THE INDECOMPOSABLES OF RANK 3 PERMUTATION MODULES

Thesis by
Michael Robert Lewy

In Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California

1985
(Submitted May 22,1985)

ACKNOWLEDGMENTS

My advisor, Professor David Wales, originally suggested the problem of determining what the rank 3 restrictions on the centralizer algebra tell about the projections of the permutation module, noticing that one can write an explicit expression for the projections. He patiently supervised the research, and corrected a number of errors. It is hard to overstate his contribution to this work. It is a pleasure to thank him. I would also like to thank Professor Michael Aschbacher for help in preparing the table.

Boris Hasselblatt, Ivo Klemes, and Kris Odencrantz have been helpful in reviewing the readability of the thesis, and Chi Fai Ho helped with computer consistency-checking of some of the table. Mario Blaum has been a continuing source of encouragement to me in group theory, and I remember with gratitude the many patient, personal explanations of group theory I received from Professor Jack Hayden when he was visiting at Caltech some years ago. None of the above should be held responsible for any errors occurring, however.

I am happy to thank Lillian Chappelle for a fine typing job.

Caltech, and through it the National Science Foundation and the College Work Study Program, have kindly provided support for me while I have been a graduate student.

My parents, Helen and Hans Lewy, have shown through countless acts such solicitude for my well-being and good cheer that it is quite difficult to thank them properly. Many friends have shown me their kindness and given me their encouragement; Alvin Joran will have to stand for many. Last but not least, I would like to thank Lynne Jackson and Mike Palter, whose music and consciously positive spirits buoyed me--an evening with them often starting with glumness, and ending with a smile and a renewed vision of the beauty which really does exist in this world.

ABSTRACT

Transitive permutation groups of finite order are viewed as linear groups over fields of characteristic $p > 0$ by having the group permute the basis elements of a vector space M. The decomposition of M into the direct sum of invariant subspaces is investigated, and criteria given for whether M is decomposable, and if it is, how many direct summands occur, in the special case the group has rank 3, i.e., it has 3 orbits on ordered pairs of points. In the case that each orbit is self-paired, M decomposes into the maximum possible number of indecomposables, and the group has every p'-element conjugate to its inverse, irreducibility results are obtained for the indecomposables. This last result holds for any rank. It applies in particular to the symmetric and thence to the alternating groups, which enables us to describe certain modular irreducibles of these groups.

TABLE OF CONTENTS

I. DIRECT SUM DECOMPOSITIONS

1.INTRODUCTION

Let G be a group consisting of permutations of a finite set Ω of $n > 1$ points. If $\omega \in \Omega$, we write ω^g for the image under $g \in G$ of the point $\omega \in \Omega$. We assume throughout that given two points $\omega_1, \omega_2 \in \Omega$, there is a $g \in G$ such that $\omega_1{}^g = \omega_2$, i.e., that G is transitive.* If we let G act on $\Omega \times \Omega$ by setting $(\omega_1, \omega_2)^g = (\omega_1{}^g, \omega_2{}^g)$, we partition $\Omega \times \Omega$ into orbits. The number of such orbits on $\Omega \times \Omega$ is called the *rank* of G. Notice that $D = \{(\omega, \omega): \omega \in \Omega\}$ is always an orbit of Ω. Thus there are always at least 2 orbits on $\Omega \times \Omega$. When the number of these orbits is in fact 2, G is called doubly- or 2-transitive. If $L \subseteq \Omega \times \Omega$ is an orbit under G, then $\bar{L} = \{(\omega_1, \omega_2) \in \Omega \times \Omega: (\omega_2, \omega_1) \in L\}$ is also an orbit. If $L = \bar{L}$, L is said to be *self-paired*.

Our interest, in the present work, is to study the *permutation module* M over a field F of characteristic

---

(*) One may study the case where G is intransitive by looking at the constituent transitive actions on its orbits.

$p > 0$. To construct M, let the points of Ω be linearly independent generators of a vector space M over F, which will then have the same dimension over F as Ω has elements; i.e., $n = |\Omega|$. Here the bars indicate cardinality. To complete the definition of M, the action of G on M is given as follows:

$$\Big(\sum_{\omega\in\Omega} \alpha_\omega \omega\Big)^g = \sum_{\omega\in\Omega} \alpha_\omega \omega^g, \text{ where } \alpha_\omega \in F.$$

In this work we investigate in the rank 3 case whether M can be written as a direct sum of G-invariant subspaces, and, in case it can, how many direct summands it has. One might initially suspect that the answer to these questions could only be obtained by an elaborately detailed consideration of the permutation representation, perhaps together with a study of the internal structure of the group itself. Actually, we show that--at least in the rank 3 case--the answer as to how the permutation module decomposes can be obtained by knowing only certain combinatorial parameters, which were previously introduced by D.G. Higman [4]. (The rank 2 case is well known and easy.) These parameters describe the cardinalities of various sets obtained from the orbits of G on ordered pairs of points, and will be defined in the next section. The proof proceeds by using the fact that projections must be linear combinations of 3 known matrices, as the rank is

3. By explicit calculations with these known matrices, which involve only combinatorial properties, all possible projections are determined, and thus the decomposition properties of M are established.

As is well-known, in case the characteristic divides the order of the group, it may happen that a submodule cannot be split up as a direct sum of invariant subspaces, but it may possess an invariant subspace which is not a direct summand, there being no complementary *invariant* subspace. So we may wonder whether the indecomposables we obtain are actually irreducible. In the case of the symmetric and alternating groups, we obtain a result on this, thereby showing the irreducibility of certain modular representations of these groups. How can the study of rank 3 representations provide a demonstration of the irreducibility of certain representations? The secrets here are the limited centralizer algebra dimension and the self-duality of symmetric group representations.

Rank 3 groups are actually very common, and we shall provide tables for the convenience of the reader with which one can determine the decomposition of the permutation modules for many cases which have been reported in the literature.

2. PRELIMINARIES

The *centralizer algebra* C is defined to be the algebra of all linear maps c of M into itself which commute with the action of G, i.e., such that $c \circ g = g \circ c$, for all $g \in G$, where g is viewed here as a linear map on M. The centralizer algebra C is spanned by the linearly independent matrices $\{A_T\}_{T \subseteq \Omega \times \Omega \text{ a G-orbit}}$, where

$$(A_T)_{ij} = \begin{cases} 1, & \text{if } (i,j) \in t \\ 0, & \text{otherwise} \end{cases}$$

and thus C has the same dimension as the rank of G (see I. Schur [10] or H. Wielandt [11]).

DECOMPOSITIONS AND PROJECTIONS

The principal topic of investigation in this work is the decomposition of the permutation module M into the direct sum of submodules which cannot themselves be decomposed. However, we find it easier to conduct the computations using *projections*. A linear map $P \in C$ is called a projection when $P^2 = P$. Of course 1, the identity map on M, is always a projection, as is 0, the map sending everything to 0. In general, if P is a projection, 1 - P is too.

