Journal of Pure and Applied Algebra 29 (1983) 1-12
North-Holland

ON THE MODULAR REPRESENTATION OF PERMUTATION GROUPS OF PRIME POWER DEGREE

Prabir BHATTACHARYA
St. Stephen's College, University of Delhi, Delhi 110 007, India

Communicated by H. Bass
Received 8 November 1982

Permutation groups of prime power degree are investigated here through the study of the corresponding group algebra of the set of all functions from the underlying set on which the permutation group acts to a finite field of characteristic p. For the case when the permutation group is of degree p^2 acting on a set consisting of the direct product of two elementary abelian p-groups, the structure of a minimal permutation module is obtained under certain conditions. The proofs do not depend on the recent classification results of finite simple groups.

AMS Subject Classification: Primary 20B20, 20C05, 20C20.

1. Introduction and notation

Let G be a transitive permutation group on a set Ω where $|\Omega| = p^m$, p an odd prime. Let F be a finite field of characteristic p. Then the set

$$F\Omega := \left\{ \sum_{\omega\in\Omega} a_\omega \omega : a_\omega \in F \right\}$$

is a G-module in a natural way. Now $F\Omega$ can be identified with $F^\Omega := \{f : \Omega \to F\}$ by the map $\sum a_\omega \omega \leftrightarrow f$ where $f : \omega \mapsto a_\omega$. The action of G on F is given by $f^g(\omega) = f(\omega g^{-1})$ for $g \in G$ and $\omega \in \Omega$. The set F^Ω is a G-algebra (called the *Wielandt algebra*) under point-wise multiplication and addition of functions. In F^Ω a G-invariant bilinear form is defined by

$$\langle f_1, f_2 \rangle = \sum_{\omega\in\Omega} f_1 f_2(\omega),$$

for all $f_1, f_2 \in F^\Omega$. If U is a G-submodule of F^Ω then $U^\perp$ is also a G-submodule of F^Ω and the correspondence $U \mapsto U^\perp$ is an anti-isomorphism. Let C be the set of all constant functions. By a result of Wielandt ([7], Theorem 14.7), if U is a proper G-submodule of F^Ω then $C \leq U \leq C^\perp$. The G-module $H := C^\perp / C$ is called the *Heart* of the module F^Ω following J.A. Green. The simplicity of the Heart of F^Ω as a G-module is a condition stronger than 2-fold transitivity (cf. [6]). For permutation groups of prime degree the structure of F^Ω is well understood. By a result of

Neumann [5] which is also implicit in Feit [3], if G is an insoluble transitive permutation group of degree p then the heart H is simple as a G-module. An elegant proof of this result is given by Klemm [4]. In this paper we investigate permutation groups of degree p^2 and examine the heart of the corresponding permutation module. By Klemm [4] if G is primitive, $|\Omega| = p^m$, $m \geq 2$, and G contains a transitive cyclic subgroup then the heart of F^Ω is simple. The classification of permutation groups of degree p^2 is given by Wielandt [7] who proved that if G is a transitive permutation group of degree p^2 and H is a Sylow p-subgroup of G then one of the following holds:

(i) $H \lhd G$ and $G \leq \mathrm{AGL}(2, p)$,

(ii) G is imprimitive,

(iii) G contains an imprimitive normal subgroup of index 2,

(iv) G is 2-fold transitive.

This classification does not give any information about 2-fold transitive permutation groups of degree p^2.

Consider a transitive permutation group G of degree p^2. We assume from now onwards that $\Omega = \mathbb{Z}_p \times \mathbb{Z}_p$. By Wielandt ([7], Proposition 17.5) every element f in F^Ω can be written uniquely as a polynomial in two variables x and y where $x^p = x$ and $y^p = y$. Thus

$$F^\Omega \cong \{\textstyle\sum a_{ij} x^i y^j : a_{ij} \in F,\ x^p = x,\ y^p = y\}.$$

If f is a non-zero element of F^Ω of the form $\sum a_{ij} x^i y^j$, then we define the degree of f to be $\max(i+j)$, $0 \leq i, j \leq p-1$ and $a_{ij} \neq 0$. If $f = 0$ then we set degree of f to be $-\infty$. Now define $T_i := \{f \in F^\Omega : \text{degree}(f) < i\}$. Let T be the group of translations on Ω, that is all permutations of the form $f_t : \omega \mapsto \omega + t$ for $\omega, t \in \Omega$. Then clearly each T_i is a T-submodule of F^Ω and we have a filtration

$$T_0 = 0 < T_1 < \cdots < T_{2p-2} < T_{2p-1} = F^\Omega. \tag{1}$$

Here $T_1 = C$, the set of all constant functions of F^Ω and $T_{2p-2} = C^\perp$ and so these two are also G-submodules of F^Ω. Observe that for any i, we have that T_i / T_{i-1} is isomorphic to the module of all homogeneous polynomials over F of degree $i-1$ in the variables x and y with the restriction that $x^p = x$ and $y^p = y$.

