ON THE FACTORIZATION OF GENERALIZED QUATERNIONS

By Gordon Pall

1. A fundamental theorem in the arithmetic of Lipschitz[1] integral quaternions

$$v = v_0 + i_1 v_1 + i_2 v_2 + i_3 v_3 , \tag{1}$$

where the v_i are rational integers and the i_α are the familiar Hamilton units ($i_\alpha^2 = -1$, etc.), is that any proper v (i.e., one in which $v_0 , \cdots , v_3$ are coprime), whose norm $\sum v_i^2$ is divisible by an odd positive integer m, has exactly eight right-divisors t of norm m, these forming a class of left-associates

$$\pm t, \qquad \pm i_1 t, \qquad \pm i_2 t, \qquad \pm i_3 t. \tag{2}$$

In this article a connection is set up between the problems of factoring "generalized quaternions" (defined in §3) and of representing the number 1 in a certain quaternary quadratic form S. Hence the problem is reduced to that of equivalence of quaternary quadratic forms. However, the order and genus of S is readily identified. Hence in all cases where there is but one class in this quaternary genus, a theorem of the type quoted above will follow; and when several classes occur in that genus, some similar theorem may be deducible.

Our definition of generalized quaternion, based on Hermite's identity,[2] connects the theory with ternary and quaternary quadratic forms, rather than with binary Hermitian forms as in Dickson's definition. For results similar to ours in Dickson's generalized quaternions, perhaps the best reference is *Ideals in generalized quaternion algebras*, Trans. Amer. Math. Soc., vol. 38(1935), pp. 436–446, by C. G. Latimer.

2. Our method is based on a process of Hermite's,[3] who in turn was guided by Gauss's algorithm for reducing the representation of numbers in a binary quadratic form to the solution of a quadratic congruence and to identifying the class of a form constructed from the solution. We shall introduce the method by exhibiting a similar device for quadratic fields. We shall confine ourselves, however, to fields in which the integers are of the form

$$v = v_0 + v_1\omega, \qquad v_0 \text{ and } v_1 \text{ rational integers}, \tag{3}$$

where $\omega^2 = -D$ is a non-square rational integer. There is no difficulty in extending the theory to $\omega^2 + \omega + \frac{1}{4}(1 - \Delta) = 0$. Similarly, in this article we

Received May 18, 1938.

[1] R. Lipschitz, Jour. de Math., (4), vol. 2(1886), French translation by J. Molk.

[2] C. Hermite, Jour. für Math., vol. 47(1854), pp. 313–330; *Oeuvres*, vol. 1, 1905, pp. 200–220, especially p. 212.

[3] Hermite, Jour. für Math., vol. 47(1854), pp. 343–345; *Oeuvres*, vol. 1, pp. 234–237.

shall treat only the simpler case of quaternions associated with Hermite's identity.[4] The extension by means of Brandt's generalization[5] of Hermite's identity is being investigated by students of the writer.

Let p be an odd prime not dividing D. How many divisors of norm p does v possess? For this we must consider

$$v_0 + v_1\omega = (u_0 + u_1\omega)(t_0 + t_1\omega), \qquad t_0^2 + Dt_1^2 = p. \tag{4}$$

On taking norms we see that p must divide $Nv = v_0^2 + Dv_1^2$. Assuming this and multiplying both sides of (4) by $\bar{t} = t_0 - t_1\omega$, we get

$$(v_0 + v_1\omega)(t_0 - t_1\omega) \equiv 0 \pmod{p},$$

$$v_0t_0 + Dv_1t_1 \equiv 0, \qquad v_1t_0 - v_0t_1 \equiv 0, \pmod{p}. \tag{5}$$

Now assume that p does not divide both (and hence either) of v_0, v_1. Then the condition $p \mid Nv$ makes either of conditions (5) imply the other. Either of them reduces to $t_0 \equiv et_1 \pmod{p}$, where e is an integer $\equiv v_0/v_1 \pmod{p}$.

