ANNALS OF MATHEMATICS
Vol. 41, No. 4, October, 1940

ON THE RATIONAL AUTOMORPHS OF $x_1^2 + x_2^2 + x_3^2$

BY GORDON PALL

(Received July 5, 1939)

1. *Notations.* References followed by Q refer to an associated article.[1] We use the notations of §1Q. In addition to the sets $\mathfrak{Q}$, $\mathfrak{C}$, $\mathfrak{M}$ there defined, we employ German capitals for the following sets:

$\mathfrak{L}$: the 48 automorphs obtained from any one by shuffling rows;

$\mathfrak{A}$: all automorphs obtained from a given one by shuffling rows and shuffling columns;

$\mathfrak{C}$: the pure quaternion residues (mod m) obtained from a set $\mathfrak{M}$ by shuffling v_1, v_2, v_3;

$\mathfrak{K}$: all pure quaternions obtained from a pure one x by shuffling x_1, x_2, x_3.

Here *shuffling* denotes "permuting and changing signs of." In §3, letters which elsewhere represent integers denote real numbers.

We shall establish a one-to-one-to-one interconnection between the rational automorphs of $x_1^2 + x_2^2 + x_3^2$ and certain sets of solutions of (1_1Q) and (1_2Q). Numerous arithmetical properties of the automorphs and some additional properties of quaternions are obtained.

2. The rational automorphs of $x_1^2 + x_2^2 + x_3^2$ are the matrices

$$A = (a_{\alpha\beta}/m) \tag{1}$$

$$(\alpha, \beta = 1, 2, 3; \gcd(a_{11}, a_{12}, \cdots, a_{33}, m) = 1; m > 0)$$

such that, if A^* denotes the transpose matrix and I the identity,

$$A^*A = I = AA^*, \qquad A^* = A^{-1}. \tag{2}$$

Here $|A| = \theta = \pm 1$, and the relations (2) expand into the following:

$$\sum_\beta a_{\alpha\beta}^2 = \sum_\beta a_{\beta\alpha}^2 = m^2, \qquad \sum_\beta a_{\alpha\beta}a_{\gamma\beta} = 0 = \sum_\beta a_{\beta\alpha}a_{\beta\gamma} \quad \text{if } \alpha \neq \gamma, \tag{3}$$

$$\text{the cofactor of each element } a_{\alpha\beta} \text{ in } (a_{\alpha\beta}) \text{ is } \theta m a_{\alpha\beta}. \tag{4}$$

If m could be even (3_1) would imply that every $a_{\alpha\beta}$ is even. Similarly no prime factor $4f + 3$ of m can divide any $a_{\alpha\beta}$.

THEOREM 1. *The denominator m of any automorph* (1) *is odd. Each row and column of* $(a_{\alpha\beta})$ *satisfies*

$$x_1^2 + x_2^2 + x_3^2 = m^2, \tag{5}$$

[1] G. Pall, *On the Arithmetic of Quaternions*, Trans. Amer. Math. Soc., vol. 47 (1940), pp. 487–500. This article was originally intended to precede the present article in these Annals, but was transferred to the Transactions.

(6) *the g.c.d. of* x_1, x_2, x_3 *being* 1 *or a product of primes* $4f + 1$.

Trivially, two x_α *in* (5) *are even and one is odd. If* $m > 0$,

(7) *the even* x_α *in* (5) *are* $\equiv 0$ *if* $m \equiv 1$, $\equiv 2$ *if* $m \equiv 3 \pmod 4$.

In §8Q we proved a generalization of the fact that

(8) $x_1 = t_0^2 + t_1^2 - t_2^2 - t_3^2, \qquad x_2 = 2(-t_0t_3 + t_1t_2), \qquad x_3 = 2(t_0t_2 + t_1t_3)$

is the general solution of (5)–(6) with x_1 odd, t being a proper quaternion of norm m. For the purpose of proving (7), since any common factor of the x_α is $\equiv 1$ (4), it will suffice to show that every proper solution of (5) with x_1 odd is given by (8) for a proper t. Since $x = i_1x_1 + i_2x_2 + i_3x_3$ is proper and $Nx = m^2$, $x = vt$ with $Nt = m$ by Theorem 1Q, $Nv = m$, $v = \bar{t}a$ with $Na = 1$ since $\bar{x} = -x$ has t for a left divisor, whence $x = \bar{t}at$; x_1 being odd and $\bar{t}at \equiv (Nt)a \pmod 2$, $a = \pm i_1$; the case $a = -i_1$ reduces to $a = i_1$, since $\bar{t}(-i_1)t = \bar{u}i_1u$ if $t = i_2u$. Expanding $x = \bar{t}i_1t$ gives us (8). Finally, (7) follows on considering (8) with one or three of the t_i odd.

An automorph will be called *odd* if

(9) $|A| = 1$, and a_{11}, a_{22}, a_{33} are odd.

A class $\mathfrak{K}$ contains four odd automorphs obtainable from each other by changing signs of two rows.

3. The matrix function $\mathfrak{A}(t)$ of a *real* quaternion t, defined by

$$(10) \quad \mathfrak{A}(t) = \frac{1}{Nt}\begin{bmatrix} t_0^2 + t_1^2 - t_2^2 - t_3^2 & 2(-t_0t_3 + t_1t_2) & 2(t_0t_2 + t_1t_3) \\ 2(t_0t_3 + t_1t_2) & t_0^2 - t_1^2 + t_2^2 - t_3^2 & 2(-t_0t_1 + t_2t_3) \\ 2(-t_0t_2 + t_1t_3) & 2(t_0t_1 + t_2t_3) & t_0^2 - t_1^2 - t_2^2 + t_3^2 \end{bmatrix}$$

is considered in this section. By the homogeneity,

(11) $\mathfrak{A}(\lambda t) = \mathfrak{A}(t)$ for any real number $\lambda \neq 0$.

If a matrix $B = (b_{\alpha\beta})$ is of the form $\mathfrak{A}(t)$ for some real quaternion t, then t is unique up to a factor λ. For by choice of λ we can suppose Nt to have any value $m > 0$. Equating (10) to $(b_{\alpha\beta}) = (a_{\alpha\beta}/m)$ we get the ten equations

(12) $4t_0^2 = m + a_{11} + a_{22} + a_{33}, \qquad 4t_1^2 = m + a_{11} - a_{22} - a_{33}, \cdots,$

(13) $4t_0t_1 = a_{32} - a_{23}, \qquad 4t_2t_3 = a_{23} + a_{32}, \cdots,$

which determine $t_ft_g (f, g = 0, 1, 2, 3)$ and hence an unique $\pm t$.

