A CHARACTERIZATION OF CERTAIN EXTREME FORMS

BY

MAURICE CRAIG

1. Introduction

The symmetric group S_3 has a matrix representation $\mathbf{F}$, given by

$$\mathbf{F}(12) = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{F}(23) = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}.$$

With

$$\mathbf{U}(d) = \begin{pmatrix} d & 1 \\ 0 & 1 \end{pmatrix} \quad \text{for } d = 1 \text{ or } 3,$$

the $\mathbf{U}(d)^{-1}\mathbf{F}\mathbf{U}(d)$ are $\mathbf{Z}$-representations, both $\mathbf{Q}$-equivalent to $\mathbf{F}$, but not mutually $\mathbf{Z}$-equivalent. Every $\mathbf{Z}$-representation of S_3 rationally equivalent to $\mathbf{F}$ is integrally equivalent to one of these two. (Cf. [5, Example 1, p. 505].)

Again, taking

$$\mathbf{F}(12) = \begin{bmatrix} 1 & 1 & \\ & -1 & \\ & & -1 \end{bmatrix},$$

$$\mathbf{F}(23) = \begin{bmatrix} -1 & & \\ 1 & 1 & 1 \\ & & -1 \end{bmatrix},$$

$$\mathbf{F}(34) = \begin{bmatrix} -1 & & \\ & -1 & \\ & 1 & 1 \end{bmatrix}$$

(with blanks representing zeros) and

$$\mathbf{U}(d) = \begin{bmatrix} d & & -1 \\ & d & 2 \\ & & 1 \end{bmatrix}, \quad d = 1, 2, \text{ or } 4,$$

a similar statement may be made on behalf of S_4.

More generally, for a certain integral representation $\mathbf{F}$ of S_{n+1} of degree n, we give representatives for the $\mathbf{Z}$-equivalence classes of $\mathbf{Z}$-representations $\mathbf{Q}$-equivalent to $\mathbf{F}$. The precise statement is contained in the theorem of Section 3. In Section 4, the resulting groups of integral matrices are interpreted as giving automorphisms of certain quadratic forms. These were first described by Coxeter, and are of interest for their arithmetic properties (see [3]). Section 2

Received August 25, 1975.

provides the theoretical background for the later sections. The reference [5] cited above contains the representation theory used here.

2. Preliminaries

We write $\mathbf{e}_j$ for the jth column of the $n \times n$ identity matrix $\mathbf{I}_n$ $(= \mathbf{I})$. For a real $n \times n$ matrix $\mathbf{A} \neq \mathbf{I}$, we adopt the conventions: a_{ij} is the (i, j) entry, $\mathbf{a}_j$ is the jth column,

$$\langle \mathbf{A} \rangle = \mathbf{Z}\mathbf{a}_1 + \cdots + \mathbf{Z}\mathbf{a}_n.$$

$\mathbf{A}$ is *unimodular* if both $\mathbf{A}, \mathbf{A}^{-1} \in M_n(\mathbf{Z})$.

Also, G will denote a finite group of order g, and $\mathbf{F}\colon G \to M_n(\mathbf{Z})$ a matrix representation of degree n which is irreducible in the complex field. Thus for $h \in G$, we have $h \to \mathbf{F}(h)$, where by an adaptation of our convention for matrices, we write

$$\mathbf{F}(h) = (\mathbf{F}_1(h), \ldots, \mathbf{F}_n(h)) = (F_{ij}(h)).$$

Finally, $\mathbf{\Phi} = \mathbf{U}^{-1}\mathbf{F}\mathbf{U}$ will be a $\mathbf{Q}$-representation of G which is $\mathbf{Q}$-equivalent to $\mathbf{F}$. We can clearly suppose the u_{ij} to be integers, with

$$\text{G.C.D. } (u_{ij}) = 1. \tag{1}$$

LEMMA 1. *If* $\mathbf{\Psi} = \mathbf{V}^{-1}\mathbf{F}\mathbf{V}$ *is a second such representation, then* $\mathbf{\Phi}$, $\mathbf{\Psi}$ *are* $\mathbf{Z}$*-equivalent iff for some unimodular* $\mathbf{W}$, *we have* $\mathbf{V} = \mathbf{U}\mathbf{W}$.

Proof. Given that $\mathbf{\Psi} = \mathbf{W}^{-1}\mathbf{\Phi}\mathbf{W}$, we obtain $(\mathbf{U}\mathbf{W}\mathbf{V}^{-1})\mathbf{F} = \mathbf{F}(\mathbf{U}\mathbf{W}\mathbf{V}^{-1})$. Since $\mathbf{F}$ is absolutely irreducible, by Schur's Lemma $\mathbf{U}\mathbf{W}\mathbf{V}^{-1}$ must be a scalar matrix, that is, $\mathbf{U}\mathbf{W} = t\mathbf{V}$. However, t can only be $+1$ or -1, because $\mathbf{U}\mathbf{W}$ has the same G.C.D. of coefficients as $\mathbf{U}$ itself ($\mathbf{W}$ being unimodular), namely 1, while the same is true for $\mathbf{V}$. The converse is trivial.

Consider now, the action of G as a group of linear transformations of $\mathbf{R}^n$, which is given by

$$(h, x) \to \mathbf{F}(h)\mathbf{x}, \quad \text{for } h \in G,\ \mathbf{x} \in \mathbf{R}^n.$$

Then $\mathbf{F}(h)$ is just the matrix of $(h, -)$, taken with respect to $\mathbf{e}_1, \ldots, \mathbf{e}_n$ as basis for $\mathbf{R}^n$. Also, $\mathbf{\Phi}(h)$ is the matrix with respect to $\mathbf{u}_1, \ldots, \mathbf{u}_n$. Since $\mathbf{F}$ is an integral representation, the lattice $\langle \mathbf{I}_n \rangle$ becomes a G-module, and we have:

LEMMA 2. *The condition for* $\mathbf{\Phi}$ *to be a* $\mathbf{Z}$*-representation, is that* $\langle \mathbf{U} \rangle$ *should be a G-submodule* (*invariant sublattice*) *of* $\langle \mathbf{I}_n \rangle$.

