NONASSOCIATIVE COMMUTATIVE ALGEBRAS FOR TRIPLE COVERS OF 3-TRANSPOSITION GROUPS

Stephen D. Smith

Recently, nonassociative commutative algebras have come to the attention of finite group theorists; or viewed another way, it appears that many interesting groups arise as orthogonal groups of cubic forms on suitable modules. For example, the conjectured "monster" group of Bernd Fischer would support such an algebra in 196883 dimensions; and Peter Cameron has observed that most rank-3 permutation groups provide such algebras. More explicitly, Simon Norton has provided a construction of the module with cubic form, and consequent algebra structure, for 3-transposition groups. John Conway has called these "Norton algebras", and has described analogous examples for the covering groups $3S_7$ and $3F_{24}$. In this note, we show that there are exactly five such examples, and they may be simultaneously constructed under a suitable axiomatization.

R. L. Griess [5] has shown that each symmetric group S_n is the full automorphism of an algebra it defines on its $(n - 1)$-dimensional irreducible module. In an analogous way, we are able to show that $3S_7$ is the full automorphism group of our smallest (12-dimensional) example. For this problem the five examples do not seem to admit a unified treatment. In general, Jordan's theorem for cubic forms [8] leads us to expect finite automorphism groups; indeed, Schneider's theorem [9] would restrict the eigenvalue structure of possible operators. But the exact determination of the group seems difficult.

1. HYPOTHESES AND CONSEQUENCES

We operate under the axioms:

(1) Z is a group of order 3 normal in a finite group H, and H/Z is generated by a class of 3-transpositions;

(2) $H' = C_H(Z)$ and is of index 2 in H, with H'/Z simple.

We explore the extensive consequences of these requirements.

It will be convenient to denote H/Z by G, and consider this quotient first. For the language of 3-transposition groups, we follow Fischer [3]: we say an involution class d^G forms a class of 3-transpositions if for any $d, e \in d^G$ the product de has order 1, 2, or 3. Note in particular that $|de| = 2$ if and only if d and e commute; and $|de| = 3$ if and only if $d^e = e^d$. We may compare the list of 3-transposition groups in [3] with the table of Schur multipliers [2], [4] to see that G' is restricted. The condition $|H: H'| = 2$ prevents the occurrence of the cases $G' = PSU(3n, 2)$, F_{22}, and $PS\Omega_7^-(3)$ with d a reflection by a vector of "plus" type. Consequently:

Received December 13, 1976.

Michigan Math. J. 24 (1977).

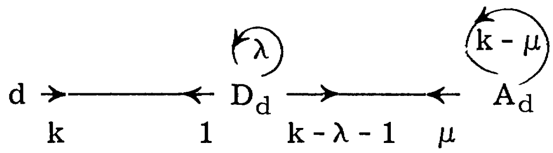
(3) G' is equal to one of A_6, A_7, $P S\Omega_6^-(3)$, $P S\Omega_7^-(3)$, F'_{24}. For $G' = P S\Omega_7^-(3)$, d is reflection by a vector of "minus" type.

(We remark that Fischer has recently given elegant presentations for the extensions H of the groups G' in (3) as well as $PSU(6, 2)$ and F_{22}; these appear to form a natural sequence leading toward the "monster".)

Fischer shows that G acts with rank 3 on d^G, and we form the usual graph on these by joining commuting pairs. The nontrivial $C_G(d)$-orbits are

$$D_d = \{e \in d^G\colon |de| = 2\} \quad \text{and} \quad A_d = \{e \in d^G\colon |de| = 3\};$$

with these orbits we may describe the graph in the (fairly standard) notation;



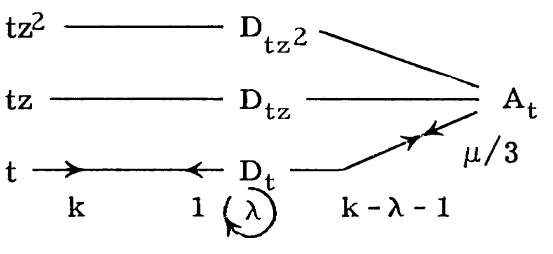
Here we set $v = |d^G| = 1 + k + \ell$, where $k = |D_d|$ and $\ell = |A_d|$. The arrows give the intersection numbers, indicating commuting between orbits; in particular,

$$|D_e \cap D_d| = \begin{cases} \lambda & \text{for } e \in D_d \\ \mu & \text{for } e \in A_d. \end{cases}$$

The rank-3 parameters v, k, ℓ, λ, μ for our examples are listed in Table 1.

We let the notation given for G stand, and turn to the covering group H. For fixed $d \in G$ we choose a preimage $t \in H$, and consider the class t^H. Multiplication in H is determined by that in G together with a factor set, the exact nature of which will not concern us at this point. We denote by z a fixed generator of Z, and by analogy set $D_t = \{u \in t^H\colon |tu| = 2\}$ and $A_t = \{u \in t^H\colon |tu| = 3\}$. Our assumptions require that the involutions t^H invert z, so that the class t^H consists of all $3v$ preimages of the class d^G. We see that elements of form uz, for $u \in D_t$, commute with t only modulo Z; such elements in fact form the set D_{tz}. Elements of A_t do not commute with t even modulo Z. In fact we have:

(4) t^H is a class of $\{3, 6\}$-transpositions of H. Furthermore, the graph on t^H may be described by:



,

where the nodes are $C_{H'}(t)$-orbits.

A proof of (4) is not difficult but rather tedious, and so is omitted.