If further m and the $b_{\alpha\beta}$ are rational, every t_f^2 and t_ft_g is rational; $t_f = u_fn^{\frac{1}{2}} (f = 0, 1, 2, 3)$ with rational u_f and n, $B = \mathfrak{A}(u)$. Choice of a factor λ makes u proper. Hence we have

Lemma 1. *If a matrix B with rational elements is of the form* $\mathfrak{A}(u)$ *for some real quaternion u, then there are two and only two proper integral quaternions, t and* $-t$, *such that* $\mathfrak{A}(t) = B$.

The matrix $\mathfrak{A}(t)$ has the multiplicative property

$$\mathfrak{A}(t)\cdot\mathfrak{A}(u) = \mathfrak{A}(tu). \tag{14}$$

This can be verified as follows. Let x denote either the

(15) pure quaternion $i_1x_1 + i_2x_2 + i_3x_3$, or matrix (x_α) of one column;

similarly for y. The columns of $Nt\mathfrak{A}(t)$ are $ti_\alpha\bar{t}$ ($\alpha = 1, 2, 3$). Hence $Nt\mathfrak{A}(t)x$ corresponds to $\sum x_\alpha ti_\alpha\bar{t} = t(\sum x_\alpha i_\alpha)\bar{t} = tx\bar{t}$, that is, if $A = \mathfrak{A}(t)$ the matrix equation

$$Ax = y \tag{16}$$

corresponds to the quaternion equation

$$tx\bar{t} = my, \text{ where } m = Nt. \tag{17}$$

Hence (14) follows when we observe that for arbitrary x and y,

$$t(ux\bar{u})\bar{t}/(NuNt) = y \textit{ is equivalent to } (tu)x(\overline{tu})/N(tu) = y,$$

$$\mathfrak{A}(t)\mathfrak{A}(u)x = y \textit{ is equivalent to } \mathfrak{A}(tu)x = y.$$

For any non-zero real quaternion t, $\mathfrak{A}(t)$ is a real automorph of $x_1^2 + x_2^2 + x_3^2$; for by taking norms in (17), $Nx = Ny$. Also $|\mathfrak{A}(t)|$ is $+1$, and not -1, for every t, since by continuous transformation of t we can reach $t = \pm 1$ when $\mathfrak{A}(t)$ is the identity matrix. It is worth noting the following identity in the x_α and t_i, the expressions in the matrix of (10) being substituted for the $a_{\alpha\beta}$:

$$(x_1^2 + x_2^2 + x_3^2)(t_0^2 + t_1^2 + t_2^2 + t_3^2)^2 = \sum_\alpha (a_{\alpha 1}x_1 + a_{\alpha 2}x_2 + a_{\alpha 3}x_3)^2.$$

We now prove conversely that every real automorph of $x_1^2 + x_2^2 + x_3^2$, with determinant $+1$, is of the form $\mathfrak{A}(t)$ for real t; and it will follow from lemma 1 that every rational automorph is of that form for proper t.

It suffices to prove that if $m > 0$ and (3)–(4) hold with $\theta = 1$, the ten equations (12)–(13) are solvable in real t_i. By (3_1) and (4),

$$a_{32}^2 - a_{23}^2 = a_{13}^2 - a_{31}^2 = a_{21}^2 - a_{12}^2 \ (= \varepsilon, \text{ say}), \tag{18}$$

(19) $\quad ma_{12} = a_{23}a_{31} - a_{21}a_{33}, \qquad ma_{21} = a_{13}a_{32} - a_{12}a_{33}$, etc. cyclically.

Thus $a_{12} = \pm a_{21}$ implies $a_{23}a_{31} = \pm a_{13}a_{32}$ with the same sign; and similarly on permuting subscripts cyclically. Hence, if $\varepsilon = 0$:

a) we can set $a_{23} = \eta_1 a_{32}$ etc., each $\eta_\alpha = \pm 1$, $\eta_1\eta_2\eta_3 = 1$;

b) if a_{23}, a_{31}, or a_{12} vanishes, at least two of them vanish.

CASE I, $\varepsilon = 0$, at least two of a_{23}, a_{31}, a_{12} zero; say a_{31} and a_{12}. Then $a_{23} = \pm a_{32}$. For the $+$ sign, (3) and $|A| > 0$ imply $a_{33} = -a_{22}$, $a_{11} = -m$; take $t_0 = t_1 = 0$, $2t_2t_3 = a_{23}$, $t_2^2 + t_3^2 = m$; then $a_{22}^2 = m^2 - a_{23}^2 = (t_2^2 - t_3^2)^2$, and by permuting t_2, t_3, $a_{22} = t_2^2 - t_3^2$. The rest of (12)–(13) follows. If $a_{23} = -a_{32}$, $t_2 = t_3 = 0$ yields a similar result.

CASE II, $\varepsilon = 0$, no $a_{\alpha\beta} = 0 (\alpha \neq \beta)$. According to the cases 0) $\eta_1 = \eta_2 = \eta_3 = 1$, 1) $\eta_2 = \eta_3 = -1$, 2) $\eta_3 = \eta_1 = -1$, 3) $\eta_1 = \eta_2 = -1$, we take t_0, t_1, t_2, or t_3 to be zero. Three of equations (13) become trivial, the rest determine an unique $\pm t$, and imply respectively: 0) $2t_1^2 = a_{31}a_{12}/a_{23}, \cdots$; 1) $2t_0^2 = a_{21}a_{13}/a_{23}$, $2t_2^2 = a_{13}a_{23}/a_{21}$, $2t_3^2 = a_{21}a_{23}/a_{13}$; and similarly in cases 2) and 3). Equations (12) now follow. For example in case 0), by (4) and (3_2), $a_{12}(m + \sum a_{\alpha\alpha}) = a_{12}a_{11} + a_{12}a_{22} + a_{12}(m + a_{33}) = a_{12}a_{11} + a_{22}a_{21} + a_{31}a_{32} = 0 = 4t_0^2 a_{12}$, $a_{23}(m + a_{11} - a_{22} - a_{33}) = a_{21}a_{31} - a_{22}a_{32} - a_{23}a_{33} = 2a_{21}a_{31} = 4t_1^2 a_{23}$, etc. In case 1), $a_{23} = a_{32}$, $a_{31} = -a_{13}$, and $a_{12} = -a_{21}$, whence for example, $a_{23}(m + \sum a_{\alpha\alpha}) = a_{12}a_{31} + a_{23}a_{22} + a_{23}a_{33} = -a_{21}a_{31} + a_{22}a_{32} + a_{23}a_{33} = -2a_{21}a_{31} = 4t_0^2 a_{23}$.