Suppose $M = M_1 \oplus M_2 \oplus \cdots \oplus M_t$, where the M_i are submodules of M. We obtain t projections π_i by considering the map that sends $m \in M$ to m_i, where m_i is defined by the unique expression $m = m_1 + m_2 + \cdots + m_t$, each $m_j \in M_j$. These *canonical projections* satisfy (1) $\pi_i\pi_j = \delta_{ij}\pi_i$ and (2) $1 = \pi_1 + \cdots + \pi_t$, where $\delta_{ij} = \begin{Bmatrix} 1, & \text{if } i = j \\ 0, & \text{otherwise} \end{Bmatrix}$. Notice that we can recover the M_i from the π_i: $M_i = M\pi_i$. Conversely, suppose we start with a family $\{\pi_i\}_{i=1}^{t}$ satisfying the above conditions (1) and (2). Define $M_i = M\pi_i$. Now $M = M_1 \oplus \cdots \oplus M_t$, the sum being M by property (2); it is direct because $m_1 + \cdots \oplus + m_t = 0$, with all $m_j \in M_j$, implies $m_1\pi_i + \cdots + m_t\pi_i = 0$. Since $m_j = m_j\pi_j$, property (2) gives $m_j = 0$. Finally, note that $\pi_i = 0$ is equivalent to $M_i = 0$.

Now M always has the 1-dimensional submodule $\mathcal{S} = \langle \sum_{\omega\in\Omega} \omega \rangle$, and C always has the map $\sum_{\omega\in\Omega} \alpha_\omega \omega \mapsto \sum_{\omega\in\Omega} (\sum_{\tau\in\Omega} \alpha_\tau)\omega$. Now we notice that G acts on M by maps which are orthogonal with respect to the inner product

$(\sum_{\omega\in\Omega} \alpha_\omega \omega, \sum_{\omega\in\Omega} \beta_\omega \omega) = \sum_{\omega\in\Omega} \alpha_\omega \beta_\omega$. Thus the perpendicular space

$T^\perp$ of a submodule T of M is also a submodule. In particular, $\mathcal{S}^\perp$ is always a submodule of M.

Now if $p \nmid n$, $M = \mathcal{S} \oplus \mathcal{S}^{\perp}$, as $\sum_{\omega \in \Omega} \notin \mathcal{S}^{\perp}$, since $n = \sum_{\omega \in \Omega} 1 \neq 0$ in F.

In the case $p \mid n$, $\mathcal{S}$ is never a direct summand of M. For suppose $M = \mathcal{S} \oplus S$. Then $S^{\perp} \cong S^{\perp}/M^{\perp} \cong (M/S)^{*} \cong \mathcal{S}^{*} \cong \mathcal{S}$, where the * indicates the dual module (for a discussion of dual modules, see Huppert and Blackburn [6]). Since G is transitive on Ω, all fixed vectors are mutually proportional. Thus $S^{\perp} = \mathcal{S}$, so $S = \mathcal{S}^{\perp}$. But $\mathcal{S} \subseteq \mathcal{S}^{\perp}$, as $n = 0$ in F.

Now let $r = \mathrm{rank}(G)$. In the case where n is invertible in F and $M = M_1 \oplus M_2 \oplus \cdots \oplus M_r$, where the $M_i \neq 0$, or where $n = 0$ in F and $M = M_1 \oplus \cdots \oplus M_{r-1}$, the $M_i \neq 0$, we say M *decomposes fully*.

3. SOLUTION OF RANK 2 CASE--A PREVIEW OF RANK 3

As an example we can now easily solve the decomposition problem for rank 2 groups. (For more on the rank 2 case, including the question of reducibility of direct summands, see Mortimer [9], and the work of M. Klemm and L. L. Scott referred to therein.) Let's suppose we have a projection P so that $1 = P + (1 - P)$ provides a decomposition of M. Since $P \in \mathcal{C}$, $P = \alpha I + \beta J$, where I is the identity, J the all 1's matrix, and P is viewed as a matrix by considering the basis formed by the points of Ω. The above equation holds for some $\alpha, \beta \in F$, as I and J are linearly independent and $\mathcal{C}$ is 2-dimensional by the fact that G has rank 2. Now $P^2 = (\alpha I + \beta J)^2 = \alpha^2 I + (2\alpha\beta + n\beta^2)J$. The condition $P^2 = P$ becomes

$$\begin{cases} \alpha = \alpha^2 \\ \beta = 2\alpha\beta + n\beta^2 \end{cases}$$

so the solutions are

$$\begin{cases} \alpha = 0, \ \beta = 0 \\ \alpha = 0, \ \beta = 1/n, \text{ if } n \not\equiv 0 (\text{mod } p) \\ \alpha = 1, \ \beta = 0 \\ \alpha = 1, \ \beta = -1/n, \text{ if } n \not\equiv 0 (\text{mod } p) \end{cases}, \text{ i.e.,}$$

$$P = \begin{cases} 0, \ \frac{1}{n}J, \ I, \ I - \frac{1}{n}J, \text{ if } n \neq 0 \text{ in } F \\ 0, \ I, \text{ if } n = 0 \text{ in } F \end{cases}.$$

But in the latter case the decomposition is trivial; in the former the images of $\frac{1}{n}J$, $I - \frac{1}{n}J$ are $\mathcal{S}$ and $\mathcal{S}^{\perp}$, respectively. Thus we see that:

If G *has rank* 2,

(1) M is decomposable if and only if $n \not\equiv 0 \pmod p$;

(2) If M does decompose, there are exactly 2 indecomposable summands, and there are no other nontrivial proper submodules which are direct summands.

4. D.G. HIGMAN'S COMBINATORIAL PARAMETERS FOR A RANK 3 GROUP

Suppose now that G has rank 3. Let G act on $\Omega \times \Omega$. Let G_ω, the stabilizer of ω, act on $\{\omega\} \times \Omega$. Since G has rank 3, we know $\{\omega\} \times \Omega$ partitions into 3 orbits. (By transitivity of G on Ω, each orbit in $\Omega \times \Omega$ contains an ordered pair (ω,τ), $\tau \in \Omega$, and thus a G_ω orbit in $\{\omega\} \times \Omega$. Conversely, if we start with a G_ω-orbit K in $\{\omega\} \times \Omega$, we get a G-orbit in $\Omega \times \Omega$, which contains no new (ω,τ) that weren't in K.) Call the 3 orbits

$$\{\omega\},\ \Delta(\omega),\ \Gamma(\omega).$$

Here we choose the notation so that $\Delta(\omega^g) = \Delta(\omega)^g$, $\Gamma(\omega^g) = \Gamma(\omega)^g$. Higman's parameters are defined by

$$n = |\Omega|$$

$$k = |\Delta(\omega)|$$

$$l = |\Gamma(\omega)|$$

$$|\Delta(\omega) \cap \Delta(\tau)| = \begin{Bmatrix} \lambda, \text{ if } \tau \in \Delta(\omega) \\ \mu, \text{ if } \tau \in \Gamma(\omega) \end{Bmatrix}$$

$$d = (\lambda - \mu)^2 + 4(k - \mu).$$

Notice that λ and μ are well-defined, as G_ω is transitive on $\Delta(\omega)$ and $\Gamma(\omega)$, so the choice of τ does not matter.

5. STATEMENT OF DECOMPOSITION THEOREM FOR RANK 3

<u>Theorem 1</u>. Let G be a rank 3 permutation group of degree n and even order. Let p be a prime and F a field of characteristic $p > 0$. Let M be the corresponding permutation module of G over F. Then

(1) If $p | n$, M is decomposable if and only if $d \not\equiv 0 \pmod p$. In case decomposition occurs, there are exactly 2 indecomposable summands, and there are no other nontrivial, proper direct summands of M;

(2) If $p \nmid n$, write $M = \mathcal{S} \oplus \mathcal{S}^{\perp}$.