Now let U be a minimal, proper G-submodule of F^Ω. By Wielandt [7], Theorem 14.7, one has that

$$C = T_1 < U \leq C^\perp = T_{2p-2}.$$

We want to investigate the 'position' of U with respect to the filtration (1) of the module F^Ω. A natural question is to ask whether U contains T_2 and if not, what is then the structure of U in that case? We prove the following:

Theorem A. *Let G be a primitive permutation group on a set Ω where $\Omega = \mathbb{Z}_p \times \mathbb{Z}_p$ and G contains the set of all translations on Ω. Let F be the field with p elements. Let U be a minimal G-submodule of F^Ω such that U does not contain T_2, the set of* *all polynomials of degree* 1 *in the variables x and y over F where $x^p = x$ and $y^p = y$. Then, after a certain linear change of variables, the module U as an F-vector space has a basis*

$$\{1, u_1(x, y), \dots, u_k(x, y)\}$$

where

$$u_i(x, y) = x^i + c_{i,i-2}x^{i-2}y + \cdots + c_{i,i-2s}x^{1-2s}y^s + \cdots, \tag{2}$$

for $1 \le i \le k$ *such that*

$$c_{i,i-2s} = \binom{i}{2s} \frac{(2s)!}{s!\, 2^s}\,. \tag{3}$$

Further, we have

$$2(p-1)/3 \le k < p - 1. \tag{4}$$

Illustration. We have $u_2 = x^2 + y$, $u_3 = x^3 + 3xy$, $u_4 = x^4 + 6x^2 + 3y^2$. Note that it follows from Theorem A that x^2, for example, does not lie in U: this fact is proved in Lemma 3.2.

The modules $\{T_i\}$ can be thought of as the 'grid-lines' with respect to which we want to investigate the position of a minimal G-submodule U of F.

Definition. The *Height* of $U = \min\{i : U \le T_i\} = h$ (say), and the *Depth* of $U = \max\{i : T_i \le U\} = d$ (say).

Let $V_i := (U \cap T_i)/(U \cap T_{i-1})$, $1 \le i \le p-1$. Then clearly for $i > h$, $V_i = 0$ and for $i \le d$ we have that V_i is the module of homogeneous polynomials of degree $i-1$. We prove:

Theorem B. *With the above notation, we have that* $\dim V_{i+1} \le \dim V_i$, *for* $d < i \le h$.

We have been informed recently by H. Wielandt (private communication) that the module U described in the paragraph just before the statement of Theorem A always contains T_2 if G is assumed to be 2-closed (see [7] for definition) and that this fact appears as Lemma 21.6 in [7]. Finally we mention a conjecture of Neumann [6] that if G is a transitive permutation group of degree p^2, then either the Heart of F^Ω is simple or G is similar to a subgroup of $S_p \operatorname{wr} C_2$ or $\mathrm{AGL}(2, p)$. We have obtained in [2] the lattice diagram of the G-module F^Ω when G is the group $S_p \operatorname{wr} C_2$. The classification of transitive permutation groups of degree p^2 by Wielandt described earlier and the above conjecture of Neumann are somewhat complementary to one another and a proof of the conjecture would immediately lead to another proof of Wielandt's classification theorem as a corollary.

Section 2 gives the proof of Theorem B and Section 3 gives the proof of Theorem

A through a series of results. We mention that our work has relevance in the theory of generalized Reed–Muller codes.

2. Proof of Theorem B

Since each element f in F^{Ω} is a polynomial of the form $\sum a_{ij}x^iy^j$, one can define partial derivatives $\partial f/\partial x$ and $\partial f/\partial y$. By Wielandt [7], Theorem 18.2 a subspace U of F^{Ω} is a T-module if and only if for f in F^{Ω} we have that both $\partial f/\partial x$, $\partial f/\partial y$ lie in U. To prove Theorem B is is enough to prove:

Lemma 2.1. *Let U be a proper G-submodule of F^{Ω}. Then for $1 \leq r \leq 2p-2$, we have that if* $\dim V_r \leq t < \dim(T_r/T_{r-1}) = r-1$, *then* $\dim V_{r+1} \leq t$.