CASE III, $\varepsilon \neq 0$. Then all of (13) are implied by the conditions $16t_0t_1t_2t_3 = \varepsilon$, $4t_2t_3 = a_{23} + a_{32}$, $4t_3t_1 = a_{31} + a_{13}$, $4t_1t_2 = a_{12} + a_{21}$, which determine $\pm t$ uniquely. Also (12) follow. For example by (19),

$$(a_{12} + a_{21})(m + a_{11} + a_{22} + a_{33}) = a_{13}a_{32} + a_{31}a_{23} + a_{21}a_{11} + a_{12}a_{22} + a_{21}a_{22} + a_{12}a_{11}$$
$$= (a_{32} - a_{23})(a_{13} - a_{31}) = 4t_0^2(a_{21} + a_{12}) \text{ by (13).}$$

4. THEOREM 2. *A rational automorph $A = (a_{\alpha\beta}/m)$ of denominator m and determinant $+1$ is of the form $\mathfrak{A}(t)$ for an unique pair of proper quaternions $\pm t$; Nt is m, $2m$, or $4m$ according as A contains three, one, or no odd $a_{\alpha\alpha}$.*

The first part follows from §3. If in (10) the denominator reduces to m, $Nt = hm$ for some integer h dividing all nine elements of the matrix $Nt\mathfrak{A}(t)$. Since t is proper and obvious combinations of the diagonal elements with Nt produce $4t_f^2 (f = 0, 1, 2, 3)$, $h = 1, 2$, or 4. Conversely if t is proper and Nt is m, $2m$, or $4m$ (m odd), the denominator to which $\mathfrak{A}(t)$ reduces is indeed m; for any prime dividing m and the three diagonal terms divides each t_i. The possible parities of the t_i in each case show that three $a_{\alpha\alpha}$ are odd if $Nt = m$, one is odd if $Nt = 2m$, and all even if $Nt = 4m$, every t_i odd.

THEOREM 3. *Let u be proper, m odd. If $Nu = 2m$, $\mathfrak{A}(u)$ can be derived from an odd A by interchanging two rows and changing the signs of one row. If $Nu = 4m$, $\mathfrak{A}(u)$ is obtainable from an odd A by permuting the rows cyclically.*

For if $2 \mid Nu$, the u_i are congruent (mod 2) in pairs. Hence $u = (1 + i_\alpha)t$ with t integral, $\alpha = 1, 2$, or 3; $Nt = \frac{1}{2}Nu$, $\mathfrak{A}(u) = \mathfrak{A}(1 + i_\alpha)\mathfrak{A}(t)$; and

$$\mathfrak{A}(1 + i_1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}.$$

The case $Nu = 4m$ is solved by two applications of this process, and

LEMMA 2. *The three automorphs obtained from $\mathfrak{A}(t)$ by changing the signs of two of its rows are $\mathfrak{A}(i_1t)$, $\mathfrak{A}(i_2t)$, $\mathfrak{A}(i_3t)$.*

The four odd automorphs of a class $\mathfrak{K}$ (end §2) are, in view of Theorem 2 and lemma 2, associated with an unique set $\mathfrak{Q}$ (§1Q).

We denote the set of quaternions conjugate to those of $\mathfrak{E}$ by $\mathfrak{E}^*$; the set of automorphs transpose to those of $\mathfrak{A}$ by $\mathfrak{A}^*$. Thus $\mathfrak{E}^* = \mathfrak{E}$ if and only if

(20) *an equality occurs among* $t_0^2, t_1^2, t_2^2, t_3^2, 0$.

THEOREM 4. *As t ranges over a set $\mathfrak{E}$ (or $\mathfrak{Q}$) of odd norm m, $\mathfrak{A}(t)$ ranges twice, as $\mathfrak{A}(t) = \mathfrak{A}(-t)$, over the odd automorphs of a set $\mathfrak{A}$(or $\mathfrak{L}$) of denominator m. If $\mathfrak{A}$ corresponds in this way to $\mathfrak{E}$, $\mathfrak{A}^*$ corresponds to $\mathfrak{E}^*$.*

The proof for $\mathfrak{Q}$ and $\mathfrak{L}$ was given above. We can restrict t to one value in every subset $\mathfrak{Q}$ of $\mathfrak{E}$, say that given in lemma 13Q. By forming the automorphs $\mathfrak{A}(\eta)$, for η in (15Q), we find that $\mathfrak{A}(\eta t\bar{\eta}) = \mathfrak{A}(\eta)\mathfrak{A}(t)\mathfrak{A}(\bar{\eta})$ is obtained by the following respective operations:

$$\text{(21)}\qquad \begin{aligned} &\text{identity},\ \sigma_\alpha,\ \sigma_{\alpha+1}\pi_{\alpha+1,\alpha+2},\ \sigma_{\alpha+2}\pi_{\alpha+1,\alpha+2},\ \pi_{\alpha+1,\alpha+2},\ \sigma_\alpha\pi_{\alpha+1,\alpha+2},\\ &\pi_{123},\ \pi_{123}\sigma_\alpha,\ \pi_{321},\ \pi_{321}\sigma_\alpha;\quad (\alpha = 1, 2, 3).\end{aligned}$$

Here the subscripts are to be reduced (mod 3) to 1, 2, 3; σ_α denotes the operation of changing the sign of the α-th row, then of the α-th column; $\pi_{\alpha\beta}$ indicates the interchange of the α-th and β-th rows, then of the α-th and β-th columns; π_{123} represents a cyclic permutation of rows, and then columns.

If an *odd* A' is derived by shuffling (§1) rows, and columns, from an odd A, any rearrangement of rows must be accompanied by the same rearrangement of columns, and since $|A| > 0$, the number of sign-changes must be even. All such possibilities, except for sign-changes of two rows, which are provided for in the $\mathfrak{L}$-classes, are expressed in (21). Theorem 4 follows, the last part being obvious from (10): $\mathfrak{A}(\bar{t}) = \mathfrak{A}^*(t)$.