Note that by (4), H' is of rank 7 on t^H, and H of rank 5. We introduce the permutation module V with basis $\{v_u\colon u \in t^H\}$ and the action $(v_u)^h = v_{(u^h)}$ for

TABLE 1. PARAMETERS FOR CERTAIN 3-TRANSPOSITION GROUPS

G'	v	k	ℓ	λ	μ	a	b	r = (dim Y)/2	s	n	m	N
A_6	15	6	8	1	3	3	2	6	9	3	3	S_3
A_7	21	10	10	3	6	5	2	6	15	3	3	S_3
$PS\Omega_6^-(3)$	126	45	80	12	18	15	3	21	105	6	6	S_6
$PS\Omega_7^-(3)$	378	117	260	36	12	39	3	27	351	6	6	S_6
F'_{24}	306,936	31,671	275,264	3,510	3,240	3,519	9	783	306,153	24	12	M_{24}

$h \in H$. If ω is a primitive cube root of unity, we may write $V = V_0 \oplus W \oplus \overline{W}$, a decomposition as H'-module into the 1, ω, ω^2 eigenspaces of z. Observe that the sets $\{v_u, v_{uz}, v_{uz^2}\}$ give blocks of imprimitivity, so that the block sums exhibit V_0 as the rank-3 module of $H/Z = G$ on d^G. Since H has rank 5 on t^H, the module $W \oplus \overline{W}$ affords two H-irreducible characters. The corresponding submodules will appear explicitly. By analogy with D. G. Higman [6], we define linear operators A, B on V by

$$(v_u)A = \sum_{x \in D_u} v_x \quad \text{and} \quad (v_u)B = \sum_{x \in A_u} v_x .$$

The operators commute with the action of H and so preserve the subspaces V_0, W, $\overline{W}$. The projections w_u and $\overline{w}_u$ of v_u into W, $\overline{W}$ are

$$w_u = v_u + \omega \cdot v_{uz} + \overline{\omega} \cdot v_{uz^2} ;$$

$$\overline{w}_u = v_u + \overline{\omega} \cdot v_{uz} + \omega \cdot v_{uz^2} .$$

Note also that $w_{uz} = \overline{\omega} \cdot w_u$ and $\overline{w}_{uz} = \omega \cdot \overline{w}_u$. Since $(v_u)B = (v_{uz})B$, we have $(w_u)B = (w_{uz})B = (\overline{\omega} \cdot w_u)B = \overline{\omega}(w_u)B$. We conclude $B|_{W \oplus \overline{W}} = 0$, and so study A on $W \oplus \overline{W}$. From the graph we may evaluate A^2:

$$A^2 = \lambda A + k + uB/3 ;$$

$$(A^2 - \lambda A - k)_{W \oplus \overline{W}} = 0 .$$

Since λ, $k > 0$, we see that $A|_{W \oplus \overline{W}}$ has eigenvalues of opposite sign, which we denote by a, -b with $a > b > 0$. The values of a, b are given in Table 1. We observe further that $(v_u)A$ does not involve any of $\{v_u, v_{uz}, v_{uz^2}\}$, so that

$$\operatorname{trace}(A|_{W \oplus \overline{W}}) = 0 .$$

Thus if r, s are the dimensions of the a, -b eigenspaces in W, we can solve for them via:

$$r + s - v; \quad ar - bs = 0 .$$

The values of r, s for each example appear in Table 1. By our earlier remark, the two eigenspaces in $W \oplus \overline{W}$ are irreducible H-modules.

2. NORTON'S FORM

So far we have obtained A-eigenspaces on which $B = 0$. This, with 3-transposition structure, is the basis for what follows, and we could work equally well with either space. For specificity, we choose the a-eigenspace (for practical purposes, it is the smaller one), and denote it by $Y = X \oplus \overline{X}$, where X is the part in W, and $\overline{X}$ in $\overline{W}$. Thus dim $Y = 2r$. We will show that H preserves a quadratic form on Y, with certain properties that allow us to define Norton's cubic form, also preserved by H. Then it is easy to define an H-invariant commutative multiplication on Y.

We observe first that Y is an irreducible H-module isomorphic to its contragredient, since $r \neq s$; and appearing just once in the permutation representation on t^H. It follows (see [1, (11.4)]) that the representation on Y is "of the first kind", and so H preserves a nondegenerate *symmetric* bilinear map $(\cdot, \cdot)$: $Y \times Y \to \mathbb{C}$. (We could in fact choose an $\mathbb{R}$-basis of Y and map to $\mathbb{R}$, but it is sometimes convenient to have ω available.) We can discuss $(\cdot, \cdot)$ without giving it explicitly. If we had $X \cap X^{\perp} = 0$, the H'-module would admit such a form, whereas the module is not even isomorphic to its contragredient. So by H'-irreducibility, we must have $X^{\perp} = X$. This simplifies the evaluation of the map. If we let x_t, $\bar{x}_t$ be the projections of v_t in X, $\bar{X}$, we see that $(x_t + \bar{x}_t, x_u + \bar{x}_u) = (x_t, \bar{x}_u) + (\bar{x}_t, x_u)$. Now Y may be spanned by vectors $\{x_u, \bar{x}_u\}$ as u varies over a set of preimages, one for each $e \in d^G$. We can even restrict attention to a subset of u's such that the $\{x_u, \bar{x}_u\}$ form a basis and recover the others by transitivity. And now, with suitable normalization, we obtain the conditions (due to S. Norton):

$$(5) \qquad (x_t, \bar{x}_u) = \begin{cases} 0 & \text{for } u \in A_t \\ 1 & \text{for } u \in D_t . \end{cases}$$

