrak{p})$ whose second components are divisible by $\mathfrak{p}$. By Theorem 2, $\mathfrak{p}$ is the second component of exactly $\Psi(m)$ of these ideals.

Let f be one of the f_i of Theorem 4 and let $\mathcal{C}$ be the class of ideals in $\mathfrak{G}$ determined by f'. By Lemma 2 and (2), every representation $f(r, s)=mN(\mathfrak{p})$, where r, s are in $\mathfrak{p}$ belongs to an ideal $\mathfrak{L}$ in $\mathcal{C}$ of norm $mN(\mathfrak{p})$ whose second component is divisible by $\mathfrak{p}$. Then $f(r/\mathfrak{p}, s/\mathfrak{p})=m$ is a generalized representation of m belonging to $\mathfrak{p}$ and this representation is proper if the second component of $\mathfrak{L}$ is $\mathfrak{p}$. Conversely, by the same reference, for every such ideal $\mathfrak{L}$, there is a representation $f(r, s)=mN(\mathfrak{p})$ which belongs to $\mathfrak{L}$ and the generalized representation $f(r/\mathfrak{p}, s/\mathfrak{p})=m$ is proper only if $\mathfrak{p}$ is the second component of $\mathfrak{L}$. We have then

THEOREM 5. *Let m be a positive integer prime to $2\alpha\Delta$, let $\mathfrak{p}$ be an ideal in G, and let f_i, k_i be as in Theorem* 4. *The total number of generalized* [*proper*] *representations of m belonging to $\mathfrak{p}$ by $f_1, f_2, \cdots, f_H$ is exactly $\sigma(m)$* $[\Psi(m)]$, *it being understood that a representation by f_i is counted as $1/k_i$.*

It will be observed that for the case $\mathfrak{p}=\{1\}$, Theorem 5 becomes Theorem 4; also, that Theorem 5 includes Humbert's theorem quoted above.

6. **Applications.** Consider the case $\Delta=-4$, $\alpha=-1$. By p. 445 of Tr., $H=1$ and we may take $f_1=xx'+yy'$. f_1 has exactly eight automorphs corresponding to the eight units in $\mathfrak{G}$. Hence we have by Theorem 4, Jacobi's well known result that the number of representations of an odd positive integer m by $u^2+v^2+z^2+w^2$ is exactly $8\sigma(m)$. We also note that by Theorem 4, the number of representations with z^2+w^2 prime to m is $\Psi(m)$. Similarly, for the case $\Delta=-8$, $\alpha=-1$, we obtain Liouville's result that the number of representations of m by $u^2+v^2+2z^2+2w^2$ is $4\sigma(m)$.*

Consider the case $\Delta=-7$, $\alpha=-1$. By p. 445 of Tr., all the regular ideals in $\mathfrak{G}$ are principal and by Lemma 6 of Tr., all the ideals in $\mathfrak{G}$ are regular. Then $H=1$, $f_1=xx'+yy'$. There are exactly three ideals in $\mathfrak{G}$ of norm 2, namely, those defined by $1+E$, $\theta=(1+\Delta^{1/2})/2$ and θ'. More generally, it may be shown by induction that the number of ideals of norm 2^n is $2^{n+1}-1=\sigma(2^n)$. Furthermore, there is only one ideal of norm 7^n, namely, that defined by $(2\theta-1)^n$. Then, employing Theorem 3 of this paper and Theorem 4 of Tr., it may be shown that if $m=7^n m_1$, where m_1 is a positive integer prime to 7, the number of ideals of norm m is exactly $\sigma(m_1)$. Since $\mathfrak{G}$ contains exactly four units, it follows that the number of representations of m by f_1 is exactly $4\sigma(m_1)$. Noting that f_1 may be written $f_1=u^2+uz+2z^2+v^2$

* Journal de Mathématiques, (2), vol. 5 (1860), p. 270.

$+vw+2w^2$, we see that this result was obtained by Dickson.* If m is prime to $2\cdot 7$, by Theorem 4 there are exactly $4\Psi(m)$ representations with $v^2+vw+2w^2$ prime to m.

Consider the case $\Delta=-8$, $\alpha=-3$. Let m be a positive integer prime to 6. It may be shown that $H=k_1=k_2=2$ and that we may take $f_1=xx'+3yy'$, $f_2=2xx'+(1+\theta)x'y+(1-\theta)xy'+3yy'$, where $\theta^2=-2$. By Theorem 4, the total number of representations of m by f_1 and f_2 is exactly $2\sigma(m)$.

f_1 may be written $u^2+2v^2+3z^2+6w^2$. The problem of determining the number $T(m)$, of representations of m by f_1 has long been recognized as a very difficult problem. Liouville stated that $T(m)\leqq 2\sigma(m)$,† an immediate consequence of our result above. By the corollary of Theorem 1, the problem of determining $T(m)$ is equivalent to that of determining how many of the $\sigma(m)$ ideals of norm m are principal. This is the same sort of problem which arises in the determination of the integers represented by a binary quadratic form when there is more than one class in a genus.

By a result due to Griffiths,‡ $T(m)<2\sigma(m)$ if $m>1$. Since $f_2(\theta x, \theta y)=2f_2(x, y)$, $f_2[(1+\theta)x, (1+\theta)y]=3f_2(x, y)$, it follows that f_2 represents every integer >1.

---

* *Algebren und ihre Zahlentheorie*, p. 197.

† Journal de Mathématiques, (2), vol. 9 (1864), p. 305.

‡ American Journal of Mathematics, vol. 51 (1929), p. 66, Theorem 6.

UNIVERSITY OF KENTUCKY,
LEXINGTON, KY.