COROLLARY. *Equivalently,* $\mathbf{\Phi}$ *is integral iff all columns of* $\mathbf{F}(h)\mathbf{U}$ *lie in* $\langle \mathbf{U} \rangle$, *for all* $h \in G_0$, *where* G_0 *denotes a fixed set of generators for G.* (*That is, instead of testing* $\mathbf{F}(h)\mathbf{x} \in \langle \mathbf{U} \rangle$ *for all* $h \in G$ *and* $\mathbf{x} \in \langle \mathbf{U} \rangle$, *it is enough to examine the action of generators for G upon generators for* $\langle \mathbf{U} \rangle$.)

Taking different bases for $\langle \mathbf{U} \rangle$ (namely the columns of matrices $\mathbf{UW}$, where $\mathbf{W}$ is unimodular), we obtain all representations $\mathbf{Z}$-equivalent to $\mathbf{\Phi}$. The next result shows that only finitely many classes of $\mathbf{Z}$-equivalent representations of G, rationally equivalent to $\mathbf{F}$, consist of $\mathbf{Z}$-representations. In fact, for $\mathbf{\Phi}$ to be integral, the index of $\langle \mathbf{U} \rangle$ in $\langle \mathbf{I}_n \rangle$ is bounded.

LEMMA 3. *If $\mathbf{\Phi}$ is a $\mathbf{Z}$-representation, then $\langle \mathbf{U} \rangle$ has $\langle (g/n)\mathbf{I} \rangle$ as a sublattice.*

Proof. We may write $\mathbf{U} = \mathbf{X} \cdot \operatorname{diag}(d_1, \ldots, d_n) \cdot \mathbf{Y}$, where $\mathbf{X}$, $\mathbf{Y}$ are unimodular matrices and $d_1, \ldots, d_n$ (the invariant factors of $\mathbf{U}$) are positive integers satisfying $d_i \mid d_{i+1}$, for $1 \le i < n$. By (1), we must have $d_1 = 1$. Thus $\mathbf{x}_1$ is the first column of $\mathbf{UY}^{-1}$. As $\mathbf{Y}^{-1}$ is integral, it follows that $\mathbf{x}_1 \in \langle \mathbf{U} \rangle$, and so by Lemma 2, $\mathbf{F}(h)\mathbf{x}_1 \in \langle \mathbf{U} \rangle$ for all $h \in G$. Hence $\langle \mathbf{U} \rangle$ must contain $\sum_h \theta(h^{-1})\mathbf{F}(h)\mathbf{x}_1$ for any integers $\theta(h^{-1})$, where the sum is taken over all $h \in G$.

Setting $\Theta = \mathbf{X}^{-1}\mathbf{FX}$, a $\mathbf{Z}$-representation of G (being $\mathbf{Z}$-equivalent to $\mathbf{F}$), we have then

$$\sum_h \theta_{1k}(h^{-1})\mathbf{F}(h)\mathbf{x}_1 \in \langle \mathbf{U} \rangle.$$

However, $\mathbf{F}(h)\mathbf{x}_1 = \mathbf{X}\boldsymbol{\theta}_1(h) = \sum_m \mathbf{x}_m \theta_{m1}(h)$, so the sum above can be rewritten as

$$\sum_m \left(\sum_h \theta_{1k}(h^{-1})\theta_{m1}(h) \right) \mathbf{x}_m.$$

From the theory of group representations, the inner sum equals $(g/n)\,\delta_{km}$, where δ_{km} is the Kronecker symbol. Thus $(g/n)\mathbf{x}_k$ is contained in $\langle \mathbf{U} \rangle$. Letting k vary, we see $\langle \mathbf{U} \rangle$ contains all columns of $(g/n)\mathbf{X}$, hence $\langle \mathbf{U} \rangle \supset \langle (g/n)\mathbf{X} \rangle$. However, $\langle \mathbf{X} \rangle = \langle \mathbf{I} \rangle$, which gives the result sought.

A further technical simplification in constructing the G-invariant lattices $\langle \mathbf{U} \rangle$, is provided by the primary decomposition for finite abelian groups, as follows.

LEMMA 4. *Suppose $m = p_1^{a_1} \cdots p_r^{a_r}$ is the factorization of $m = g/n$ in powers of distinct primes, and set $q_i = m/p_i^{a_i}$. Then the G-invariant lattices $\langle \mathbf{U} \rangle$ with $\langle \mathbf{I} \rangle \supset \langle \mathbf{U} \rangle \supset \langle m\mathbf{I} \rangle$, are precisely the $\langle \mathbf{U} \rangle = \sum_1^r q_i \langle \mathbf{U}_i \rangle$, where for each i, $\langle \mathbf{U}_i \rangle$ denotes a G-invariant lattice such that $\langle \mathbf{I} \rangle \supset \langle \mathbf{U}_i \rangle \supset \langle p^{a_i}\mathbf{I} \rangle$.*