For transitivity of $C_{H'}(t)$ on A_t implies for $u \in A_t$ that

$$3v(x_t, \bar{x}_u) = \Big(x_t, \sum_{v \in A_t} \bar{x}_v\Big) = (x_t, (\bar{x}_t)B) = (x_t, 0) = 0 .$$

Similarly, transitivity on D_t implies for $u \in D_t$ that

$$k(x_t, \bar{x}_u) = (x_t, (\bar{x}_t)A) = a(x_t, \bar{x}_t) .$$

Now if $(x_t, \bar{x}_t) = 0$, these two conditions force $x_t \in Y^{\perp}$, a contradiction. Thus if we normalize so as to make $(x_t, \bar{x}_t) = k/a = b$, we obtain $(x_t, \bar{x}_u) = 1$, as required by (5).

We are now in a position to construct Norton's cubic form. For t, u, v taken from a basic subset, we may define $(x_t, x_u, x_v) = (x_t, \bar{x}_{(v^u)}) + (x_t, \bar{x}_u)(x_v, \bar{x}_u)$. We observe that the definition is symmetric in t, v because

$$(x_t, \bar{x}_{v^u}) = (x_t, \bar{x}_{v^u})^u = ((x_t)^u, (\bar{x}_{v^u})^u) = (\bar{x}_{t^u}, x_v) = (x_v, \bar{x}_{t^u}) .$$

But it is also symmetric in u, v:

Case 1: $u = v$. Here there is nothing to prove.

Case 2: $[u, v] \in Z$. Here $(x_u, \bar{x}_v) \in \langle \omega \rangle$, so on altering by a scalar factor we may as well assume that $v \in D_u$. Then $u^v = u$, $v^u = v$, and by (5) we have $(x_u, \bar{x}_v) = 1 = (x_v, \bar{x}_u)$. Thus

$$(x_t, x_u, x_v) = (x_t, \bar{x}_v) + (x_t, \bar{x}_u) = (x_t, \bar{x}_u) + (x_t, \bar{x}_v) = (x_t, x_v, x_u) .$$

Case 3: $v \in A_u$. Here $u^v = v^u$ and by (5), $(x_u, \bar{x}_v) = 0 = (x_v, \bar{x}_u)$ so that $(x_t, x_u, x_v) = (x_t, \bar{x}_{v^u}) = (x_t, \bar{x}_{u^v}) = (x_t, x_v, x_u)$.

Similarly, we can define $(\bar{x}_t, \bar{x}_u, \bar{x}_v) = (\bar{x}_t, x_{v^u}) + (\bar{x}_t, x_u)(\bar{x}_v, x_u)$, simply putting bars in the previous expression. We set the product equal to 0 for triples of transposition vectors from both X and $\bar{X}$, and obtain a definition of $(\cdot, \cdot, \cdot)$ on a basis of $Y \times Y \times Y$. We may extend by linearity to a symmetric trilinear map: $Y \times Y \times Y \rightarrow \mathbb{C}$. Action of H preserves this map, since it preserves the bilinear map. Of course, $(\cdot, x_u, x_v)$ is a linear functional on Y, and so is of the form $(\cdot, y)$ for some $y \in Y$. It is natural to take this y as the algebra product $x_u * x_v$. Indeed, we see from the definition that $x_u * x_v = \bar{x}_{v^u} + (x_v, \bar{x}_u)\bar{x}_u$. The multiplication is commutative, by the symmetry of $(\cdot, \cdot, \cdot)$, and H preserves the multiplication; that is, $(a * b)^h = a^h * b^h$ for $a, b \in Y$, $h \in H$, since it preserves both maps.

We make some basic remarks about the multiplication. Note that $X * \overline{X} = 0$, $X * X \leq \overline{X}$, and $\overline{X} * \overline{X} \leq X$. In fact we have:

THEOREM (S. Norton and J. Conway). Y *is an* H-*invariant algebra with:*

$$x_u * x_u = (b+1)\bar{x}_u;$$

$$(6) \qquad x_u * x_v = \begin{cases} \bar{x}_u + \bar{x}_v & \text{for } v \in D_u \\ \bar{x}_{v^u} & \text{for } v \in A_u . \end{cases}$$

We conclude this section with some information about the various examples. Proofs are not given, though most of the facts are easy to obtain.

From the embedding of $3S_6$ in $3S_7$ and comparison of the permutation representation, we can check that the eigenspace for $a = 3$ with $H = 3S_6$ may be taken to be the eigenspace for $a = 5$ with $H = 3S_7$; and as a result, the two groups determine the same 12-dimensional algebra Y. Notice that the other eigenvalue b, which is an algebra structure constant by (6), takes the value 2 for both groups. In a similar way, the 42-dimensional algebra for the case $G' = P S\Omega_6^-(3)$ is a subalgebra of the 54-dimensional algebra for $G' = P S\Omega_7^-(3)$; for both cases $b = 3$. If we had chosen Y instead as the $(-b)$-eigenspace in each example, we would not obtain the corresponding algebra inclusions.