(i) If $p \neq 2$, $\mathcal{S}^{\perp}$ is decomposable if and only if $d \not\equiv 0 \pmod p$ and $\sqrt{d} \in F$;

(ii) If $p = 2$, and F contains a 3rd root of unity other than 1, $\mathcal{S}^{\perp}$ is decomposable if and only if $d \not\equiv 0 \pmod p$;

(iii) If $p = 2$, and F contains no 3rd root of unity other than 1, $\mathcal{S}^{\perp}$ is decomposable if and only if $d \not\equiv 0$ and $\mu \equiv 0 \pmod p$.

In case $\mathcal{S}^{\perp}$ decomposes, it has exactly 2 indecomposable summands, and there are no other nontrivial, proper direct summands of $\mathcal{S}^{\perp}$.

If $\mathcal{S}^{\perp}$ decomposes for $F \supseteq GF(p)$, but not for $GF(p)$, i.e., when $p \neq 2$, $d \equiv 0 (\mathrm{mod}\ p)$, $\sqrt{d} \in F$, $\sqrt{d} \notin GF(p)$, or $p = 2$, $\mu \equiv d \equiv 1 (\mathrm{mod}\ 2)$, F containing a 3rd root of unity other than 1, let $\mathcal{S}^{\perp} = K_1 \oplus K_2$. Then K_1 and K_2 are algebraically conjugate under the automorphism $x \mapsto x^p$ of $GF(p^2)$.

Remark 1. Notice that just as the congruence of n mod p determined decomposition for the rank 2 case, the congruence of n and d determine the decomposition in the rank 3 case, except possibly for the case where certain algebraic equations are insoluble in F (for the odd order case, see the Appendix).

Remark 2. By the result of Guralnick and Wales [2], we can compute the degrees of the indecomposables, as follows. If the irreducible complex constituents have degrees 1, f_2, f_3, the degrees of the indecomposables over an algebraically closed field of characteristic p are sums of these. If $p \nmid n$, the degrees are 1, f_2, f_3, if $p \nmid d$, and 1, $f_2 + f_3$ if $p | d$. If $p | n$, they are $n = 1 + f_2 + f_3$, if $p | d$, and $1 + f_2$, f_3 or $1 + f_3$, f_2, if $p \nmid d$. The latter choice is made by determining whether $1 + f_2$ or $1 + f_3$ is divisible by p.

We prepare for the proof by listing some results we shall need from D.G. Higman [4]. Note that $n = 1 + k + l$.

In the following,

$$A_{ij} = \begin{Bmatrix} 1, & \text{if } i \in \Delta(j) \\ 0, & \text{otherwise} \end{Bmatrix}$$

and all occurrences of the symbol $\equiv$ will mean that arithmetic is being carried out modulo p.

(a) $\mu l = k(k - \lambda - 1)$

(b) A has exactly k 1's in each row and in each column; the other entries are 0;

(c) $A^2 = kI + \lambda A + \mu(J - I - A)$

$= (k - \mu)I + \mu J + (\lambda - \mu)A;$

(d) A is symmetric;

(e) I,A,J form a basis of C;

(f) d is a square in $\mathbb{Z}$ and $\sqrt{d} \mid [2k+(\lambda-\mu)(n-1)]$, except possibly when $k = 1$, $\mu = \lambda + 1 = k/2$.

(The above for $|G|$ even)

<u>Lemma 1</u>. Let $n \equiv 0$. Then $\lambda - \mu \equiv 2k$ if and only if $d \equiv 0$.

Proof. (1) Suppose $\lambda - \mu \equiv 2k$. Then

$d = (\lambda - \mu)^2 + 4(k - \mu) \equiv 4k^2 + 4k - 4\mu = 4[k(k+1) - \mu]$.

Recalling (a), $\mu l = k(k - \lambda - 1)$, and noting that

$l \equiv -k - 1$ (as $n \equiv 0$), we get

$-\mu(k + 1) \equiv k[k - (2k+\mu) - 1]$. Thus

$-\mu \equiv -k^2 - k = -k(k + 1)$. Therefore, $d \equiv 0$.

(2) Suppose $d \equiv 0$. By (f), $\sqrt{d} \mid [2k+(\lambda-\mu)(n-1)]$, so

$2k + (\lambda - \mu)(-1) \equiv 0$, unless $k = 1$, $\mu = \lambda + 1 = k/2$. In

the latter case, $\lambda - \mu \equiv 2k$ holds if and only if $-1 \equiv 2k$;

i.e., $n \equiv 0$, which holds by hypothesis. q.e.d.

Lemma 2. If $n \equiv 0$, d is a quadratic residue modulo p.

Proof. By (f), d is a square in $\mathbb{Z}$, hence also mod p,

unless we fall into the case $k = 1$, $\mu = \lambda + 1 = k/2$. In

this case, $d = (\lambda - \mu)^2 + 4(k - \mu) = (-1)^2 + 4(k - k/2) =$

$1 + 2k = n \equiv 0^2$. q.e.d.

Lemma 3. Let $p = 2$, $d \not\equiv 0$. Then $k \equiv \mu(n - 1)$.

Proof. As $d = (\lambda - \mu)^2 + 4(k - \mu) \equiv (\lambda - \mu)^2$, $\lambda - \mu \equiv 1$.

By (a), $k(k - \lambda - 1) = \mu l$, so $k(k - \mu) \equiv \mu(n - k - 1)$.

Cancelling the $k\mu$-terms, $k \equiv k^2 \equiv \mu(n - 1)$. q.e.d.

6. PROOF OF DECOMPOSITION THEOREM

As in the rank 2 case, we notice that any projection P is in the centralizer algebra C, which is--according to (e)--spanned by I, J, and A. Thus

$$P = \alpha I + \beta J + \gamma A, \quad P^2 = P, \quad \alpha, \beta, \gamma \in F.$$

Conversely, if P is a linear combination of I, J, and A, and $P^2 = P$, then P is a projection. The equation $P^2 = P$ gives

$$P^2 = (\alpha I + \beta J + \gamma A)^2 = [\alpha^2 + \gamma^2(k-\mu)]I + [\beta^2 n + \gamma^2\mu + 2\alpha\beta + 2\beta\gamma k]J + [\gamma^2(\lambda-\mu) + 2\alpha\gamma]A,$$

using $J^2 = nJ$ and the expressions for AJ, JA, and A^2 given in (b) and (c). Linear independence of I, J, A (result (e)) now turns the condition $P^2 = P$ into the system

$$(1) \qquad \begin{cases} \alpha = \alpha^2 + \gamma^2(k - \mu) \\ \beta = \beta^2 n + \gamma^2\mu + 2\alpha\beta + 2\beta\gamma k, \\ \gamma = \gamma^2(\lambda - \mu) + 2\alpha\gamma \end{cases}$$

which must be solved for $\alpha, \beta, \gamma \in F$.