It may be observed from the last part of §3 that some t_i vanishes if and only if $\varepsilon = 0$, and that then A becomes symmetric on changing signs of certain rows. From (10) we see that if $t_1 = t_2$, then $a_{11} = a_{22}$, $a_{31} = a_{23}$, $a_{13} = a_{32}$, and A becomes symmetric on interchanging the last two rows; and similarly if any equality occurs among $t_0^2, t_1^2, t_2^2, t_3^2, 0$. Conversely, by (10), if $a_{11} = a_{22}$, then $t_1^2 = t_2^2$; if $a_{12} = a_{31}$, then $t_0 = -t_1$ or $t_2 = t_3$; the possibility $a_{11} = \pm a_{23}$ implies $(t_0 \pm t_1)^2 = (t_2 \pm t_3)^2$ and is excluded by residues (mod 2) if Nt is odd. Thus we have two theorems:

THEOREM 5. *If some two elements not in the same row or column of A are numerically equal, then the class $\mathfrak{L}$ of A contains a symmetric automorph.*

THEOREM 6. *A class $\mathfrak{A}$ contains a symmetric automorph if and only if two of $t_0^2, t_1^2, t_2^2, t_3^2, 0$ are equal in the corresponding proper $\mathfrak{E}$.*

5. In view of the equivalence of (16) and (17), the identities

$$t(t - t_0)\bar{t} = (t - t_0)Nt, \qquad t(i_\alpha t + t_\alpha)\bar{t} = (ti_\alpha + t_\alpha)Nt,$$

give us the lemma and corollary:

LEMMA 3. *On multiplying by $\mathfrak{A}(t)$ on the left, the column vector (t_1, t_2, t_3) becomes (t_1, t_2, t_3), $(t_0, -t_3, t_2)$ becomes $(t_0, t_3, -t_2)$, $(t_3, t_0, -t_1)$ becomes $(-t_3, t_0, t_1)$, $(-t_2, t_1, t_0)$ becomes $(t_2, -t_1, t_0)$.*

COROLLARY 1. *If $\mathfrak{A}(t) = (a_{\alpha\beta}/Nt)$ in (10), then*

$$\sum_\beta a_{\alpha\beta} y_\beta \equiv 0 (\text{mod } Nt)\ (\alpha = 1, 2, 3) \text{ for each of } (y_1, y_2, y_3) \tag{22}$$
$$= (t_1, t_2, t_3), (t_0, -t_3, t_2), (t_3, t_0, -t_1), (-t_2, t_1, t_0).$$

In fact (22) gives the identities in the proof of Theorem 5′Q. Hence

COROLLARY 2. *If $p^r \mid Nt$ and $p \nmid t_0^2 + t_\alpha^2$, the four congruences*

$$\begin{aligned} u_0t_0 - u_1t_1 - u_2t_2 - u_3t_3 &\equiv 0, & u_0t_1 + u_1t_0 + u_2t_3 - u_3t_2 &\equiv 0, \\ u_0t_2 - u_1t_3 + u_2t_0 + u_3t_1 &\equiv 0, & u_0t_3 + u_1t_2 - u_2t_1 + u_3t_0 &\equiv 0, \end{aligned} \tag{23}$$

obtained on expanding $ut \equiv 0$ (mod p^r), can be expressed as linear combinations of (23_1) *and* $(23_{\alpha+1})$.

6. THEOREM 7. *For any automorph* (1) *we can choose pure quaternions u and v such that*

$$a_{\alpha\beta} \equiv u_\alpha v_\beta\ (\text{mod } m), \qquad \alpha, \beta = 1, 2, 3. \tag{24}$$

Here u and v must satisfy

$$Nu \equiv Nv \equiv 0, \ u \text{ and } v \text{ proper } (\text{mod } m). \tag{25}$$

Also, u and v are uniquely determined (mod m) *except that we can replace* (u, v) *by* (eu, fv), *where e, f are any integers such that* $ef \equiv 1$ (mod m).

By the Chinese Remainder Theorem it suffices to determine u and v (mod p^r), for each p^r dividing m. Some $a_{\alpha\beta}$ is prime to p,[2] say a_{11}. Then let $u_1 = 1$, $v_\beta \equiv a_{1\beta}$, and determine u_2 and u_3 from $a_{21} \equiv u_2a_{11}$, $a_{31} \equiv u_3a_{11}$; (24) holds for every α and β, since by (4) every minor determinant of order 2 in $(a_{\alpha\beta})$ is divisible by p^r.

Since $m, a_{11}, a_{12}, \cdots, a_{33}$ are coprime, u and v must be proper; this with (3_1) implies that $m \mid Nu$ and Nv.

If $u_\alpha v_\beta \equiv u'_\alpha v'_\beta$ (mod m), $(\alpha, \beta = 1, 2, 3)$, we can find integers r_α, s_β such that $\sum r_\alpha u_\alpha \equiv 1 \equiv \sum s_\beta v_\beta$ (mod m). Set $e = \sum s_\beta v'_\beta$, $f = \sum r_\alpha u'_\alpha$. Then $u_\alpha \equiv \sum u_\alpha v_\beta s_\beta \equiv \sum u'_\alpha v'_\beta s_\beta \equiv eu'_\alpha$, $v_\beta \equiv fv'_\beta$, and $ef \equiv \sum s_\beta v'_\beta \sum r_\alpha u'_\alpha \equiv \sum \sum r_\alpha s_\beta u'_\alpha v'_\beta \equiv \sum\sum r_\alpha s_\beta u_\alpha v_\beta \equiv 1$ (mod m).

If $B = (b_{\alpha\beta}/n)$ is an automorph of denominator n, and $m \mid n$, we write

$$B \sim v\ (\text{mod } m) \tag{26}$$

to indicate that the three rows of $(b_{\alpha\beta})$ belong to the set $\mathfrak{M}$ (mod m) determined by v. By (24), $A \sim v$ and $A^* \sim u$ (mod m). Since u is proper (mod m) the set $\mathfrak{M}$ (mod m) containing all three rows of mA is evidently unique.

[2] Examples with no $a_{\alpha\beta}$ prime to m may appear when m has three prime factors $4f + 1$. If $m = 5 \cdot 13 \cdot 17$, $v = 775i_1 + 51i_2 + 533i_3$ is effective for $\mathfrak{A}(t)$, $t = 28 + 11i_1 + 10i_2 + 10i_3$; likewise for $t = 24 + 22i_1 + 6i_2 + 3i_3$, every $a_{\alpha\beta}$ is divisible by 5, 13, or 17.

LEMMA 4. *If v is pure and proper* (mod m), *and $m \mid Nv$, we can secure*

$$m^2 \mid Nv \tag{27}$$

by adding multiples of m to v_1 and v_2.

Set $Nv = sm$, $w = hi_1 + ki_2$. Then $N(v + mw) = m(s + 2hv_1 + 2kv_2) + (h^2 + k^2)m^2$, and we can choose h and k to make $m \mid s + 2hv_1 + 2kv_2$, since v_1, v_2, m are coprime.