Thus if $p \mid Nv$, (5) will be satisfied if and only if

$$\begin{aligned} t_0 &= pX_0 + eX_1, \\ t_1 &= \qquad X_1, \end{aligned} \tag{6}$$

in integers X_0, X_1; and then $v\bar{t} \equiv 0 \pmod{p}$, $v\bar{t} = pu$, $v\bar{t}t = put$, $v = ut$, provided for the last step $Nt = \bar{t}t = t_0^2 + Dt_1^2 = p$. If we substitute from (6), the condition $Nt = p$ becomes

$$pX_0^2 + 2eX_0X_1 + fX_1^2 = 1, \tag{7}$$

where $f = (e^2 + D)/p$. The form $[p, 2e, f]$ is of determinant D, and will represent 1 if and only if the prime p happens to be represented in $x_0^2 + Dx_1^2$; and then the number of divisors t of norm p of v will be 2 if $D > 1$, and 4 if $D = 1$; if $D > 1$, the divisors are $\pm t$, if $D = 1$ they are $\pm t$ and $\pm it$. When there is only one class in each genus, the condition for p to be presented in $x_0^2 + Dx_1^2$ can be expressed simply in terms of Legendre symbols.

3. With a symmetric matrix $a = (a_{\alpha\beta})$ of order 3 in a field $\mathfrak{F}$, we associate a system of quaternions

$$t = t_0 + i_1t_1 + i_2t_2 + i_3t_3, \tag{8}$$

where the t_i range over $\mathfrak{F}$ and i_1, i_2, i_3 satisfy the following multiplication table, $A_{\alpha\beta}$ denoting the cofactor of $a_{\alpha\beta}$ in a:

$$i_\alpha^2 = -A_{\alpha\alpha} \qquad (\alpha = 1, 2, 3).$$

$$\begin{aligned} i_2i_3 &= -A_{23} + a_{11}i_1 + a_{12}i_2 + a_{13}i_3, \\ i_3i_2 &= -A_{32} - a_{11}i_1 - a_{12}i_2 - a_{13}i_3, \end{aligned} \tag{9}$$

[4] See footnote 2.

[5] H. Brandt, Math. Annalen, vol. 91(1924), pp. 308-309.

i_3i_1, etc., being obtained by permuting subscripts cyclically. Multiplication by scalars (in $\mathfrak{F}$) is defined in the obvious way, addition by adding corresponding coördinates. Addition is commutative and associative, and scalar factors can be taken in and out of products. Multiplication is distributive over addition. In general, $ut = v$ is given by the formulas (which are essentially those of Hermite):[6]

$$
\begin{aligned}
v_0 &= u_0t_0 - \sum_{\alpha,\beta=1}^{3} A_{\alpha\beta}u_\alpha t_\beta, \\
v_\alpha &= u_0t_\alpha + u_\alpha t_0 + \sum_{\beta=1}^{3} w_\beta a_{\beta\alpha} \qquad (\alpha = 1, 2, 3),
\end{aligned} \tag{10}
$$

$$w_1 = u_2t_3 - u_3t_2, \qquad w_2 = u_3t_1 - u_1t_3, \qquad w_3 = u_1t_2 - u_2t_1.$$

Seeing that multiplication is associative reduces to verifying

$$(i_\alpha i_\beta)i_\gamma = i_\alpha(i_\beta i_\gamma) \tag{11}$$

for all choices of subscripts 1, 2, 3. Forming the products by means of (9), we readily find

$$
\begin{aligned}
(i_\alpha i_\alpha)i_\beta &= i_\alpha(i_\alpha i_\beta) = -A_{\alpha\alpha}i_\beta, \\
i_\alpha(i_\beta i_\beta) &= (i_\alpha i_\beta)i_\beta = -A_{\beta\beta}i_\alpha, \\
(i_\alpha i_\beta)i_\alpha &= i_\alpha(i_\beta i_\alpha) = -2A_{\alpha\beta}i_\alpha + A_{\alpha\alpha}i_\beta, \\
(i_1i_2)i_3 &= i_1(i_2i_3) = -\Delta - A_{23}i_1 + A_{31}i_2 - A_{12}i_3, \\
(i_2i_1)i_3 &= i_2(i_1i_3) = \Delta + A_{32}i_1 - A_{13}i_2 - A_{21}i_3,
\end{aligned} \tag{12}
$$