Proof. As $\langle m\mathbf{I} \rangle$ is a G-invariant sublattice of $\langle \mathbf{I} \rangle$, there is a natural module action of G on the difference lattice $\langle \mathbf{I} \rangle - \langle m\mathbf{I} \rangle$, making $\langle \mathbf{U} \rangle - \langle m\mathbf{I} \rangle$ a G-submodule. We have

$$\langle \mathbf{I} \rangle - \langle m\mathbf{I} \rangle = \sum_i q_i(\langle \mathbf{I} \rangle - \langle m\mathbf{I} \rangle) = \sum_i \langle q_i\mathbf{I} \rangle - \langle m\mathbf{I} \rangle$$

for the primary decomposition of $\langle \mathbf{I} \rangle - \langle m\mathbf{I} \rangle$. Let the decomposition of the subgroup $\langle \mathbf{U} \rangle - \langle m\mathbf{I} \rangle$ be $\sum_i \langle \mathbf{V}_i \rangle - \langle m\mathbf{I} \rangle$, where $\langle q_i\mathbf{I} \rangle \supset \langle \mathbf{V}_i \rangle \supset \langle m\mathbf{I} \rangle$.

Then the $\langle \mathbf{V}_i \rangle$ must be G-invariant. For G, acting as a group of automorphisms of $\langle \mathbf{U} \rangle - \langle m\mathbf{I} \rangle$, must fix the primary components $\langle \mathbf{V}_i \rangle - \langle m\mathbf{I} \rangle$ (these being characteristic subgroups). Setting $\mathbf{U}_i = q_i^{-1}\mathbf{V}_i$, we conclude that

$$\langle \mathbf{U} \rangle = \sum_i q_i \langle \mathbf{U}_i \rangle \quad \text{where } \langle \mathbf{I} \rangle \supset \langle \mathbf{U}_i \rangle \supset \langle p_i^{a_i}\mathbf{I} \rangle$$

and $\langle \mathbf{U}_i \rangle$ is G-invariant. Conversely, every such $\langle \mathbf{U} \rangle$ is clearly an invariant lattice lying over $\langle m\mathbf{I} \rangle$.

We proceed to consider the quadratic forms associated with our representations.

LEMMA 5. *The transformations* $\mathbf{x} \to \mathbf{F}(h)\mathbf{x}$, $h \in G$, *are automorphisms of a positive quadratic form* $\mathbf{x}^T\mathbf{H}\mathbf{x}$ ($\mathbf{H}$ *symmetric*), *uniquely determined to within a constant factor.*

Proof. The real quadratic form $\sum_h |\mathbf{F}(h)\mathbf{x}|^2 = \mathbf{x}^T\mathbf{H}_1\mathbf{x}$ is clearly fixed by the above transformations. As the sum of positive definite forms, it is itself positive definite, hence nondegenerate. If $\mathbf{x}^T\mathbf{H}_2\mathbf{x}$ is a second real invariant quadratic (possibly degenerate), then for all $h \in G$, we have

$$\begin{aligned}(\mathbf{H}_1^{-1}\mathbf{H}_2)\mathbf{F}(h) &= \mathbf{H}_1^{-1}(\mathbf{F}(h)^T)^{-1}\mathbf{H}_2\\ &= (\mathbf{F}(h)^T\mathbf{H}_1)^{-1}\mathbf{H}_2\\ &= (\mathbf{H}_1\mathbf{F}(h)^{-1})^{-1}\mathbf{H}_2\\ &= \mathbf{F}(h)(\mathbf{H}_1^{-1}\mathbf{H}_2).\end{aligned}$$

Thus $\mathbf{H}_2$ is a constant multiple of $\mathbf{H}_1$, by Schur's Lemma.

LEMMA 6. *The quadratic invariant for* $\mathbf{\Phi} = \mathbf{U}^{-1}\mathbf{F}\mathbf{U}$ *has matrix* $\mathbf{U}^T\mathbf{H}\mathbf{U}$, *where* $\mathbf{H}$ *is the matrix of the form fixed by* $\mathbf{F}$.

The proof is an easy exercise. In particular, the quadratic forms associated with $\mathbf{Z}$-equivalent representations (rationally equivalent to $\mathbf{F}$) are seen to be equivalent forms.

Finally, we remark that the last two lemmas clearly continue to hold without the assumption that $\mathbf{F}$ be integral. ("Automorphisms" must in this case be interpreted as meaning "rational" automorphisms of the invariant form.)

3. The Representations $\mathbf{F}_n^d$

Define the matrices $\mathbf{E}^{ij}$ (or $\mathbf{E}^{i,j}$) by $E_{kl}^{ij} = \delta_{ik}\delta_{jl}$, for $1 \leq k, l \leq n$. Multiplication is given by $\mathbf{E}^{ij}\mathbf{E}^{st} = \delta_{js}\mathbf{E}^{it}$. This notation allows us to avoid space-consuming matrix displays; however, the reader will find it worthwhile to reconstruct these (say for $n = 3, 4$). Undefined matrices like $\mathbf{E}^{0,1}$ are zero.

We borrow from A. Young's representation theory of the symmetric group, the fact that S_{n+1} has an absolutely irreducible $\mathbf{Q}$-representation $\mathbf{P}_n$ of degree n, given by

$$\mathbf{P}_n(k\ k+1) + \mathbf{I}_n = \frac{k-1}{k}\mathbf{E}^{k-1,k-1} + \left(1 - \frac{1}{k^2}\right)\mathbf{E}^{k-1,k} + \mathbf{E}^{k,k-1} + \frac{k+1}{k}\mathbf{E}^{kk}, \qquad 1 \le k \le n.$$

Specifically, $\mathbf{P}_n$ is the "rational seminormal" representation corresponding to the partition $(2, 1^{n-1})$ of $n+1$. (See [2, Theorem 5.6, p. 131], [6, Fundamental Theorem, p. 38].) Recall that the adjacent transpositions $(k \quad k+1)$ serve to generate S_{n+1}. The multiplication of permutations is taken to be such that, for example, $(12)(23) = (123)$.