Proof. Let H_r denote the space of homogeneous polynomials of degree r. Then we have that V_r is isomorphic to a submodule of H_{r-1}. Let D_x, D_y denote partial differentiation operations with respect to x and y respectively. Then $\mathrm{D}_x : H_r \to H_{r-1}$ and $\mathrm{D}_y : H_r \to H_{r-1}$ and we know that U is closed under the linear maps D_x and D_y. So by considering the restrictions of D_x and D_y we have that $\mathrm{D}_x : V_{r+1} \to V_r$ and $\mathrm{D}_y : V_{r+1} \to V_r$. It follows that

$$V_{r+1} \leq \mathrm{D}_x^{-1}(V_r) \cap \mathrm{D}_y^{-1}(V_r). \tag{5}$$

The kernel of D_x is the one-dimensional space $\langle y^r \rangle$ if $r \leq p-1$, otherwise D_x is injective. Similarly the kernel of D_y is the one-dimensional sace $\langle x^r \rangle$ if $r \leq p-1$ otherwise D_y is injective. So if $r > p-1$ then both D_x and D_y are injective maps and it follows from (5) that $\dim V_{r+1} \leq \dim V_r$ proving the theorem in this case.

Now consider the case when $r < p-1$. In this case the kernel of D_x is the space $\langle y^r \rangle$. It follows that $\dim \mathrm{D}_x^{-1}(V_r) \leq \dim V_r + 1$. Similarly $\dim \mathrm{D}_y^{-1}(V_r) \leq \dim V_r + 1$. Suppose if possible that $\dim V_{r+1} > \dim V_r + 1$. Then it follows from (5) that $V_{r+1} = \mathrm{D}_x^{-1}(V_r) = \mathrm{D}_y^{-1}(V_r)$. Now $y^r \in V_{r+1}$. So $y^{r-1} \in V_r$ which means that $xy^{r-1} \in V_{r+1}$. Proceeding in this way we get that $H_{r-1} = \langle y^{r-1}, xy^{r-2}, \ldots, x^{r-1} \rangle$ is contained in V_r which is a contradiction to our assumption that $\dim V_r \leq t < \dim H_{r-1}$. Hence $\dim V_{r+1} < \dim V_r$ proving the theorem in this case.

3. Proof of Theorem A

In this section we assume throughout that U is a minimal G-module such that $U \not> T_2$. Also we set $F = \mathrm{GF}(p)$. Then $U \cap T_2 = \langle 1, ax + by \rangle$ where $a, b \in F$ and without loss in generality we may assume that a is not equal to zero. Since $F = \mathrm{GF}(p)$ we may assume by a change of variables that $U \cap T_2 = \langle 1, x \rangle$ where the new variables which we still write as x and y satisfy the relations: $x^p = x$ and $y^p = y$. We assume from now on that p is an odd prime.

Proposition 3.1. *With the above notation and hypothesis, let $p(x, y) \in U \setminus T_2$. Write $p(x, y)$ in the form*

$$p(x, y) = f_0(x) + f_1(x)y + \cdots + f_k(x)y^k.$$

Then we have:

(i) $\deg f_{i+1} \leq \deg f_i - 2$, $0 \leq i \leq k-1$,

(ii) $\deg f_0(x) = \deg p(x, y)$,

(iii) $k \leq (p-1)/2$.

Proof. (i) We prove the result by induction on the degree of $p(x, y)$. First suppose that $p(x, y) \in U \cap T_3$ and that the degree of $p(x, y)$ is 2. So $p(x, y)$ is of the form $p(x, y) = (\alpha_0 + \alpha_1 x + \alpha_2 x^2) + (\beta_0 + \beta_1 x)y + \gamma y^2$ where α_i, β_i and $\gamma \in F$. Now U is closed under partial differentiations with respect to x and y. So $\partial p/\partial x = (\alpha_1 + 2\alpha_2 x) + \beta_1 y$ lies in $U \cap T_2$. Since $U \cap T_2$ is spanned by 1 and x, we must have $\beta_1 = 0$. Again $\partial p/\partial y \in U \cap T_2$ gives by a similar reasoning that $\gamma = 0$. Thus $p(x, y)$ is a polynomial of the required type and so (i) holds for all polynomials $p(x, y)$ of degree less than or equal to 2.