$i_2i_3i_1$, etc., being obtained by cyclic permutation. Here $\Delta = |a_{\alpha\beta}|$.

We define conjugates by

$$\bar{t} = t_0 - i_1t_1 - i_2t_2 - i_3t_3, \tag{13}$$

so that by (9), $i_3i_2 = \overline{i_2i_3}$, and readily obtain

$$t\bar{t} = \bar{t}t = t_0^2 + \sum A_{\alpha\beta}t_\alpha t_\beta, \tag{14}$$

which we call the *norm of* t, or Nt. Since $\overline{i_\alpha i_\beta} = (-i_\beta)(-i_\alpha) = \bar{i}_\beta\bar{i}_\alpha$, and $\overline{t + u} = \bar{t} + \bar{u}$, we see that the conjugate of $(u_0 + \sum u_\alpha i_\alpha)(t_0 + \sum t_\beta i_\beta)$ is $(t_0 - \sum t_\beta i_\beta)(u_0 - \sum u_\alpha i_\alpha)$, that is,

$$\overline{ut} = \bar{t}\bar{u}. \tag{15}$$

Hence from $v = ut$ follows $\bar{v} = \bar{t}\bar{u}$, whence $v\bar{v} = ut\bar{t}\bar{u}$, or

$$Nv = Nu \cdot Nt. \tag{16}$$

This is Hermite's identity.

[6] See footnote 2.

4. In case the $a_{\alpha\beta}$ are rational integers we define an *integral quaternion* by (8) with rational integral t_i. By (9) the sum and product of integral quaternions are integral. If $v = ut$ in integral quaternions, we call t a *right-divisor* of v. Then by (16), $Nt \mid Nv$.

If t is a right-divisor of v, $\bar{t}$ is a left-divisor of $\bar{v}$. If $t_1 = t_2 = t_3 = 0$ so that t is a rational integer, t is a right-divisor of v if and only if $t \mid v_i$ $(i = 0, 1, 2, 3)$, and we can write $t \mid v$.

For a given v such that $p \nmid v$ but $p \mid Nv$, how many right-divisors of norm p does v possess? From

$$v = ut, \qquad Nt = p \tag{17}$$

follows $v\bar{t} = up$, $v\bar{t} \equiv 0 \pmod{p}$, or (cf. (10)) the system of homogeneous, linear congruences in t_0, t_1, t_2, t_3 with the matrix W obtained from

$$V \equiv \begin{bmatrix} 0 & \sum A_{1\alpha}v_\alpha & \sum A_{2\alpha}v_\alpha & \sum A_{3\alpha}v_\alpha \\ v_1 & a_{31}v_2 - a_{21}v_3 & a_{11}v_3 - a_{31}v_1 & a_{21}v_1 - a_{11}v_2 \\ v_2 & a_{32}v_2 - a_{22}v_3 & a_{12}v_3 - a_{32}v_1 & a_{22}v_1 - a_{12}v_2 \\ v_3 & a_{33}v_2 - a_{23}v_3 & a_{13}v_3 - a_{33}v_1 & a_{23}v_1 - a_{13}v_2 \end{bmatrix}$$

by adding v_0, $-v_0$, $-v_0$, $-v_0$ to the elements of the principal diagonal. In general if $p \mid Nv$, W is of rank 3, (mod p). If $p \mid v_0$, W becomes V and the crux of our method lies in

LEMMA 1. *If $p \mid v_0$, $p \mid Nv = \sum A_{\alpha\beta}v_\alpha v_\beta$, and $p \nmid \Delta v$, then two and at most two rows in V are linearly independent* (mod p).