The algebra Y may also be studied by decomposition under the action of subgroups of H. In particular, if J is an abelian subgroup of H or even of $\mathrm{Aut}(Y)$, we have $Y = \bigoplus \sum_{\alpha \in \mathrm{Char}(J)} Y_\alpha$, where J acts with character α on Y_α. Since $Y_\alpha * Y_\beta \leq Y_{\alpha\beta}$, any subgroup $S \leq \mathrm{Char}(J)$ produces a subalgebra Y_S via $Y_S = \bigoplus \sum_{\alpha \in S} Y_\alpha$. Note also that $N_{\mathrm{Aut}(Y)}(J)$ permutes the spaces $\{Y_\alpha\}$ and the algebras $\{Y_S\}$ in the obvious way.

A natural choice for J inside H arises from 3-transposition structure. The *width* of d^G is the size of a maximal pairwise commuting subset L of d^G. We will set $n = |L|$, and $2^m = |\langle L \rangle|$. As $\langle L \rangle$ is elementary, it splits over Z, so we may also regard L as a pairwise commuting subset of t^H, on choosing suitable preimages. In Table 1 we have listed the values of m, n and structure of

$$N = N_H(L)/C_H(L).$$

Note that $C_H(L) = \langle L \rangle$ in each case except $G' = P S\Omega_7^-(3)$, when we must add a reflection by a vector of "plus" type. Observe also that in the first four examples, $m = n$ with N acting as S_n on L. For $H = 3F_{24}$; however, $N \cong M_{24}$ acts on $\langle L \rangle$ as on cosets of the Golay code.

For the first four examples, we let $L = \{t_1, \cdots, t_n\}$ with N in its natural action. We can isolate the character λ sending each t_i to -1. We discover for each α that $\dim Y_\alpha = \dim Y_{\lambda\alpha}$. In particular, we look at $\alpha = 1$. If we set $y_t = x_t + \bar{x}_t$, we can set $C = \langle y_t : t \in L \rangle$ and see $C \leq C_Y(L) = Y_1$. Indeed, it is not difficult to check in each case that $C = Y_1$ of dimension n, and N acts on C in its natural permutation representation. Further, $Y_\lambda = \langle x_t - \bar{x}_t : t \in L \rangle$ also has dimension n. In general, we say α is of *type* k if it sends exactly k of $\{t_1, \cdots, t_n\}$ to -1. Thus 1, λ have types 0, n. Action of S_n fuses the $\binom{n}{k}$ characters of type k (and also those of type n - k, the λ-multiples of those of type k). On closer investigation, we discover the following facts:

G'	type of α	dim Y_α
A_6, A_7	1, 2	1
$P S\Omega_6^-(3)$	2, 4	1
	1, 3, 5	0
$P S\Omega_7^-(3)$	1, 2, 4, 5	1
	3	0

Conway produces analogous information for the case $3F_{24}$. Here the dual space of $\langle L \rangle$ corresponds to the Golay code. One finds $\dim Y_1 = 24$ with $N = M_{24}$ in its natural action; $\dim Y_\alpha = 1$ for α corresponding to octads or their complements, and $\dim Y_\alpha = 0$ for dodecads.

In the next section, we make just such an analysis of the 12-dimensional algebra, and in a more explicit way.

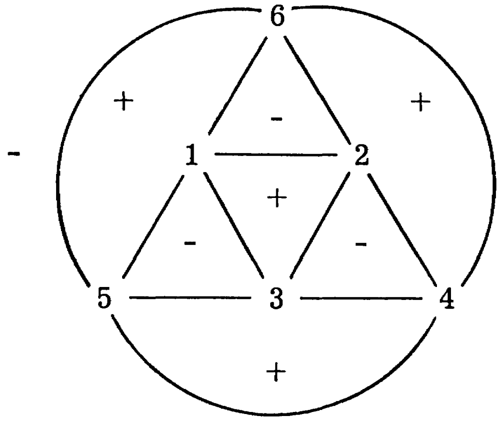
3. THE AUTOMORPHISM GROUP OF Y, dim Y = 12

In this section, $Y = X \oplus \bar{X}$ is the 12-dimensional algebra constructed in the previous section. We shall determine the group A = Aut(Y) of operators a satisfying $(y * y')^a = y^a * y'^a$ for y, y' $\in$ Y. To do this, we first examine multiplication operators M_y for certain $y \in Y$; we will have to examine these rather closely, much as Griess does in [5]. By Jordan's theorem we will be able to decide that A is finite; and then we show that A has a subgroup A* of index 2 fixing X and $\bar{X}$. From the classification of 6-dimensional finite linear groups, we can determine $A^* = 3A_7$, so that $A = 3S_7$.

We will now need to discuss the exact nature of the extension $3S_7$, and we describe a factor set provided by Conway. We have preimages (ij) for $0 \leq i \neq j \leq 6$ of the corresponding transpositions satisfying:

$$(7) \qquad (ij)^{(ik)} = (jk) \cdot z^{[ijk]},$$

for suitable exponents $[ijk] \in \mathbb{Z}_3$ (i, j, k distinct). We set [ijk] = 0 if $0 \in \{i, j, k\}$. Otherwise, we may refer to the figure:



If $\{i, j, k\}$ is a triangle, we let $[ijk]$ be the number inside the triangle, regarding $\{4, 5, 6\}$ as a triangle containing $^-$; and put $[ijk] = 0$ otherwise. Note in particular that $[ijk] = 0$ if $3 \nmid (i + j + k)$. We may then use (7) to describe multiplication of transposition preimages that commute modulo Z. If we adopt the notation $(ij)^{(k\ell)} = (ij) \cdot z^{[ij|k\ell]}$, for i, j, k, ℓ distinct, then we discover:

$$(8) \qquad \begin{aligned} [ij|k\ell] &= -[k\ell|ij], \\ [0j|k\ell] &= -[jk\ell], \\ [ij|k\ell] &= -[ik\ell] - [jk\ell] \qquad \text{if } 0 \notin \{i, j, k, \ell\}. \end{aligned}$$