Our starting point in the present section will be the $\mathbf{Z}$-representation $\mathbf{F}_n$ obtained from $\mathbf{P}_n$ as follows. Set

$$\mathbf{X} = \mathbf{I}_n + \sum_1^{n-1} \frac{i}{i+1}\mathbf{E}^{i,i+1}.$$

We claim $\mathbf{X}^{-1}\mathbf{P}_n\mathbf{X} = \mathbf{F}_n$, where (for $1 \le k \le n$)

$$\mathbf{F}_n(k\ k+1) + \mathbf{I}_n = \mathbf{E}^{k,k-1} + 2\mathbf{E}^{kk} + \mathbf{E}^{k,k+1}.$$

For clearly, $\det \mathbf{X} = 1$, while an easy calculation gives

$$(\mathbf{P}_n(k\ k+1) + \mathbf{I}_n)\mathbf{X} = \mathbf{X}(\mathbf{F}_n(k\ k+1) + \mathbf{I}_n),$$

the common value of the two sides being

$$\frac{k-1}{k}(\mathbf{E}^{k-1,k-1} + 2\mathbf{E}^{k-1,k} + \mathbf{E}^{k-1,k+1}) + (\mathbf{E}^{k,k-1} + 2\mathbf{E}^{kk} + \mathbf{E}^{k,k+1}).$$

For a positive integer d, define the matrix $\mathbf{U}_n(d)$ by

$$\mathbf{U}_n(d) = \sum_1^{n-1} (d\mathbf{E}^{ii} + (-1)^{n-i+1} i\mathbf{E}^{in}) + \mathbf{E}^{nn}.$$

Our aim in the present section is to establish:

THEOREM. *The* $\mathbf{F}_n^d = \mathbf{U}_n(d)^{-1}\mathbf{F}_n\mathbf{U}_n(d)$ *for* $d \mid n+1$ *are* $\mathbf{Z}$*-inequivalent* $\mathbf{Z}$*-representations of* S_{n+1}, *and give all classes of integral representations rationally equivalent to* $\mathbf{F}_n$.

The $\mathbf{Z}$-representations $\mathbf{Q}$-equivalent to $\mathbf{F}_n$ will be determined by finding the S_{n+1}-invariant lattices $\langle \mathbf{U}_n \rangle$ lying over $\langle m\mathbf{I}_n \rangle$, where $m = (n+1)!/n = p_1^{a_1} \cdots p_r^{a_r}$. We first determine those lying over $\langle p^a \mathbf{I}_n \rangle$, where p is any prime and

$a > 0$. Since $\langle \mathbf{U}_n \rangle = \langle \mathbf{U}_n \mathbf{W} \rangle$ for any unimodular $\mathbf{W}$, we can suppose that $u_{ii} > 0$ for all i, and $u_{ij} = 0$ for $i > j$. Hence $\mathbf{U}_n$ may be partitioned as

$$\mathbf{U}_n = \begin{bmatrix} \mathbf{U}^*_{n-1} & \mathbf{v} \\ 0 & u_{nn} \end{bmatrix},$$

where $\mathbf{U}^*_{n-1}$ has the same specifications.

Inspection of $\mathbf{F}_n$ above, shows that for $1 \leq k < n$,

$$\mathbf{F}_n(k\ k+1) = \begin{bmatrix} \mathbf{F}_{n-1}(k\ k+1) & \mathbf{f}(k\ k+1) \\ 0 & -1 \end{bmatrix}.$$

Here, $\mathbf{f}(k\ k+1)$ equals $\mathbf{e}_{n-1}$ if $k = n-1$, and is zero otherwise. Hence for $k < n$, and for suitable vectors $\mathbf{w}(k\ k+1)$,

$$\mathbf{F}_n(k\ k+1)\mathbf{U}_n = \begin{bmatrix} \mathbf{F}_{n-1}(k\ k+1)\mathbf{U}^*_{n-1} & \mathbf{w}(k\ k+1) \\ 0 & -u_{nn} \end{bmatrix}.$$

Using the rule provided by the corollary to Lemma 2, we conclude:

LEMMA 7. *The submatrix* $\mathbf{U}^*_{n-1}$ *has the property that* $\langle \mathbf{U}^*_{n-1} \rangle$ *is an* S_n-*invariant lattice over* $\langle p^a \mathbf{I}_{n-1} \rangle$.

We immediately have:

COROLLARY. $\mathbf{U}^*_{n-1}$ *is a multiple of some* $\mathbf{U}_{n-1}$. (*Note that the matrices* $\mathbf{U}_{n-1}$ *are constrained by* (1), *which* $\mathbf{U}^*_{n-1}$ *will not in general satisfy.*)

Clearly, $\mathbf{F}_n(k\ k+1)\mathbf{U}_n$ has columns in $\langle \mathbf{U}_n \rangle$ *iff* $(\mathbf{F}_n(k\ k+1) + \mathbf{I}_n)\mathbf{U}_n$ has. The latter equals

$$(\mathbf{E}^{k,k-1} + 2\mathbf{E}^{kk} + \mathbf{E}^{k,k+1}) \sum_{i,j} u_{ij}\mathbf{E}^{ij} = \sum_j (u_{k-1,j} + 2u_{kj} + u_{k+1,j})\mathbf{E}^{kj}. \quad (2)$$

Hence, for $1 \leq j, k \leq n$, we have

$$u_{k-1,j} + 2u_{kj} + u_{k+1,j} \equiv 0 \pmod{u_{kk}}. \quad (3)$$

LEMMA 8. $\mathbf{U}_n$ *has the property that* $u_{ij} \equiv 0 \pmod{u_{nn}}$, $1 \leq i, j \leq n$.