To show that two rows are independent, it suffices since $p \nmid v$ to show that one of $\sum A_{\beta\alpha}v_\alpha$ is prime to p; if this were not so, p would divide

$$\sum_\beta a_{\beta\gamma} \sum_\alpha A_{\beta\alpha}v_\alpha = \Delta v_\gamma \qquad (\gamma = 1, 2, 3),$$

contrary to hypothesis. For the rest, it suffices to show that every three columns are linearly dependent. For the second, third, and fourth columns we use the multipliers v_1, v_2, and v_3, and adding obtain $(Nv, 0, 0, 0)$. For the second, third, and first columns we multiply by $\sum A_{2\alpha}v_\alpha$, $-\sum A_{1\alpha}v_\alpha$, and Δv_3, and on adding obtain $(0, a_{31}Nv, a_{32}Nv, a_{33}Nv)$. If these multipliers are all 0 (mod p), a glance at V shows that the second and third columns are proportional.

COROLLARY 1. *With the hypotheses of Lemma* 1, *if of the conditions*

$$\begin{aligned} &(\textstyle\sum A_{1\alpha}v_\alpha)t_1 + \cdots \equiv 0, \qquad v_1t_0 + (a_{31}v_2 - a_{21}v_3)t_1 + \cdots \equiv 0, \\ &v_2t_0 + (a_{32}v_2 - a_{22}v_3)t_1 + \cdots \equiv 0, \qquad v_3t_0 + \cdots \equiv 0, \pmod{p}, \end{aligned} \tag{18}$$

the first is satisfied together with the α-th one of the others, where $p \nmid v_\alpha$, then all four conditions are satisfied. Further, for all such t_i,

$$p \mid Nt = t_0^2 + \sum A_{\alpha\beta}t_\alpha t_\beta . \tag{19}$$

To secure (19) we need only observe that $p \mid v\bar{t}$, $p \mid v\bar{t}t$, $p \mid v(Nt)$, $p \mid Nt$.

Conversely, any solution t of (18) satisfying $Nt = p$ is a right-divisor of v. For, $v\bar{t} = pu$, $v\bar{t}t = put$, $v = ut$.

For definiteness we can suppose that $\sum A_{1\alpha}v_\alpha$ is prime to p, and solve (18) in the form

$$t_0 \equiv at_2 + bt_3\,, \qquad t_1 \equiv ct_2 + dt_3\,, \qquad (\mathrm{mod}\ p), \tag{20}$$

where a, b, c, d are certain integers. Then (18) is equivalent to

$$\begin{aligned} t_0 &= pX_0 + aX_2 + bX_3\,, \qquad t_2 = X_2\,, \\ t_1 &= pX_1 + cX_2 + dX_3\,, \qquad t_3 = X_3\,, \end{aligned} \tag{21}$$

in integers X_i. Substituting these expressions in $t_0^2 + \sum A_{\alpha\beta}t_\alpha t_\beta = p$, we get

$$\sum_{i,j=0}^{3} r_{ij}X_iX_j = p. \tag{22}$$

By (19), $p \mid \sum r_{ij}X_iX_j$ for all integers X_i, whence p divides every r_{ij}; set $r_{ij} = ps_{ij}$. Thus (22) reduces to the equation

$$\sum s_{ij}X_iX_j = 1. \tag{23}$$

The number of divisors equals the number of solutions of (23).