LEMMA 5. *If* (24) *holds for the automorph* (1), *and $m^2 \mid Nv$, the integers $h_{\alpha\beta}$ defined by $a_{\alpha\beta} = u_\alpha v_\beta + mh_{\alpha\beta}$ satisfy*

$$\sum h_{\alpha\beta} v_\beta \equiv 0 \ (\text{mod } m), \ \alpha = 1, 2, 3. \tag{28}$$

For on substituting $a_{\alpha\beta} = u_\alpha v_\beta + mh_{\alpha\beta}$ in (3) and using (27) we get

$$m \mid u_\alpha \sum h_{\alpha\beta} v_\beta, \qquad m \mid u_\gamma \sum h_{\alpha\beta} v_\beta + u_\alpha \sum h_{\gamma\beta} v_\beta. \tag{29}$$

Multiply the latter by u_γ. Since m, u_α, u_γ^2 are coprime, (28) follows.

COROLLARY 3. *With the same hypotheses, $m^2 \mid \sum a_{\alpha\beta} v_\beta$.*

LEMMA 6. *If v is pure and proper, and Nv is odd,*

$$\mathfrak{A}(v) \sim v \ (\text{mod } Nv). \tag{30}$$

For $\mathfrak{A}(v)$ is then of denominator Nv; (30) follows from (10) with t replaced by v, $v_0 = 0$: $a_{\alpha\beta} \equiv 2v_\alpha v_\beta$ (mod m).

We note here the similar fact that for proper t of odd norm,

$$\text{if } t_0 = t_1, \quad \mathfrak{A}(t) \sim 2t_1 i_1 + (t_2 - t_3)i_2 + (t_2 + t_3)i_3 \ (\text{mod } Nt); \tag{30'}$$

two like results being obtained by permuting subscripts 1, 2, 3 cyclically.

COROLLARY 4. *The preceding remarks furnish quickly a value of v for any symmetric automorph.*

LEMMA 7. *If x is proper and Nx odd, and $x = ut$, $Nt = m$, then the rows of $Nx\mathfrak{A}(x)$ are in the set $\mathfrak{M}$* (mod m) *containing the rows of $m\mathfrak{A}(t)$.*

For by (14), $Nx\mathfrak{A}(x) = Nu\mathfrak{A}(u) \cdot Nt\mathfrak{A}(t)$, whence the rows of $Nx\mathfrak{A}(x)$ are linear combinations with integer coefficients of the rows of $m\mathfrak{A}(t)$.

THEOREM 8. *Let v be pure and proper* (mod m), $m \mid Nv$, *t proper, $Nt = m$; then*

$$\mathfrak{A}(t) \sim v \ (\text{mod } m) \text{ if and only if } t \text{ is a right divisor of } v. \tag{31}$$

By adding multiples of m to the v_α we make v actually proper and of odd norm; then (30) holds. I. Let $v = ut$. By lemma 7, if $\mathfrak{A}(t) \sim z(m)$, $\mathfrak{A}(v) \sim z(m)$. By (30), v and z are proportional (mod m), $\mathfrak{A}(t) \sim v(m)$. II. Conversely, let $\mathfrak{A}(t) \sim v(m)$. By lemmas 4 and 1Q we can make $m^2 \mid Nv$. Set $\mathfrak{A}(t) = (a_{\alpha\beta}/m)$, $a_{\alpha\beta} = u_\alpha v_\beta + mh_{\alpha\beta}$ as in lemma 5. Let $v = uy$, $Ny = m$. We must show that t and y are left-associates. By case I, $\mathfrak{A}(y) \sim v(m)$. Set $\mathfrak{A}(y) = (b_{\alpha\beta}/m)$, $b_{\alpha\beta} = w_\alpha v_\beta + mk_{\alpha\beta}$ as in lemma 5. Then $\mathfrak{A}(t\bar{y}) = \mathfrak{A}(t)\mathfrak{A}(y)^* = (c_{\alpha\gamma}/m^2)$, where

$$c_{\alpha\gamma} = \sum a_{\alpha\beta} b_{\gamma\beta} = u_\alpha w_\gamma \sum v_\beta^2 + mu_\alpha \sum k_{\gamma\beta} v_\beta + mw_\gamma \sum h_{\alpha\beta} v_\beta + m^2 \sum h_{\alpha\beta} k_{\gamma\beta},$$

is divisible by m^2. Hence $\mathfrak{A}(t\bar{y})$ has denominator 1, $t\bar{y} = m\eta$ with $N\eta = 1$, $t = \eta y$.

In (24) if A is odd, and corresponds to t, the vectors u and v are, respectively pure right and left multiples of t. By Theorem 3Q all left multiples (and similarly all right multiples) are proportional (mod m). By Theorem 9Q, u and v belong to the same set $\mathfrak{C}$ if and only if (20) holds.

If $A \sim v(m)$, and v' is obtained by shuffling v_1, v_2, v_3, and A' is obtained by the same shuffle of the columns of A, then $A' \sim v'$ (m). Theorems 4, 7, 8, and 4Q imply

THEOREM 9. *Every set* $\mathfrak{M}$ (mod m) *contains all three rows* $(\times m)$ *of the automorphs in one and only one class* $\mathfrak{K}$ *of denominator* m, *and conversely; likewise for* $\mathfrak{C}$ *and* $\mathfrak{A}$.

We have thus, *for any odd positive* m, *a one-to-one-to-one association between sets* $\mathfrak{K}$, $\mathfrak{M}$, $\mathfrak{O}$; *and* $\mathfrak{A}$, $\mathfrak{E}$, $\mathfrak{C}$.

7. THEOREM 10. *Let* x *be proper and of odd norm* m'', $m \mid m''$, $A'' = \mathfrak{A}(x)$. *The rows and columns of* $m''A''$ *are in the same set* $\mathfrak{C}$ (mod m) *if and only if*

(32) $\qquad$ *m divides one of* x_f, $x_f \pm x_g (f \neq g)$, $x_0 \pm x_1 \pm x_2 \pm x_3$.

For set $x = at$, $\bar{x} = bt'$, $Nt = m = Nt'$. By Theorem 8Q, (32) holds if and only if t and t' are in the same set $\mathfrak{E}$. The columns of $\mathfrak{A}(x)$ being the rows of $\mathfrak{A}(\bar{x})$, the theorem follows from lemma 7.

COROLLARY 5. *If* mA *is symmetrical* (mod m), *the class* $\mathfrak{K}$ *of* A *contains a symmetrical automorph.*

For the sets $\mathfrak{M}$ containing the rows and columns of mA coincide.