Now suppose that the result (i) holds for all polynomials with degree less than the degree of $p(x, y)$ where the degree of $p(x, y)$ is now assumed to be greater than 2. As U is closed under partial differentiations, $\partial p/\partial y \in U$. Now the degree of $\partial p/\partial y$ is less than the degree of $p(x, y)$ and also $\partial p/\partial y$ does not lie in T_2. So by induction hypothesis it follows that $\deg f_{i+1} \leq \deg f_i - 2$, $1 \leq i \leq k-1$. Note that this means that $\deg f_1$ is at least 2 otherwise the inequalities would be meaningless. Now it remains to compare the degrees of $f_0(x)$ and $f_1(x)$. Let $m := \deg f_1(x)$. We know that $m \geq 2$. So by using the inequalities we have obtained so far, we get

$$\frac{\partial^{m-1}}{\partial x^{m-1}} p(x, y) = f_0^{m-1}(x) + (cx + d)y \in U,$$

where c and d are some elements of GF(p) and c is non-zero. As the degree of $(\partial^{m-1}/\partial x^{m-1})p(x, y)$ is less than the degree of $p(x, y)$, so by induction hypothesis it follows that the degree of $f_0^{m-1}(x) \geq 3$. Now $f_0^{m-1}(x)$ has degree equal to $\deg f_0 - (m-1)$. So $\deg f_0 \geq m - 1 + 3$, or $\deg f_0(x) \geq \deg f_1(x) + 2$ which is what we wanted prove. Hence (i) follows by induction for all $0 \leq i \leq k-1$.

The parts (ii) and (iii) now follow easily.

Lemma 3.2. *Let U be a minimal G-submodule of F^{Ω} where G is primitive on Ω. Then U cannot contain the polynomial x^2.*

Proof. Suppose that $x^2 \in U$. Choose $g \in G$ such that $x^g := q(x, y)$ has the maximum y-degree in the set $\{x^h : h \in G\}$ which is the same as U by its minimality. Let k be the y-degree of $q(x, y)$. By Lemma 3.1 we have that $k \leq (p-1)/2$. Now since U is a G-module and $x^2 \in U$, we have

$$(x^2)^g = (x^g)^2 = q(x, y)^2 \in U.$$

If k is not equal to zero then $q(x,y)^2$ has y-degree $2k$ which contradicts the fact that $q(x,y)$ has the maximum y-degree. Thus it follows that x^g is a polynomial in the variable x only. So $U \leq F[x]$.

Let $P \in \mathrm{Syl}_p(G)$. As $U \leq F[x]$, the generator of P that corresponds to the translation $y \mapsto y+1$ lies in the kernel of the action of G on U. So G has a non-trivial normal subgroup N, say. Now N must be transitive on Ω for otherwise $\Omega = \{\omega h : h \in N\}$ for any point $\omega \in \Omega$ and then for $f \in U$, $f(\omega) = f^h(\omega) = f(\omega h^{-1})$ which means f is a constant and so $U = C$ which is not the case. Thus N is an intransitive normal subgroup and so G is imprimitive which is contrary to our assumption. Hence x^2 does not belong to U.

The following lemma gives some elements which generate $U \cap T_3$ and $U \cap T_4$.

Lemma 3.3. *Assume the hypothesis of Lemma* 3.2. *Then we have:*

(i) $U \cap T_3 = \langle 1, x, x^2 + y \rangle$,

(ii) $U \cap T_4 = \langle 1, x, x^2 + y, x^3 + 3xy \rangle$.

Proof. (i) We know that $U \cap T_2 = \langle 1, x \rangle$. Now by Theorem B we have that $U \cap T_3 = \langle 1, x, q(x,y) \rangle$ where $q(x,y)$ is some element of $U \cap T_3$. By Proposition 3.2 (i) we have that $q(x,y)$ must be of the form $q(x,y) = f_0(x) + f_1(x)y + f_2(x)y^2$, where $\deg f_1(x) \leq \deg f_0(x) - 2$ and $\deg f_2(x) \leq \deg f_1(x) - 2$. Also, $f_0(x)$ has degree at most 2 by Proposition 3.1 (ii). It follows that $q(x,y)$ is of the form $(\alpha_0 + \alpha_1 x + \alpha_2 x^2) + \alpha_2 y$ where $\alpha_i \in F$. Since 1 and x belong to $U \cap T_3$ we can take $q(x,y)$ to be $\alpha_2 x^2 + \alpha_3 y$ or rather $x^2 + \alpha_4 y$ where $\alpha_4 \in F$. Note that α_4 is non-zero otherwise $x^2 \in U$ contradicting Lemma 3.2. We may take $\alpha_4 = 1$ by a change in variable, the new variables which we still call x and y satisfy the conditions $x^p = x$, $y^p = y$.