We must first investigate what happens when $\gamma = 0$. In this case, (1) is equivalent to

$$(2) \qquad \begin{cases} \alpha = \alpha^2 \\ \beta = \beta^2 n + 2\alpha\beta \end{cases} .$$

Thus $\alpha = 0$ or 1. If $\alpha = 0$, the second equation of (2) becomes $\beta(\beta n - 1) = 0$. We then get the solutions $\beta = 0$, and $\beta = 1/n$ (if $n \not\equiv 0$). If $\alpha = 1$, the second equation of (2) becomes $\beta(\beta n + 1) = 0$, so $\beta = 0$, or $-1/n$ (if $n \not\equiv 0$). Thus the projections which are linear combinations of I and J alone are 0 and I, if $n \equiv 0$, and 0, I, $(1/n)J$, $I - (1/n)J$, if $n \not\equiv 0$.

Suppose, then, that we are looking for solutions in which $\gamma \neq 0$. Dividing the third equation of (1) by γ, we get

$$(3) \qquad \begin{cases} \alpha = \alpha^2 + \gamma^2(k - \mu) \\ \beta = \beta^2 n + \gamma^2\mu + 2\alpha\beta + 2\beta\gamma k \\ 1 = \gamma(\lambda - \mu) + 2\alpha . \end{cases}$$

Notice that we may immediately solve for γ, as follows. Write the third equation of (3) as $1 - 2\alpha = \gamma(\lambda - \mu)$ and square both sides. Now add 4 times the first equation of (3), to get
$(1 - 2\alpha)^2 + 4\alpha = \gamma^2(\lambda - \mu)^2 + 4\alpha^2 + 4\gamma^2(k - \mu)$. Thus

$1 = \gamma^2 d$. In this way we see that necessary conditions for the existence of a projection which is not a linear combination of I and J are that $d \equiv 0$, and that $\sqrt{d} \in F$. We are forced to restrict ourselves to the case $\gamma = 1/\sqrt{d}$ (if $\gamma = -1/\sqrt{d}$, change that notation so that the negative square root is meant by $\sqrt{d}$). Thus (3) is equivalent to

$$(4) \qquad \begin{cases} 0 = \alpha^2 - \alpha + \frac{k-\mu}{d} \\ \beta = \beta^2 n + \frac{\mu}{d} + 2\alpha\beta + 2\beta\frac{k}{\sqrt{d}} \\ 2\alpha = 1 - \frac{\lambda-\mu}{\sqrt{d}} \\ \gamma = \frac{1}{\sqrt{d}} \end{cases} .$$

By this system being equivalent to (3) we mean that for $\alpha,\beta,\gamma \in F$, (α,β,γ) satisfies (3) if and only if it satisfies (4). We also assume that all the symbols in the equations are defined, in order to say that a system is satisfied; in particular, denominators are not 0 and square roots shown exist in F.

Suppose first that $p \neq 2$.

Substituting for α in the 1st and 2nd equations of (4), we find that the 1st equation is satisfied automatically given the 3rd, and (4) is equivalent to

$$(5)\qquad \begin{cases} 0 = n\beta^2 - \dfrac{\lambda-\mu-2k}{\sqrt{d}}\,\beta + \dfrac{\mu}{d} \\ \alpha = \frac{1}{2}\left(1 - \dfrac{\lambda-\mu}{\sqrt{d}}\right) \\ \gamma = \dfrac{1}{\sqrt{d}} \end{cases} .$$

If $p \mid n$, we obtain, using Lemma 1,

$$(6)\qquad \begin{cases} \alpha = \frac{1}{2}\left(1 - \dfrac{\lambda-\mu}{\sqrt{d}}\right) \\ \beta = \dfrac{\mu}{(\lambda-\mu-2k)\sqrt{d}} \\ \gamma = \dfrac{1}{\sqrt{d}} \end{cases} .$$

If $p \nmid n$, we obtain

$$(7)\qquad \begin{cases} \alpha = \frac{1}{2}\left(1 - \dfrac{\lambda-\mu}{\sqrt{d}}\right) \\ \beta = \dfrac{\lambda-\mu-2k}{2n\sqrt{d}} \pm \dfrac{1}{2n} \\ \gamma = \dfrac{1}{\sqrt{d}} \end{cases} . \qquad (p \neq 2)$$

Here the second equation of (7) is obtained by solving the first of (5), simplifying using (a). The $\pm$ is chosen independently of the choice of the sign for $\sqrt{d}$.

We turn now to the case where $p = 2$. Then (4) is equivalent to

$$(8) \qquad \begin{cases} 0 = \alpha^2 + \alpha + \frac{k-\mu}{d} \\ 0 = n\beta^2 + \frac{\lambda-\mu}{\sqrt{d}}\beta + \frac{\mu}{d} \\ \gamma = \frac{1}{\sqrt{d}} \end{cases} .$$

If (8) has a solution, then $d \equiv 1 \pmod 2$, for otherwise $\sqrt{d}$ is not invertible. Thus (8) is equivalent to

$$(9) \qquad \begin{cases} 0 = \alpha^2 + \alpha + \frac{k-\mu}{d} \\ 0 = n\beta^2 + \beta + \frac{\mu}{d} \\ \gamma = 1 \\ d \not\equiv 0 \end{cases} .$$

We now get in case $2|n$, using Lemma 3 to show $k - \mu \equiv 0$,

$$(10) \qquad \begin{cases} \alpha = 0 \text{ or } 1 \\ \beta = \frac{\mu}{d} \\ \gamma = 1 \\ d \not\equiv 0 \end{cases} \qquad (p = 2)$$

whilst in case $2 \nmid n$, again using Lemma 3, we get

$$(11) \qquad \begin{cases} 0 = \alpha^2 + \alpha + \mu \\ 0 = \beta^2 + \beta + \mu \\ \gamma = 1 \\ d \not\equiv 0 \end{cases} \qquad (p = 2) .$$

If $F \supseteq GF(4)$, then we always find 4 solutions to (11), viz.

$$\begin{cases} \text{in case } \mu \equiv 0, \ \alpha = 0 \text{ or } 1, \ \beta = 0 \text{ or } 1, \ \gamma = 1 \\ \text{in case } \mu \equiv 1, \ \alpha = \varepsilon \text{ or } \varepsilon^2, \ \beta = \varepsilon \text{ or } \varepsilon^2, \ \gamma = 1 \end{cases},$$

where $\varepsilon^2 + \varepsilon + 1 = 0$, and the choices for α and β are made independently.

If $F \not\supseteq GF(4)$, there is no solution to (11) if $\mu \equiv 1$; as before, there are 4 solutions, $\alpha = 0$ or 1, $\beta = 0$ or 1, $\gamma = 1$, if $\mu \equiv 0$.

Reviewing the solutions we have obtained, we find that in case $p|n$, there is a projection (other than 0 or 1) if and only if $d \not\equiv 0$, and in the case that $d \not\equiv 0$, there are exactly two projections besides 0 and 1. Thus in this case the direct summands are unique.