Let P denote the matrix of transformation (21), which has determinant p^2; let q, s denote the matrices of the forms $Q = t_0^2 + \sum A_{\alpha\beta}t_\alpha t_\beta$, $S = \sum s_{ij}X_iX_j$. That the determinants of q and s are equal follows from

$$ps = P'qP. \tag{24}$$

We shall see that the orders of Q and S coincide. Since the index is unaltered by the real transformation (21), this will follow if we show for $k = 1$, 2, and 3 that the g.c.d. of the principal minor determinants and the doubles of the non-principal minor determinants of order k is the same for q and s.[7] Let σ denote a subsequence of k elements of (1234); for any matrix R let $R[\sigma_1\sigma_2]$ denote the minor determinant whose rows have the positions indicated by σ_1, and the columns those of σ_2. Then by (24) and a simple determinantal theorem,

$$p^k s[\sigma_1\sigma_2] = \sum_{\sigma,\sigma'} q[\sigma\sigma']P[\sigma\sigma_1]P[\sigma'\sigma_2], \tag{25}$$

where the summation ranges over the $({}^4C_k)^2$ pairs σ, σ'. Since $p \nmid \Delta$, p cannot divide every $q[\sigma\sigma']$; if $\sigma_1 = \sigma_2$, the terms with $q[\sigma\sigma']$ and $q[\sigma'\sigma]$ are equal; hence the g.c.d. of the $q[\sigma\sigma]$ and $2q[\sigma\sigma']$ divides every $s[\sigma\sigma]$ and $2s[\sigma\sigma']$. The converse follows on solving (24) for q in terms of s.

In terms of the order invariants[8] recently introduced by the writer, let the divisor and o-invariants of the ternary form $f = \sum a_{\alpha\beta}x_\alpha x_\beta$ be d_1, o_1, and o_2. Since the $a_{\alpha\beta}$ are assumed integral, d_1 is even if o_1 is odd. The order invariants

[7] G. Pall, Quart. Jour. of Math., vol. 6(1935), pp. 30–51, Theorem 2.

[8] Same as footnote 7, Theorem 1.

of the primitive form Q, and therefore of S, are found to be $(o_1 d_1^2, o_2, o_1)$. Denote the primitive concomitants by $Q_1 = Q, Q_2, Q_3$. The genus of Q is characterized by the values of the principal characters $(Q_k \mid \omega_k)$ for the odd primes ω_k dividing $o_1 d_1^2$, o_2, o_1, respectively, and possibly certain supplementary characters $(-1|Q_k)$, $(2|Q_k)$, or $(-2|Q_k)$.[9] It is evident that if $(Q_3|\omega)$ is a character the same is true of $(Q_1|\omega)$. It is not difficult to verify also, by using a canonical form[10]

$$2^{\beta_1} m_1 x_1^2 + 2^{\beta_2} m_2 x_2^2 + 2^{\beta_3} m_3 x_3^2 \quad \text{or} \quad 2^{\beta_1} m_1 x_1^2 + 2^{\gamma}(m x_2^2 + m' x_2 x_3 + n x_3^2) \pmod{2^h}$$

for f, that if any of $(-1|Q_3)$, $(2|Q_3)$, or $(-2|Q_3)$ is a character, the same is true of Q_1. It should be observed that the simultaneous characters need not be considered here, since for forms in less than five variables their values are fixed by those of the others.[11] Further, since Q represents 1, the value of any character due to Q_1 is $+1$.

Finally, it is evident from the process by which S was derived (or from (25)) that if S_k represents n, then Q_k represents $p^k n$. Hence the characters due to S_2 and Q_2 are equal, while the values of those of S_1 (or S_3) are obtained from those of Q_1 (or Q_3) by multiplying by the quadratic character of p. The form S will therefore not represent 1 unless for each character $(Q_1|\omega)$, $(-1|Q_1)$, $(2|Q_1)$, and $(-2|Q_1)$ which may happen to be an invariant of Q, the value obtained on substituting p for Q_1 is $+1$. When this holds, we may say that *p is consistent with the genus of Q.*