For simplicity, we now adopt the notation ij, $\overline{ij}$ for the vectors $x_{(ij)}$, $\bar{x}_{(ij)}$. With (7), (8) we may now give rules for the evaluation of $(\cdot, \cdot)$:

$$(9) \qquad \begin{aligned} (ij, \overline{ij}) &= 2, && \\ (ij, \overline{ik}) &= 0, && j \neq k, \\ (ij, \overline{k\ell}) &= \overline{(k\ell, \overline{ij})}, && i, j, k, \ell \text{ distinct}, \\ (0j, \overline{k\ell}) &= \omega^{[jk\ell]}, && \\ (ij, \overline{k\ell}) &= \omega^{-[ik\ell]-[jk\ell]}, && 0 \notin \{i, j, k, \ell\}. \end{aligned}$$

Then we obtain corresponding results about multiplication:

$$(10) \qquad ij * k\ell = \begin{cases} 3\,\overline{ij} & \text{if } i = k,\ j = \ell \text{ (here } b = 2), \\ \omega^{[ij\ell]}\,\overline{j\ell} & \text{if } i = k,\ j \neq \ell; \\ \omega^{[k\ell|ij]}\,\overline{k\ell} + \omega^{-[k\ell|ij]}\,\overline{ij} & \text{if } i, j, k, \ell \text{ distinct}. \end{cases}$$

We obtain similar rules (with complex conjugate coefficients) for multiplying in $\overline{X}$.

It will be convenient to use two different bases for Y, the first being a little simpler to introduce, the second more convenient for analysis of multiplications. If we set $x_i = 0i$ and $\bar{x}_i = \overline{0i}$ for $1 \leq i \leq 6$, we see we obtain a basis for Y since $(x_i, \bar{x}_j) = 2\delta_{ij}$. The basis is as near to being "orthonormal" as we can expect if we work in $X = X^{\perp}$.

We find the other basis by making the analysis described at the end of the previous section. We can choose $L = \{(14), (25), (36)\}$. Since we are restricting attention to X, we need the characters of $\langle L \rangle \cap H'$. We let α, β, $\alpha\beta$, respectively, be the characters trivial on (25)(36), (14)(36), (14)(25). A few computations enable us to obtain vectors $y_1, y_2, y_3 \in X_1 = \langle 14, 25, 36 \rangle$ and $y_4 \in X_\alpha$, $y_5 \in X_\beta$, $y_6 \in X_{\alpha\beta}$, and corresponding $\bar{y}_1, \cdots, \bar{y}_6 \in \bar{X}$, so that $(y_i, \bar{y}_j) = \delta_{ij}$. We may obtain these in terms of the vectors $\{ij, \overline{ij}\}$ which we know how to manipulate. A suitable choice is:

$$\begin{aligned}
y_1 &= 1/2\ (25 + 36 - 14)\\
y_2 &= 1/2\ (14 + 36 - 25)\\
y_3 &= 1/2\ (14 + 25 - 36)\\
y_4 &= (26 + 35 - 23 - 56)/\sqrt{12}\\
y_5 &= (13 + 46 - 16 - 34)/\sqrt{12}\\
y_6 &= (12 + 45 - 15 - 24)/\sqrt{12}
\end{aligned} \tag{11}$$

Correspondingly, we may express the $\{ij\}$ in terms of the $\{y_i\}$ with coefficients given by:

$$\begin{array}{c|ccc|ccc}
 & y_1 & y_2 & y_3 & y_4 & y_5 & y_6 \\
\hline
14 & 0 & 1 & 1 & 0 & 0 & 0 \\
25 & 1 & 0 & 1 & 0 & 0 & 0 \\
36 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
26 & 1/2(-1 & 1 & 1 & \sqrt{3} & -i & i) \\
13 & 1/2(\ 1 & -1 & 1 & i & \sqrt{3} & -i) \\
12 & 1/2(\ 1 & 1 & -1 & i & -i & \sqrt{3})
\end{array} \quad . \tag{12}$$

Expressions for other ij are easily deduced using $(\cdot, \cdot)$ and the table. In the basis of the $\{y_i, \bar{y}_i\}$, we may use (10) - (12) to compute the multiplication operators M_y for y in the basis. For $y = y_1$, we note that M_y annihilates $\bar{X}$ and takes X into $\bar{X}$. Consequently, we need only exhibit the nonzero lower-left 6×6 submatrix, with i-th column expressing $y_i * y_1$ in terms of $\bar{y}_1, \cdots, \bar{y}_6$. We obtain:

$$(13)\quad M_{y_1} = 1/2\left|\begin{array}{ccc|ccc} 3 & 1 & 1 & & & \\ 1 & 1 & -1 & & & \\ 1 & -1 & 1 & & & \\ \hline & & & -3 & & \\ & & & & 1 & \\ & & & & & 1 \end{array}\right|,\quad M_{y_4} = 1/2\left|\begin{array}{ccc|ccc} & & & 3 & & \\ & & & 1 & & \\ & & & 1 & & \\ \hline -3 & 1 & 1 & 0 & 0 & 0 \\ & & & 0 & 0 & \frac{1}{\sqrt{3}} \\ & & & 0 & \frac{1}{\sqrt{3}} & 0 \end{array}\right|$$

Then M_{y_2}, M_{y_5} may be obtained by applying the row/column permutations (12)(45) to these matrices; and M_{y_3}, M_{y_6} by applying (13)(46). Similarly these are the 6×6 upper-right submatrices of $M_{\bar{y}_1}, \cdots, M_{\bar{y}_6}$.