Proof. Suppose inductively, that every $\mathbf{U}_{n-1}$ (normalized as described above) has this property. By the preceding corollary, this implies with regard to $\mathbf{U}_n$ that

$$u_{ij} \equiv 0 \pmod{u_{n-1,n-1}}, \quad 1 \leq i, j \leq n-1.$$

Next, set $j = k - 1$ in (3). Recalling that $\mathbf{U}_n$ is upper-triangular, we get $u_{k-1,k-1} \equiv 0 \pmod{u_{kk}}$. Hence with u_{nn} as the modulus of the remaining congruences, all $u_{kk} \equiv 0$. For $j = n$, (3) therefore implies

$$u_{k-1,n} + 2u_{kn} + u_{k+1,n} \equiv 0.$$

Letting k run through the values 2, 3, . . . , n in reverse order, we conclude that all $u_{kn} \equiv 0$.

The relations $u_{n-1,n-1} \equiv 0$, $u_{kn} \equiv 0$ thus established are sufficient to prove the claim in the case $n = 2$. This provides a base for the induction. The same relations then combine with the inductive hypothesis to give the result for larger values of n.

COROLLARY. *The coefficient u_{nn} is* 1. (This follows from the lemma by (1).)

Example. It is now a simple matter to determine all possibilities for

$$\mathbf{U}_2 = \begin{bmatrix} u_{11} & u_{12} \\ 0 & 1 \end{bmatrix}.$$

The lattice $\langle \mathbf{U}_2 \rangle$ is to contain the columns of the matrices given by (2), for $k = 1, 2$. The second columns of these matrices (from the terms for $j = 2$) are

$$\begin{bmatrix} 2u_{12} + 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 \\ u_{12} + 2 \end{bmatrix}.$$

The requirement that $\langle \mathbf{U}_2 \rangle$ should contain these is expressed by the conditions

$$2u_{12} + 1 \equiv 0,$$
$$u_{12}(u_{12} + 2) \equiv 0,$$

where congruences are modulo u_{11}. Multiplying the second congruence by 2 and using the first, we conclude that $u_{12} \equiv -2$. Substitution in the first then gives $3 \equiv 0$. Hence $\langle \mathbf{U}_2 \rangle = \langle \mathbf{U}(d) \rangle$ for $d = 1$ or 3, as stated in the introduction. (Taken in conjunction with Lemma 11 below, this also proves the theorem in the case $n = 2$.)

LEMMA 9. *Let $\langle \mathbf{U}_n \rangle$ be invariant over $\langle p^a \mathbf{I}_n \rangle$, and let* G.C.D. $(u_{ij}) = 1$. *Then $\langle \mathbf{U}_n \rangle = \langle \mathbf{U}_n(p^b) \rangle$ for some b $(a \geq b \geq 0)$ such that $p^b \mid n + 1$.*

Proof. The case $n = 2$ having been worked as an example, assume the statement correct with $n - 1$ in place of n. Notice that when p does not divide $n + 1$, $p^b \mid n + 1$ is possible only for $b = 0$, in which case we have $\langle \mathbf{U}_n(p^b) \rangle = \langle \mathbf{I}_n \rangle$.

(i) Suppose $p \nmid n$ $(= (n - 1) + 1)$. Thus $\langle \mathbf{U}^*_{n-1} \rangle = \langle p^b \mathbf{I}_{n-1} \rangle$, where $a \geq b \geq 0$. Congruences being modulo p^b, (3) gives

$$u_{k-1,n} + 2u_{kn} + u_{k+1,n} \equiv 0 \quad \text{for } 1 \leq k \leq n - 1.$$

These may be solved, to yield

$$u_{k+1,n} \equiv (-1)^k (k + 1) u_{1n}. \tag{4}$$

In particular, $u_{n-1,n} \equiv (-1)^{n-2}(n - 1)u_{1n}$ and

$$1 \equiv (-1)^{n-1} n u_{1n}, \tag{5}$$

so

$$u_{1n} \equiv (-1)^{n-1}(u_{n-1,n} + 1). \tag{6}$$

Setting $k = n$ in (2) and selecting the term corresponding to $j = n$, we see $\langle \mathbf{U}_n \rangle$ must contain $(u_{n-1,n} + 2)\mathbf{e}_n$. This implies that $u_{jn}(u_{n-1,n} + 2) \equiv 0$ for $j < n$, and so $u_{1n}(u_{n-1,n} + 2) \equiv 0$. Multiplying by n and using (5), we conclude that $u_{n-1,n} \equiv -2$. Therefore $u_{1n} \equiv (-1)^n$, by (6), and (5) now gives $n + 1 \equiv 0$. That is, $p^b \mid n + 1$. Using (4), we then obtain $\mathbf{v} \equiv \mathbf{v}_{n-1} \pmod{p^b}$, where

$$\begin{bmatrix} \mathbf{v}_{n-1} \\ 1 \end{bmatrix} = \mathbf{u}, \text{ say,} \tag{7}$$

is the last column of all the matrices $\mathbf{U}_n(d)$.