Integral quaternions of norm 1 are called *units*. Their number, possibly infinite, is equal to the number ρ of solutions of

$$t_0^2 + \sum A_{\alpha\beta} t_\alpha t_\beta = 1. \tag{25'}$$

If θ denotes an arbitrary unit, the ρ quaternions θt are called *left-associates*. If t is a right-divisor of v, the left-associates θt form ρ right-divisors of the same norm. We have now proved the following theorem in the case $p \mid v_0$, and shall remove this restriction in §5:

THEOREM 1. *Let $(a_{\alpha\beta})$ be a symmetric matrix of order 3, the $a_{\alpha\beta}$ integers, $(A_{\alpha\beta})$ the adjoint. Set $Q = t_0^2 + \sum A_{\alpha\beta} t_\alpha t_\beta$. Let p be an odd prime not dividing $|a_{\alpha\beta}|$, v an integral quaternion of the type defined in §3 and the beginning of §4, $p \mid Nv$, $p \nmid v$. Then v has no right-divisors of norm p unless p is consistent with the genus of Q, and then the number of right-divisors is equal to the number of representations of 1 in a certain form of the same genus as Q. If this genus contains but one class, there are exactly ρ right-divisors of norm p, these forming a class of left-associates.*

COROLLARY. *The last sentence of the theorem holds with p replaced by m, where m is a product of primes each consistent with the genus of Q, and*

$$m \text{ is prime to } 2\Delta,\ m \mid Nv, \text{ and } m, v_0, v_1, v_2, v_3 \text{ are coprime.} \tag{26}$$

[9] H. J. S. Smith, *Coll. Math. Papers*, I, pp. 513–514.

[10] Same as footnote 7, Lemma 3.

[11] H. J. S. Smith, loc. cit., p. 515 (relation (A)).

We prove this by induction assuming the theorem as stated. Assume the corollary to be true for products m of h or fewer primes consistent with the genus of Q and dividing neither 2Δ nor v. Let p be such a prime.

Existence. From $v = ut$, $Nt = m$, $pm \mid Nv = NuNt$, follow $p \mid Nu$, $u = wx$, where $Nx = p$, $v = w(xt)$, $N(xt) = pm$.

Uniqueness. If $v = ux = wy$, $Nx = Ny = pm$, then $x = at$ and $y = bt'$, where $Nt = Nt' = m$, t and t' are left-associates since they are both right-divisors of v; by absorbing the unit factor on the left we can make $t = t'$; thus $ua = wb$, where a and b are both of norm p and hence are left-associates. Consequently, $x = at$ and $y = bt$ are left-associates.

There are no characters $(Q_1|\omega)$, $(-1|Q_1)$, $(2|Q_1)$, $(-2|Q_1)$ if and only if

$$\begin{aligned} &d_1 = 1,\ o_1 = 4 \text{ or } 8,\ 16 \nmid o_2; \text{ or} \\ &d_1 = 1,\ o_1 = 4,\ 16 \mid o_2,\ (-1|f_2) = -1; \text{ or} \\ &d_1 = 2,\ o_1 = 1, \end{aligned} \tag{27}$$

f_2 denoting the reciprocal of $f = \sum a_{\alpha\beta}x_\alpha x_\beta$. *In these cases then, if there is but one class in the genus of Q, there will be exactly ρ right-divisors of norm m, for any positive m satisfying* (26). An attempt to extend the theorem to such an m in any case seems to fail because of the difficulty of securing that some minor determinant of order 2 in V is prime to m.

We may note that if m were negative we would have -1 at the right of the equation corresponding to (23), since we would divide by $|m|$ to keep the index unaltered. It may be worth while observing also that the chain of leading principal minor determinants in the matrix of (23) is p, $A_{11}p^2$, $pa_{33}\Delta$, Δ^2; which are independent of v.