(ii) By Theorem B and (i) above, we have $U \cap T_4 = \langle 1, x, x^2 + y, p(x,y) \rangle$ where $p(x,y)$ is a polynomial of the form $f_0(x) + f_1(x)y + f_2(x)y^2 + f_3(x)y^3$. By Proposition 3.1 we have that $f_0(x)$ has degree 3, $f_1(x)$ has degree less than or equal to 1 and $f_2(x) = 0 = f_3(x)$. Thus $p(x,y)$ is of the form $(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3) + (\alpha_4 + \alpha_5 x)y$. Since 1 and x lie in U we may by subtracting suitable multiples assume that $p(x,y) = x^3 + (cx + d)y$ where c and d are elements of F. Now $\partial p/\partial x$ belongs to $U \cap T_3$ and so it must be a scalar multiple of $x^2 + y$. Thus we must have that $c = 3$ and so $p(x,y) = x^3 + (3x + d)y$.

Now we assert that d must be zero. This can be seen as follows: Let $P \in \mathrm{Syl}_p(G)$. Then $N_G(P)$ consists of affine transformations of the form

$$\begin{cases} x \mapsto rx + r'y, \\ y \mapsto s'x + sy, \end{cases}$$

where $rs - r's'$ is non-zero. These transformations leave $U \cap T_3$ invariant. Now under such a transformation as above we have $x^2 + y \mapsto (rx + r'y)^2 + (s'x + sy)$ and the image lies in $U \cap T_3$. As the image is a linear combination of the spanning set $\{1, x, x^2 + y\}$ we must have $r' = 0$ and $s = r^2$. By the *Burnside transfer* theorem, P

cannot be in the centre of its normaliser, otherwise G will have a normal p-complement and this case is excluded by our hypothesis. So there must be transformations in $N_G(P)$ of the form we are considering with $r \neq 1$. Then replacing y by $y+(s'/r^2-r)x$ we may assume that $x \mapsto rx$ and $y \mapsto r^2y$ where $r \neq 1$. Note that the new variables which we still write as x and y satisfy the relations $x^p = x$ and $y^p = y$. Unde such transformations we have $x^3+(3x+d)y \mapsto r^3x^3+(3rx+d)r^2y$ and the image lies in $U \cap T_3$ and so is a linear combination of the spanning set $\{1, x, x^2+y, x^3+(3x+d)y\}$. We have

$$r^3x^3+(3r^3x+dr^2)y = r^3[x^3+(3x+d/r)y].$$

So it follows that $d/r = d$. This means that either $r=1$ or $d=0$. However, by our choice $r \neq 1$. So $d=0$. It then follows that $U \cap T_4 = \langle 1, x, x^2+y, x^3+3xy \rangle$. This completes the proof of the lemma.

We remark that is possible to calculate $U \cap T_5$ etc. by using methods similar to that used above.

Lemma 3.4. *Let $g \in G$ such that the y-degree of x^g is maximal. Let $x^g := q(x,y) = f_0(x)+f_1(x)y+\cdots+f_k(x)y^k$. Then we have that $k > (p-1)/3$.*

Proof. From Proposition 3.1(iii) it follows that $k \leq (p-1)/2$. Let $y^g := r(x,y)$. Now U is a G-module and $g \in G$. As $x^2+y \in U$ it follows that $(x^2+y)^g \in U$. Further

$$(x^2+y)^g = (x^2)^g + y^g = (x^g)^2 + y^g = q(x,y)^2 + r(x,y)$$

implies $r(x,y) = -q(x,y)^2 + r_0(x,y)$ where $r_0(x,y) \in U$. Now, $(x^3+3xy)^g \in U$ and is equal to

$$\begin{aligned} q(x,y)^3 + 3q(x,y)r(x,y) &= q^3(x,y) + 3q(x,y)[-q(x,y)^2 + r_0(x,y)] \\ &= -2q^3(x,y) + 3q(x,y)r_0(x,y). \end{aligned}$$

Suppose that $k \leq (p-1)/3$. Then it follows from above that $(x^3+3xy)^g$ is an element of U whose y-degree is $3k$ which is a contradiction to the maximality of k unless $k=0$. But surely k is not zero since for example $x^2+y \in U$. Hence we must have that $k > (p-1)/3$.