Examine now the case $p\nmid n$, $p > 2$. We now know that $d \equiv 0$ or $\sqrt{d} \notin F$ implies that the only projections are 0, I, $\frac{1}{n}J$, $I - \frac{1}{n}J$. Conversely, $d \not\equiv 0$ and $\sqrt{d} \in F$ guarantees that there are additional projections, according to (7). In the latter case we show that $\mathcal{S}^{\perp}$ is decomposable, by looking at $P = \frac{1}{2}(1 - \frac{\lambda-\mu}{\sqrt{d}})I + (\frac{\lambda-\mu-2k}{2n\sqrt{d}} - \frac{1}{2n})J + \frac{1}{\sqrt{d}}A$, a solution to (7). Direct calculation shows $PJ = JP = 0$. Since $I - \frac{1}{n}J = (I - \frac{1}{n}J - P) + P$ and

$(I - \frac{1}{n}J - P)P = P(I - \frac{1}{n}J - P) = 0$, $\mathcal{S}^{\perp}$ is decomposable. If we write $\mathcal{S}^{\perp} = K_1 \oplus K_2$, where $K_1, K_2 \neq 0$, then we see that we have accounted for 8 projections of $M = \mathcal{S} \oplus K_1 \oplus K_2$ by adding together the various canonical projections. But we have already seen that there are at most 8 solutions to equations (1), when $p \nmid n$: $0, I, \frac{1}{n}J, I - \frac{1}{n}J$ for $\gamma = 0$, and 4 solutions to (7). Since any direct summand must have a corresponding projection, and we have listed all projections, there can be no unlisted direct summands.

Finally, we consider the case $p \nmid n$, $p = 2$, $d \not\equiv 0$. If ε satisfies $\varepsilon^2 + \varepsilon + \mu = 0$, and $\varepsilon \in F$, then $\mathcal{S}^{\perp}$ decomposes. As when $p > 2$, we check that $PJ = JP = 0$ for $P = \varepsilon I + \varepsilon J + A$. For $PJ = JP = (n\varepsilon + \varepsilon + k)J = kJ$, and Lemma 3 gives $k \equiv \mu(1 - 1) = 0$. Again we find $\mathcal{S}^{\perp} = K_1 \oplus K_2$ decomposes, and we have exhausted all possibilities for projections.

As to the algebraic conjugacy of K_1 and K_2, in case $\mathcal{S}^{\perp}$ is decomposable over F but not over $GF(p)$, we just note that I, J, and A have entries in $GF(p)$, so by algebraic conjugation the canonical projection onto K_1 becomes another projection P', and $P \neq P'$ since the coefficients of I, J, and A in the expression for P are not all in $GF(p)$. Now the relations $PJ = JP = 0$ carry over to P': $JP' = P'J = 0$. Thus the image of P' must be K_1 or K_2, since these are the only indecomposable direct summands contained in $\mathcal{S}^{\perp}$, and the image of P' must be indecomposable, as that of P was. But $P \neq P'$ shows, from our knowledge that each projection is the sum of canonical ones onto $\mathcal{S}$, K_1, and K_2, respectively, that the image of P is one of $\{K_1, K_2\}$ and that of P' the other.   q.e.d.

II. IRREDUCIBILITY OF CERTAIN INDECOMPOSABLES

Lemma (I. Schur). Let G be a transitive permutation group of rank r. Then the centralizer algebra has dimension r, and has basis $\{E_\Phi\}_\Phi$, where Φ runs over the different orbits of G on ordered pairs, and

$$(E_\Phi)_{ij} = \begin{cases} 1, & \text{if } (i,j) \in \Phi \\ 0, & \text{otherwise} \end{cases}$$

Proof. Clearly the centralizer algebra is an algebra. Now the equation $Ag = gA$ says that $a_{i,(j)\sigma} = a_{(i)\sigma^{-1},j}$, where σ is the permutation g induces on the columns of A, when $A \mapsto Ag$, and a_{ij} is the (i,j)-entry of A. Thus $a_{(\alpha)\sigma,(j)\sigma} = a_{\alpha,j}$, letting $i = (\alpha)\sigma$. Thus our condition says simply that the (i,j)- and (i',j')-entries are the same if they lie in the same orbit of G on ordered pairs. The lemma now follows. q.e.d.

Proposition 1. Let G be a finite permutation group which is transitive on the n points $\Omega = \{1,2,\ldots,n\}$, and suppose that the rank is r. Let M be the corresponding permutation module over a field of characteristic p. Write $M = M_1 \oplus \cdots \oplus M_t$, where the M_i are indecomposable submodules. Then if $p \mid n$, $t \leq r - 1$; if $p \nmid n$, $t \leq r$ (in case equality holds, we say M *decomposes fully*). There is one and only one M_i containing a non-zero vector fixed by all $g \in G$. Renumber to call it M_1. If M decomposes fully, M_2, M_3, ..., M_t have scalar centralizer algebras (which will also be true of M_1, if $p \nmid n$), and if $p \nmid n$ there is no other way than

$M = M_1 \oplus M_2 \oplus \cdots \oplus M_r$ to write M as a sum of indecomposable submodules.

Note. The fact that there can be only one indecomposable in a direct decomposition which contains a vector fixed by all $g \in G$ is a well known consequence of transitivity of G; the submodule is then known as a Scott module. The fact that there can be no more than r direct summands in a decomposition can also be obtained by the result of Guralnick and Wales [2]. For more on Scott modules in general, see Burry [1].

Proof. Let P_i be the canonical projections of $M \to M_i$, which will be FG-endomorphisms of M. Then $\lambda_1 P_1 + \cdots + \lambda_t P_t = 0$ implies that $\lambda_i P_i = 0$, by multiplying through by P_i. Since $P_i \neq 0$, $\lambda_i = 0$. Thus the P_i are linearly independent elements of the centralizer algebra. Thus by Schur's lemma above, $t \leq r$. As to fixed vectors, the transitivity of G certainly implies that they are all multiples of $s = \sum_{\omega \in \Omega} \omega$.

Now write $s = m_1 + \cdots + m_t$, where $m_i \in M_i$. As $sg = s$, for all $g \in G$, $m_i g = m_i$. But then transitivity implies $m_i = \kappa_i s$, for scalars κ_i. If $\kappa_i, \kappa_j \neq 0$, for $i \neq j$, then $M_i \cap M_j \neq 0$. Thus $s \in M_i$, for a unique i, and we renumber so that $i = 1$. We now show that $P_1, \ldots, P_t$, J are linearly independent, in case $p | n$. Here J is the FG-endomorphism determined by the all 1's matrix, for the basis $\{\tau\}_{\tau \in \Omega}$. Suppose that $\lambda_1 P_1 + \cdots + \lambda_t P_t + \lambda_{t+1} J = 0$. Then $\lambda_i P_i = -\lambda_{t+1} J P_i = 0$, if $i \neq 1, t+1$. Thus $\lambda_2 = \cdots = \lambda_t = 0$. Now $\lambda_1 P_1 = -\lambda_{t+1} J P_1$ gives $\lambda_1 P_1 = -\lambda_{t+1} J$, as $s \in M_1$. Thus

$\lambda_1 \neq 0$ implies $M_1 = \langle s \rangle$. Let $C = M_2 + \cdots + M_t$. Now $\langle s \rangle \cong \langle s \rangle^* \cong (M/C)^* \cong C^\perp$. Thus $C^\perp$ is spanned by a fixed vector. Transitivity of G again gives $C^\perp = \langle s \rangle$. Thus $C = \langle s \rangle^\perp$. But $p | n$ implies $s \in \langle s \rangle^\perp$. This contradicts $C \cap \langle s \rangle = 0$. We conclude that λ_1, and hence finally λ_{t+1} are also 0. Thus in the case $p | n$, $t \leq r - 1$.