8. *Factorization of Automorphs.* We call A a *right divisor of* A'' if

(33) $\qquad A'' = A'A$, and $m'' = m'm$ holds for the denominators.

Then every automorph in the set $\mathfrak{K}$ of A is a right divisor of every automorph in the set $\mathfrak{K}$ of A''.

LEMMA 8. *If* A *is a right divisor of* A'', *and* t *and* t'' *are in the corresponding sets* $\mathfrak{O}$ *and* $\mathfrak{O}''$, *then* t *is a right divisor of* t''.

For we can suppose A and A'' replaced by odd automorphs in their sets $\mathfrak{K}$, and have (33) with $A = \mathfrak{A}(t)$, $A'' = \mathfrak{A}(t'')$. A product of odd automorphs being obviously odd, we have $A' = A''A^* = \mathfrak{A}(t''\bar{t})$ of denominator m', whence $t''\bar{t} = \lambda t'$, $Nt' = m'$. By the norms $\lambda = \pm m$. Hence $t'' = \pm t't$.

LEMMA 9. *If* z *is proper* (mod m), *and* t *is a right divisor of* z *of norm* m, *then* $\mathfrak{A}(t)$ *is a right divisor of* $\mathfrak{A}(z)$.

For we can write $z = \lambda vy$, where λ is an integer prime to m, $Nv = 2^r$, y proper, Ny odd. Then $\mathfrak{A}(z)$ is in the class $\mathfrak{K}$ of $\mathfrak{A}(y)$ and is of denominator Ny. By Cor. 1'Q, the right divisors of y and z of norm m are the same. Hence $y = ut$, $\mathfrak{A}(t)$ is a right divisor of $\mathfrak{A}(y)$, hence of $\mathfrak{A}(z)$.

However, A need not be a right divisor of $A'A$, for the denominator of $A'A$ may be less than $m'm$. By shuffling rows of A, columns and rows of A', the problem is reduced to the case where A' and A are odd, say $A' = \mathfrak{A}(u)$, $A = \mathfrak{A}(t)$. If ut is proper, A is a right divisor of $A'A$. This is trivially the case if m' and m are coprime (e.g. by lemma 9Q). We now have:

(a) The right divisors of denominator m of an automorph whose denominator is divisible by m, form an unique class $\mathfrak{L}$.

(b) An automorph of denominator $m_1 m_2 \cdots m_s$ (each m_ν odd) can be expressed in the form $A'A'' \cdots A^{(s)}$ where $A^{(\nu)}$ is of denominator $m_\nu (\nu = 1, \cdots, s)$, in essentially only one way; the general such expression being

$$(A'K'^*)(K'A''K''^*)(K''A'''K'''^*) \cdots (K^{(s-1)}A^{(s)}),$$

where the $K^{(i)}$ are integral automorphs. That is, the $K^{(i)}$ are matrices having one element ± 1 in each row and column, the rest 0; whence KAK' is in the class $\mathfrak{A}$ of A, and KA in the class $\mathfrak{L}$.

(c) If z is proper (mod m) and $m \mid Nz$, the right divisors of denominator m of $\mathfrak{A}(z)$ and $\mathfrak{A}(z + xm)$ are the same.

(d) If (33) holds, suppose $A'' \sim v$ (mod m''). By lemma 7, $A \sim v$ (mod m). Conversely, let A'' be of denominator $m'' = m'm$, $A'' \sim v(m'')$, and let $A \sim v(m)$. The right divisor of denominator m of A'' being also $\sim v(m)$, it is in the class $\mathfrak{L}$ of A. Hence A is a right divisor of A''.

It may be worth noting that if (33) holds, $m''A'' = (u_\alpha v_\beta) + m''(h_{\alpha\beta})$, and $(m'')^2 \mid Nu$ and Nv, as in lemma 5, and we set

$$mA = (s_\alpha v_\beta) + m(k_{\alpha\beta}), \qquad m'A' = (u_\alpha r_\beta) + m'(l_{\alpha\beta}),$$

then, as is easily seen by multiplying out $mA = mA'^*A''$,

$$s_\alpha \equiv (1/m') \sum u_\gamma l_{\gamma\alpha} \text{ (mod } m), \qquad r_\beta \equiv (1/m) \sum k_{\beta\alpha} v_\alpha \text{ (mod } m').$$

9. A natural application of automorphs is in transforming solutions of

$$x_1^2 + x_2^2 + x_3^2 = n \tag{34}$$

into other solutions. We employ the double interpretation (15) for x, y. If $A = (a_{\alpha\beta}/m)$ the equation $Ax = y$ expands into

$$\sum_\beta a_{\alpha\beta} x_\beta = m y_\alpha, \qquad \alpha = 1, 2, 3. \tag{35}$$

We say that A *is integrally effective on* x, if x and Ax are integral.

As A ranges over a set $\mathfrak{L}$, Ax ranges over a set $\mathfrak{K}$ (§1) precisely $2/k$ times, where k, called the *weight of* $\mathfrak{K}$, has the following values:

$$k = 2, \textit{ if no two of } y_1^2, y_2^2, y_3^2, 0 \textit{ are equal;}$$

$$k = 1 \textit{ if there is only one equality among } y_1^2, y_2^2, y_3^2, 0; \tag{36}$$

$$k = \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{1}{4} \textit{ resp. for the types } (g, g, 0), (g, g, g), (g, 0, 0).$$

As A ranges over the four odd automorphs of a set $\mathfrak{L}$, Ax ranges over a set $[y]((23Q))$. We can then use the notation (17).

THEOREM 11. *Let $Nt = m$, t proper, m as always odd. Use the double notation* (15), *x integral but not necessarily proper. Then $\mathfrak{A}(t)$ is integrally effective on x, that is*

$$(txt̄)/m \text{ is integral,} \tag{37}$$

if and only if t is a right-divisor of $x_0 + x$ for some integer x_0.

Sufficiency. $x_0 + x = ut$, $tx\bar{t} = t(ut - x_0)\bar{t} = (tu - x_0)m$.