The following result improves Proposition 3.1.

Proposition 3.5. *Assume the hypothesis of Lemma 3.3. Let $p(x,y) \in U \setminus T_2$. Write $p(x,y)$ in the form*

$$p(x,y) = f_0(x) + f_1(x)y + \cdots + f_k(x)y^k. \tag{6}$$

Then we have:

(i) $\deg f_{i+1} = \deg f_i - 2$, $0 \leq i \leq k-1$,

(ii) $\deg f_k = 0$ or 1.

Proof. (i) We already know by Proposition 3.1 that $\deg f_{i+1} \le \deg f_i - 2$. Now suppose that for some j, $0 \le j \le k-1$, we have that $f_{j+1}(x)$ has degree less by 3 or more than the degree of $f_j(x)$. Let d be the degree of $f_j(x)$ and c_d be the coefficient of x^d in $f_j(x)$, c_d is non-zero and $d \ge 3$. Then we get from (6)

$$\frac{\partial^{d-2}}{\partial x^{d-2}}\left(\frac{\partial^j}{\partial y^j} p(x,y)\right) = \frac{d!}{2} c_d x^2,$$

belongs to U. So we have that $x^2 \in U$ contradicting Lemma 3.2. Hence it follows that $\deg f_{i+1}(x) = \deg f_i(x) - 2$, $0 \le i \le k-1$.

Part (ii) now follows readily.

Proposition 3.6. *The module U is generated by $\{1, u_1(x,y), \dots, u_m(x,y)\}$ for some integer m, where*

$$u_k(x,y) = x^k + c_{k,k-2}x^{k-2}y + \cdots + c_{k,k-2s}x^{k-2s}y^s + \cdots, \tag{7}$$

$1 \le k \le m$, *and we have that*

$$c_{k,k-2s} = \binom{k}{2s} \frac{(2s)!}{s!\,2^s}. \tag{8}$$

Proof. By Proposition 3.5, the polynomial $u_k(x,y)$ is of the form (6). Suppose that $u_k(x,y)$ is given by

$$u_k(x,y) = x^k + (c_{k,k-2}x^{k-2} + \cdots)y + \cdots + (c_{k,k-2s}x^{k-2s} + \cdots)y^s + \cdots \tag{9}$$

Now $\partial u_k/\partial x \in U$ and so must be a linear combination of the generators of U. From the form of $u_k(x,y)$ given by (9) it is clear that we must have

$$\frac{\partial u_k}{\partial x} = k u_{k-1}(x,y). \tag{10}$$

So from (9) and (10) we have

$$c_{k,k-2s} = \frac{k}{k-2s} c_{k-1,k-1-2s},$$

provided $k - 2s \ge 1$. Again by similar reasoning we have

$$c_{k-1,k-1-2s} = \frac{k-1}{k-1-2s} c_{k-2,k-2-2s},$$

etc. Proceeding in this way, we have,

$$c_{k,k-2s} = \frac{k(k-1)\cdots(k-(k-2s-1))c_{2s,0}}{(k-2s)(k-1-2s)\cdots(k-2s-k+2s+1)} = \binom{k}{k-2s} c_{2s,0} \tag{11}$$

provided $k - 2s \ge 1$. Now we evaluate $c_{2s,0}$ as follows: From (9) we have

$$u_{2s}(x,y) = x^{2s} + (c_{2s,2s-2}x^{2s-2} + \cdots)y + \cdots \tag{12}$$

So $\partial u_{2s}/\partial y = c_{2s,2s-2}u_{2s-2}$ + a linear combination of $u_j(x, y)$, $0 \leq j \leq 2s-2$. Thus by comparing coefficients we have,

$$c_{2s,0} = s^{-1}c_{2s,2s-2}c_{2s-2,0}, \tag{13}$$

provided s is non-zero. From (11) we have $c_{2s,2s-2} = \binom{2s}{2}c_{2,0} = \binom{2s}{2}$ since $c_{2,0} = 1$ as $u_2(x, y) = x^2 + y$. So (13) becomes