5. The problem is reduced to the case $p \mid v_0$ by two lemmas:

LEMMA 2. *If v and w are integral quaternions, and m an integer prime to Nw, then v and wv have the same right-divisors of norm m.*

For if $v = ut$, $wv = (wu)t$. Conversely, if $wv = ut$, and $Nt = m$ is prime to $Nw = k$, then $kv = (\bar{w}u)t$, $kv\bar{t} = \bar{w}um$,

$$v\bar{t} = \bar{w}u(m/k) = \text{integral quaternion}.$$

Hence the coördinates of $\bar{w}u$ are each divisible by k, $v = (\bar{w}u/k)t$.

LEMMA 3. *Let p be an odd prime not dividing Δ, nor all of v_1, v_2, v_3. Then we can find a pure quaternion w such that Nw is prime to p but the real part of wv is divisible by p.*

It is clear that the condition on v_1, v_2, v_3 is satisfied if $p \mid Nv$, $p \nmid v$. I am indebted to R. E. O'Connor for the following simple proof of this lemma. The problem is to find integers w_1, w_2, w_3 to satisfy

$$\begin{aligned} &(\sum A_{1\beta}v_\beta)w_1 + (\sum A_{2\beta}v_\beta)w_2 + (\sum A_{3\beta}v_\beta)w_3 \equiv 0, \\ &\sum A_{\alpha\beta}w_\alpha w_\beta \not\equiv 0, \qquad (\mathrm{mod}\ p). \end{aligned} \tag{28}$$

Using matrix notation, we can write these in the form

$$w'Av \equiv 0, \qquad w'Aw \not\equiv 0, \qquad (\text{mod } p), \tag{28'}$$

where A is a symmetric matrix of order 3 with integer elements, of determinant prime to p, v and w are vertical vectors and the prime denotes transposition. By a sequence of elementary transformations we can find a matrix C of integer elements, non-singular (mod p), such that $C'AC \equiv B$ (mod p), where B is a diagonal matrix, no diagonal element being zero (mod p). Then (28') becomes

$$x'Bu \equiv 0, \qquad x'Bx \not\equiv 0, \qquad (\text{mod } p), \tag{29}$$

where $u \equiv C^{-1}v$ and $x \equiv C^{-1}w$ (mod p). Hence we have only to solve

$$a_1u_1x_1 + a_2u_2x_2 + a_3u_3x_3 \equiv 0, \qquad a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \not\equiv 0, \qquad (\text{mod } p), \tag{30}$$

where the a_α are prime to p, and at least one u_α is prime to p since $p \nmid (v_1, v_2, v_3)$.

By symmetry we can suppose $p \nmid u_1$, and solve for x_1 from (30) in the form

$$x_1 \equiv dx_2 + ex_3 \qquad (\text{mod } p).$$

Substituting this in $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$, we get

$$(a_2 + a_1d^2)x_2^2 + 2dex_2x_3 + (a_3 + a_1e^2)x_3^2,$$

which has a coefficient prime to p, the first if $d \equiv 0$, the third if $e \equiv 0$, the second if $de \not\equiv 0$. This completes the proof of Theorem 1.

6. We shall give a few special cases, making use of Charve's table[12] of positive quaternary quadratic forms of determinant $\leqq 20$. Instances of our theory will undoubtedly be far more numerous among indefinite forms, where one class in the genus is the rule rather than the exception; and among forms in which some cross-product coefficients are odd, which may be attained by extending our results through Brandt's generalization of Hermite's identity.