Necessity. Let $\mathfrak{A}(t) \sim v(\text{mod } m)$. By Theorem 8, $v = ut$. By Theorem 7, the condition that $\mathfrak{A}(t)$ be integrally effective on x is equivalent to

$$v_1x_1 + v_2x_2 + v_3x_3 \equiv 0 \pmod{m}. \tag{38}$$

Corollary 7Q completes the proof. In place of cor. 7Q we may use

LEMMA 10. *Let m not have a factor in common with two of v_1, v_2, v_3. Every integral solution x of* (38) *is of the following form for certain integers w_1, w_2, w_3:*

$$x_1 \equiv w_2v_3 - w_3v_2, \qquad x_2 \equiv w_3v_1 - w_1v_3, \qquad x_3 \equiv w_1v_2 - w_2v_1 \pmod{m}. \tag{39}$$

By the C. R. T. the proof reduces to modulus p^r. Let v_2 and v_3 be prime to p. Solve $w_2v_3 - w_3v_2 \equiv x_1(p^r)$ for w_2 and w_3; (38) becomes $v_3(x_3 + v_1w_2) \equiv v_2(v_1w_3 - x_2) \pmod{p}$. Hence $x_3 + v_1w_2 \equiv w_1v_2$ for a certain w_1, amd $w_1v_3 \equiv v_1w_3 - x_2$.

Set $x_0 = \sum w_\alpha v_\alpha$. Then $x_0 + x \equiv wv = (wu)t \pmod{m}$.

THEOREM 12. *Let x be pure and proper* (mod m). *An automorph A of denominator m is integrally effective on x if and only if A is a right divisor of $\mathfrak{A}(x_0 + x)$ for some integer x_0.*

We can replace A by an odd automorph, $A = \mathfrak{A}(t)$, in its class $\mathfrak{K}$. If Ax is integral, $x_0 + x = ut$ for some x_0, by Theorem 11. By lemma 9, $\mathfrak{A}(t)$ is a right divisor of $\mathfrak{A}(x_0 + x)$. Conversely, if $\mathfrak{A}(t)$ is a right divisor of $\mathfrak{A}(x_0 + x)$, set $x_0 + x = \lambda vy$ as for lemma 9. Then $\mathfrak{A}(t)$ is a right divisor of $\mathfrak{A}(y)$, $y = ut$ by lemma 8, $x_0 + x = (\lambda vu)t$. By Theorem 11, $\mathfrak{A}(t)$ is integrally effective on x.

By lemma 1Q and corollary 6Q we have

LEMMA 11. *The $\mathfrak{K}$-classes of denominator m which are integrally effective on x in Theorem* 12, *are different for incongruent values x_0, and the same for congruent values x_0* (mod m).

THEOREM 13. *Let x be pure and proper* (mod m), *$Nx = n$. The number of sets $\mathfrak{K}$ of denominator m which are integrally effective on x, is equal to the number of solutions x_0* (mod m) *of*

$$x_0^2 \equiv -n \pmod{m}. \tag{40}$$

For $x_0 + x$ has an unique set $\mathfrak{Q}$ of right divisors of norm m.

The number depends only on n and m, not on the particular proper x. If $m = p^r$, $(-n \mid p) = 1$, the number is 2; if $(-n \mid p) = -1$, zero.

COROLLARY 6. *Let x be a proper pure quaternion of norm n, m odd and positive. To each solution x_0 of* (40) *appertains uniquely:*

(a) *a set $\mathfrak{Q}$ of proper right divisors of norm m of $x_0 + x$;*

(b) *a set $\mathfrak{Q}$ of proper quaternions t of norm m satisfying $tx\bar{t} \equiv 0$* (mod m);

(c) *a set $\mathfrak{M}$ of pure quaternions v* (mod m) *all satisfying* (38);

(d) *a set* $\mathfrak{L}$ *of automorphs of denominator* m *integrally effective on* x.
Conversely each such set corresponds to one and only one $x_0 \pmod m$. *Hence the number of such sets is in each case equal to the number of solutions of* (40).

COROLLARY 7. *The two sets appertaining to* x_0 *and* $-x_0 \pmod m$ *are in the same* $\mathfrak{E}$, $\mathfrak{E}$, $\mathfrak{C}$, $\mathfrak{A}$ *respectively if and only if* (32) *holds; hence certainly if two of* $x_1^2, x_2^2, x_3^2, 0$ *are equal.*

10. The degenerate cases, in which a set $\mathfrak{A}$ contains less than 24 sets $\mathfrak{L}$ are worth classifying. For any such case,

$$v \equiv k(\pm\, i_1 v_\alpha \pm i_2 v_\beta \pm i_3 v_\gamma) \pmod m \tag{40'}$$

for a choice of signs, permutation α, β, γ of 1, 2, 3, and k prime to m.

If $v \equiv k(-v_1, v_2, v_3)$ then since $\gcd(v_2, v_3, m) = 1$, $k \equiv 1$, $v_1 \equiv 0$. If $v \equiv k(v_1, v_3, -v_2)$ then $v_2 \equiv -k^2 v_2$, $v_3 \equiv -k^2 v_3$, $k^2 + 1 \equiv 0$, $k - 1$ prime to m, $v_1 \equiv 0$. Similarly in all cases σ_α, $\sigma_{\alpha+1}\pi_{\alpha+1,\alpha+2}$, $\sigma_{\alpha+2}\pi_{\alpha+1,\alpha+2}$ in (21), $m \mid v_\alpha$. The only possible corresponding column of mA is by (3_1), $(\pm m, 0, 0)$. By (3) an automorph

$$\begin{pmatrix} m & 0 & 0 \\ 0 & e & f \\ 0 & -f & e \end{pmatrix} \Bigg/ m \tag{41}$$

is contained in $\mathfrak{A}$. If e is odd comparison with (10) gives $m = t_0^2 + t_1^2$, $e = t_0^2 - t_1^2$, $f = 2t_0t_1$ in coprime integers t_0, t_1.

If $v \equiv k(v_1, v_3, v_2)$, $v_2 \equiv k^2 v_2$, $v_3 \equiv k^2 v_3$, $k^2 \equiv 1$; $k + 1$ is prime to m, for else a prime p would divide m and v_1, $v_2^2 + v_3^2 = Nv - v_1^2$, $2v_2^2$, v_2, v_3; $k \equiv 1$, $v_2 \equiv v_3$. Similarly in all cases $\pi_{\alpha+1,\alpha+2}$, $\sigma_\alpha\pi_{\alpha+1,\alpha+2}$, in (21), $v_{\alpha+1} \equiv \pm v_{\alpha+2}$. We can take the first two columns congruent $\pmod m$, $a_{11} = e$ and $a_{22} = g$ odd and positive, the remaining $a_{\alpha1}$ and $a_{\alpha2}$ even. If $a_{31} = a_{32} \pm 2m$, $a_{32} = \mp m$, and we have (41). Hence $a_{31} = a_{32}$, $a_{12} = e - m$, $a_{21} = g - m$; $e^2 + a_{21}^2 = a_{12}^2 + g^2$ by (3_1), $g = e$. The two columns are $(e, e - m, f)$, $(e - m, e, f)$, where by (3_2), $f^2 = 2e(m - e)$. The third column is determined by cofactors as in (4), and we find (42), where $m = t_0^2 + 2t_1^2$, $e = t_0^2$, $f = 2t_0t_1$:

$$\begin{pmatrix} e & e - m & f \\ e - m & e & f \\ f & f & m - 2e \end{pmatrix} \Bigg/ m, \qquad m^2 = (2e - m)^2 + 2f^2. \tag{42}$$