$$c_{2s,0} = \binom{2s}{2}s^{-1}c_{2s-2,0}. \tag{14}$$

Now similarly we can compute $c_{2s-2,0}$ in terms of $c_{2s-4,0}$ etc. Proceeding in this way we finally obtain that

$$c_{2s,0} = \frac{(2s)!}{s!\,2^s}c_{0,0} = \frac{(2s)!}{s!\,2^s}\,. \tag{15}$$

Combining (11) and (15) we get

$$c_{k,k-2s} = \binom{k}{2s}\frac{(2s)!}{s!\,2^s}\,. \tag{16}$$

Now we calculate the 'non-leading' terms in the brackets in $u_k(x, y)$ as given by (9). In (9) let the coefficient of $x^{k-2s-\lambda}y^s$ be denoted by $c_{k,k-2s-\lambda,s}$. By generalising the process to obtain (16), one gets quite easily that

$$c_{k,k-2s-\lambda,s} = \binom{k}{2s+\lambda}\frac{(2s)!}{s!\,2^s\lambda!}c_{\lambda,0,0}, \tag{17}$$

for $\lambda \neq 0$. Now $c_{\lambda,0,0}$ is obviously zero as can be seen by looking at $u_k(x, y)$ and observing that since it is of the form given by (9) there cannot be any constant term. Hence it follows that $c_{k,k-2s-\lambda,s} = 0$ for all $\lambda \neq 0$. So $u_k(x, y)$ has the form given by (7). This completes the proof of the Proposition.

Using Lemma 3.4 and the equation (7) of the above Proposition 3.6 we now readily obtain:

Corollary 3.7. *With the same notation and hypothesis as in Proposition* 3.6 *we have that* $m > \frac{2}{3}(p-1)$.

We now prove:

Proposition 3.8. *Assume the notation and hypothesis as in Proposition* 3.6. *Then we have that* $m < p-1$.

Proof. Suppose if possible that $m = p-1$. Then from (7) we have

$$u_{p-1}(x, y) = x^{p-1} + c_{p-1,p-3}x^{p-3}y + \cdots + c_{p-1,0}x^0y^{(p-1)/2}, \tag{18}$$

where

$$c_{p-1,p-1-2s}=\frac{(p-1)!}{(p-1-2s)!\,s!\,2^s}\,. \tag{19}$$

So the coefficient of $x^{p-1}y^{p-1}$ in $u^3_{p-1}(x,y)$ is easily seen to be equal to

$$\sum c_{p-1,p-1-2r}c_{p-1,p-1-2s}c_{p-1,p-1-2t} \tag{20}$$

where the sumation is over all r, s, t such that each of them is less than or equal to $(p-1)/2$ and further $r+s+t=p-1$. Using (19), this expression can be written after some simplifications, as congruent (mod p) to

$$\sum \frac{(2r)!}{r!}\,\frac{(2s)!}{s!}\,\frac{(2t)!}{t!} \tag{21}$$

where the summation is over all r, s, t as specified in (20). We now show:

Lemma 3.9. *The expression* (21) *is not congruent to zero* (mod p) *for* $p\neq 3$.

Proof. (E. Lander.) We have

$$((p-1)/2)!\equiv -\left(\frac{1}{p}\right) \pmod p \tag{22}$$

and

$$2^{(p-1)/2}\equiv\left(\frac{a}{p}\right) \pmod p, \tag{23}$$

where $\left(\frac{a}{p}\right)$ denotes the usual Legendre symbol in number theory. Further,

$$\frac{(2s)!}{s!}\equiv 2^{2s}(-1)^s\,\frac{((p-1)/2)!}{((p-1)/2-s)!} \pmod p. \tag{24}$$