(ii) Suppose $p \mid n$. By the inductive hypothesis, $\langle \mathbf{U}^*_{n-1} \rangle$ equals

$$p^{b-c}\langle \mathbf{U}_{n-1}(p^c) \rangle,$$

for some b, c where $a \geq b \geq c \geq 0$. As before (cf. (5)), we obtain

$$(-1)^{n-1} n u_{1n} \equiv 1 \pmod{p^{b-c}}.$$

This implies G.C.D. $(n, p^{b-c}) = 1$, which is impossible for $b > c$. So $\langle \mathbf{U}^*_{n-1} \rangle = \langle \mathbf{U}_{n-1}(p^c) \rangle$. In particular, $u_{n-1,n-1} = 1$, hence we may assume $u_{n-1,n} = 0$. Set $k = n$ in (2), and take the term given by $j = n - 1$. We see $\langle \mathbf{U}_n \rangle$ contains $\mathbf{e}_n$, which (as $u_{n-1,n} = 0$) requires that $u_{n-2,n} \equiv 0 \pmod{p^c}$. Finally, set $k = n - 1$ in (2) and take the term given by $j = n$. We find that $\langle \mathbf{U}_n \rangle$ contains $(u_{n-2,n} + 1)\mathbf{e}_{n-1}$, so $(u_{n-2,n} + 1)\mathbf{v}_{n-2} \equiv \mathbf{0} \pmod{p^c}$. Combined with the preceding congruence, this implies $\mathbf{v}_{n-2} \equiv \mathbf{0}$, hence $1 \equiv 0 \pmod{p^c}$. In other words, $\langle \mathbf{U}_n \rangle = \langle \mathbf{I}_n \rangle$.

LEMMA 10. *Let $\langle \mathbf{U}_n \rangle$ be invariant over $\langle m\mathbf{I}_n \rangle$, where* G.C.D. $(u_{ij}) = 1$ *and* $m = (n + 1)!/n$. *Then $\langle \mathbf{U}_n \rangle = \langle \mathbf{U}_n(d) \rangle$ for some $d \geq 1$ such that $d \mid n + 1$.*

Proof. By Lemma 4, we have

$$\langle \mathbf{U}_n \rangle = \sum_1^r q_i \langle p_i^{b_i - c_i} \mathbf{U}_n(p_i^{c_i}) \rangle$$

for some b_i, c_i, where $a_i \geq b_i \geq c_i \geq 0$ and $p_i^{c_i} \mid n + 1$. The sum of several sublattices of $\langle \mathbf{I}_n \rangle$ is simply the sublattice generated by the union of their generators, in this case the columns of the matrices $q_i p_i^{b_i - c_i} \mathbf{U}_n(p_i^{c_i})$.

Now these have as their jth columns, the vectors $q_i p_i^{b_i} \mathbf{e}_j$ for $j < n$, and $q_i p_i^{b_i - c_i} \mathbf{u}$ for $j = n$. (See (7).) We have

$$\text{G.C.D. } (q_i p_i^{b_i - c_i}) = \prod p_i^{b_i - c_i} = t, \text{ say,}$$

and

$$\text{G.C.D. } (q_i p_i^{b_i}) = \prod p_i^{b_i} = td,$$

where $d = \prod p_i^{c_i}$. Hence reduction to a basis gives $\langle \mathbf{U}_n \rangle = t \langle \mathbf{U}_n(d) \rangle$. Then $t =$ G.C.D. $(u_{ij}) = 1$, while d is a divisor of $n + 1$.

COROLLARY. *Every* $\langle \mathbf{U}_n(d)\rangle$ *for which* $d \mid n+1$ *is indeed invariant over* $\langle m\mathbf{I}\rangle$.

Proof. Requiring $\langle \mathbf{U}_n(d)\rangle$ to contain the columns of

$$(\mathbf{E}^{k,k-1} + 2\mathbf{E}^{kk} + \mathbf{E}^{k,k+1})\mathbf{U}_n(d) \quad \text{for } 1 \le k \le n-2$$

imposes no restraints on d. For $k = n-1$ and $k = n$, the matrices are respectively

$$d\mathbf{E}^{n-1,n-2} + 2d\mathbf{E}^{n-1,n-1} + (n+1)\mathbf{E}^{n-1,n} \quad \text{and} \quad d\mathbf{E}^{n,n-1} + (n+1)\mathbf{E}^{nn}.$$

LEMMA 11. *Suppose, for divisors* d_1, d_2 *of* $n+1$, *the representations* $\mathbf{F}_n^{d_1}$, $\mathbf{F}_n^{d_2}$ *are* $\mathbf{Z}$*-equivalent. Then* $d_1 = d_2$.

Proof. Applying Lemma 1, we obtain $\mathbf{U}_n(d_1) = \mathbf{U}_n(d_2)\mathbf{W}$, for a unimodular matrix $\mathbf{W}$. Now compare determinants.

This completes the proof of the theorem.

4. The forms A_n^d

Let $\overline{\mathbf{A}}_n$ denote the symmetric, tri-diagonal matrix

$$\sum_1^n (\mathbf{E}^{i,i-1} + 2\mathbf{E}^{ii} + \mathbf{E}^{i,i+1}).$$

It is easily verified that $\mathbf{x}^T\overline{\mathbf{A}}_n\mathbf{x}$ gives the quadratic invariant for $\mathbf{F}_n$. (Alternatively,

$$\mathbf{x}^T\left(\sum \frac{i+1}{i}\mathbf{E}^{ii}\right)\mathbf{x}$$

is the quadratic for $\mathbf{P}_n$. The matrix $\overline{\mathbf{A}}_n$ may then be computed as prescribed in Lemma 6.) By Lemma 6, the form fixed under $\mathbf{F}_n^d$ has matrix $\mathbf{U}_n(d)^T\overline{\mathbf{A}}_n\mathbf{U}_n(d)$. Dropping the scalar factor d^2, we get the (tri-diagonal) matrix

$$\overline{\mathbf{A}}_n^d = \begin{bmatrix} \overline{\mathbf{A}}_{n-1} & q\mathbf{e}_{n-1} \\ q\mathbf{e}_{n-1}^T & nq/d \end{bmatrix},$$

where $q = (n+1)/d$.