If $v \equiv k(v_2, v_3, v_1)$, $k^3 \equiv 1$; if $v \equiv k(-v_2, v_3, v_1)$, $k^3 \equiv -1$. In either case each v_α is prime to m, $\sum v_\alpha^2 \equiv v_1^2(1 + k^2 + k^4)$, $1 + k^2 \pm k \equiv 0$, $v_1 + v_2 \pm v_3 \equiv 0$. Thus in the last eight cases (21), $\mathfrak{A}$ contains an $(a_{\alpha\beta})$ with $a_{\alpha1} + a_{\alpha2} + a_{\alpha3} \equiv 0$. By the parities, $a_{\alpha1} + a_{\alpha2} + a_{\alpha3} = \pm m$, whence as $\sum a_{\alpha\beta}^2 = m^2$, $a_{\alpha1}a_{\alpha2} + a_{\alpha2}a_{\alpha3} + a_{\alpha3}a_{\alpha1} = 0$. If (e, f, g) and (q, r, s) are two rows, an easy elimination from

$ef + fg + ge = 0 = eq + fr + gs$ and $qe + rf + sg = qr + rs + sq$ yields $q/e = r/f = s/g$; which leads to (43) with $m = t_0^2 + 3t_1^2$, $e = t_0^2 - t_1^2$, etc.:

$$(43)\qquad \begin{pmatrix} e & f & g \\ g & e & f \\ f & g & e \end{pmatrix} \Bigg\| \, m, \qquad e + f + g = m, \qquad e^2 + f^2 + g^2 = m^2.$$

The case $m = 3$ belongs to both the types (42) and (43):

$$(44)\qquad \begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix} \Bigg\| \, 3.$$

THEOREM 14. *The automorph sets characterized by* (41)–(43) *are the only ones in which a set* $\mathfrak{A}$ *contains less than the maximum number,* 24, *of sets* $\mathfrak{L}$; *they are also the only ones corresponding to sets* $\mathfrak{E}$ *in which* (*cf.* (20))

$$(45)\qquad \text{two equalities occur among } t_0^2,\ t_1^2,\ t_2^2,\ t_3^2,\ 0;$$

also the only ones in which two rows of $(a_{\alpha\beta})$ *form, apart from shuffling of the* x_α, *the same solution of* (5).

To prove the last part observe that distinct rows of $(a_{\alpha\beta})$ cannot have the same divisor. Hence if two rows become identical after shuffling, their divisors are 1, and as is evident from (24), (40′) holds non-trivially.

The number of sets $\mathfrak{L}$ contained in an $\mathfrak{A}$ is easily verified to be

$$(46)\qquad 4 \text{ for } (44), \qquad 6 \text{ for } (41); \qquad \text{if } m > 3,\ 12 \text{ for } (42),\ 8 \text{ for } (43).$$

The same proportions hold for sets $\mathfrak{Q}$ in an $\mathfrak{E}$, and sets $\mathfrak{M}$ in a $\mathfrak{C}$.

11. Let m be prime to the square part of n, x_0 a solution of (40). The form $\varphi = [m, 2x_0, l]$ of determinant $-n$, is primitive. A certain completeness is obtained in treating simultaneously automorphs of denominator m appertaining to x_0 or $-x_0$. As in §6Q every $[x]$ of norm n is carried by φ into a certain $[y]$, and by $\varphi' = [m, -2x_0, l]$ into a certain $[z]$. Here $x_0 + x = ut$, $y = (tx\bar{t})/m = tu - x_0$; $-x_0 + x = vw$, $z = wv + x_0$; $Nt = Nw = m$. Similarly, $[y]$ and $[z]$ are each carried by φ and φ' into $[x]$ and one other set [ ] not necessarily new. This chain of transformations eventually closes, and if it does not exhaust the pure quaternions of norm n, we can start a new chain with any x not already included.

If x' is obtained from x by interchanges and sign-changes of the x_α, then according as the number of these changes is even or odd, x' is carried into the similarly formed $[y']$ and $[z']$ by φ and φ', or φ' and φ; (cf. (16Q)). Thus an entire set $\mathfrak{K} = \mathfrak{K}(x)$ is carried by odd automorphs in two sets $\mathfrak{A}_1$ and $\mathfrak{A}_2$ appertaining to x_0 and $-x_0$, into two entire sets $\mathfrak{K}_1 = \mathfrak{K}(y)$ and $\mathfrak{K}_2 = \mathfrak{K}(z)$. Here $\mathfrak{A}_1 =$

$\mathfrak{A}_2$ if (32) holds. Evidently if $\mathfrak{K}$ is of weight 2, either $\mathfrak{K}_1 \neq \mathfrak{K}_2$, or $\mathfrak{K}_1 = \mathfrak{K}_2$ and is also of weight 2.

Sets $\mathfrak{K}$ of weights $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$ are carried into themselves. For example, Ax is integral for $x = (g, g, 0)$ only if integral for $(1, 1, 0)$.

If $x_1 = 0$, then $x = i_1xi_1$; $-x_0 + x = i_1(x_0 + x)i_1 = (i_1u)(ti_1)$, $(ti_1)(i_1u) + x_0 = -(tu - x_0) = -y$; $\mathfrak{K}_1 = \mathfrak{K}_2$. If also $m \mid x_0$, t and ti_1 are in the same $\mathfrak{O}$, $\mathfrak{A}(t)$ is of type (41) and carries x into $(0, y_2, y_3)$ of the same type.

If $x_2 = x_3$, then $t' = t_0 - i_1t_1 - i_2t_3 - i_3t_2$ is a right divisor of $-x_0 + x$, $\mathfrak{A}(t')$ differs from $\mathfrak{A}(t)$ mainly in having the last two columns interchanged, and again $\mathfrak{K}_1 = \mathfrak{K}_2$. If also $m \mid x_0$, t and t' are left-associates, $\mathfrak{A}(t)$ is of type (42) and carries x into a vector $(y_1, y_2, \pm y_2)$ of the same type.

McGill University.