With the above information in hand, we are ready to proceed with our main project. The first step is comparatively easy:

(14) The map $(\cdot, \cdot, \cdot)$ gives a nonsingular cubic form, so that A is finite.

Proof. With indeterminates $X_1, \cdots, X_6, \overline{X}_1, \cdots, \overline{X}_6$ and basis $x_1, \cdots, x_6, \bar{x}_1, \cdots, \bar{x}_6$, we see that the associated cubic form f is in fact the sum of forms on X and $\overline{X}$:

$$f = \sum_{i,j,k=1}^{6} (x_i, x_j, x_k) X_i X_j X_k + \sum_{i,j,k=1}^{6} (\bar{x}_i, \bar{x}_j, \bar{x}_k) \overline{X}_i \overline{X}_j \overline{X}_k .$$

Call the two parts g and h. To show f is nonsingular, we prove that the quadratic forms $\frac{\partial g}{\partial X_i}, \frac{\partial h}{\partial \overline{X}_j}$ have no common zero. (This is equivalent to showing that Y has no square-roots of 0 other than 0.) We can use (9) to evaluate:

$$(x_i, x_j, x_k) = \begin{cases} 6, & i = j = k; \\ \omega^{-[ijk]}, & i, j, k \text{ distinct}; \\ 0, & \text{otherwise}. \end{cases}$$

It follows that $\frac{\partial g}{\partial X_1}$ has matrix:

$$\frac{\partial g}{\partial X_1} = 3\begin{pmatrix} 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & & & & \\ 0 & & 0 & & & \\ 0 & & & 0 & & \\ 0 & & & & 0 & \\ 0 & & & & & 0 \end{pmatrix} \longleftarrow \text{entry } \omega^{-[1jk]} \text{ in } (j, k) \text{ position}.$$

Matrices for $x_2, \cdots, x_6$ are obtained similarly. We see that the sum has matrix:

$$\sum_{i=1}^{6} \frac{\partial g}{\partial X_i} = 3 \left(\begin{array}{ccc|ccc} 6 & & & 4 & & \\ & 6 & & & 4 & \\ & & 6 & & & 4 \\ \hline 4 & & & 6 & & \\ & 4 & & & 6 & \\ & & 4 & & & 6 \end{array} \right) \longleftarrow \text{entry 1 elsewhere.}$$

Thus

$$\frac{1}{3} \sum_{i=1}^{6} \frac{\partial g}{\partial X_i} = \left(\sum_{i=1}^{6} X_i \right)^2 + 3[(X_1 + X_4)^2 + (X_2 + X_5)^2 + (X_3 + X_6)^2] + 2 \sum_{i=1}^{6} X_i^2 \,,$$

which is positive-definite. In the same way $\sum_{i=1}^{6} \frac{\partial h}{\partial \overline{X}_i}$ is positive-definite, so that $\frac{\partial g}{\partial X_1}, \cdots, \frac{\partial h}{\partial \overline{X}_6}$ can have no common zero, and f is nonsingular. It follows by Jordan's theorem [8] or by Schneider [9] that A is finite, and (14) is established.

The next step is the difficult one:

(15) Elements of A either interchange or fix $\{X, \overline{X}\}$.

The proof is quite tedious, and we postpone it in favor of showing the final argument:

(16) $A = 3S_7$.

Proof. Assuming (15), we see $A^* = N_A(X, \overline{X})$ is of index 2 in A. As X is an irreducible module in 6 dimensions for A^*, we may consult the classification of 6-dimensional groups [7]. Already $A^* \geq 3A_7$. If we had $A^* = 6 \cdot PSU(4, 3)$, the central involution would act as -1 on Y, and so would not preserve the multiplication. We conclude $A^* = 3A_7$, so that $A = 3S_7$.

Now we will begin the proof of (15). It is convenient to define for $S \leq Y$ the annihilator $A(S) = \{y \in Y\colon s * y = 0 \text{ for each } s \in S\}$. For instance, we see by (13) that $A(y_1) = \overline{X}$, and so $A(X) = \overline{X}$. Now for $a \in A$ we must have $A(X^a) = A(X)^a = \overline{X}^a$. Thus to prove (15) it will suffice to show $X^a = X$ or $\overline{X}$. We will now write T for some such conjugate X^a, and U for $\overline{X}^a = A(T)$.

It will also be convenient to let a subscript X or $\overline{X}$ indicate the image of projection into X or $\overline{X}$. We obtain easily a strong restriction on the intersections of T, U with X, $\overline{X}$:

(17) $T = T_X \oplus T_{\overline{X}}$ and $U = U_X \oplus U_{\overline{X}}$.

Proof. Take $t \in T$ and $u \in U$. We have

$$0 = (t_X + t_{\overline{X}}) * (u_X + u_{\overline{X}}) = (t_X * u_X) + (t_{\overline{X}} * u_{\overline{X}}).$$

As the first term on the right is in $\overline{X}$ and the second in X, both are 0. We conclude:

$$(18) \qquad T_X \leq A(U_X) \quad \text{and} \quad T_{\overline{X}} \leq A(U_{\overline{X}})$$

(and of course symmetrically with T, U interchanged). But we also have trivially that $T \leq T_X \oplus T_{\overline{X}}$, and similarly for U. We have U_X contained in $A(T_{\overline{X}})$ trivially, and in $A(T_X)$ by (18); and we obtain the same inclusions for $U_{\overline{X}}$. Thus

$$U \leq U_X \oplus U_{\overline{X}} \leq A(T_X) \cap A(T_{\overline{X}}) \leq A(T_X \oplus T_{\overline{X}}) \leq A(T) = U.$$

Consequently, we get $U = U_X \oplus U_{\overline{X}}$; and similarly for T, proving (17).