In order to recognize the above, set

$$\mathbf{X}_1 = \sum_1^n (-1)^{i-1}\mathbf{E}^{ii}, \quad \mathbf{X}_2 = I_n + \sum_1^q (q-i)\mathbf{E}^{n-i,n}, \quad \mathbf{X}_3 = \sum_1^{n-1} \mathbf{E}^{i,n-i} + \mathbf{E}^{nn}.$$

Then $\mathbf{x} \to (\mathbf{X}_1\mathbf{X}_2\mathbf{X}_3)\mathbf{x}$ is an equivalence transformation which carries the form $\frac{1}{2}\mathbf{x}^T\overline{\mathbf{A}}_n^d\mathbf{x}$ into

$$x_1^2 - x_1x_2 + x_2^2 - x_2x_3 + \cdots + x_{n-1}^2 - x_qx_n + \tfrac{1}{2}q(1-d^{-1})x_n^2,$$

provided $d \neq 1$. This, however, is just A_n^d in the notation of [3]. When $d = 1$, the last two terms above must be replaced by $+x_{n-1}x_n + x_n^2$. Changing the sign of the last variable x_n then produces the known form A_n of [3].

Appendix 1

The forms A_n^d were given a separate treatment by Barnes [1]. In order to relate this to the present work, set $\mathbf{X}' = \sum_{i\le j} (-1)^i \mathbf{E}^{ij}$. Thus

$$\mathbf{X}'^{-1} = \sum_i (-1)^i(\mathbf{E}^{ii} + \mathbf{E}^{i,i+1}),$$

and $\mathbf{F}_n' = \mathbf{X}'^{-1}\mathbf{F}_n\mathbf{X}'$ is $\mathbf{Z}$-equivalent to $\mathbf{F}_n$. Corresponding to the divisor d of $n + 1$, the lattice $\langle \mathbf{U}_n'(d)\rangle$ is found to be invariant, where

$$\mathbf{U}_n'(d) = d \sum_1^{n-1} \mathbf{E}^{ii} + \sum_1^n \mathbf{E}^{in}.$$

In fact, the $\mathbf{Z}$-representations $\mathbf{Q}$-equivalent to $\mathbf{F}_n'$ are the

$$\mathbf{F}_n^d = (\mathbf{X}'^{-1}\mathbf{U}_n(d))^{-1}\mathbf{F}_n'(\mathbf{X}'^{-1}\mathbf{U}_n(d)),$$

and when $\mathbf{X}'^{-1}\mathbf{U}_n(d)$ is computed, it is easily seen to be column-equivalent to $\mathbf{U}_n'(d)$.

The matrix defining the quadratic invariant for $\mathbf{F}_n'$ is

$$\mathbf{X}'^T\overline{\mathbf{A}}_n\mathbf{X}' = \mathbf{I}_n + \sum_{i,j} \mathbf{E}^{ij}.$$

That for $\mathbf{U}_n'(d)^{-1}\mathbf{F}_n'\mathbf{U}_n'(d)$ is accordingly

$$\mathbf{U}_n'(d)^T \left(\mathbf{I}_n + \sum_{i,j} \mathbf{E}^{ij}\right) \mathbf{U}_n'(d),$$

which may now be compared with the following definition (cf. [1, p. 69]): A_n^t is the form $\sum_1^n x_i^2 + (\sum_1^n x_i)^2$ with lattice the integer sublattice given by $x_1 \equiv \cdots \equiv x_n \pmod t$.

Appendix 2

S_{n+1} has a second irreducible $\mathbf{Q}$-representation of degree n, $\mathbf{P}_n^*$ say, which is inequivalent to $\mathbf{P}_n$. This is the rational, seminormal representation associated with $(n, 1)$ (the partition conjugate to $(2, 1^{n-1})$) and given by

$$\mathbf{P}_n^*(k\ k + 1) - \mathbf{I}_n = -\frac{k+1}{k}\mathbf{E}^{k'k'} + \left(1 - \frac{1}{k^2}\right)\mathbf{E}^{k',k'+1} + \mathbf{E}^{k'+1,k'} - \frac{k-1}{k}\mathbf{E}^{k'+1,k'+1},$$

where $k' = n - k + 1$. Our purpose is to deduce the classes of $\mathbf{Z}$-representations $\mathbf{Q}$-equivalent to $\mathbf{P}_n^*$ from the corresponding results (obtained above) for $\mathbf{P}_n$.

Set

$$\mathbf{Y} = \mathbf{I}_n - \sum_1^{n-1} \frac{n-i}{n-i+1}\mathbf{E}^{i,i+1},$$

$$\mathbf{F}_n^*(k\ k + 1) - \mathbf{I}_n = \mathbf{E}^{k'-1,k'} - 2\mathbf{E}^{k'k'} + \mathbf{E}^{k'+1,k'}.$$

Then

$$\mathbf{Y}(\mathbf{P}_n^*(k\ k+1) - \mathbf{I}_n) = (\mathbf{F}_n^*(k\ k+1) - \mathbf{I}_n)\mathbf{Y}, \quad \det \mathbf{Y} = 1,$$

so $\mathbf{F}_n^* = \mathbf{Y}\mathbf{P}_n^*\mathbf{Y}^{-1}$ is a **Z**-representation **Q**-equivalent to $\mathbf{P}_n^*$.