We turn now to the case when M decomposes fully. If $p \nmid n$, $P_1, \ldots, P_r$ form a basis of the centralizer algebra, so any FG-endomorphism ε of M many be written $\varepsilon = \alpha_1 P_1 + \cdots + \alpha_r P_r$. Thus $\varepsilon^2 = \varepsilon$ implies $\alpha_i^2 = \alpha_i$ (so $\alpha_i = 0$ or 1), for all i. Thus $M = M_1 \oplus \cdots \oplus M_r$ is the only way to write M as a direct sum of indecomposable submodules. Now any FG-endomorphism of M_i becomes, by composition with the canonical injection into and the canonical projection onto M_i, an FG-endomorphism ε of M. Now $\varepsilon P_j = 0$, for $j \neq i$, so we find $\alpha_j = 0$, for $j \neq i$.

If $p \mid n$, $P_1, \ldots, P_{r-1}, J$ form a basis of the centralizer algebra, so write

$$\varepsilon = \alpha_1 P_1 + \cdots + \alpha_{r-1} P_{r-1} + \alpha_r J$$

for the FG-endomorphism of M resulting from composition with the canonical maps of an arbitrary FG-endomorphism of M_i, $i \neq 1$, as before. Since ε maps M into M_i, then $0 = \varepsilon P_1 = \alpha_1 P_1 + \alpha_r J$. Thus $\alpha_1 = \alpha_r = 0$. For $j \neq 1, r, i$, we have $0 = \varepsilon P_j = \alpha_j P_j$, so $\alpha_j = 0$. Thus $\varepsilon = \alpha_i P_i$, and the centralizer algebra of M_i is scalar. q.e.d.

Proposition 2. Let G be a transitive permutation group and M the corresponding permutation module over the field F. Suppose every orbit of G on ordered pairs of points is self-paired. Let $M = M_1 \oplus \cdots \oplus M_t$ be a decomposition into indecomposables. Then the M_i's are mutually orthogonal (with respect to the point-basis standard inner product) and $M_i^* \cong M_i$.

Proof. As usual, let P_i be the canonical projection onto M_i. We have $(vP_i, wP_j) = (vP_i P_j^T, w) = (vP_i P_j, w) = (0, w) = 0$, as $P_j^T = P_j$. This latter is true because, by the above lemma of Schur, the P_i can be written as linear combinations of the E_Φ's, and Φ self-paired means that $E_\Phi = E_\Phi^T$. But an arbitrary element of M_u can be written as

xP_u, for some $x \in M$. Thus the M_i are mutuallly orthogonal. Because $\sum_{j \neq i} M_j \subseteq M_i^{\perp}$, and the dimensions of the two must be the same, $M^{\perp} = \sum_{j \neq i} M_j$. Now

$$M_i^* \cong ((M_i + M_i^{\perp})/M_i^{\perp})^* \cong M_i/(M_i^{\perp} \cap M_i) \cong M_i.$$

q.e.d.

Theorem 2. Let G be a transitive permutation group on Ω, and M the corresponding permutation module over the field F of characteristic $p > 0$. Suppose that M decomposes fully, and that every orbit of G on ordered pairs is self-paired. Let G have the property that every p'-element of G is conjugate to its inverse. If we write $M = M_1 \oplus \cdots \oplus M_t$, with M_i indecomposable, and $s = \sum_{\tau \in \Omega} \tau \in M_1$, then M_2, ..., M_t are *irreducible.*

Remark. The irreducibility of $\mathcal{S}^{\perp}$ in the natural representation for the symmetric group on $u \geqslant 4$ letters, or that for the alternating group on $u \geqslant 5$ letters, has been known since at least Dickson (see Mortimer[9]). Notice also that in the case of Alt(4), the natural representation on 4 points has degree 4, so $\mathcal{S}^{\perp}$ has dimension 3, but the group has no absolutely irreducible representation of degree 3 over characteristic 2, so $\mathcal{S}^{\perp}$ is reducible. In this case the 2-regular element (123) is not conjugate to its inverse, so the hypothesis of the theorem fails. Our results are rarely--if ever--new with regard to these 2-transitive representations, which also occur as constituents of the rank 3 representation on unordered pairs of letters. New results are obtained for the other constituent, however. Results on the irreducibility of $\mathcal{S}^{\perp}$ in the case of various 2-transitive representations, as well as a review of the literature, are to be found in Mortimer [9]. Our results also apply to constituents of higher rank representations, however.

Proof. Suppose first the field F is algebraically closed. By Prop. 1, $M_2, \ldots, M_t$ have scalar centralizer algebras, and by Prop 2, $M_i \cap M_i^{\perp} = 0$ and $M_i^{*} \cong M_i$, for $i = 2, \ldots, t$. By taking any irreducible $S \subseteq M_i$, $S \neq 0$, we notice that $M_i/S^{\perp} \cong S^{*}$, where $\perp$ refers to the usual inner product in the point basis restricted to M_i. Now we show $S \cong S^{*}$. The Brauer character ρ afforded by S is the complex conjugate of that afforded by S^{*}. Now the G-conjugacy of a p'-element g to its inverse will imply that $\rho(g) = \rho(g^{-1}) = \overline{\rho(g)}$. Thus S and S^{*} have the same Brauer character, and must therefore be isomorphic. Now consider $\pi : M_i \rightarrow M_i/S^{\perp}$, the canonical projection, ϕ the isomorphism between $M_i/S^{\perp}$ and S, and the canonical injection $\iota : S \rightarrow M_i$. Then $\pi\phi\iota$ is an FG-endomorphism of M_i, and thus must be scalar. But then $S \neq 0$ gives $S^{\perp} \neq M_i$, so the endomorphism is not 0. Since $\kappa\varphi\iota$ is scalar, $S^{\perp} = 0$, so $S = M_i$. If F is not algebraically closed, extension of the field cannot cause the M_i to further decompose, as already over the original F, M decomposes fully. Furthermore, irreducibility over the algebraic closure of a field F implies *a fortiori* irreducibility over F. Thus our result with algebraically closed F implies the result for unclosed fields as well.

q.e.d.

Corollary. *Let G be the symmetric group on the ν letters of Ω, S_ν, $\nu \geqslant 4$, or the alternating group on ν letters, A_ν, $\nu \geqslant 5$, and let G act on unordered pairs of points. Let $p \nmid \nu - 2$. Let M be the corresponding permutation module over a field F of characteristic $p > 0$, where $F \supseteq GF(p^2)$. Then the indecomposables of M not containing $s = \sum_{\tau \in \Omega} \tau$ are irreducible.*

Proof. By evenness of S_ν's order, the orbits of the 1-point stabilizer in the rank 3 action on unordered pairs are self-paired. By Theorem 1, if $p \nmid d = (\nu - 2)^2$, the permutation module decomposes fully, and by Theorem 2, the indecomposables not containing s are irreducible.

To handle A_ν, notice that if we consider the module M_i for S_ν, the module for A_ν is simply $(M_i)_{A_\nu}$. This is because the Higman parameters are the same, as are the basis matrices I, J, and A. Let T be an A_ν-irreducible submodule of $(M_i)_{A_\nu}$. We now apply Clifford's argument. We have that $\sum_{g\epsilon S_\nu} Tg$ is an S_ν-submodule of M_i; hence by irreducibility of M_i, $\sum_{g\epsilon S_\nu} Tg = M_i$. Now Tg is an irreducible A_ν-submodule. Thus by selecting just some of the g's we get a direct sum $M_i = T_1 \oplus \cdots \oplus T_u$, where the T_i's are A_ν-submodules. But M_i is already known to be A_ν-indecomposable. Thus $M_i = T$.

q.e.d.