In view of (17), since we assume $T \neq X$ or $\overline{X}$, it intersects both nontrivially. Thus $T_X = T \cap X$ and so on; $\dim T_X + \dim U_X = 6$ and so on. Since

$$\overline{X} \leq A(T_X) \leq \overline{X} \oplus X,$$

we have $A(T_X) = \overline{X} \oplus A(T_X)_X$. By nonsingularity, there are no square-roots of 0, so $\dim A(T_X) = 12 - \dim T_X$; and as $\overline{X} \oplus U_X \leq A(T_X)$, we must have

$$U_X = A(T_X)_X = A(T_X) \cap X.$$

By choice, if necessary, $\dim T_X \leq 3$, so that T_X is a subspace of elements whose multiplications have rank at most 3. We will be able to derive a contradiction from this condition. Indeed, on inspecting (13) we see that the obvious multiplications all have rank greater than or equal to 4; and we will show how difficult it is to reduce rank below that. We further break down X into "left" and "right" parts

$$L = \langle y_1, y_2, y_3 \rangle \quad \text{and} \quad R = \langle y_4, y_5, y_6 \rangle.$$

Define $\overline{L}$ and $\overline{R}$ analogously on $\overline{X}$. Subscripts L and R will again denote projection into these spaces. Our first step is to show:

(19) For $y \in L$ we have $\mathrm{rk}(M_y) \geq 4$, and consequently $T_X \cap L = 0$.

Proof. Take some $y \in L$. If $y \in T$, then $\mathrm{rk}(M_y) \leq 3$, so $\dim (A(y)_X) \geq 3$. We analyze how this might happen. Since $L * L \subseteq \overline{L}$ and $L * y_i \subseteq \langle \bar{y}_i \rangle$ for $i = 4, 5, 6$, we see that $A(y)_X = A(y)_L \oplus A(y)_{\langle y_4 \rangle} \oplus A(y)_{\langle y_5 \rangle} \oplus A(y)_{\langle y_6 \rangle}$. We first examine the possibility that $A(y)_R \neq 0$. From (13) we see that

$$A(y_4)_X = \langle y_1 + 3y_2, y_1 + 3y_3 \rangle,$$

and analogously for y_5, y_6. Then $\dim A(y_4)_X = 2$, $\dim A(y_4, y_5)_X = 1$, and $A(R)_X = 0$. Thus $\dim A(y)_R = 3$ is impossible. Now if $\dim A(y)_R = 2$, we may assume without loss of generality that $A(y)_R = \langle y_4, y_5 \rangle$, and then we may take $y = y_1 + y_2 + 2y_3$. But we can check that $\{(y * y_i)_{\overline{L}}: i = 1, 2, 3\}$ are independent, so $A(y)_L = 0$ and $\mathrm{rk}(M_y) = 4$. Thus we assume $\dim A(y)_R = 1$, and without loss of generality, $A(y)_R = \langle y_4 \rangle$ and we can take $y = y_1 + ay_2 + (3 - a)y_3$ for some a. We can consider the coefficients of the vectors $(y * y_i)_{\overline{L}}$ for $i = 1, 2, 3$:

	$\bar{y}_1$	$\bar{y}_2$	$\bar{y}_3$
$y * y_1$	3	2	2 - a
$y * y_2$	-1	2 + a	1
$y * y_3$	2 - a	1	5 - a

If these three vectors span only a line, we have $2 + a = -2/3$, $2 - a = 3/2$, which is a contradiction. Thus here $\mathrm{rk}(M_y) \geq 4$ also. Finally, consider the case $A(y)_R = 0$, so that $A(y)_X = A(y)_L$. If $\mathrm{rk}(M_y) = 3$, then $L = A(y)_X$, forcing $y^2 = 0$, contradicting nonsingularity. Thus (19) is proved.

One consequence of (19) is that we are reduced to the case $\dim (T_X) = 3$. Not surprisingly, we also obtain a right analogue of (19):

(20) $$T_X \cap R = 0 .$$

Proof. Take $y = ay_4 + by_5 + cy_6 \in R$. For any $u \in X$, note $u_L * y \in \bar{R}$; and if $u_R = dy_4 + ey_5 + fy_6$, then $(u * y)_{\bar{L}} = (u_R * y)_{\bar{L}}$ is the combination

$$\frac{1}{2}[ad(-3, 1, 1) + be(1, -3, 1) + cf(1, 1, -3)] .$$

Suppose first $a, b, c \neq 0$. Then independence of the above vectors forces $d = e = f = 0$ wherever $u \in A(y)$; that is, $A(y)_X \subseteq L$. If $y \in T$, then $U_X \subseteq A(y)_X$, and we contradict (19). Recall also from that proof that if $b = c = 0$ and $y \in \langle y_4 \rangle$, then $A(y)_X \subseteq L$, again forcing $y \notin T$. Thus without loss of generality we can take $a, b \neq 0$ and $c = 0$. The argument above forces $d = e = 0$ for $u \in A(y)$; that is, $A(y)_R \subseteq \langle y_6 \rangle$. Consequently, if $\mathrm{rk}(M_y) \leq 3$, then $\dim (A(y) \cap L) \geq 2$. Choosing some $u \in A(y) \cap L$, the argument of (19) gives $\langle y_4, y_5 \rangle \subseteq A(y)$, since $a, b \neq 0$. But recall that $\dim (A(y_4, y_5)_X) = 1$, contradicting $\dim (A(y) \cap L) \geq 2$. Hence (20) is established.