The congruences (22) and (23) follow readily and (24) follows by induction since the ratio of consecutive $(s+1)$-th and s-th terms on both sides is $2(2s-1)$ modulo p. Using (24), the sum (21) can be written as congruent to

$$\sum 2^{2(r+s+t)}(-1)^{r+s+t}(((p-1)/2)!)^2\left[\frac{((p-1)/2)!}{((p-1)/2-r)!((p-1)/2-s)!((p-1)/2-t)!}\right] \tag{25}$$

where the summation is over all r, s and t as specified in (20). Set $u:=(p-1)/2-r$, $v:=(p-1)/2-s$, $w:=(p-1)/2-t$. Changing the variables in (25) to u, v, w and using (22) and (23), one obtains that (25) is congruent to

$$\sum_{u,v,w} -\left(\frac{-1}{p}\right)\binom{(p-1)/2}{u,\,v,\,w}, \tag{26}$$

where the summation is over all u, v, w such that each of them is less than or equal to $(p-1)/2$ and further that $u+v+w=(p-1)/2$ and $\binom{(p-1)/2}{u,v,w}$ denotes a trinomial coefficient. Now (26) is congruent to

$$-(-\frac{1}{p})3^{(p-1)/2} \equiv -(\frac{3}{p}) \pmod{p}.$$

From this the lemma now follows readily.

We now continue the proof of Proposition 3.8. Now by Lemma 3.9 we have that the coefficient of $x^{p-1}y^{p-1}$ in $u_{p-1}^{3}(x,y)$ is non-zero. If U^3 is a proper G-submodule of F^{Ω} we have by Wielandt [7], Theorem 14.7, that $C \leq U \leq C^{\perp}$. However, U^3 is not contained in $C^{\perp}$ since U^3 contains $u_{p-1}^{3}(x,y)$ with a term $x^{p-1}y^{p-1}$ which has a non-zero coefficient and by Wielandt [7], Proposition 17.7, the coefficient of $x^{p-1}y^{p-1}$ in $f \in F^{\Omega}$ is the value of the inner product $\langle f, 1 \rangle$. So $U^3 = F^{\Omega}$. It follows that $U \cdot U^2 = F$ implying that U is not orthogonal to U^2. On the other hand, x is orthogonal to the module U^2. For, if $f \in U^2$ then the coefficient of $x^{p-1}y^{p-1}$ in $x.\ f$ is zero since the coefficient of y^{p-1} in f is a constant by observing the form of the polynomial f using Proposition 3.6. Now since x is orthogonal to U, the G-submodule $\langle x^g : g \in G \rangle$ is orthogonal to U^2. But by the minimality of U, we have that $U = \langle x^g : g \in G \rangle$. So we get that U is orthogonal to U^2 contradicting the earlier statement that U is not orthogonal to U^2. Hence m cannot be equal to $p-1$ proving Proposition 3.8.

Piecing together the results of this section we establish the proof of Theorem A.

Acknowledgements

Part of this material is taken from a chapter of the author's thesis [1] written under the supervision of P.M. Neumann to whom we express our sincere thanks for his suggestions and encouragement. We thank D.N. Verma for stimulating discussions. Also we thank E. Lander who kindly supplied the proof of Lemma 3.9. This material was presented at a Group theory conference at Oberwolfach, West Germany in July, 1981. We thank the University of Manitoba, Canada for warm hospitality during part of the summer of 1981 when this paper was drafted.

Postscript

After writing this paper, Prof. W. Feit has informed us in a letter that since all doubly transitive permutation groups are now known (see for example, P.J. Cameron, Bull. London Math Soc. 13 (1981), p. 8), it follows that a doubly transitive group of degree $p^m > 9$ which does not contain a cycle of length p^m is either A_{2^m} or contains a normal elementary abelian group of order p^m. According to him, "This latter class is also known but the results have unfortunately not yet appeared. In view of this it should be possible to describe the Heart of such a permutation representation directly". Our work was started before the classification of doubly transitive permutation groups was completed.

References

[1] P. Bhattacharya, A Study of some Multiply Transitive Permutation groups, D. Phil. thesis, University of Oxford (1979).

[2] P. Bhattacharya, On the tensor product of permutation modules, J. Algebra (1983) to appear.

[3] W. Feit, Groups with a cyclic Sylow subgroup, Nagoya Math. J. 27 (1966) 571-584.

[4] M. Klemm, Primitive Permutationsgruppen von Primzahlpotenzgrad, Comm. Algebra 5 (2) (1977) 193-205.

[5] P.M. Neumann, Transitive permutation groups of prime power degree, J. London Math. Soc. (2) 5 (1972) 202-208.

[6] P.M. Neumann, The simplicity of the Green Heart, in: Seminar on Permutation Groups and related topics (Kyoto Univ. Press, Kyoto 1978) 1-19.

[7] H. Wielandt, Permutation Groups Through Invariant Relations and Invariant Functions (Ohio State Univ. Press, Columbus, 1969).