III. EXAMPLES

1. Alt(5)

Let the alternating group on 5 points permute the set of all unordered pairs of distinct elements of $\{1,2,3,4,5\}$, using the natural permutation representation on $\{1,2,3,4,5\}$. We have now that

$$\Omega=\{\{1,2\};\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,5\};\\ \{3,4\},\{3,5\},\{4,5\}\},$$

so $n=\binom{5}{2}=10$. Now under the stabilizer of $\{1,2\}$, the pairs after the second semicolon, which are the pairs not intersecting $\{1,2\}$, are permuted among themselves; there are $l=\binom{5-2}{2}=3$ of them. Finally, there are $k=2(5-2)=6$ pairs intersecting $\{1,2\}$. Now we may still wonder whether the group is really rank 3; we have seen so far only that each set of 3 (resp. 6) pairs is mapped into itself; but is the stabilizer of $\{1,2\}$ transitive on each of these sets? If we want to map $\{3,4\}$ to $\{3,5\}$, for example, we may take 3 to 3, 4 to 5, and then see whether the permutation doing this and fixing every other point is even or odd. If it chances to be odd, we multiply it by $(1\ 2)$, which--of course--stabilizes $\{1,2\}$. Since $(4\ 5)$ is odd, the desired element of the stabilizer is $(1\ 2)(4\ 5)$. If we want to show transitivity on the set Δ of pairs intersecting $\{1,2\}$, we may without loss of generality assume that the problem is to map $\{1,3\}$ to $\{1,4\}$. This can be done by $(3\ 4\ 5)$. Thus Alt(5) really is rank 3 on unordered pairs. Notice now that $\Delta(\{1,2\})\cap\Delta(\{1,3\})=\{\{1,4\},\{1,5\},\{2,3\}\}$, so $\lambda=3$, and $\Delta(\{1,2\})\cap\Delta(\{3,4\})=\{\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}$, so $\mu=4$. The two complex irreducibles which occur in the rank 3 representation have degrees $5-1=4$ and $\frac{5(5-3)}{2}=5$ (using the formulas from Higman[4]). We have $d=(3-4)^2+4(6-4)=9=3^2$. Using the result of Guralnick and Wales[2], the fact that the indecomposable direct summand containing $\mathcal{S}$ must have degree divisible by the highest power of the characteristic dividing n, and Theorem 1 of the present work, we see that in

char. 2, $M=6\oplus4$

char. 3, $M=1\oplus9$

char. 5, $M=5\oplus 5$,
where the numbers indicate by the dimensions the indecomposable direct summands of the permutation module M. Notice that since d is a square and $2|n$, there is no dependence of the decomposition on field extension (see Theorem 1).

2. <u>The Hall-Janko Group HJ</u>.
We see from the literature that this group has a rank 3 representation of degree $n=100$, and is of order $2^7.3^3.5^2.7$. We are also given that $k=36, l=63, \lambda=14, \mu=12$. Thus $\sqrt{d}=10$, and again by the formulas found in Higman, the degrees of the complex constituents are 36 and 63. We obtain:

char. 2: $M = 100$

char. 3: $M = 1 \oplus 36 \oplus 63$

char. 5: $M = 100$

char. 7: $M = 1 \oplus 36 \oplus 63$.

By examining the table for the Hall-Janko group in M. Hall and Wales[3], we see that every element of this even order group is conjugate to its inverse, and so by Theorem 2 there are absolutely irreducible representations of degrees 36 and 63 over characteristics 3 and 7.

3. <u>Alt(25)</u>.
Let Alt(25) act on unordered pairs of distinct letters, of which there are $25.24/2=300$. Here $\sqrt{d}=25-2=23$, $f_2=275$, $f_3=24$. Now over characteristic 7, we must have M breaking up as a direct sum of a 1-dimensional, a 24 dimensional, and a 275 dimensional module (full decomposition), by our results and the result of Guralnick and Wales. By Theorem 2, the summands of degree 24 and 275 are *irreducible* (notice that these two representations lie in 7-blocks of defect 3).

APPENDIX

THE ODD ORDER CASE

We have relegated the treatment of the odd order rank 3 case to this appendix. Our notation is the same as before.

Theorem A1. Let G have odd order and permutation rank 3. Let M be the permutation module over the field F of characteristic $p > 0$. Then

(1) If $p \mid n$, M is indecomposable.

(2) Let $p \nmid n$, so $M = \mathcal{S} \oplus \mathcal{S}^{\perp}$.

If $p > 2$, $\mathcal{S}^{\perp}$ is decomposable iff. $\sqrt{-n} \in F$;

if $p = 2$, and $F \supseteq GF(4)$, $\mathcal{S}^{\perp}$ is decomposable;

if $p = 2$, and $F \not\supseteq GF(4)$, then $\mathcal{S}^{\perp}$ is decomposable iff. λ is odd.

Remark. An example is the semidirect product of the multiplicative group of quadratic residues modulo 7 with the additive group of integers modulo 7.

Proof of Theorem. As is well-known, for the odd order case we must have $n = 4\lambda + 3$, $k = 1 = f_2 = f_3 = 2\lambda + 1$, $\mu = \lambda$. This follows from our known relations on the rank 3 parameters, together with the fact that a group of odd order has no real irreducible complex characters. Writing, as before, $P = \alpha I + \beta J + \gamma A$, we find $P^2 = P$ is equivalent to:

$$
\text{(A1)} \qquad \begin{cases} \alpha = \alpha^2 - (\lambda+1)\gamma^2 \\ \beta = n\beta^2 + (\lambda+1)\gamma^2 + 2\alpha\beta + 2(2\lambda+1)\beta\gamma \\ \gamma = -\gamma^2 + 2\alpha\gamma \end{cases} .
$$

Note that to derive these equations, we use that $A + A^T = J - I$, as the two nontrivial orbits of G_ω are paired. As before, we know that for $\gamma = 0$, $P = I$ or $I - \frac{1}{n}J$ (if $p \nmid n$). So for $\gamma \neq 0$, the last equation of (A1) becomes $\gamma = 2\alpha - 1$, so the first equation of (A1) becomes $\alpha = \alpha^2 - (\lambda + 1)(2\alpha - 1)^2$. This gives that $-n\alpha^2 + n\alpha - (\lambda + 1) = 0$. Thus if $p \mid n$, $\lambda \equiv -1$, so $n = 4\lambda + 3 \equiv -1$. This is a contradiction. Thus if a projection other than 1 or 0 exists, $p \nmid n$. This proves (1).

To prove (2), assume first that $p = 2$, $2 \nmid n$. For our $\gamma \neq 0$ solution, we must have

$$
\text{(A2)} \qquad \begin{cases} -n\alpha^2 + n\alpha - (\lambda+1) = 0 \\ \beta = n\beta^2 + (\lambda+1)\gamma^2 \\ \gamma = 2\alpha - 1 \end{cases} ;
$$

i.e.,

$$\text{(A3)} \qquad \begin{cases} \alpha^2 + \alpha + (\lambda+1) = 0 \\ \beta^2 + \beta + (\lambda+1) = 0 \\ \gamma = 1 \end{cases} .$$

If λ is odd, $I - J = [J + A] + [I + A]$ is a decomposition of $I - J$ into two orthogonal, nonzero projections. Thus $\mathcal{S}^{\perp}$ is decomposable.