Starting with the matrix $(a_{\alpha\beta})$ of the ternary quadratic form (2, 2, 2, 1, 1, 1) of determinant 4, we have $Q = t_0^2 + 3t_1^2 + 3t_2^2 + 3t_3^2 - 2t_2t_3 - 2t_3t_1 - 2t_1t_2$, and find for the adjoint,

$$4Q^{(3)} = 4(4x_0^2 + 2x_1^2 + 2x_2^2 + 2x_3^2 + 2x_2x_3 + 2x_3x_1 + 2x_1x_2).$$

Since $Q^{(3)}$ is improperly primitive, and there is only one such form of determinant 16 in Charve's table, it belongs to a genus (and order) of one class. The same is therefore true of Q. Since no generic characters are due to Q and $Q^{(3)}$ ($Q^{(2)}$ however represents only $(8n + 3)$'s), S is equivalent to Q. Since Q represents 1 for two values $t_0, \cdots, t_3$, quaternions v with the multiplication table

$$i_1^2 = i_2^2 = i_3^2 = -3, \qquad i_2i_3 = 1 + 2i_1 + i_2 + i_3 = \overline{i_3i_2}, \qquad \text{etc.}$$

[12] Charve, Comptes Rendus, vol. 96(1883), pp. 773–775.

have exactly two right-divisors (t and $-t$) of odd norm m, where m (>0) is assumed to divide Nv but to have no prime factor dividing all of v_0, v_1, v_2, v_3.

Similarly we find that ρ (the number of right-divisors) is 2, if m is prime to 2Δ, for the quaternions arising from $2x_1^2 - 2x_1x_2 + 2x_2^2 + x_3^2$ (having $\Delta = 3$), or from $2x_1^2 + 2x_2^2 + x_3^2$ (having $\Delta = 4$). But $\rho = 4$ if m is prime to 2λ (and the divisors are $\pm t$ and $\pm i_1 t$) in the cases of $\lambda x_1^2 + x_2^2 + x_3^2$ ($\lambda = 2$ or 3), for which the multiplication table is

$$\begin{aligned} i_1^2 = -1, \quad i_2^2 = i_3^2 = -\lambda, \quad i_1 i_2 = i_3 = -i_2 i_1, \\ i_3 i_1 = i_2 = -i_1 i_3, \quad i_2 i_3 = \lambda i_1 = -i_3 i_2. \end{aligned} \tag{31}$$

For ordinary quaternions ($\lambda = 1$), $\rho = 8$ as stated in the introduction.

If there is more than one class in the genus, as for $\lambda = 5$, when there are at least the two classes represented by

$$x_0^2 + x_1^2 + 5x_2^2 + 5x_3^2, \qquad 2x_0^2 - 2x_0x_1 + 3x_1^2 + 2x_2^2 - 2x_2x_3 + 3x_3^2,$$

we may replace the requirement $Nt = p$, in connection with (22), by $Nt = 2p$ (or hp) and deduce that $2v$ has right-divisors of norm $2p$ (or a like theorem).

We mention one type of application. The general solution of $hm^2 = \sum A_{\alpha\beta} v_\alpha v_\beta$ may be obtained by observing that the pure quaternion $v = i_1v_1 + i_2v_2 + i_3v_3$ has its left-divisors the conjugates of its right-divisors, whence $v = \bar{t}wt$, where w is pure and of norm h, and $Nt = m$. For a given h all solutions w of $Nw = h$ can be written down.

7. B. W. Jones and G. Pall[13] have used the results for $\lambda = 1, 2$, and 3 above in proving certain "automorphisms" among the representations of numbers $8n + 1$ or $24n + 1$ in $\lambda x_1^2 + x_2^2 + x_3^2$. E. Rosenthall and C. Solin employ these results in McGill University theses together with that for $f = 2x_1^2 - 2x_1x_2 + 2x_2^2 + x_3^2$ to obtain an arithmetical proof of Glaisher's[14] result for $4(4n + 1) = 2x_1^2 + x_2^2 + x_3^2$, and of new automorphisms for $24n + 1 = f$, $24n + 1 = 3x_1^2 + 3x_2^2 + x_3^2$, and $2(24n + 1) = 3x_1^2 + x_2^2 + x_3^2$.

McGill University.

[13] B. W. Jones and G. Pall, to appear in Acta Mathematica.

[14] J. W. L. Glaisher, Quart. Jour. Math., vol. 20(1884), p. 84.