A consequence of (19) and (20) is that $T_L = L$ and $T_R = R$. In particular, T must contain an element $y = (y_1 + y_2 + y_3) + dy_4 + ey_5 + fy_6$. Some calculation with this element will now produce a contradiction. We first list the coordinates of $y * y_i$ $i = 1, \cdots, 6$:

	$\bar{y}_1$	$\bar{y}_2$	$\bar{y}_3$	$\bar{y}_4$	$\bar{y}_5$	$\bar{y}_6$
$y * y_1$	5	1	1	-3d	e	f
$* y_2$	1	5	1	d	-3e	f
$* y_3$	1	1	5	d	e	-3f
$* y_4$	-3d	e	f	-1	$\frac{f}{\sqrt{3}}$	$\frac{e}{\sqrt{3}}$
$* y_5$	d	-3e	f	$\frac{f}{\sqrt{3}}$	-1	$\frac{d}{\sqrt{3}}$
$* y_6$	d	e	-3f	$\frac{e}{\sqrt{3}}$	$\frac{d}{\sqrt{3}}$	-1

(For simplicity we have omitted a factor of 1/2 in all entries of this table.)

Now if $\mathrm{rk}(M_y) = 3$, then the bottom three rows must be dependent on the top three. Indeed, we may invert the upper-left 3×3 matrix in order to determine coefficients of linear combinations. First we claim $d, e, f \neq 0$. For if the fourth row is expressed as a combination of the first three, its entry -1 in the fourth column forces $d \neq 0$. In a similar way, we see that $e, f \neq 0$.

In order to determine the coefficients, we note

$$\begin{pmatrix} 5 & 1 & 1 \\ 1 & 5 & 1 \\ 1 & 1 & 5 \end{pmatrix}^{-1} = \frac{1}{28}\begin{pmatrix} 6 & -1 & -1 \\ -1 & 6 & -1 \\ -1 & -1 & 6 \end{pmatrix} .$$

The coefficients for the fourth row, for example, are

$$\frac{1}{28}\,[-18d - e - f,\ 3d + 6e - f,\ 3d - e + 6f] .$$

On applying these in the columns 4, 5, 6, we obtain

$$(21)\qquad \begin{aligned} -1 &= \frac{d}{7}(15d + 2e + 2f) \\ \frac{f}{\sqrt{3}} &= \frac{e}{7}(-6d - 5e + 2f) \\ \frac{e}{\sqrt{3}} &= \frac{f}{7}(-6d + 2e - 5f) . \end{aligned}$$

We can do the same for the fifth and sixth rows, obtaining six more equations. On comparing such equations with the same left-hand side, we obtain equations like

$$(22)\qquad \begin{aligned} (d - e)(15(d + e) + 2f) &= 0 \\ (d - e)(5(d + e) - 2f) &= 0 , \end{aligned}$$

and similar ones with $\{d, f\}$ interchanged and $\{e, f\}$ interchanged. Then if $d \neq e$, we conclude from (22) that $f = 0$ and $d = -e$. But $f = 0$ contradicts our earlier remark. Thus $d = e$, and from similar calculations we conclude $d = e = f$.

Now the coefficients for the fourth row become $\left(\frac{d}{7}\text{ times}\right)$ $-5, 2, 2$. Looking down the fourth column, we obtain the requirement $-1 = \frac{19d^2}{7}$. But this is impossible. This contradiction completes the proof of (15), and hence of our main result.

ACKNOWLEDGMENT

The debt to work of John Conway is obvious. Conversations with Bob Griess were very helpful, and Bill Kantor pointed out the relevance of Schneider's work.

REFERENCES

1. W. Feit, *Characters of Finite Groups.* Benjamin Press, Inc., N.Y., 1967.

2. ———, *The current situation in the theory of finite simple groups.* Actes. Congrès Int. Math., Tome 1, 1970, 55-93.

3. B. Fischer, *Finite groups generated by* 3-*transpositions*, I. Inv. Math. 13 (1971), 232-246.

4. R. L. Griess, Jr., *Schur multipliers of the finite simple groups of Lie type.* Trans. Amer. Math. Soc. 183 (1973), 355-421.

5. ———, *Nonassociative commutative algebras whose automorphism groups are the symmetric groups.* Michigan Math. J., to appear.

6. D. G. Higman, *Finite permutation groups of rank* 3. Math. Z. 86 (1964), 145-156.

7. J. H. Lindsey, II, *On a projective representation of the Hall-Janko group.* Bull. Amer. Math. Soc. 74 (1968), p. 1094.

8. C. Jordan, *Memoire sur l'equivalence des formes.* J. Éc. Pol. XLVIII (1880), 112-150 (Oeuvres, t.3, p. 421-460; cf. p. xviii par J. Dieudonné).

9. J. E. Schneider, *Orthogonal groups of nonsingular forms of higher degree.* J. Algebra. 27 (1973), 112-116.

Department of Mathematics
University of Illinois at Chicago Circle
Chicago, Illinois 60680