If λ is even, we have a solution if and only if $F \supseteq GF(4)$. We find that $I - J = [\alpha I + (\alpha+1)J + A] + [(\alpha+1)I + \alpha J + A]$ is a decomposition into orthogonal nonzero projections, where $\alpha^2 + \alpha + 1 = 0$. Thus $\mathcal{S}^{\perp}$ is decomposable.

Having disposed of the characteristic 2 case, we now assume $p > 2$. We find after calculation that

$I - J = [\frac{1}{2}(1+\frac{1}{\sqrt{-n}})I - \frac{1}{2}(\frac{1}{\sqrt{-n}}+\frac{1}{n})J + \frac{1}{\sqrt{-n}}A] + [\frac{1}{2}(1-\frac{1}{\sqrt{-n}})I - \frac{1}{2}(-\frac{1}{\sqrt{-n}}+\frac{1}{n})J - \frac{1}{\sqrt{-n}}A]$ is a decomposition into two orthogonal, nonzero projections, if $\sqrt{-n} \in F$. To see that it is necessary that $\sqrt{-n} \in F$, in order that a solution with $\gamma \neq 0$ exist, we recall that $-n\alpha^2 + n\alpha - (\lambda + 1) = 0$, so the discriminant $-n$ must be a square in F.

q.e.d.

A NOTE ON THE TABLES

In the following tables the author has attempted to list the parameters of some rank 3 representations, together with the number d, so the reader can conveniently apply the Decomposition Theorem to his favorite groups. Unfortunately, the author was not able to check more than an occasional set of parameters, and so the table is really just an incomplete compendium from the literature. Also, the literature the author looked at was sometimes ambiguous as to whether the parameters were obtained from a rank 3 group; sometimes there were misprints, which the author has corrected when he became aware of them. Thus these tables cannot claim originality, certainty, nor completeness. The following references were quite helpful: Liebeck and Saxl [8] and Hubaut [5].

RANK 3 REPRESENTATIONS RELATED TO SPORADIC GROUPS

G	G_ω	n	k	l	λ	μ	$\sqrt{d}$	f_2	f_3
M_{11}	$M_9.2$	55	18	36	9	4	9	10	44
M_{12}	$M_{10}.2$	66	20	45	10	4	10	11	54
M_{22}	$2^4.Alt(6)$	77	16	60	0	4	8	21	55
M_{22}	$Alt(7)$	176	70	105	18	34	20	21	154
M_{23}	$M_{21}.2$	253	42	210	21	6	21	22	230
M_{23}	$2^4.Alt(7)$	253	112	140	36	60	28	22	230
M_{24}	$M_{22}.2$	276	44	231	22	4	22	23	252
$2^{11}.M_{24}$	M_{24}	2048	1288	759	792	840	64	276	1771
M_{24}	$M_{12}.2$	1288	792	495	476	504	44	252	1035
HJ	$G_2(2)$	100	36	63	14	12	10	36	63
HS	M_{22}	100	22	77	0	6	10	22	77
McL	$U_4(3)$	275	162	112	105	81	30	22	252
$G_2(4)$	HJ	416	100	315	36	20	24	65	350
Suz	$G_2(4)$	1782	416	1365	100	96	36	780	1001
Co.2	$U_6(2).2$	2300	1408	891	840	896	72	275	2024
Rudvalis	${}^2F_4(2)$	4060	1755	2304	730	780	80	783	3276
Fi_{22}	$2.U_6(2)$	3510	693	2816	180	126	72	429	3080
Fi_{22}	$\Omega_7(3)$	14080	3159	10920	918	648	288	429	13650
Fi_{23}	$2.Fi_{22}$	31671	3510	28160	693	351	360	782	30888
Fi_{23}	$P\Omega_8^+(3).S_3$	137632	28431	109200	6030	5832	360	30888	106743
Fi_{24}'	Fi_{23}	306936	31671	275264	3510	3240	$432=2^4.3^3$	57477	249458

RANK 3 TOWERS

G	G_ω	n	k	l	λ	μ	$\sqrt{d}$	f_2	f_3
Higman-Sims tower									
M_{22}	2^4A_6	77	60	16	47	45	8	21	55
HS	M_{22}	100	77	22	60	56	10	22	77
McLaughlin tower									
$PSU_4(3)$	$PSL_3(4)$	162	105	56	72	60	18	21	140
McL	$PSU_4(3)$	275	162	112	105	81	30	22	252
Suzuki tower									
$G_2(2) \cong PSU_3(3^2)$	$PSL_3(2) \cong PSL_2(7)$	36	14	21	4	6	6	14	21
HJ	$G_2(2)$	100	36	63	14	12	10	36	63
$G_2(4)$	HJ	416	100	315	36	20	24	65	350
Suz	$G_2(4)$	1782	416	1365	100	96	36	700	1001
Fischer tower									
$PSU_6(2^2)$	$2^9.PSU_4(2^2)$	693	180	512	51	45	24	252	440
Fi_{22}	$PSU_6(2^2)$	3510	693	2816	180	126	72	429	3080
Fi_{23}	$2.Fi_{22}$	31 671	3510	28160	693	351	360	782	30 888
Fi'_{24}	Fi_{23}	306 936	31 671	275 264	3510	3240	432	57477	249 458
Conway tower									
$PSU_6(2^2)$	$PSU_4(3^2)$	1408	840	567	488	520	48	252	1155
Co.2	$2.PSU_6(2^2)$	2300	1408	891	840	896	72	275	2024
Mathieu tower									
M_{24}	$2.M_{12}$	1288	792	495	476	504	44	252	1035
$2^{11}.M_{24}$	M_{24}	2048	1288	759	792	840	64	276	1771

REFERENCES

[1] Burry, D. Scott modules and lower defect groups, Comm. Alg. 10(1982), 1855-1872.

[2] Guralnick, R.M. and Wales, D.B. Subgroups Inducing the Same Permutation Representation II, preprint.

[3] Hall Jr., M. and Wales, D. The simple group of order 604 800. J. Alg. 9(1968), 417-450.

[4] Higman, D.G. Finite permutation groups of rank 3, Math. Zeitschr. 86(1964), 145-156.

[5] Hubaut, Xavier L. Strongly Regular Graphs, Discrete Math 13(1975), 357-381.

[6] Huppert, B. and Blackburn, N. Finite Groups II, Springer Verlag, 1982, Section 8, esp. Lemma 8.3(a).

[7] Liebeck, M.W. Permutation Modules for Rank 3 Unitary Groups, J. Alg. 88(1984), 317-329.

[8] Liebeck, M.W. and Saxl, J. The Finite Primitive Permutation Groups of Rank Three, preprint.

[9] Mortimer, B. The Modular Permutation Representations of the Known Doubly Transitive Groups, Proc. London Math. Soc. (3) 41(1980), 1-20.

[10] Schur, I. Zur Theorie der einfach transitiven Permutationsgruppen. S. B. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 598-623.

[11] Wielandt, H. Finite Permutation Groups, Academic Press, 1964 (Theorem 28.4).