Next, let $\boldsymbol{\phi}_n$ stand for the first-degree representation affording the alternating character: $\boldsymbol{\phi}_n(k\ k+1) = -1$ for $1 \leq k \leq n$. (In Young's theory, $\boldsymbol{\phi}_n$ arises as the rational, seminormal representation for the partition (1^{n+1}).) We define the representation $\mathbf{F}_n^{\bullet}$ by $\mathbf{F}_n^{\bullet} = \mathbf{F}_n^* \otimes \boldsymbol{\phi}_n$, with $\otimes$ denoting the Kronecker product of matrices. Note that $\phi_n \otimes \phi_n$ is simply the trivial representation (affording the principal character), whence also $\mathbf{F}_n^* = \mathbf{F}_n^{\bullet} \otimes \boldsymbol{\phi}_n$.

LEMMA 12. *The mappings*

$$\mathbf{X}^{-1}\mathbf{F}_n^*\mathbf{X} \to \mathbf{X}^{-1}\mathbf{F}_n^*\mathbf{X} \otimes \boldsymbol{\phi}_n, \quad \mathbf{X}^{-1}\mathbf{F}_n^{\bullet}\mathbf{X} \to \mathbf{X}^{-1}\mathbf{F}_n^{\bullet}\mathbf{X} \otimes \boldsymbol{\phi}_n,$$

are mutually inverse, and give a one-to-one correspondence between the **Z**-*representations of* S_{n+1} *rationally equivalent to* $\mathbf{F}_n^*$ *and those rationally equivalent to* $\mathbf{F}_n^{\bullet}$.

Proof. In fact, $\mathbf{X}^{-1}\mathbf{F}_n^*\mathbf{X} \otimes \boldsymbol{\phi}_n = \mathbf{X}^{-1}\mathbf{F}_n^{\bullet}\mathbf{X}$.

It follows from the lemma that $\mathbf{F}_n^*$ has the same number of classes of **Z**-representations as $\mathbf{F}_n^{\bullet}$. But the same remains true with $\mathbf{F}_n$ in place of $\mathbf{F}_n^{\bullet}$. For, setting

$$\mathbf{Y}^{\bullet} = \sum_1^n (-1)^{i-1}(\mathbf{E}^{i,n-i} + 2\mathbf{E}^{i,n-i+1} + \mathbf{E}^{i,n-i+2}),$$

we find that $\det \mathbf{Y}^{\bullet} = n + 1$, and

$$\mathbf{Y}^{\bullet}(\mathbf{F}_n(k\ k+1) + \mathbf{I}_n) = (\mathbf{F}_n^{\bullet}(k\ k+1) + \mathbf{I}_n)\mathbf{Y}^{\bullet}.$$

That is, $\mathbf{F}_n^{\bullet}$ is **Q**-equivalent to $\mathbf{F}_n$. It remains only to check that for each $d \mid n + 1$, an invariant lattice is determined by the columns of the matrix

$$\mathbf{V}_n(d) = d\mathbf{E}^{11} + \sum_2^n (\mathbf{E}^{ii} + (n - i + 1)\mathbf{E}^{1i}).$$

The details are left to the reader.

The invariant quadratic for $\mathbf{P}_n^*$ is

$$\mathbf{x}^T\left(\sum_1^n \frac{n - i + 1}{n - i + 2}\mathbf{E}^{ii}\right)\mathbf{x},$$

hence that for $\mathbf{F}_n^*$ is $\mathbf{x}^T\mathbf{H}_n\mathbf{x}$, where

$$\mathbf{H}_n^{-1} = \mathbf{Y}\left(\sum_1^n \frac{n - i + 2}{n - i + 1}\mathbf{E}^{ii}\right)\mathbf{Y}^T = \sum_1^n (-\mathbf{E}^{i,i-1} + 2\mathbf{E}^{ii} - \mathbf{E}^{i,i+1}).$$

(Equivalently, one may check $\mathbf{F}_n^*(k\ k+1)\mathbf{H}_n^{-1}\mathbf{F}_n^*(k\ k+1)^T = \mathbf{H}_n^{-1}$. Note that all $\mathbf{F}_n^*(k\ k+1)$ are self-inverse.) The invariant for $\mathbf{V}_n(d)^{-1}\mathbf{F}_n^*\mathbf{V}_n(d)$ is also most easily recognized from its reciprocal, which is equivalent to A_n^d. The form itself is therefore equivalent to A_n^q, where $qd = n + 1$.

Acknowledgments

It is a pleasure to record my great indebtedness to Professor G. E. Wall, who supplied the ideas assembled in the Preliminaries. This work formed part of a master's thesis prepared under his guidance. Thanks are due also to Professors H. S. M. Coxeter and D. J. Lewis for their helpful comments at a later date. Professor Coxeter kindly drew attention to the fact that for certain of the forms, such as A_8^3, the group of automorphisms is distinctly larger than the corresponding symmetric group, in this case S_9.

Financial support in the form of a Senior Postgraduate Studentship was generously provided by the C.S.I.R.O.

BIBLIOGRAPHY

1. E. S. Barnes, *The construction of perfect and extreme forms I*, Acta Arith., vol. V (1958), pp. 57–79.
2. H. Boerner, *Representations of groups*, North Holland, Amsterdam, 1970.
3. H. S. M. Coxeter, *Extreme forms*, Canad. J. Math., vol. 3 (1951), pp. 391–441.
4. M. Craig, M.Sc. Thesis, University of Sydney, 1968.
5. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics Series, vol. XI, Interscience, New York, 1962.
6. G. de B. Robinson, *Representation theory of the symmetric group*, Univ. of Toronto Press, Toronto, 1961.

State University of New York at Buffalo
Buffalo, New York